EFAv2.0

Aus Hl7wiki
Spezifikation

Dieses Dokument gibt wieder:

*Spezifikation **EFAv2.0**.*

Die Teilmaterialien gehören der Kategorie [cdaefa](#) an.

[+] Kontributoren

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "[Kommentierung EFAv2.0](#)".

Inhaltsverzeichnis

- 1 Einleitung
  - 1.1 Von EFA 1.2 zu EFA 2.0
  - 1.2 EFA 2.0 Spezifikation
  - 1.3 Weiterführende Themen
    - 1.3.1 Methodische Grundlagen
  - 1.4 Offene Punkte und ToDos
    - 1.4.1 ToDos aus der Kommentierung (Fraunhofer)

        - 1.4.2 Diskussionsbedarfe - operativ (7er-Gruppe)
        - 1.4.3 Diskussionbedarfe - strategisch (Lenkungsgruppe)
        - 1.4.4 Abschnitte, die ggf. in das Cookbook verschoben werden können
        - 1.4.5 Externe Abhängigkeiten
- 2 Conceptual Perspective - Enterprise Dimension
    - 2.1 Die EFA als zweckgebundene Akte
        - 2.1.1 Der "medizinische Fall"
        - 2.1.2 Auswirkungen der Zweckbindung auf die Nutzung von Fallakten
        - 2.1.3 Referenzen und Querverweise
    - 2.2 Die EFA als Gesundheitsdatendienst
        - 2.2.1 Gesundheitsdatendienste (GDD)
        - 2.2.2 GDD Referenzmodell
        - 2.2.3 Referenzen und Querverweise
    - 2.3 EFA Sicherheitsstrategie
    - 2.4 Kernkonzepte
        - 2.4.1 Synchronität von Behandlungsteam und Berechtigungen
        - 2.4.2 Übertragbarer Sicherheitskontext
        - 2.4.3 Deklarative Sicherheit
        - 2.4.4 Policy Enforcement dicht an den Ressourcen
        - 2.4.5 Referenzen und Querverweise
    - 2.5 Akteure der EFA
        - 2.5.1 Patient (Versicherter)
        - 2.5.2 Fallaktenmanager
        - 2.5.3 EFA-Teilnehmer
        - 2.5.4 EFA Provider
        - 2.5.5 Datenerhebende und datenverantwortliche Stellen
        - 2.5.6 Referenzen und Querverweise
    - 2.6 Affinity Domain vs. Versorgungsdomänen
        - 2.6.1 Krankenhäuser als EFA Provider
        - 2.6.2 Referenzen und Querverweise
- 3 Conceptual Perspective - Information Dimension
    - 3.1 EFA als Instanz des GDD Referenzmodells

        - 3.1.1 Kontext
        - 3.1.2 EFA-Anwendung und EFA-Peers
        - 3.1.3 Ressourcen der EFA
        - 3.1.4 Querverweise und Referenzen
    - 3.2 Patienteneinwilligung zur EFA
        - 3.2.1 Querverweise und Referenzen
    - 3.3 Hierarchisches Informationsmodell der EFA
        - 3.3.1 Klasse *Patient*
        - 3.3.2 Klasse *Fallakte (Medizinischer Fall)*
            - 3.3.2.1 Verteilung von Fallakten über mehrere EFA-Provider
        - 3.3.3 Klasse *Partition*
        - 3.3.4 Klasse *Datenobjekt*
        - 3.3.5 Querverweise und Referenzen
    - 3.4 Lebenszyklus einer Fallakte
        - 3.4.1 Querverweise und Referenzen
- 4 Conceptual Perspective - Computational Dimension
- 5 Interaktionsmuster der EFA
    - 5.1 Arbeiten mit Fallakten
    - 5.2 Verwaltung von Fallakten
    - 5.3 Referenzen und Querverweise
    - 5.4 Interaktionsmuster zum Anlegen einer EFA
        - 5.4.1 Anwendungsszenario: Anlegen einer Fallakte
        - 5.4.2 Varianten des Anwendungsszenarios
        - 5.4.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.4.4 Definition der Interaktionsmuster
            - 5.4.4.1 Interaktionsmuster: Fallakte anlegen
        - 5.4.5 Peer-to-Peer Semantik
        - 5.4.6 Querverweise und Referenzen
    - 5.5 Interaktionsmuster
        - 5.5.1 Anwendungsszenario: Anlegen einer Partition zu einer bestehenden Fallakte
    - 5.6 Varianten des Anwendungsszenarios
    - 5.7 Abbildung der Szenarien und Varianten auf Interaktionsmuster

- 5.8 Definition der Interaktionsmuster
  - 5.8.1 Interaktionsmuster: Partition anlegen und registrieren
- 5.9 Peer-to-Peer Semantik
- 5.10 Referenzen und Querverweise
- 5.11 Interaktionsmuster zum Einstellen von Daten in eine Fallakte
  - 5.11.1 Anwendungsszenario: Einstellen von Daten in eine Fallakte
  - 5.11.2 Varianten des Anwendungsszenarios
    - 5.11.2.1 Aktualisieren eines Dokuments
    - 5.11.2.2 Ergänzen eines Dokuments
  - 5.11.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
  - 5.11.4 Definition der Interaktionsmuster
    - 5.11.4.1 Interaktionsmuster: Daten einstellen
  - 5.11.5 Peer-to-Peer Semantik
  - 5.11.6 Querverweise und Referenzen
- 5.12 Interaktionsmuster "Auffinden der Fallakten eines Patienten"
  - 5.12.1 Anwendungsszenario: Auffinden und Öffnen einer Fallakte eines Patienten
  - 5.12.2 Varianten des Anwendungsszenarios
    - 5.12.2.1 Resource Discovery Token (Offline Token)
  - 5.12.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
  - 5.12.4 Definition der Interaktionsmuster
    - 5.12.4.1 Interaktionsmuster: Partitionen auflisten
  - 5.12.5 Peer-to-Peer Semantik
  - 5.12.6 Querverweise und Referenzen
- 5.13 Interaktionsmuster "Browsing über einer Fallakte oder einer Partition"
  - 5.13.1 Anwendungsszenario: Browsing über eine Fallakte
  - 5.13.2 Varianten des Anwendungsszenarios
    - 5.13.2.1 Suchen und Filtern anhand von definierten Kriterien
    - 5.13.2.2 Browsing über einer einzelnen Partition
  - 5.13.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
  - 5.13.4 Definition der Interaktionsmuster
    - 5.13.4.1 Interaktionsmuster: Partition abrufen
    - 5.13.4.2 Interaktionsmuster: Fallakte abrufen

        - 5.13.5 Peer-to-Peer Semantik
        - 5.13.6 Querverweise und Referenzen
    - 5.14 Interaktionsmuster "Abruf von Datenobjekten"
        - 5.14.1 Anwendungsszenario: Abruf von Daten aus einer Fallakte
        - 5.14.2 Varianten des Anwendungsszenarios
        - 5.14.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.14.4 Definition der Interaktionsmuster
            - 5.14.4.1 Interaktionsmuster: Daten abrufen
        - 5.14.5 Peer-to-Peer Semantik
        - 5.14.6 Querverweise und Referenzen
    - 5.15 Interaktionsmuster "Schließen einer Fallakte"
        - 5.15.1 Anwendungsszenario: Rücknahme der Einwilligung durch den Patienten
        - 5.15.2 Varianten des Anwendungsszenarios
            - 5.15.2.1 Wegfall des Zwecks der Akte
        - 5.15.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.15.4 Definition der Interaktionsmuster
            - 5.15.4.1 Interaktionsmuster: EFA Schließen
        - 5.15.5 Peer-to-Peer Semantik
        - 5.15.6 Querverweise und Referenzen
    - 5.16 Interaktionsmuster zum Invalidieren von Daten in einer Fallakte
        - 5.16.1 Anwendungsszenario: Invalidieren von Daten in einer Fallakte
        - 5.16.2 Varianten des Anwendungsszenarios
        - 5.16.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.16.4 Definition der Interaktionsmuster
            - 5.16.4.1 Interaktionsmuster: Daten invalidieren
        - 5.16.5 Peer-to-Peer Semantik
        - 5.16.6 Querverweise und Referenzen
    - 5.17 Interaktionsmuster zum Anpassen einer EFA
        - 5.17.1 Anwendungsszenario: Anpassen des Teilnehmerkreises
        - 5.17.2 Varianten des Anwendungsszenarios
            - 5.17.2.1 Variante: Anpassung der Zweck-Parameter
            - 5.17.2.2 Variante: Verlängerung der Gültigkeit

        - 5.17.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.17.4 Definition der Interaktionsmuster
            - 5.17.4.1 Interaktionsmuster: Fallakte anpassen
        - 5.17.5 Peer-to-Peer Semantik
        - 5.17.6 Querverweise und Referenzen
    - 5.18 Interaktionsmuster zur Autorisierung eines weiteren Teilnehmers
        - 5.18.1 Anwendungsszenario: Offline-Token
        - 5.18.2 Varianten des Anwendungsszenarios
            - 5.18.2.1 Variante: Online-Token
        - 5.18.3 Abbildung der Szenarien und Varianten auf Interaktionsmuster
        - 5.18.4 Definition der Interaktionsmuster
            - 5.18.4.1 Interaktionsmuster: Token ausstellen
            - 5.18.4.2 Interaktionsmuster: Teilnehmer per Token autorisieren
        - 5.18.5 Peer-to-Peer Semantik
        - 5.18.6 Querverweise und Referenzen
- 6 Logical Perspective - Enterprise Dimension
    - 6.1 Identifizierung und Authentifizierung von EFA-Teilnehmern
        - 6.1.1 Anforderungen
    - 6.2 Autorisierung von EFA-Teilnehmern
        - 6.2.1 Anforderungen
    - 6.3 Vertraulichkeit
        - 6.3.1 Anforderungen
        - 6.3.2 EFA Secure Channels
    - 6.4 Authentizität und Integrität von EFA Daten
        - 6.4.1 Anforderungen
        - 6.4.2 Digital Signature
    - 6.5 Nicht-Abstreitbarkeit, Dokumentation und Audit-Trail
        - 6.5.1 Anforderungen
    - 6.6 Verfügbarkeit von EFA-Teilnehmern und EFA-Daten
        - 6.6.1 Anforderungen
    - 6.7 Querverweise und Referenzen
- 7 Logical Perspective - Information Dimension

- 7.1 EFA Informationsmodell
  - 7.1.1 Patient
  - 7.1.2 Fallakte
  - 7.1.3 Partition
  - 7.1.4 document
- 7.2 PIM Data Structures
  - 7.2.1 patientID
  - 7.2.2 purpose
  - 7.2.3 ecrInfo
  - 7.2.4 consentInfo
  - 7.2.5 consentDoc
  - 7.2.6 partitionID
  - 7.2.7 partitionList
  - 7.2.8 ecrRef
  - 7.2.9 partitionInfo
  - 7.2.10 docMetadata
  - 7.2.11 docRelationship
  - 7.2.12 documentID
  - 7.2.13 communityID
- 7.3 Querverweise und Referenzen
- 7.4 EFA Sicherheitskontext
- 7.5 PIM Data Structures
  - 7.5.1 context
  - 7.5.2 subjectIdentity
  - 7.5.3 subjectAccessPolicy
  - 7.5.4 accessToken
- 7.6 Querverweise und Referenzen
- 7.7 Fehler und Warnungen
  - 7.7.1 Sicherheit(skontext)
  - 7.7.2 Operationsaufruf -und abwicklung
  - 7.7.3 Querverweise und Referenzen

- 8 Logical Perspective = Computational Dimension

- 8.1 Technische Akteure der EFA
  - 8.1.1 Querverweise und Referenzen
- 8.2 Kommunikationsmuster
  - 8.2.1 Aufbau des Sicherheitskontextes
  - 8.2.2 Anlegen einer Fallakte
    - 8.2.2.1 Neu-Anlage einer Fallakte
    - 8.2.2.2 Fusion mit einer bestehenden Fallakte
  - 8.2.3 Anlegen einer Partition zu einer bestehenden Fallakte
  - 8.2.4 Schließen einer Fallakte
  - 8.2.5 Auflisten von Partitionen
  - 8.2.6 Einstellen von Dokumenten
  - 8.2.7 Auflisten von Dokumenten
  - 8.2.8 Abrufen von Dokumenten
  - 8.2.9 Registrierung einer neuen Einwilligung
  - 8.2.10 Anfordern eines Berechtigungstoken
  - 8.2.11 Einlösen eines Berechtigungstoken
  - 8.2.12 Querverweise und Referenzen
- 8.3 EFA Anwendungsarchitektur: Service Functional Model
  - 8.3.1 Operationen des EFA Ressource Manager
    - 8.3.1.1 *createECR*
    - 8.3.1.2 *createPartition*
    - 8.3.1.3 *closeECR*
    - 8.3.1.4 *listPartitions*
    - 8.3.1.5 *registerConsent*
    - 8.3.1.6 *issueAccessToken*
    - 8.3.1.7 *redeemAccessToken*
  - 8.3.2 Operationen des EFA Document Registry
    - 8.3.2.1 *registerData*
    - 8.3.2.2 *listPartitionContent*
  - 8.3.3 Operationen des EFA Document Repository
    - 8.3.3.1 *provideData*
    - 8.3.3.2 *retrieveData*

        - 8.3.4 Querverweise und Referenzen
    - 8.4 Sicherheitstoken und Sicherheitstokendienste
    - 8.5 EFA Sicherheits(token)dienste
    - 8.6 Querverweise und Referenzen
    - 8.7 EFA Context Manager
        - 8.7.1 Authentisierung eines EFA-Teilnehmers
            - 8.7.1.1 Optionen zur Authentisierung von EFA-Teilnehmern (nicht-normativ)
            - 8.7.1.2 Operation: OpenContext
        - 8.7.2 Referenzen und Querverweise
    - 8.8 EFA Identity Provider
        - 8.8.1 Querverweise und Referenzen
    - 8.9 EFA Policy Provider
        - 8.9.1 requestPolicy
        - 8.9.2 Querverweise und Referenzen
    - 8.10 Gruppierung von Anwendungs- und Sicherheitsdiensten
        - 8.10.1 Policy Pull
        - 8.10.2 Client Policy Push
        - 8.10.3 Querverweise und Referenzen
- 9 Implementable Perspective - Enterprise Dimension
    - 9.1 Verwendete Standards: Sicherheit
        - 9.1.1 Security Assertion Markup Language (SAML)
        - 9.1.2 eXtensible Access Control Markup Language (XACML)
        - 9.1.3 Web Service Security (WS-Security)
        - 9.1.4 Web Services Trust Language (WS-Trust)
        - 9.1.5 Referenzen
    - 9.2 ECR Namespace Prefixes
- 10 Implementable Perspective - Information Dimension
    - 10.1 Mapping of Core Information Model Classes
    - 10.2 Mapping of PIM Classes
        - 10.2.1 ecrInfo
    - 10.3 Querverweise und Referenzen
    - 10.4 Folder Metadata

        - 10.4.1 codeList
            - 10.4.1.1 Example: Diagnosis (ICD-10)
            - 10.4.1.2 Example: DMP
            - 10.4.1.3 Example: IV Vertrag
        - 10.4.2 Querverweise und Referenzen
    - 10.5 Document Metadata
        - 10.5.1 classCode
        - 10.5.2 typeCode
        - 10.5.3 Comments
    - 10.6 German Profile
        - 10.6.1 Author Institution
        - 10.6.2 Author Person
        - 10.6.3 HealthcareFacilityTypeCode
        - 10.6.4 sourcePatientInfo
    - 10.7 Querverweise und Referenzen
    - 10.8 Security Object Bindings
        - 10.8.1 Querverweise und Referenzen
    - 10.9 SAML 2.0 Profile for ECR Identity Assertions
        - 10.9.1 German Profile
        - 10.9.2 Assertion Signature
        - 10.9.3 HCP Identity Attributes
            - 10.9.3.1 German Extensions
        - 10.9.4 Example Assertion
        - 10.9.5 Querverweise und Referenzen
    - 10.10 SAML 2.0 Profile for ECR Policy Assertions
        - 10.10.1 PolicySet Profile
        - 10.10.2 Policy Assignment
        - 10.10.3 Policy Attachment
        - 10.10.4 Assertion Signature
        - 10.10.5 Example Assertion
        - 10.10.6 Querverweise und Referenzen
    - 10.11 EFA Audit Trail Binding for XDS-based Transactions

        - 10.11.1 Event Identification
        - 10.11.2 Encoding of the User Identifier
- 11 Implementable Perspective - Computational Dimension
    - 11.1 EFA Setup
        - 11.1.1 Querverweise und Referenzen
    - 11.2 EFA XDR/XDS Binding
        - 11.2.1 Constraints and Triggers
    - 11.3 Querverweise und Referenzen
    - 11.4 EFA Resource Manager XDR/XDS Binding
    - 11.5 EFA XDS/XDR Binding: createECR
        - 11.5.1 Constraints on the Request Message
        - 11.5.2 Expected Actions
        - 11.5.3 Response Message (Full Success Scenario)
        - 11.5.4 Response Message (Failure or Partial Failure Scenario)
        - 11.5.5 Security Considerations
            - 11.5.5.1 Message Protection
                - 11.5.5.1.1 Transport Layer Security with SAML Issued Endorsing Token
                    - 11.5.5.1.1.1 WS-Security-Policy Example
                - 11.5.5.1.2 Asymmetric Message Protection
                    - 11.5.5.1.2.1 WS-Security-Policy Example
                - 11.5.5.1.3 WS-SecureConversation bootstrapped with SAML Issued Token
            - 11.5.5.2 Audit Trail
    - 11.6 EFA XDS/XDR Binding: createPartition
        - 11.6.1 Constraints on the Request Message
        - 11.6.2 Expected Actions
        - 11.6.3 Response Message (Full Success Scenario)
        - 11.6.4 Response Message (Failure or Partial Failure Scenario)
        - 11.6.5 Security Considerations
            - 11.6.5.1 Message Protection
            - 11.6.5.2 Audit Trail
    - 11.7 EFA XDS/XDR Binding: closeECR
        - 11.7.1 Constraints on the Request Message

        - 11.7.2 Expected Actions
        - 11.7.3 Response Message (Full Success Scenario)
        - 11.7.4 Response Message (Failure or Partial Failure Scenario)
        - 11.7.5 Security Considerations
            - 11.7.5.1 Message Protection
            - 11.7.5.2 Audit Trail
    - 11.8 EFA XDS Binding: listPartitions
        - 11.8.1 Constraints on the Request Message
            - 11.8.1.1 Example
        - 11.8.2 Expected Actions
        - 11.8.3 Response Message (Full Success Scenario)
        - 11.8.4 Response Message (Failure or Partial Failure Scenario)
        - 11.8.5 Security Considerations
            - 11.8.5.1 Message Protection
            - 11.8.5.2 Audit Trail
    - 11.9 EFA XDS/XDR Binding: registerConsent
        - 11.9.1 Constraints on the Request Message
        - 11.9.2 Expected Actions
        - 11.9.3 Response Message (Full Success Scenario)
        - 11.9.4 Response Message (Failure or Partial Failure Scenario)
        - 11.9.5 Security Considerations
            - 11.9.5.1 Message Protection
            - 11.9.5.2 Audit Trail
        - 11.9.6 Referenzen und Querverweise
    - 11.10 EFA Document Registry XDS Binding
    - 11.11 EFA XDS Binding: registerData
        - 11.11.1 Constraints on the Request Message
        - 11.11.2 Expected Actions
        - 11.11.3 Response Message (Full Success Scenario)
        - 11.11.4 Response Message (Failure or Partial Failure Scenario)
        - 11.11.5 Security Audit Considerations
    - 11.12 EFA XDS Binding: listPartitionContent

        - 11.12.1 Constraints on the Request Message
            - 11.12.1.1 Example
        - 11.12.2 Expected Actions
        - 11.12.3 Response Message (Full Success Scenario)
        - 11.12.4 Response Message (Failure or Partial Failure Scenario)
        - 11.12.5 Security Considerations
            - 11.12.5.1 Audit Trail
    - 11.13 Querverweise und Referenzen
    - 11.14 EFA Document Repository XDS Binding
    - 11.15 EFA XDS Binding: provideData
        - 11.15.1 Constraints on the Request Message
        - 11.15.2 Expected Actions
        - 11.15.3 Response Message (Full Success Scenario)
        - 11.15.4 Response Message (Failure or Partial Failure Scenario)
        - 11.15.5 Security Considerations
            - 11.15.5.1 Audit Trail
    - 11.16 EFA XDS Binding: retrieveData
        - 11.16.1 Constraints on the Request Message
            - 11.16.1.1 Example
        - 11.16.2 Expected Actions
        - 11.16.3 Response Message (Full Success Scenario)
        - 11.16.4 Response Message (Failure or Partial Failure Scenario)
        - 11.16.5 Security Considerations
            - 11.16.5.1 Audit Trail
    - 11.17 Querverweise und Referenzen
    - 11.18 Bindung von Policies an Schnittstellen
        - 11.18.1 Bausteine des Access Control System
        - 11.18.2 Referenzen
- 12 Anhang
    - 12.1 HL7 SAIF
    - 12.2 HL7 ECCF Framework
    - 12.3 IHE White Paper "Access Control"

- 12.3.1 Access Control Subsysteme
- 12.3.2 5-Domänen-Modell
- 12.3.3 Nutzung des 5-Domänen-Modells

Einleitung

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Epif.01}

Die Elektronische Fallakte (EFA) ist eine 2006 gestartete Initiative des stationären Sektors (d.h. Krankenhäuser und Kliniken). Seit 2009 wird sie vom Verein "Elektronische FallAkte e.V." - einer Interessengemeinschaft aus Krankenhäusern, Krankenhausketten, Verbänden der Leistungserbringer im Gesundheitswesen sowie regionalen Gesundheitsnetzen - getragen.

Elektronische Fallakten ermöglichen eine strukturierte und integrierte Sicht auf einem Patienten zugeordnete, medizinische Daten. Ein Fall beginnt mit einer Erstdiagnose und integriert alle weiteren notwendigen Abrechnungs- und Behandlungsdaten. Ein Arzt betreut die Fallakte zusammen mit weiteren behandelnden Ärzten, die für die Inhalte und deren Vollständigkeit verantwortlich sind.

Die dezentrale Handhabung und Pflege der Fallakten basiert auf der Metapher eines Versorgungsnetzes als Interessengemeinschaft autonomer Akteure mit bestimmten Aufgaben. Medizinische Daten und administrative Informationen (z.B. Benutzerkonten) werden bevorzugt dezentral in bestehenden Systemen verwaltet und können bei Bedarf zu einer integrierten, für alle behandelnden Ärzte einheitlichen Sicht auf den Patienten zusammengeführt werden. Daher kann die Fallakte sehr einfach in bestehende Netze integriert werden und erleichtert somit die Zusammenarbeit auf regionaler Ebene.

Von EFA 1.2 zu EFA 2.0

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Epif.02}

Nach einer nur im Rahmen eines Proof-of-Concept implementierten Version 1.0 der EFA-Spezifikation wurde im Februar 2008 mit der EFA Version 1.2 das erste öffentliche Major-Release der EFA-Spezifikation von den Trägern der EFA-Initiative freigegeben. Bereits Ende 2008 konnten drei namhafte Hersteller (Siemens, ISPro, iSoft) auf dem ersten EFA-Connectathon Produkte präsentieren, die die interoperablen Schnittstellen der EFA implementierten und so miteinander in einem Peer-to-Peer Netzwerk zusammengeschaltet werden konnten. In den folgenden Jahren wurden in

verschiedenen Bundesländern EFA-Pilotprojekte gestartet und 2011 konnte am Städtischen Klinikum München das erste regionale EFA-Netzwerk in den Regelbetrieb überführt werden.

Während die EFA-Sicherheitsarchitektur auch fünf Jahre nach ihrer Veröffentlichung noch dem State-of-the-Art entspricht (und durch Übernahme in Projekte wie z.B. epSOS und Prozessdatenbeschleuniger (P23R) den State-of-the-Art auch mit geprägt hat) haben sich in dieser Zeit im Bereich der Fachschnittstellen von elektronischen Aktensystemen die meisten Hersteller mit ihren Produkten in Richtung des IHE-Profils XDS bewegt, das von der EFA Version 1.2 lediglich logisch aber nicht syntaktisch berücksichtigt wurde - wobei auch die Synchronizität des EFA-1.2-Informationsmodells zu IHE XDS auf die Ebene der Dokumentenverwaltung beschränkt war.

Im März 2012 haben daher der EFA-Verein als Träger der EFA-Spezifikation und der bvitg als Vertreter der im ambulanten und stationären Sektor tätigen Hersteller von IT-Lösungen beschlossen, gemeinsam eine Version 2.0 der EFA-Spezifikation zu erarbeiten. Diese Version soll

- auf den bewährten und in verschiedenen Gesundheitsnetzen erfolgreich erprobten Kernprinzipien und -konzepten der EFA v1.2 aufbauen,
- in Produkten der Industrie verfügbare Schnittstellenstandards aufgreifen und eine Abbildbarkeit des EFA-Informationsmodells auf das Aktenkonzept von IHE herstellen,
- durch Verzahnung mit dem IHE-D Cookbook auf Basis generischer XDS-konformer Lösungsbausteine elektronischer Akten implementierbar sein.

EFA 2.0 Spezifikation

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Epif.03}`

Die folgende Tabelle stellt die einzelnen Kapitel der EFA 2.0 Spezifikation im Strukturraster des HL7 Enterprise Conformance and Compliance Frameworks dar. Eine Zusammenstellung aller Seiten der Spezifikation zu einem Dokument finden Sie unter den folgenden Links:

- **Aktuelle Spezifikation auf einer Wiki-Seite**

EFA v2.0	**Enterprise Dimension** ***"Why"*** ***Policy***	**Information Dimension** ***"What"*** ***Content***	**Computational Dimension** ***"How"*** ***Behavior***

Conceptual Perspective	• Die EFA als zweckgebundene Akte
	• Die EFA als Gesundheitsdatendienst
	• Prinzipien für Datenschutz und Datensicherheit
	• Akteure und Rollen
	• Versorgungsdomänen
		• Kontext, Akte, Ressource
		• Patienteneinwilligung zur EFA
		• EFA Geschäftsobjekte
		  ○ Lebenszyklus einer Fallakte
			• Interaktionsmuster der EFA
			  ○ Anlegen einer Fallakte
			  ○ Anlegen und Registrieren einer Partition
			  ○ Einstellen von Datenobjekten
			  ○ Auffinden der Fallakten eines Patienten
			  ○ Browsing über eine Akte oder eine Partition
			  ○ Abruf von Datenobjekten
			  ○ Schließen einer Fallakte
			  ○ Invalidieren von Datenobjekten
			  ○ Ändern der Einwilligung
			  ○ Autorisierung eines weiteren Teilnehmers
			  ○ Zusammenführen von Fallakten (P2P)

Logical Perspective	• EFA Sicherheitsanforderungen	• Informationsmodelle der EFA Geschäftsobjekte
		• Informationsmodelle der EFA Sicherheitsobjekte
		• Fehlermeldungen und Warnungen
			• EFA Dienste
			• EFA Kommunikationsmuster
			• EFA Anwendungsdienste (logische Spezifikation)
			• EFA Sicherheitsdienste (logische Spezifikation)
			  ○ EFA Context Manager SFM
			  ○ EFA Identity Provider SFM
			  ○ EFA Policy Provider SFM
			• Gruppierung von Anwendungs- und Sicherheitsdiensten

Implementable Perspective	• Verwendete Standards
	• Namespaces
		• EFA Metadata Bindings
		  ◦ EFA XDS Folder Metadata Binding
		  ◦ EFA XDS Document Metadata Binding
		• EFA Security Objects Bindings
		  ◦ EFA Identity Assertion SAML2 Binding
		  ◦ EFA Policy Assertion SAML2 Binding
		• EFA Audit Trail Binding
		• EFA Error Codes and Warning Codes
			• EFA IHE Setup and Flow of Control
			• EFA XDS Bindings
			  ◦ EFA XDS Binding: ResourceManager
			  ◦ EFA XDS Binding: DocumentRegistry
			  ◦ EFA XDS Binding: DocumentRepository
			• EFA Access Control System

Weiterführende Themen

In der EFA-Spezifikation wird an verschiedenen Stellen auf weiterführende Informationen oder Grundlagenpapiere verwiesen, die in der ECCF-Matrix nicht verzeichnet sind. Diese "Anhänge" zur EFAv2.0-Spezifikation sind hier verzeichnet.

Methodische Grundlagen

- HL7 SAIF ECCF: Kurze Einführung in das HL7 SAIF *Enterprise Conformance and Compliance Framework*, das dem Aufbau dieser Spezifikation zugrunde liegt
- IHE Access Control Domains: Zusammenfassung des IHE White Paper "Access Control" mit Fokus auf in der EFAv2.0-Spezifikation genutzte Konzepte und Begrifflichkeiten

Offene Punkte und ToDos

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Epif.04}

ToDos aus der Kommentierung (Fraunhofer)

- Informationsmodell: Übersichtsgrafik als UML-Klassenmodell
- EFA Anwendungsdienste: Fehlercodes konsolidieren und auf einer Seite zusammenfassen
- Akteure und Rollen: Akteursdiagramm einfügen
- Darstellung des Zusammenhangs Interaktionsmuster-Kommunikationsmuster-SFM-Binding (zusätzliche Seite)
- Auf dem letzten Treffen der 7er-Gruppe wurde beschlossen, die LE-Attribute für SAML und XACML auf Basis von XUA++ und in der Profilierung des IHE-Cookbook für die EFA zu übernehmen. Da diese Attributdefinitionen erst Anfang 2014 über das Cookbook veröffentlicht werden, muss das entsprechenden Kapitel zunächst noch in der EFA-Spezifikation verbleiben, sollte aber zeitnah an die im Draft vorliegende Cookbook-Spezifikation angeglichen werden. Hiermit unterliegt das Kapitel HCP Identity Attributs noch einem Änderungsvorbehalt.

Diskussionsbedarfe - operativ (7er-Gruppe)

- Binding für die Operation issueAccessToken
- Binding für die Operation redeemAccessToken
- Informationsmodell für die Klasse accessToken
- Binding für die Klasse accessToken

Diskussionbedarfe - strategisch (Lenkungsgruppe)

Abschnitte, die ggf. in das Cookbook verschoben werden können

- cdaefa:EFA_Business_Informationsmodell#Patient: Regel "Sender does it right"
- cdaefa:EFA_Business_Informationsmodell#purpose
- cdaefa:EFA_XDS_ResourceManager#EFA_XDS.2FXDR_Binding:_createECR: "The application of security measures and the contents of the SOAP security header are specified normatively"
- cdaefa:EFA_XDS_ResourceManager#Security_Considerations
- cdaefa:EFA_Verwendete_Standards#Verwendete_Standards:_Sicherheit
- cdaefa:EFA_IHE_Setup_and_Flow_of_Control#EFA_Setup
- cdaefa:Gruppierung_von_Anwendungs-_und_Sicherheitsdiensten#Gruppierung_von_Anwendungs-_und_Sicherheitsdiensten
- cdaefa:Patienteneinwilligung_zur_EFA#Patienteneinwilligung_zur_EFA

- cdaefa:EFA_Identity_Assertion_SAML2_Binding#HCP_Identity_Attributes: Values for attribute "Structural Role"

Externe Abhängigkeiten

- Aktuell existiert keine OID für die Nutzung der Telematik-ID als Identifizierungsmechansimus für Organisationen und Leistungserbringer. Eine solche OID wird in folgenden Spezifikationsteilen benötigt:
  - Element *AuthorInstitution* im XDS Binding der Dokumentenmetadaten
  - Element *AuthorPerson* im XDS Binding der Dokumentenmetadaten
  - Subject-Identifizierung im EFA SAML Profil

- Ein Codesystem für die Klassifizierung von Fachbereichszugehörigkeiten eines Leistungserbringers muss festgelegt werden. Hier gibt es diverse KBV Schlüsseltabellen, die auf ihre Eignung zu prüfen sind. Diese Klassifizierung wird in folgenden Spezifikationsteilen benötigt:
  - Subject-Attribut im EFA SAML Profil

Conceptual Perspective - Enterprise Dimension

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Die EFA als zweckgebundene Akte

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFlsb.01}`

Die elektronische Fallakte (eFA) unterstützt einrichtungsübergreifende Dokumentations- und Kommunikationsprozesse in der Zusammenarbeit von Leistungserbringern bei der strukturierten Behandlung von spezifischen Erkrankungen.

Die grundsätzliche Entscheidung, ob die Behandlung einer Erkrankung in einer Einrichtung über eine Fallakte unterstützt werden soll, liegt bei der Einrichtung. Üblicherweise wird eine Einrichtung ihren Patienten nur dann die Nutzung einer Fallakte anbieten, wenn weitere Behandler einbezogen werden müssen und die Herstellung einer gemeinsam nutzbaren Dokumentations- und Kommunikationsplattform eine qualitative Verbesserung der Behandlung oder eine Verringerung von Unannehmlichkeiten für den Patienten mit sich bringt. In einem Versorgungsverbund legen die Fallakten anbietenden Einrichtungen (EFA Provider) im Konsens mit den einbezogenen Ärzten den jeweils erforderlichen Inhalt einer diagnose-spezifischen Fallakte fest. Ziel ist es durch die strikte Reglementierung der Fallakteninhalte sowohl eine Informationsüberflutung als auch das Fehlen von relevanten Informationen zu vermeiden. Alle behandelnden Ärzte können sich so auf die Angemessenheit und Vollständigkeit der ihnen in der Fallakte vorliegenden Informationen verlassen. Der Patient wird bei der Abfrage der Einwilligung über die regelhaft in seine Fallakte eingestellten Daten informiert; er kann jedoch lediglich die Nutzung der Fallakte als Ganzes ablehnen, nicht jedoch die Ausklammerung einzelner, von den Ärzten als wichtig erachteten Inhalte, verlangen.

Aufgrund ihrer Bindung an spezifische Krankheitsbilder im Kontext einrichtungsübergreifend strukturierter Behandlungen ist die Fallakte nicht darauf angelegt, für alle Behandlungsfälle zur Anwendung zu kommen. Vielmehr wird zunächst eine Konzentration auf diejenigen Erkrankungen im Vordergrund stehen, bei denen für bestehende Behandlungskooperationen durch die Nutzung von Fallakten deutliche Verbesserungen der Versorgung und/oder Vereinfachungen von einrichtungsübergreifenden Abstimmungsprozessen erzielt werden können.

Die Entscheidung darüber, ob im konkreten Behandlungsfall eine für eine Erkrankung mögliche und von einem Arzt vorgeschlagene Fallaktendokumentation akzeptiert wird und tatsächlich eine Fallakte angelegt werden kann, liegt beim Patienten. Lehnt der Patient die Anlage einer Fallakte ab, darf ihm daraus kein weiterer Nachteil entstehen.

Der "medizinische Fall"

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFlsb.01.01}

Ausgangspunkt einer Fallakte ist immer die medizinische Behandlung eines Patienten, welche je nach Phase eine konkrete Zusammenarbeit mehrerer medizinischer Leistungserbringer erfordert. Dies können z. B. der Hausarzt des Patienten, ein Facharzt, eine Fachabteilung eines Krankenhauses und eine Reha-Einrichtung sein. Die besonderen Charakteristika der durch die EFA abbildbaren Behandlungsphase können dabei wie folgt zusammengefasst werden:

- Es besteht ein Erfordernis der unmittelbaren Kommunikation von medizinischen Daten zwischen den in die Behandlung eingebundenen Leistungserbringern, d. h. mittels einer EFA wird vorrangig über den Patienten und nicht mit dem Patienten kommuniziert.

- Es existieren prüfbare Kriterien, die das zu erreichende Ziel der unterstützten Behandlungsphase – und damit das Schließen der Fallakte – markieren. Das Ziel der jeweiligen Phase muss dabei nicht zwingend die vollständige Genesung des Patienten implizieren, sondern bedeutet lediglich, dass kein Erfordernis einer engen Abstimmung und unmittelbaren Datenkommunikation zwischen verschiedenen Einrichtungen mehr besteht.
- Der Kreis der Leistungserbringer, der über die Fallakte Daten austauscht und die Behandlungsereignisse dokumentiert, ist zu jeder Zeit abschließend benennbar. Er umfasst die Personen, die in der aktuellen Behandlungsphase in die Behandlung eingebunden sind bzw. die Behandlung in einer definierten Rolle begleiten (z. B. als Fallmanager oder Qualitätsbeauftragter).

Wesentlich bei der Festlegung einer Fallakte ist der Behandlungsgrund, der für die intersektorale Kommunikation zwischen mitbehandelnden Organisationen als zentral erachtet werden soll. Dabei wird dieser Grund in der Regel mittels einer ICD-kodierten Diagnose oder mittels einer zwischen Organisationen vereinbarten Regelung beschrieben. Bei der Festlegung des Grundes der gemeinsamen Behandlungsphase ist es von geringer Relevanz, ob dieser eine einzelne oder mehrere, die Behandlung wechselseitig beeinflussende Diagnosen zugrunde liegen.

Zentral ist vielmehr das klare Erfordernis für die Kommunikation zwischen Ärzten und die definierte Zweckbindung der Dokumentationsinhalte (Benennung des Ziels und der Teilnehmer der Behandlung, der erwarteten Dauer des Kommunikationsbedarfs und des Kommunikationsumfanges).

Eine solche kooperative Behandlungsphase mit dem Erfordernis einer gemeinsamen, zweckbezogenen Dokumentation wird in den technischen Spezifikationen der EFA als "medizinischer Fall" bezeichnet, der inhaltlich den medizinischen Kommunikationsbedarf zwischen mitbehandelnden Organisationen festlegt.

Auswirkungen der Zweckbindung auf die Nutzung von Fallakten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFlsb.01.02}

Die erhobenen medizinischen Daten einer elektronischen Fallakte unterliegen aufgrund ihrer Bindung an einen "medizinischen Fall" einer konkreten Zweckbindung: Zweck der elektronischen Fallakte ist das kooperative Zusammenwirken verschiedener Leistungserbringer bei der Behandlung eines konkreten Behandlungsfalls. Das bedeutet, dass nur für den Behandlungsprozess relevante Informationen zu diesem definierten Behandlungsfall in der Fallakte referenziert und zugänglich gemacht werden dürfen. Eine Vorratsdatenerhebung und -speicherung allgemein zum Gesundheitszustand des Patienten ist im Rahmen der Fallakte nicht zulässig. Doppelerhebungen von medizinischen Daten sind bestmöglich zu vermeiden.

Die Zweckbindung der Datenverarbeitung durch die EFA beinhaltet zusammengefasst, dass

- medizinische Informationen über einen bestimmten Patienten in einem bestimmten Behandlungsprozess einem berechtigten Personenkreis in vollem benötigtem Umfang,
- ortsungebunden und
- korrekt zum benötigten Zeitpunkt

zur Verfügung stehen, um den Patienten schnellst- und bestmöglich behandeln zu können.

Zweckbindung und Patientenhoheit

Aus den Anforderungen des Datenschutzes und dem Streben nach einer vertrauensvollen Zusammenarbeit von Arzt und Patient heraus ist eine möglichst starke Rolle des Patienten in Bezug auf die Steuerung der Nutzung seiner medizinischen Daten anzustreben. Diese Rolle kann dabei unterschiedlich in der Interaktion von Arzt und Patient manifestiert werden, wobei die Herstellung einer starken Zweckbindung und die Autorisierung von Einzeltransaktionen zwei Strategien an den Enden des denkbaren Spektrums darstellen:

- Eine **enge Zweckbindung** schafft Transparenz und ermöglicht eine praktikable Patientenhoheit ohne Notwendigkeit einer vollständigen Datenhoheit des Patienten. Die informationelle Selbstbestimmung wird durch die Einwilligung in den Zweck und durch Transparenz bei der datensparsamen Durchsetzung des Zwecks gewahrt. Durch eine patientenbestimmte Belegung von Rollen mit Personen/Organisationen wird eine Intervenierbarkeit des Patienten hergestellt, indem die Berechtigungen jederzeit die Nutzungsanforderungen der vom Patienten als sein Behandlungsteam bestimmten Personen und Organisationen abbilden. Technische Sicherheitsmaßnahmen einer zweckgebundenen Akte dienen vorrangig zur Absicherung der Zweckbindung.
- Eine **starke Patientenhoheit** erlaubt dem Patienten die Zweckbestimmung jeder einzelnen Verarbeitung seiner Daten. Intervenierbarkeit und Selbstbestimmung werden hierbei durch die vollständige Datenhoheit des Patienten abgesichert, wozu auch eine praktikable und diskriminierungsfreie Umsetzung des Rechts auf Verweigerung gehört. Technische Sicherheitsmaßnahmen einer Akte in Patientenhoheit zielen vorrangig auf die Absicherung der Datenhoheit des Patienten ab, d. h. stellen sicher, dass jede Einzeltransaktion durch den Patienten autorisiert ist.

Die EFA ist eine Akte mit enger Zweckbindung. Die damit einher gehenden Anforderungen an das abzusichernde Zusammenspiel von Arzt und Patient werden in der Stellungnahme der Landesdatenschützer zum Datenschutzkonzept der EFA v1.2 beschrieben:

Anders als die einrichtungsübergreifende elektronische Patientenakte (eEPA), die eine Art Vorratsdatenspeicherung für in der Regel noch nicht eingetretene Behandlungsfälle darstellt und damit datenschutzrechtliche Fragen zur Sicherstellung der Zweckbindung aufwirft, wird

die eFA für konkrete Behandlungsfälle angelegt, womit eine enge Zweckbindung für die eFA definiert wird.

In die gemeinsame Fallakte werden nur für die aktuelle Behandlung erforderliche Informationen eingestellt. Mit seiner Einwilligung autorisiert der Patient den von ihm bestimmten Leistungserbringer, zur Durchführung der Behandlung auf den gesamten Inhalt der gemeinsamen Fallakte zuzugreifen. Er hat nicht das Recht, den Zugriff auf einzelne Dokumente auszuschließen. Der Patient hat jedoch das Recht, seine Einwilligung zu widerrufen. Macht er von diesem Recht Gebrauch, darf kein Leistungserbringer mehr auf die Fallakte zugreifen.

Referenzen und Querverweise

- EFA-2.0-Spezifikation
- Abgrenzung der Fallakte gegen patientengeführte Akten (Quelle: EFA-Verein)

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Die EFA als Gesundheitsdatendienst

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFsGe.01}`

Im Rahmen der Bestandsaufnahme und Neuausrichtung der Telematikinfrastruktur (TI) haben die Gesellschafter der gematik das Projekt zur „Migration von Gesundheitsdatendiensten als Mehrwertfachdienste in die Telematikinfrastruktur am Beispiel der elektronischen Fallakte“ (Migration GDD / EFA) beschlossen. Es hat die Aufgabe, (1) ein allgemeines, wieder verwendbares, an Standards orientiertes Muster für die Migration von Gesundheitsdatendiensten (GDD) in die Telematikinfrastruktur zu schaffen, um (2) damit die bestehenden EFA-Netzwerke in die Telematikinfrastruktur einzubinden und (3) die Telematikinfrastruktur als flexibel nutzbare technologische Plattform für bestehende und künftige Gesundheitsdatendienste verfügbar zu machen.

Die EFAv2.0 Spezifikation legt die elektronische Fallakte explizit als Gesundheitsdatendienst aus, so dass EFAv2.0 konforme EFA-Netzwerke über die für alle GDD anwendbaren Migrationspfade zukünftig von den Möglichkeiten der Telematikinfrastruktur profitieren können. Hierdurch ist z.B. eine größtmögliche Mit- und Nachnutzbarkeit von GDD-übergreifend definierten und betriebenen Diensten (z.B. zur Authentisierung und Autorisierung) sichergestellt. EFA-Provider können dadurch in einem regionalen Gesundheitsnetz mit wenig Mehraufwand neben der elektronischen Fallakte auch weitere Gesundheitsdatendienste betreiben und anbieten.

Gesundheitsdatendienste (GDD)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFsGe.01.01}

IHE-Deutschland beabsichtigt mit dem *Akten-Cookbook* eine gemeinsame technische Basis (in diesem Fall IHE XDS und weitere IHE Profile) für verschiedene Ausprägungen von Aktenplattformen zu schaffen. Hierdurch sollen die Gemeinsamkeiten verschiedener Akten herausgearbeitet und Aktenplattformen so neu konzipiert werden, dass diese Gemeinsamkeiten auch über einheitliche technische Bausteine abbildbar sind. Im Idealfall muss das gleiche Set technischer Bausteine für jede Ausprägung einer Aktenplattform nur neu zusammengestellt und konfiguriert werden.

Das Konzept der "Gesundheitsdatendienste" (GDD) verfolgt die gleiche Idee, setzt jedoch eine Ebene höher bei den logischen Bausteinen des Austauschs von Gesundheitsdaten zwischen Leistungserbringern an. Gesundheitsdatendienste bilden somit eine Klasse von Anwendungen, die auf identischen funktionalen Bausteinen (Kommunikationsmuster), logischen Informationsmodellen und Sicherheitsanforderungen basieren. Wesentliche Gemeinsamkeiten aller GDD sind:

- Der GDD vermittelt den Austausch von medizinischen Daten zwischen Leistungserbringern bzw. zwischen Leistungserbringern und medizinisch-fachlichen, IT-gestützten Diensten (z.B. elektronische Register)
- Der Austausch der Daten erfolgt zweckbezogen im Kontext der medizinischen Versorgung (einschließlich Vorsorge, Rehabilitation, Versorgungsforschung, etc.)
- Die ausgetauschten Daten haben einen hohen Schutzbedarf (über einen GDD vermittelte Daten können auch einen sehr hohen Schutzbedarf haben, in diesem Fall müssen jedoch die GDD-übergreifenden Datenschutzkonzepte und Sicherheitsdienste für diesen GDD spezifisch erweitert werden)
- Zu jedem GDD kann es verschiedene Anbieter geben

Diese Gemeinsamkeiten werden auf ein GDD-Referenzmodell abgebildet, das insbesondere wiederkehrende Muster in Bezug auf Nutzerinteraktion, Ablaufsequenzen und die Vernetzung elementarer Informationsbausteine aufnimmt. Hierdurch können insbesondere auch Datenschutzkonzepte, Betriebskonzepte und Sicherheitskonzepte zwischen GDD übertragen werden.

Die EFAv2.0 ist ein GDD und damit auch eine Instanz des GDD-Referenzmodells. Viele der technischen Spezifikationen der EFAv2.0 bilden valide Bindings zu den funktionalen und logischen Bausteinen von Gesundheitsdatendiensten und sind damit GDD-übergreifend wiederverwendbar. Ebenso sind viele der Sicherheits- und Datenschutzmechanismen der EFAv2.0 valide Umsetzungen der allen GDD gemeinsamen Sicherheits- und Datenschutzanforderungen und können damit ebenfalls für weitere GDD genutzt werden.

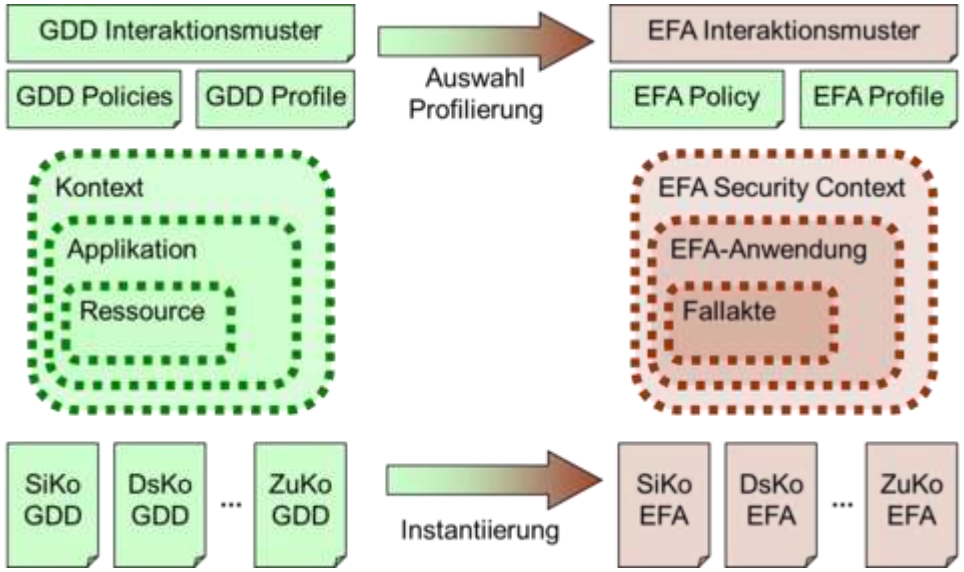
GDD Referenzmodell

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {DFsGe.01.02}

Gesundheitsdatendienste besitzen eine Vielzahl gemeinsamer Charakteristika in Bezug auf IT-Sicherheit, Datenschutz und TI-Konformität, die sich u.a. in wiederverwendbaren GDD-Artefakten (Konzepte, Spezifikationen, etc) widerspiegeln, die nur einmalig definiert werden müssen und dann für jeden einzelnen GDD profiliert bzw. instanziiert werden können. Durch solche GDD-übergreifend nutzbaren Komponenten werden die Aufwände zur Implementierung und Zulassung sowie zum Betrieb eines GDD deutlich reduziert.

Das **GDD-Referenzmodell** definiert vier generische Ablaufschritte zur Nutzung eines GDD durch einen Heilberufler:

1. Aufsetzen eines sicheren Ausführungskontextes
2. Erlangen des Zugangs zu einer von einem GDD-Anbieter bereitgestellten Anwendung aus dem sicheren Ausführungskontext heraus
3. Erlangen des Zugangs zu einer von der Anwendung verwalteten Ressource (Anwendungsinstanz, z. B. eine konkrete Fallakte eines Patienten)
4. Durchführen von Zugriffen auf die Ressource (z. B. Auslesen von Dokumenten aus einer Fallakte)



Ausführungskontext, Anwendung und Ressource sind in einander verschachtelte Klassen, die das **Referenz-Objektmodell** eines GDD bilden:

- Der Ausführungskontext bildet den aktuellen Sicherheitskontext des Nutzers ab und enthält Nachweise zur Identität, Authentizität und den Autorisierungen des Nutzers. Der Kontext wird dezentral auf Seiten des Nutzers aufgebaut und verwaltet, kann aber beim Aufruf einer GDD-Operation vollständig zum GDD-Fachdienst übermittelt werden; d.h. es wird über Dienstnutzer und Dienstanbieter hinweg ein gemeinsamer Sicherheitskontext aufgespannt.
- Anwendungen repräsentieren die von einem GDD-Anbieter bereitgestellten Dienste eines GDD. Die Mechanismen zum Zugang zu einer Anwendung kapseln die unterschiedlichen Konzepte der Dienstlokalisierung und erlauben die Umsetzung GDD-spezifischer Zugangs- und Sicherheitspolitiken.
- Der Kern eines GDD sind die Ressourcen, die die zu verarbeitenden Gesundheitsdaten repräsentieren. Das GDD-Referenzmodell definiert eine Reihe von generischen Referenz-Abläufen auf Ressourcen (abrufen, anlegen, verändern, autorisieren, etc.) die von einem GDD relativ frei instanziiert und erweitert werden können.

Durch Instanziierung, Anpassung und Erweiterung des Referenz-Objektmodells und der Referenz-Abläufe kann ein bestehender oder geplanter GDD sehr einfach in das Rahmenwerk des GDD-Referenzmodells eingepasst werden. Hierdurch können alle GDD-übergreifend angelegten

Spezifikationen, Konzepte und Software-Komponenten zur Implementierung und zum Aufsetzen des GDD sowie zu seiner Migration in die zukünftige Telematikinfrastruktur genutzt werden.

Referenzen und Querverweise

- EFAv2.0-Spezifikation
- Informationen zu den geplanten Anwendungen auf der Telematikinfrastruktur (Quelle: gematik)

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Sicherheitsstrategie

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.01}`

Die EFA ist eine zweckgebundene Akte. Der Zugriff auf die Akte ist auf Leistungserbringer beschränkt, die vom Patienten als Behandlungsteilnehmer benannt wurden und die im Kontext dieser Behandlung Patientendaten zu dem an die Akte gebundenen Zweck verarbeiten.

Maßnahmen des Datenschutzes und der IT-Sicherheit müssen daher sicherstellen, dass eine Offenbarung von über die Akte vermittelten Daten nur

- gegenüber in die Behandlung einbezogenen Personen und nur
- zu dem benannten Zweck erfolgt.

Darüber hinaus bedingt der Charakter der Akte als behandlungsbegleitende Kommunikationsplattform und Grundlage einer gemeinsamen Behandlungsdokumentation, dass

- über die Akte nur die für die Behandlung und die Behandlungsdokumentation relevanten Informationen ausgetauscht werden und

- die in der Akte enthaltenen Dokumente verlässlich sind in dem Sinne, als dass Urheber und Status der Dokumente für die Nutzer erkennbar ist.

Diese primären Zielstellungen der EFA-Sicherheit werden durch eine von den konkreten Umsetzungsmaßnahmen unabhängige Sicherheitsstrategie aufgefangen. Diese Strategie wiederum wird auf einige wenige elementare und implementierungsunabhängige Sicherheits-Kernkonzepte heruntergebrochen, die jeweils mit im EFA-Sicherheitskonzept oder der EFA-Sicherheitsarchitektur verankerten Maßnahmen hinterlegt sind.

Abgeleitet aus diesen Zielstellungen wird in der EFA eine aus sechs Kernaussagen bestehende Sicherheitsstrategie verfolgt:

Zusammenspiel von Sicherheitskonzept und Sicherheitsarchitektur

Um die spezifizierten Sicherheitsziele zu erreichen, müssen sowohl organisatorische als auch technische Umsetzungswege in Betracht gezogen werden. Basis der IT-Sicherheit der EFA sind ein integriertes, stringentes Sicherheitskonzept und eine von der Anwendung entkoppelte, einfach aufgebaute Sicherheitsarchitektur nach den Vorgaben von ISO-7498-2. Nutzungseinschränkungen und Restriktionen in Bezug auf die Umsetzung der funktionalen Anforderungen können zur Vermeidung technischer Komplexität in Kauf genommen werden.

Lose Kopplung der Sicherheitsdienste untereinander und an die abzusichernden Anwendungsdienste

Sicherheits- und Anwendungsarchitektur werden von einander entkoppelt, um die Komplexität der Systemarchitektur und ihrer Implementierungen zu reduzieren. Alle Sicherheitsdienste müssen anwendungsunabhängig sein. Anwendungsdienste dürfen sich nicht auf bestimmte Implementierungen von Sicherheitsdiensten beziehen.

Sicherheit (z. B. Integrität, Vertraulichkeit, Verbindlichkeit) wird auf der Anwendungsebene als Teil der Kontroll- und Datenflüsse umgesetzt. Kontroll- und Datenflüsse werden gestuft aufgesetzt, um die Integration von Verteidigungslinien entlang der Abläufe zu unterstützen. Verteidigungslinien entlang der Abläufe ermöglichen es datenhaltenden Diensten die Integrität von Nachrichten und Daten sowie die Gültigkeit von Autorisierungen auf Basis lokal verfügbarer Informationen zu verifizieren. Der Zugang zur EFA-Anwendung, der Abruf digitaler Identitäten, der Zugang zu einer Fallakte und der Zugriff auf medizinische Datenobjekte werden als entkoppelte Aktionen aufgefasst, die über unterschiedliche, möglichst voneinander unabhängige Maßnahmen abgesichert werden.

Sicherheitsdienste sind nicht von Eigenschaften der verwendeten Kommunikationsmechanismen abhängig.

Patienteneinwilligung und Needs-To-Know Prinzip als Grundlage aller Berechtigungen

Mechanismen zum Zugriffsschutz basieren auf Identitäten (Individuen und Organisationen). Zugriffsrechte werden ausschließlich an die vom Patienten benannten Behandlungsteilnehmer vergeben, sind synchron zu den fachlichen Zugriffserfordernissen aufgesetzt und gelten immer für eine Fallakte als Ganzes. Berechtigungen werden mit Identitäten verknüpft, indem Rollen des Fachkontextes mit Personen und/oder Organisationen instanziiert werden.

EFA-Policy als Grundlage des Datenaustauschs zwischen autonomen EFA-Netzwerken
: Die Vermittlung von Vertrauen, die Abbildung von Sicherheitsrichtlinien und die Weitergabe von Identitätsinformationen zwischen eng integrierten EFA-Netzwerken werden durch eine Föderation dieser Netzwerke realisiert.

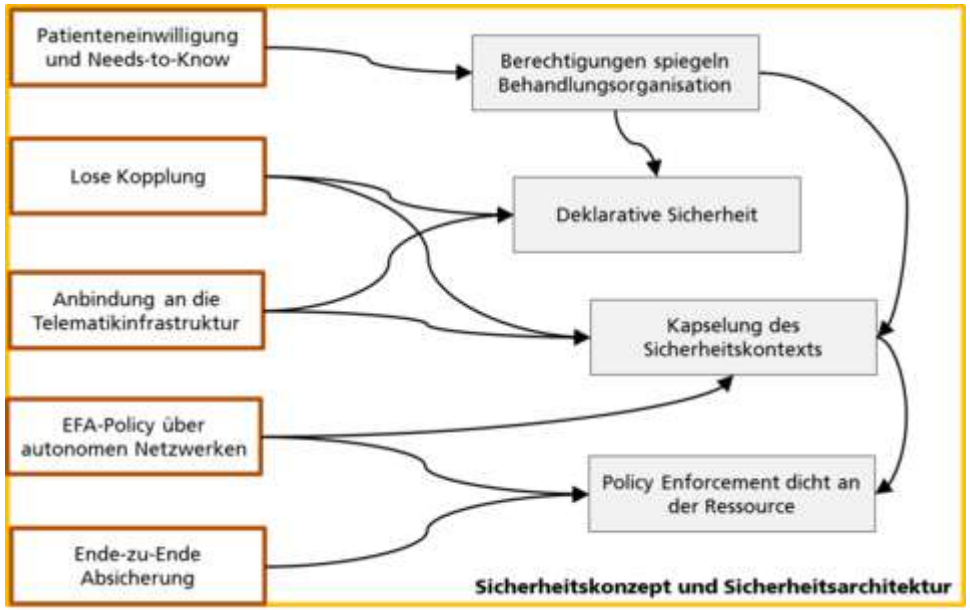
Ende-zu-Ende Absicherung des Zugriffs auf medizinische Daten
: Ende-zu-Ende-Integrität und Ende-zu-Ende-Vertraulichkeit wird zwischen den Endpunkten "EFA Teilnehmer" und "EFA Datenspeicher (Repository)" hergestellt, um einen sicheren Austausch medizinischer Datenobjekte zu realisieren.

Nutzung der Sicherheitsobjekte, -mechanismen und -maßnahmen der Telematikinfrastruktur
: Auch wenn die EFA selber keine Anwendung des § 291a SGB V darstellt, so gelten doch viele der für Anwendungen nach § 291a Absatz 3 SGB V benannten Anforderungen gleichermaßen. Um die parallele und idealerweise integrierte Nutzung von EFA und Anwendungen des § 291a SGB V zu ermöglichen, kann die EFA auf den Basis-Sicherheitsobjekten und -mechanismen der Telematikinfrastruktur (Karten, Kartenleser, Zertifikate, Algorithmen, etc.) aufgesetzt werden. Auch sind weite Teile der Datenschutz- und Sicherheitskonzepte der Telematikinfrastruktur auf die EFA abbildbar und erleichtern so den synergetischen Betrieb und die verzahnte Nutzung von EFA und Telematik-Diensten.

Kernkonzepte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.02}

Aus der Sicherheitsstrategie wurden eine Reihe von technisch abgesicherten Kernkonzepten in Bezug auf die Architektur von Fallakten, deren technische Umsetzung und operative Nutzung abgeleitet. Die nachfolgende Abbildung stellt diese Konzepte im Kontext der Sicherheitsstrategie im Überblick dar.



Synchronität von Behandlungsteam und Berechtigungen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.02.01}

Als Plattform für eine Behandlungskooperation und gemeinsame Behandlungsdokumentation muss eine Fallakte für alle an der Behandlung aktiv teilnehmenden Personen gleichermaßen zugreifbar sein. Ein Verbergen von Dokumenten für einzelne Teilnehmer oder eine differenzierende Berechtigungsvergabe stehen im Widerspruch zu dieser Zielsetzung der Fallaktennutzung.

Aus diesem Grund erhalten alle vom Patienten in seiner Einwilligungserklärung benannten aktiven Behandlungsteilnehmer die Berechtigung, auf alle in der Akte enthaltenen medizinischen Daten zuzugreifen und auch neue Daten in die Akte einzustellen.

Differenzierte Rollen und Berechtigungen können lediglich für passive Teilnehmer definiert werden, die Sonderrollen - z.B. durch rein administrative Aufgaben in der Verwaltung von Fallakten - ausfüllen. Beispiele hierfür sind im Abschnitt "Akteure und Rollen" aufgeführt.

Zugriffsberechtigungen sind immer an eine komplette Fallakte geknüpft und werden an alle Objekte innerhalb der Fallakte vererbt. Der Patient kann sowohl Einzelpersonen als auch Organisationen bzw. Organisationseinheiten als Behandlungsteilnehmer benennen. Dieses wird 1:1 auf das interne Berechtigungsmangement der EFA abgebildet, d.h. Zugriffsrechte werden dementsprechend entweder an Individuen oder Organisationen als EFA-Teilnehmer gebunden. Im Fall der Berechtigungsvergabe an eine Organisation(seinheit) muss die Zuordnung eines auf die Akte zugreifenden Individuums zu einer berechtigten Organisation und zum Behandlungskontext der Fallakte mit Hilfe eines dezentralen (technisch oder organisatorisch realisierten) Berechtigungsmanagements erreicht werden. Mit der Registrierung bei einem EFA-Provider verpflichtet sich eine Organisation, dieses sicherzustellen.

Die Granularität der für einen EFA-Provider technisch verifizierbaren Authentisierung (Individuum bzw. Organisation) muss auf die Granularität der Zugriffsrechte, die für eine Fallakte definiert sind, abgebildet werden können. Wenn z. B. eine Organisation für den Zugriff auf eine Fallakte autorisiert ist, muss die Zugehörigkeit eines Arztes zu dieser Organisation geprüft werden können, um ihm den Zugang zu gestatten. Dies kann z.B. dadurch erfolgen, dass eine vom EFA-Provider als vertrauenswürdig anerkannte Organisation die Zugehörigkeit des Mitarbeiters zu dieser Organisation in einer Form bestätigt, die vom EFA-Provider als authentisch und nachvollziehbar verifizierbar ist.

Ungeachtet dessen muss jede Authentisierung auf eine natürliche Person rückführbar sein, die auch im an die EFA-Dienste übermittelten Authentisierungsnachweis benannt sein muss und auch im Audit Trail vermerkt wird. D.h. auch wenn eine Autorisierung auf Ebene einer Organisation erfolgt, so bedeutet dies nicht, dass die handelnde natürliche Person gegenüber der EFA anonym bleibt.

Übertragbarer Sicherheitskontext

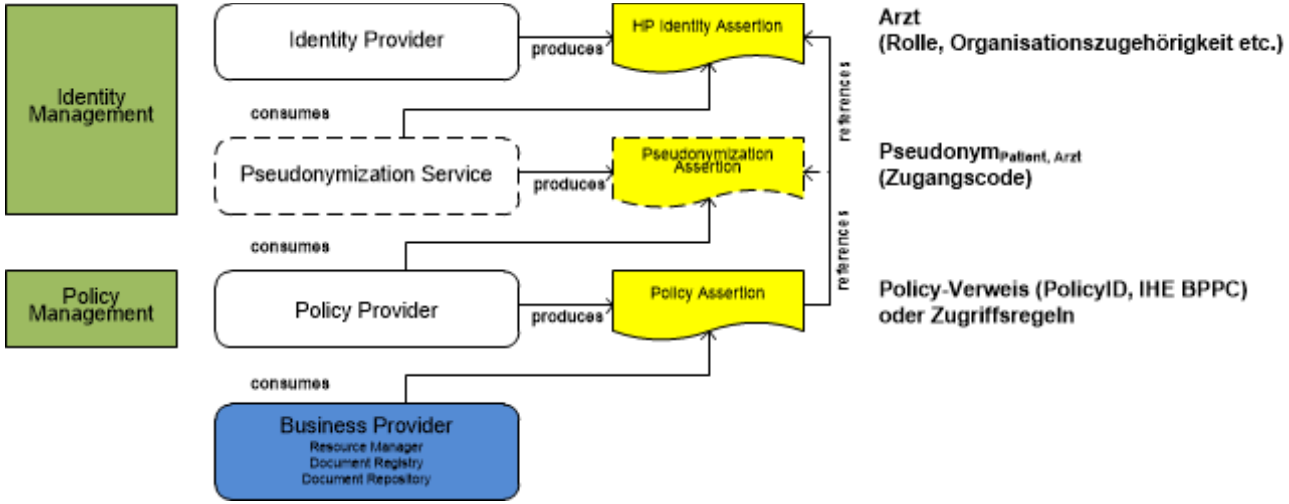
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.02.02}

Der Sicherheitskontext eines EFA-Teilnehmers wird durch dessen Identitätsdaten, einen Nachweis der Authentizität und die im aktuellen Nutzungsszenario geltenden Zugangs- und Zugriffsberechtigungen des Teilnehmers beschrieben. Ein im aktuellen Zugriffsszenario gültiger Sicherheitskontext wird über eine Menge von aufeinander aufbauenden Sicherheitsnachweisen (Assertions) kodiert. Die nachfolgende Grafik veranschaulicht dieses Prinzip:

1. der EFA-Teilnehmer authentisiert sich gegenüber einem vertrauenswürdigen lokalen oder als dediziertem Plattformdienst aufgesetzten Identity Provider.
2. der Identity Provider fasst die vom EFA Berechtigungsmanagement benötigten Identitätsdaten des Teilnehmers zu einem Sicherheitsnachweis (*HP Identity Assertion*) zusammen und versieht diesen mit einer für alle EFA-Dienste verifizierbaren Signatur.

3. sofern die Option der Pseudonymisierung von Registerdaten aktiviert ist, wird im nächsten Schritt eine sog. *Admission Assertion* erzeugt, die benötigt wird, um das für den Datenzugang benötigte Pseudonym des Patienten aufzulösen. Die zuvor ausgestellte *HP Identity Assertion* wird nicht nur für die Generierung des Pseudonyms benötigt, sondern dient auch der Absicherung, dass die bei der Pseudonymgenerierung verwendeten Daten authentisch sind.
4. die EFA unterstützt u.a. das sog. "Policy Push" Verfahren, bei dem der EFA-Teilnehmer von einem dedizierten Dienst seine aktuell gültigen Berechtigungen abruft. Die Authentisierung und Identifizierung gegenüber diesem Dienst erfolgt über die *HP Identity Assertion* bzw. im Fall pseudonymer Registerdaten über die *Admission Assertion*. Die Berechtigungen werden in einem Berechtigungsnachweis (*Policy Assertion*)zusammengefasst, der fest mit der *HP Identity Assertion* verknüpft ist. Ein Berechtigungsnachweis ist nur zusammen mit einem auf den selben Nutzer ausgestellten authentischen Identitätsnachweis gültig.
5. Alle entlang der Kette eingesammelten und miteinander verknüpften Assertions werden beim AUfruf eines Fachdiensts übergeben. Dieser prüft die Authentizität der Assertions, die Authentizität des EFA-Teilnehmers und setzt anschließend die in der *Policy Assertion* kodierten Berechtigungen des Nutzers durch.

Durch diese Verkettung von Sicherheitsnachweisen wird faktisch der beim Aufrufer gültige Sicherheitskontext an einen Fachdienst übermittelt und kann dort zur Prüfung und Durchsetzung von Berechtigungen rekonstruiert werden.



Deklarative Sicherheit

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.02.03}

Sicherheitsfunktionen zur Erfüllung von Anforderungen an die Vertraulichkeit und Authentizität von geschützten Daten folgen oftmals dem gleichen Muster: Eine die geschützte Ressource kapselnde Anwendung erhält einen Dienstaufruf. Der Aufrufende muss authentisiert und anschließend autorisiert werden. Dies führt zum Zugriff auf entsprechende Ressourcen oder eben nicht. Hier liegt es nahe, solche wiederkehrende Aufgaben in Security Frameworks auszulagern und zu beschreiben (deklarieren), welche Sicherheitsfunktionen zu aktivieren sind, um einer übergeordneten Sicherheitsstrategie gerecht zu werden. Die Ausübung dieser Sicherheitsfunktionen ist dann Sache des Frameworks. Dieser Schutzziele und Sicherheitsdienste betonende deklarative Sicherheitsansatz steht im Gegensatz zur programmierten Sicherheit, bei der konkrete Sicherheitsmechanismen und –objekte fest an die Implementierung der Anwendungslogik gebunden werden. Ziel ist es hierbei immer, die für eine Komponente oder Kommunikationsbeziehung geltenden Sicherheitsziele zu beschreiben und die Auswahl des geeigneten Mechanismus dem Framework zu überlassen.

Die Nutzung deklarativer Sicherheit bietet eine Reihe von Vorteilen:

- Sicherheitsdienste und –mechanismen können ohne Änderungen am Code der Anwendungsdienste weiterentwickelt und an neue Anforderungen angepasst werden
- In einem Framework enthaltene Stubs der Sicherheitsdienste können sehr einfach an bestehenden Anwendungen angebunden werden. Hierdurch wird eine Entkopplung von Sicherheitsdiensten - z. B. für Authentifizierung und Autorisierung – unterstützt
- Die Kongruenz der Umsetzung von Sicherheit zu ihrer Spezifikation und einer übergeordneten Sicherheitsrichtlinie ist explizit gegeben, d. h. deklarative Sicherheit kann unmittelbar aus dem Sicherheitskonzept abgeleitet werden
- Die umgesetzten Sicherheitsmechanismen und die genutzten Objekte werden an der Schnittselle der Dienste sichtbar und damit überprüfbar.

Die Sicherheitsdienste der EFA v2.0 setzen wo immer machbar und sinnvoll Konzepte einer deklarativen Sicherheit um.

Policy Enforcement dicht an den Ressourcen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Pziee.02.04}

Sofern die Organisation eines EFA-Teilnehmers nicht selbst als EFA-Provider fungiert, erfolgt die Bereitstellung von Daten dieses Teilnehmers über einen Provider den Tatbestand einer Auftragsdatenverarbeitung. Dieses legt dem Teilnehmer besondere Pflichten in der Auswahl des Providers auf; gleichzeitig muss der Provider für die im Auftrag verwalteten Daten ein den regulativen Vorgaben genügendes Niveau an Datenschutz und Datensicherheit sicherstellen.

Insbesondere in einem weitgehend auf gegenseitigem Vertrauen der EFA-Peers basierenden Verbund stellt dies große Herausforderungen, da letzten Endes jeder Provider nur die Sicherheitszusagen machen kann, die er auch selbst technisch, organisatorisch und/oder juristisch durchsetzen kann.

Um den Provider entsprechend zu befähigen, gilt für die EFA, dass jeder Provider für die bei ihm vorgehaltenen Daten für die Prüfung und Durchsetzung der aus der Patienteneinwilligung abgeleiteten Zugriffsberechtigungen verantwortlich ist und diese auch selbst durchführen muss. Zusätzlich ist jeder Provider für die korrekte Abbildung der Angaben aus der Patienteneinwilligung (insb. berechtigte Teilnehmer) auf sein Zugriffskontrollsystem verantwortlich. Da hierzu eine Verarbeitung von potenziell über andere Akteure erhobene Daten unabdingbar ist (z.B. von einem anderen Provider bestätigter Nachweise einer Nutzer-Authentisierung oder gegenüber einem Arzt gegebene Einwilligung) ist es unabdingbar, dass die Systemteilnehmer untereinander die gegenseitige Vertrauensstellung ausreichend absichernde vertragliche Bindungen eingehen.

Referenzen und Querverweise

- Datenschutzkonzept der EFA Version 1.2
- Sicherheitskonzept der EFA Version 1.2
- EFA-2.0-Spezifikation

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Akteure der EFA

Patient (Versicherter)

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Auun.01.01}`

Der Bürger tritt bei der EFA explizit in der Rolle des "Patienten" auf (und nicht als "Versicherter"), da sich hieran wesentliche Grundsatzentscheidungen für Umsetzung und Nutzung der EFA knüpfen:

- es liegt eine Erkrankung vor, aus der heraus sich der Zweck der EFA-Nutzung ergibt. Übergeordneter und vorrangiger Zweck ist dabei immer, die Effizienz und Qualität der Prozesse zur Verbesserung des Zustands des Patienten durch den Einsatz einer Fallakte zu steigern.
- der Betroffene ist auf die behandelnden Ärzte angewiesen und muss deren Entscheidungen und Handlungen in einem guten Maße vertrauen. Insbesondere muss er den behandelnden Ärzten auch vertrauen, dass diese sorgfältig mit seinen Gesundheitsdaten umgehen - unabhängig davon, ob es sich um Daten auf Papier oder in einer elektronischen Akte handelt.

Der Patient entscheidet frei darüber, ob im Zusammenhang seiner Behandlung eine Fallakte angelegt werden darf und erteilt nach seiner Einwilligung bzgl. der Nutzung der EFA auch die initialen Zugriffsberechtigungen für die Nutzung seiner Fallakte. Er kann die entsprechenden Einwilligungen jederzeit zurücknehmen. Die konkrete fachliche Ausgestaltung der Zweckbindung und Nutzung der Fallakte obliegt den behandelnden Ärzten.

Der Patient selbst ist kein EFA-Teilnehmer (s.u.), d.h. er ist nicht zum Zugriff auf die Fallakte berechtigt. Das Recht zur Einholung einer Selbstauskunft bleibt davon unberührt.

Fallaktenmanager

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Auun.01.02.01}

Der Fallaktenmanager ist üblicherweise der klinische Leiter/Direktor (oder der im Allgemeinen zuständige Disziplinarvorgesetzte) und trägt damit die Verfahrens- und Fachverantwortung der eröffnenden Stelle mit allen den daraus resultierenden Rechten und Pfichten (auch Haftung). Dieser Rolle sind bei unmittelbarer Wahrnehmung der Pflichten als Disziplinarvorgesetzter sämtliche Berechtigungen einer Fallakte zugewiesen.

Der Fallaktenmanager ist die einzige Stelle, die auf eine Fallakte im gesperrten Zustand über ein gesondertes Verfahren zugreifen kann und dem gegenüber invalidierte Daten sichtbar sind. Des Weiteren kann der Fallaktenmanager bei Bedarf jederzeit die Löschung einer Fallakte durchführen.

Die Rolle des Fallaktenmanagers muss für jede angelegte Fallakte besetzt sein. Der Fallaktenmanager muss in der Einwilligung als verfahrens- und fachverantwortliche Person benannt sein. Sofern der Fallaktenmanager seine operativen Aufgaben auf einen Vertreter delegiert, muss auch diese Person oder Organisationseinheit in der Einwilligung benannt werden.

Als Verfahrens- und Fachverantwortlicher wird der Fallaktenmanager von den Teilnehmern eines EFA-Netzwerks festgelegt. Eine Änderung dieser Festlegung durch den Patienten ist nicht möglich.

EFA-Teilnehmer

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Auun.01.02}

Der Patient legt die an seiner Behandlung teilnehmenden Akteure fest und berechtigt diese zur Teilnahme an einer zur Unterstützung der Behandlung aufgesetzten elektronischen Fallakte. EFA-Teilnehmer sind damit üblicherweise alle in die Behandlung einbezogenen Ärzte sowie das nicht-ärztliche medizinische Fachpersonal (z. B. Pflegekräfte), das in die Behandlung und Dokumentation als berufsmäßig tätige Gehilfen der Ärzte einbezogen ist.

Im Kontext der Fallakte wird der Akteur "EFA-Teilnehmer" üblicherweise als Rolleninhaber innerhalb einer Institution betrachtet, in der er als Arzt oder Gehilfe seine Berechtigung zur Nutzung der Fallakte aus seiner Mitwirkung an der Behandlung des Versicherten begründen kann. Dabei kann der Versicherte die Berechtigung an weitere Voraussetzungen gebunden haben, z. B. an die Zugehörigkeit zur behandelnden Fachabteilung im Krankenhaus.

Die Erteilung einer Berechtigung an eine Institution ist jedoch in jedem Fall an die Voraussetzung gebunden, dass den innerhalb der berechtigten Institution tätigen Heilberuflern ausschließlich im Rahmen ihrer Beteiligung an der Behandlung eine Nutzung ermöglicht wird und eine Nutzung durch nicht in die Behandlung einbezogene Personen in der Einrichtung technisch oder organisatorisch verhindert wird.

Die Verantwortung für den Inhalt der Fallakte liegt bei den teilnehmenden Ärzten, wobei jeder Arzt die Richtigkeit und Vollständigkeit der aus seinem Zuständigkeitsbereich heraus in die Akte eingestellten Daten sicherstellen muss.

Inhaber der Rolle "EFA-Teilnehmer" haben das Recht,

- Fallakten anzulegen und in einen geordneten Schließungsprozess zu überführen
- neue Partitionen zu einer Fallakte anzulegen
- alle in eine Fallakte eingestellten, gültigen Daten einzusehen und aus der Akte in ihre IT-Systeme zu übernehmen
- selbst erhobene oder von Dritten (einschießlich des Patienten) empfangene medizinische Daten in eine Fallakte einzustellen
- in eine Fallakte eingestellte Dokumente zu invalidieren

Abweichende Berechtigungen existieren lediglich für einige Sonderrollen:

Verwaltungspersonal

Auch wenn die Einwilligung zur Nutzung der Fallakte gegenüber einem Arzt gegeben werden muss, so können die damit verbundenen administrativen Aufgaben durch Verwaltungspersonal vorgenommen werden. Diesem Personal wird daher die Berechtigung eingeräumt, elektronische Fallakten für Ärzte zu eröffnen. Eine Berechtigung dieser Rolle, Fallakten einzusehen oder zu modifizieren, ist keinesfalls gewährt.

Die Umsetzung dieser Rolle in einem EFA-Netzwerk ist optional, d.h. es kann durchaus die Vorgabe definiert werden, dass der vollständige Ablauf der Einrichtung einer Fallakte vom Einwilligungsnehmer durchgeführt werden muss.

Personen mit datenschutzrechtlichen Kontrollaufgaben

Personen mit datenschutzrechtlichen Kontrollaufgaben sind im täglichen Regelbetrieb keine Zugangs- und Zugriffsrechte eingeräumt. Für geplante Audits und ungeplante oder stichprobenartige Kontrollen sind hier jedoch für die Dauer der Prüfung ausreichende Berechtigungen zur Wahrnehmung der Kontrollpflichten zu vergeben. Dies gilt auch, wenn auf Grund von Patientenbeschwerden eine außerordentliche Prüfung durch eine Kontrollinstanz notwendig wird.

Automatisierte Audits und Plausibilitätsprüfungen

Auch potenziellen automatisierten (Datenschutz-)Analysewerkzeugen können gegebenenfalls Berechtigungen zugestanden werden, damit diese im Hintergrund automatisiert Kontrollaufgaben wahrnehmen können.

EFA Provider

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Auun.01.03}

Ein EFA-Provider ist ein Dienstleister, der EFA-Teilnehmern die Dienste einer Fallakte bereit stellt. Er verantwortet und betreibt die technischen Dienste der EFA, die Leistungserbringer auf der Grundlage einer freiwilligen, informierten Einwilligung des Patienten zum Austausch medizinischer Daten nutzen. Er stellt einen expliziten Ansprechpartner für Datenschutzfragen des Versicherten.

Zu den von einem EFA-Provider verantworteten Diensten gehört z.B. die Verwaltung von Dokumenten einer Fallakte, die Authentisierung von Fallakten-Teilnehmern und die Durchsetzung der von Patienten gegebenen Einwilligungen. Die von einem EFA-Provider bereit gestellten Dienste werden in ihrer Gesamtheit auch als EFA Peer bezeichnet sofern hiermit die volle Funktionalität einer EFA abgebildet werden kann.

Datenerhebende und datenverantwortliche Stellen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Auun.01.04}

Im Normalfall wird eine elektronische Fallakte von einem niedergelassenen (Fach-)Arzt oder von einem Krankenhaus im Rahmen eines bestehenden Behandlungsvertrages eröffnet. Ein EFA-Peer wird immer von einem Provider (Betreiber) betrieben, wobei es sich dabei im Regelfall um ein Krankenhaus handelt. Datenhaltende und somit auch datenverantwortliche Stelle ist hierbei der Provider des für die Eröffnung der Fallakte verwendeten Dienstes. Dieser wird explizit auf der Einwilligung genannt.

Sofern ein Krankenhaus im Kontext einer Fallakte sowohl als EFA-Teilnehmer als auch als EFA-Provider agiert, sind die von diesem Teilnehmer bereitgestellten medizinischen Daten innerhalb einer Fallakte im Regelfall lediglich Verweise (Referenzen) auf die in den Primärsystemen abgelegten medizinischen Daten, weshalb die fachliche und datenschutzrechtliche Verantwortung für die medizinischen Daten bei den jeweiligen originären Erstellern verbleibt.

In der Praxis muss jedoch davon ausgegangen werden, dass ein niedergelassener (Fach-)Arzt nur in Ausnahmefällen über die notwendige technische Infrastruktur verfügt, welches die strengen Anforderungen des eFA-Systems erfüllt. Deshalb werden in diesem Fall die medizinischen Daten über ein Portalsystem an einen Drittanbieter (z.B. EFA-Zwischenspeicher bei einem EFA-Provider) übertragen, dort gespeichert und zugreifbar gemacht. In diesem Falle handelt es sich um eine Auftragsdatenverarbeitung. Der niedergelassene Arzt muss deshalb bei der Nutzung eines Drittanbieters als EFA-Provider zusätzlich zur Einwilligung zur Nutzung der EFA auch eine Einwilligung zu dieser Auftragsdatenverarbeitung erfragen.

Datenverantwortliche Stelle ist in beiden Szenarien die Daten erhebende Stelle, also der niedergelassene Arzt oder das Krankenhaus. Sollte der niedergelassene Arzt, wie oben beschrieben, die medizinischen Daten an einen Drittanbieter ausliefern, so erfolgt dies im Rahmen der Auftragsdatenverarbeitung nach §11 BDSG. Dabei verbleibt die Verantwortung für eine auftragsgemäße und gesetzeskonforme Verarbeitung der Daten durch den Auftragnehmer beim beauftragenden Arzt [nach: §§5, 9, 11 BDSG]. Beachtenswert hierbei ist es jedoch, dass in bestimmten Bundesländern eine Datenoffenbarung bei der Datenverarbeitung im Auftrag untersagt ist und demnach zusätzliche Maßnahmen getroffen werden müssen, sobald Daten an einen Zwischenspeicher kommuniziert werden sollen.

Referenzen und Querverweise

- EFA-2.0-Spezifikation
- Umsetzung der Rolle des EFA-Providers am Beispiel des UK Aachen (Deutsches Ärzteblatt, Jg. 109, Heft 40, 5.10.2012, S. A1978-80)

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt

und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Affinity Domain vs. Versorgungsdomänen

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Erid.01}`

Die elektronische Fallakte ist eine Plattform für die regionale Vernetzung und Verankerung von Krankenhäusern. Während z. B. Zuweiserportale lediglich einzelne Aspekte der Datenkommunikation mit Niedergelassenen effizienter gestalten, bildet die elektronische Fallakte ein vollständiges regionales Versorgungsnetzwerk ab, in dem die einzelnen Akteure beliebige Gesundheitsdatendienste aufsetzen und eigene, fallspezifische Kooperationsnetze innerhalb des Verbunds ausbilden können:

- Als **Plattform** bietet die elektronische Fallakte Sicherheits- und Datendienste an, auf denen neben der Anwendung Fallakte auch beliebige weitere Gesundheitsdatendienste (Fallkonferenz, Terminbuchung, Tele-Konsil, etc.) aufgesetzt werden können. Nutzeraccounts und Berechtigungen werden in den beteiligten Einrichtungen zentral verwaltet und können von allen Gesundheitsdatendiensten im regionalen Verbund genutzt werden; hierdurch wird nicht nur das Aufsetzen neuer Anwendungen einfacher und kostengünstiger, sondern auch der Nutzenkomfort für die Ärzte erhöht: ein Arzt muss sich nicht an jedem Portal neu anmelden und es spielt für ihn keine Rolle mehr, wo benötigte Daten nun gerade physikalisch gespeichert sind – er meldet sich einfach wie bisher an seinem System an und die Plattform sorgt dann dafür, dass er alle benötigten Dienste und Daten so nutzen kann, als wären diese lokal in seinem System verfügbar.
- Als **Anwendung** vernetzt die elektronische Fallakte alle Ärzte, die in die Behandlung einer Erkrankung eines Patienten eingebunden sind. Alle behandelnden Ärzte haben Zugriff auf alle Daten eines medizinischen Falls und pflegen über die Fallakte eine gemeinsame Falldokumentation. Über die Fallakte werden somit bestehende Kooperationsbeziehungen in einem regionalen Netzwerk technisch unterstützt und auf eine einheitliche technische Basis gesetzt.

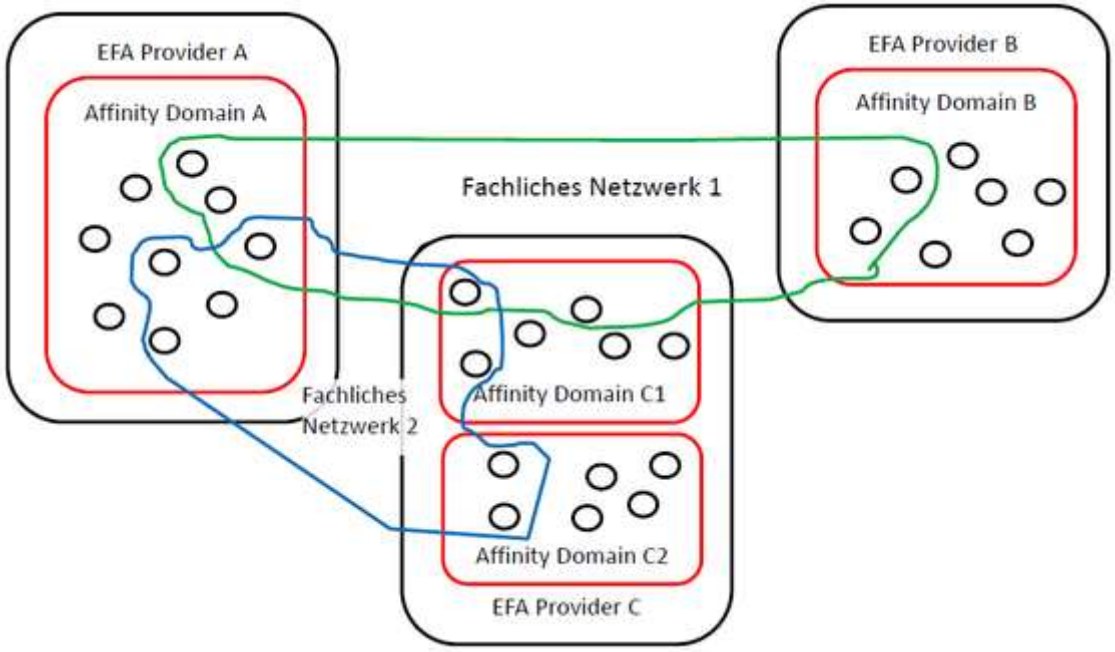
Diese unterschiedlichen Sichtweisen auf eine EFA als Plattform und als Anwendung spiegelt sich auch in den unterliegenden Konzepte der technischen und fachlichen Vernetzung der EFA Teilnehmer wider:

- EFA als Plattform: Ein Netzwerk von kooperierenden Einrichtungen, in dem es festgelegte Regeln zur technischen und semantischen Umsetzung von Diensten zum Austausch medizinischer Informationen sowie zur Umsetzung von IT-Sicherheit und Datenschutz gibt, wird als **Affinity Domain** bezeichnet. Der orginären Definition einer **Affinity Domain** durch IHE folgend wird eine Affinity Domain immer von

einem EFA-Provider mit einem EFA-Peer bedient (wobei umgekehrt ein Provider auch mehrere Affinity Domains realisieren kann). Alle Einrichtungen der Affinity Domain nutzen bevorzugt die EFA-Dienste des die Affinity Domain technisch abbildenden EFA-Peers und sind mit dem entsprechenden Provider vertraglich verbunden. Die Zugehörigkeit einer Arztpraxis oder eines Krankenhauses wird somit alleine durch die vertragliche Bindung dieser Einrichtung an einen EFA-Provider bestimmt.

- EFA als Anwendung: Diametral zu der Affinity Domain ist zusätzlich jede an einer EFA teilnehmende Einrichtung auch einer oder mehreren **Versorgungsdomänen** zugeordnet. Hierbei handelt es sich um einen regionalen (ggf. nationalen) Zusammenschluss von Einrichtungen zur kooperativen und einheitlichen fachlichen Vorgaben folgenden Behandlung von bestimmten Patientengruppen; z.B. im Rahmen eines Traumanetzwerks oder eines Palliativnetzes.

Die nachfolgende Abbildung stellt exemplarisch über mehrere EFA-Provider realisierte Affinity Domains und Versorgungsdomänen (fachliche Netzwerke) dar. Die kleinen Kreise bezeichnen dabei jeweils einzelne (Partitionen von) Fallakten.



Die vorliegende EFAv2.0 Spezifikation definiert Vorgaben für die EFA als Plattform und damit für die Umsetzung einer EFA-konformen Affinity Domain. Vorgaben für die konkrete Umsetzung von EFA-Anwendungen innerhalb von Versorgungsdomänen - z.B. Festlegungen zu den Inhalten einer Fallakte - sind nicht Gegenstand dieser Spezifikation.

Krankenhäuser als EFA Provider

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Erid.01.01}

Ein Krankenhaus ist immer sehr stark regional verankert und spielt eine besondere Rolle in regionalen Versorgungsstrukturen. Die von der Politik immer wieder gerne ausgerufenen Gesundheitsregionen sind ohne Krankenhäuser nicht denkbar und genauso ist für ein Krankenhaus eine Teilnahme an neuen Versorgungsformen ohne funktionierende Gesundheitsregion nicht denkbar. Der Betrieb eines Krankenhauses ist damit ein Geschäft, das über die stationäre Behandlung von Patienten hinausgeht. Teil dieses Geschäfts ist das Aufsetzen zeitgemäßer Angebote für andere Akteure im regionalen Verbund, um für Zuweiser und Patienten attraktiv zu bleiben und neue Kundengruppen zu gewinnen bzw. bestehenden Kunden zusätzliche Angebote zu machen.

Aus dieser Motivation heraus übernehmen in vielen Netzwerken Krankenhäuser die Funktion des EFA-Providers. Hiermit übernimmt dieses Krankenhaus innerhalb seiner Affinity Domain zwei Rollen:

- als technischer Dienstleister der die Infrastruktur zur Anlage und Pflege von Fallakten bereitstellt
- als Gesundheitsdienstleister der am medizinischen Datenaustausch über die Fallakte teilnimmt

Eine logische Trennung der beiden Rollen MUSS zwingend vorgenommen werden und hat folgende Vorteile:

- Als Gesundheitsdienstleister nutzt der EFA Provider die gleichen Schnittstellen und Funktionen die auch für die anderen Teilnehmer bereitgestellt werden müssen
- Als technischer Dienstleister kann der EFA Provider seinen administrativen Pflichten nachkommen ohne datenschutzrechtlich bedenkliche umfängliche Zugriffsrechte auf medizinische Inhalte

Diese logische Trennung schliesst nicht aus, dass ein EFA Provider besondere Integrationsbedürfnisse hat. Diese sind aber sehr spezifisch und können praktisch nicht standardisiert werden.

Referenzen und Querverweise

- EFA-2.0-Spezifikation

Conceptual Perspective - Information Dimension

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Kontext, Anwendung, Ressource**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA als Instanz des GDD Referenzmodells

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {KeAk.01}`

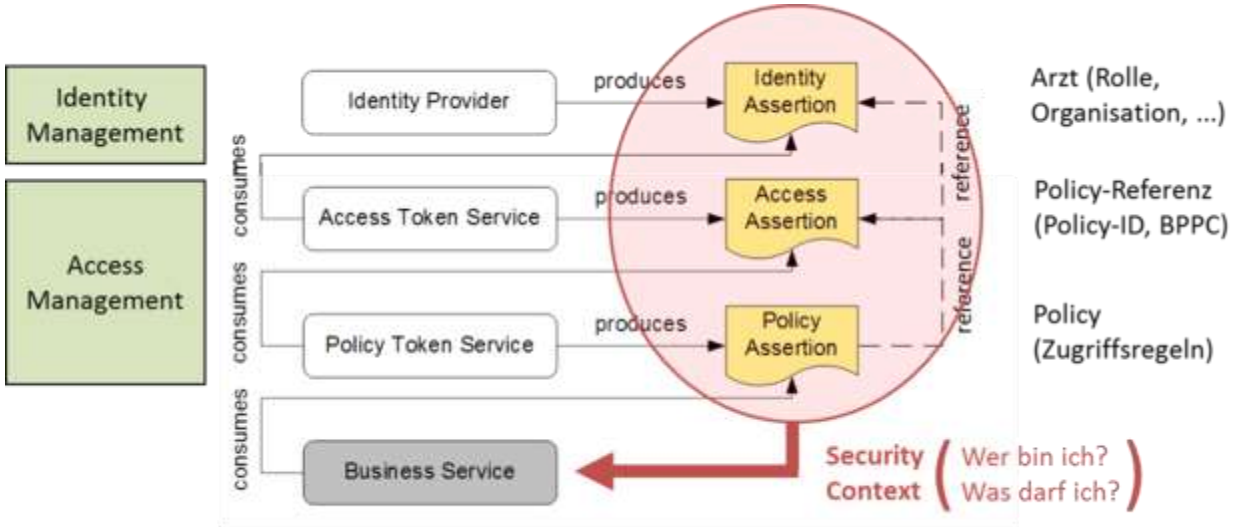
Die EFA ist ein Gesundheitsdatendienst (GDD) und damit eine Instanz des GDD-Referenzmodells. Dies bedeutet:

- im Mittelpunkt eines GDD steht die Vermittlung geschützter Ressourcen zwischen Leistungserbringern. Im Fall der EFA sind diese Ressourcen die einzelnen Fallakten, auf die berechtigte Leistungserbringer im Rahmen der Behandlung medizinischer Fälle zugreifen.
- die Vermittlung der Ressource wird durch eine Anwendung realisiert, die von einem oder mehreren GDD-Anbietern bereit gestellt wird. Im Fall der EFA bilden die EFA-2.0-konformen, über EFA-Peers realisierten Fachdienste die Anwendung "EFA" während die Rolle der GDD-Anbieter durch die EFA-Provider ausgefüllt wird.
- sämtlicher Datenaustausch findet innerhalb eines über alle Akteure gespannten Sicherheitskontextes statt. Im Fall der EFA bildet die Patienteneinwilligung die konzeptuelle Basis dieses gemeinsamen Kontextes. Die technische Umsetzung erfolgt durch zwischen den Akteuren ausgetauschte Sicherheitsnachweise.

In den nachfolgenden Abschnitten wird beschrieben, wie diese Vorgaben des GDD-Referenzmodells innerhalb des EFA-Informationsmodells konkret umgesetzt sind.

Kontext

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {KeAk.01.01}



Nach den Vorgaben des GDD-Referenzmodells sind sämtliche Operationen zur Verarbeitung der Ressource (d.h. der Fallakten und ihrer Daten) in einen Sicherheitskontext eingebettet, der potenziell alle beteiligten IT-Systeme umspannt. Konkret bedeutet dies, dass der Sicherheitskontext des Nutzers an seinem Arbeitsplatz in der Klinik auf Seiten der EFA-Dienste beim EFA-Provider so rekonstruiert werden kann, dass es für den Nutzer so aussieht, als ob würden die EFA-Dienste in seinem lokalen Sicherheitskontext auf seinem Arbeitsplatzsystem laufen (und umgekehrt: Für die EFA-Dienste ist es vollkommen egal wo der Nutzer sitzt, da die die Dienste immer in dem Sicherheitskontext laufen, in dem sich der Nutzer gerade befindet).

Um einen solchen Sicherheitskontext zu realisieren, werden alle für diesen Kontext relevanten Informationen zur Identität und zu den Berechtigungen des Nutzers in sog. Sicherheitsnachweisen (*Assertions*) gekapselt. Diese Nachweise enthalten verifizierbare, zuverlässige Aussagen darüber, wer der Nutzer ist und was er im Rahmen der Nutzung einer Ressource für Berechtigungen besitzt. Jedes IT-System im EFA-Verbund kann anhand der Sicherheitsnachweise den gleichen Sicherheitskontext aufbauen - unabhängig davon wo und in welchem Zuständigkeitsbereich das Identitäts- und Berechtigungsmanagement realisiert sind.

Für die konkreten Verfahren zur Vermittlung und Absicherung von Sicherheitsnachweisen gibt es verschiedene Paradigmen, die im wesentlichen davon abhängen, ob ein Sicherheitskontext bereits zu Beginn einer Anwendungsnutzung vollständig aufgebaut wird oder ob dieser Aufbau schrittweise erfolgt, wenn die einzelnen Nachweise benötigt werden (und dann ggf. auch nur auf den Systemen, die diese Nachweise auch wirklich benötigen). Im IHE White Paper "Access Control" werden z.B. die Strategien "Policy Push" (Client baut den vollständigen Kontext auf) "Policy Pull" (Aufbau des Kontextes erfolgt *on demand* beim Dienstanbieter) beschrieben, die auch beide von der EFA unterstützt werden.

EFA-Anwendung und EFA-Peers

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {KeAk.01.02}

Eine Anwendung im Sinne des GDD-Referenzmodells ist eine von einem Anbieter betriebene Instanz eines Dienstes, der definierten Vorgaben - insbesondere zur angebotenen Funktionalität - genügt. Anwendungen bedürfen einer Zulassung, die sich über verschiedene Ebenen - Konzeption/Spezifikation, Implementierung/Produkt, Betrieb/Einsatz - erstrecken kann.

- Jeder von einem EFA-Provider betriebene EFA-Peer ist eine solche Anwendung.
- Die Spezifikationen der EFA werden durch den EFA-Verein verantwortet. Dieser stellt die Konformität der Spezifikationen zu den regulativen Rahmenbedingungen in Deutschland sicher. Der EFA-Verein vergibt verschiedene Konformitätssiegel für den Spezifikationen entsprechende Produkte. Idealerweise setzen entsprechende Konformitätsprüfungen auf in IHE Connectathons erworbenen "conformace

statements" auf und stellen im Kern lediglich die richtige Umsetzung der in der EFA-Spezifikation festgelegten Einschränkungen und Erweiterungen auf den verschiedenen IHE-Profilen fest.
- Der Einsatz einer EFA in einem regionalen Gesundheitsnetz bedarf der Freigabe durch den zuständigen Landesdatenschutz. Dieser prüft insbesondere die vollständige Umsetzung des für alle EFA-Betreiber maßgeblichen EFA-Datenschutzkonzepts.

Anwendungen sind diskriminierungsfrei im Rahmen definierter Regeln nutzbar. Anwendungen eines GDD können in mehreren Instanzen von verschiedenen Anbietern aufgesetzt und zur Nutzung angeboten werden. Der Nutzer ist frei in der Wahl des Anbieters wobei jedoch je nach Art des GDD die Vorgaben zur Wahl eines Dienstleisters im Rahmen einer Auftragsdatenverarbeitung zu beachten sind.

- Die Spezifikationen der EFA können von jedem Anbieter umgesetzt werden. Jeder Anbieter, der die rechtlichen Vorgaben zum Schutz der verwalteten und ausgetauschten EFA-Daten nachweisbar einhält, kann am Markt als EFA-Provider agieren.
- EFA-Teilnehmer können im Rahmen ihrer Berechtigungen auf alle Fallakten und Fallaktendaten lesend zugreifen - unabhängig davon auf welchem EFA-Peer und von welchem EFA-Provider diese bereit gestellt werden.
- EFA-Teilnehmer können frei wählen, bei welchem Provider sie selber Fallakten anlegen bzw. die von ihnen in Fallakten eingestellten Daten verwaltet werden.

Ein EFA-Teilnehmer greift über den EFA-Provider auf das EFA-Netzwerk zu, mit dem er einen Vertrag über die Vorhaltung der selbst angelegten Fallakten und selbst eingestellten Daten geschlossen hat. Die Dienstadressen des von diesem Provider angebotenen EFA-Peer sind Bestandteil der statischen EFA-Konfiguration des Teilnehmers. EFA-Teilnehmer, die nicht an einen Provider gebunden sind, können nur lesend auf Fallakten zugreifen. Sie können als Einstiegspunkt in ein EFA-Netzwerk grundsätzlich jeden an dieses Netz angebundenen Peer nutzen, sofern dieser in der Lage ist die Authentizität des beim Nutzer aufgebauten Teils des Sicherheitskontextes (s.o.) zu prüfen. Die Dienstadressen von einem oder mehreren solcher EFA-Peers sind Bestandteil der statischen EFA-Konfiguration des Teilnehmers.

Ressourcen der EFA

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {KeAk.01.03}

Das EFA Geschäftsobjekt "Fallakte" bildet im Sinne des GDD-Referenzmodells die Ressource der EFA. Berechtigungen und Nutzungseinschränkungen sind ausschließlich an Objekte dieser Klasse gebunden und werden auf nachgeordnete Objekte (Partitionen, Datenobjekte) vererbt.

EFA-Ressourcen haben per se einen hohen Schutzbedarf, da Szenarien, die einen sehr hohen Schutzbedarf bedingen würden, explizit von der Umsetzung über eine EFA ausgeschlossen sind. Die hierzu definierten Maßnahmen sind im EFAv1.2-Datenschutzkonzept beschreiben.

Querverweise und Referenzen

- EFA-2.0-Spezifikation
- IHE White Paper "Access Control"
- Datenschutzkonzept der EFA Version 1.2

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Patienteneinwilligung zur EFA**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Patienteneinwilligung zur EFA

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Peen.01.01}`

Die elektronische Fallakte ist ein an § 291a SGB V angelehnter Gesundheitsdatendienst. Die EFA ist deshalb nicht durch die spezifische Erlaubnisvorschrift innerhalb der verpflichtenden §291a-Anwendungen befreit, die eine Datenverwendung *"soweit es zur Versorgung der Versicherten erforderlich ist"* [nach: § 291a (4) Satz 1 SGB V]., ohne eine vorherige spezifische Einwilligung des Patienten zulässig macht: Bei

Verarbeitung personenbezogener Daten gilt für die elektronische Fallakte das datenschutzrechtliche Prinzip "Verbot mit Erlaubnisvorbehalt". Demnach ist es nicht gestattet, personenbezogene Daten ohne vorherige Einholung einer Erlaubnis in Form einer Einwilligungserklärung des Betroffenen zu erheben. Für die an § 291a SGB V angelehnten Gesundheitsdatendienste fordert der Gesetzgeber explizit ein ausdrückliches Einverständnis (eine die Datenverarbeitung rechtfertigende Einwilligungserklärung) des Versicherten [§291a (5) Satz 1 SGB V, EU-DSRL].

Es besteht keine verpflichtende Notwendigkeit, der Nutzung der eFA zuzustimmen (Freiwilligkeit). Ein Patient kann jedoch auf Wunsch die EFA als Gesundheitsdatendient in Anspruch nehmen und durch eine *freiwillige*, *informierte* und *schriftliche* Einwilligungserklärung autorisieren.

Der Patient muss vor Abgabe der Einwilligungserklärung in geeigneter Weise über Funktion und Risiken der elektronischen Fallakte aufgeklärt werden. Da eine "informierte Einwilligung" der Patienten erforderlich ist, sollte diese Unterrichtung schriftlich erfolgen und muss zwingend die wichtigsten Eckpunkte der elektronischen Fallakte in allgemein verständlicher Form darlegen [§4a BDSG, §67b Abs. 2 SGB X, EU-DSRL Art. 7]. Die Einwilligung ist bis zur Einführung eines adäquaten elektronischen Verfahrens schriftlich festzuhalten und kann vom Patienten jederzeit widerrufen werden [nach §4a BDSG, §73 Abs. 1b SGB V].

Eine Patienteneinwilligung für eine elektronische Fallakte ist umfassend. Die am aktuellen Behandlungsprozess direkt beteiligten Leistungserbringer sind dabei im Sinne von technischen Positivberechtigungen zugriffsberechtigt. Zugriffsberechtigungen können an Personen oder Einrichtungen vergeben werden. Einrichtungen können, je nach aktuellem Behandlungskontext oder Zweckbindung, folgende Rechtseinheiten sein:

- ein bestimmter Arzt oder eine bestimmte Arztpraxis (bspw. Hausarztpraxis Dr. Peter Müller)
- eine bestimmte Arztrolle (bspw. Kardiologe) mit einer vom Patienten vorzunehmenden Instanziierung
- eine Gemeinschaftspraxis (bspw. Praxis Dr. Peter Müller + Dr. Sandra Müller)
- Fachbereiche oder Fachabteilung eines Klinikums (bspw. Kardiologen der Kardiologie im Klinikum XYZ)
- kombinierte, diagnosespezifische und spezialisierte Facharztrollen (bspw. Dermatologe + Onkologe) mit einer vom Patienten vorzunehmenden Instanziierung

Der Umstand einer Berechtigungsvergabe an eine Organisation(-seinheit) ist jedoch keinesfalls mit einer Pauschalberechtigung für sämtliches Personal einer Einrichtung zu verwechseln, sondern gestattet ausschließlich explizit und direkt Beteiligten den Zugriff nach einem vorab definierten und überprüften Berechtigungsmodell. Als Grundsatz ist hier zwingend von jedem EFA-Verbundmitglied gefordert, dass konkrete Zugriffsberechtigungen prinzipiell für die kleinstmöglichen Bereiche ausgestellt werden.

Als Verfahrens- und Fachverantwortlicher wird von den Teilnehmern eines EFA-Netzwerks ein Fallaktenmanager bestimmt. Der Fallaktenmanager muss in der Einwilligung als verfahrens- und fachverantwortliche Person benannt sein. Sofern der Fallaktenmanager seine operativen Aufgaben auf

einen Vertreter delegiert, muss auch diese Person oder Organisationseinheit in der Einwilligung benannt werden. Eine Änderung dieser Festlegungen durch den Patienten ist nicht möglich.

Die Einwilligungserklärung ist für alle Teilnehmer des EFA-Systems zumindest auf nationaler Ebene einheitlich zu gestalten. Dadurch vereinfacht sich eine umfassende datenschutzrechtliche Bewertung der Einwilligungserklärung, zugleich wird die Nutzerakzeptanz durch die einheitliche Darstellung gefördert. Im Bedarfsfall kann die Einwilligungserklärung im Verlauf der Behandlung auf Wunsch des Patienten auf weitere Leistungserbringer erweitert werden. Hierzu kann der Patient den Kreis der zugriffsberechtigten Leistungserbringer durch die Abgabe einer neuen, aktualisierten Einwilligungserklärung erweitern. Es existiert jedoch immer nur eine gültige Einwilligungserklärung. Der Patient ersetzt mit der Unterschrift der neuen Erklärung, die alle nun berechtigten Personen und Einrichtungen nennt, die vorherige Einwilligung.

Eine Rücknahme der Einwilligungserklärung durch den Patienten ist jederzeit und freimütig möglich. Eine Rücknahme entzieht der elektronischen Fallakte die rechtliche Existenzberechtigung. Diese ist dann sofort vor externen Zugriffen zu schützen und hat nach dem im Lebenszyklus der Fallakte beschriebenen Verfahren zu verfallen. Der Patient kann die Rücknahme seiner Einwilligungserklärung wahlfrei bei einer beliebigen zugriffsberechtigten Stelle seiner Wahl oder in der bisherigen Einwilligungserklärung benannten verfahrensverantwortlichen Stelle einfordern.

Die Historie der Einwilligungen wird in der Fallakte abgelegt. Falls die Einwilligungen nicht elektronisch vorliegen, wird ein Verweis auf den Archivierungsort angegeben.

Querverweise und Referenzen

- EFA-2.0-Spezifikation
- Datenschutzkonzept der EFA Version 1.2
- §291a SGB V
- Bundesdatenschutzgesetz (BDSG)
- Richtlinie 95/46/EG
- §67b Abs. 2 SGB X

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Geschäftsobjekte**.*

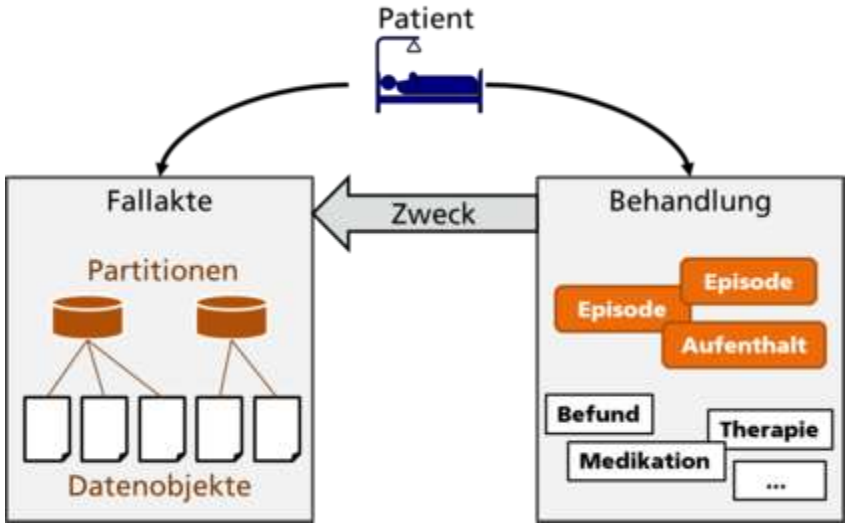
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Hierarchisches Informationsmodell der EFA

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01}`

Die eFA besitzt ein hierarchisches, vierstufiges Informationsmodell mit den Klassen „Patient“, „Fallakte“, „Partition“ und „medizinisches Datenobjekt“. Zwischen den Hierarchieebenen besteht jeweils ein 1:m Verhältnis, d. h. einem Patient können beliebig viele Fallakten zugeordnet sein, eine Fallakte kann beliebig viele Partitionen (z. B. für einzelne Klinikaufenthalte) subsumieren und jeder Partition können beliebig viele Dokumente zugeordnet sein. Die einzelnen Klassen des EFA Informationsmodells bilden damit die Modularisierung der Organisation eines "medizinischen Falls" ab.



Da der in der eFA Version 1.2 für Partitionen genutzte Begriff des "Ordners" auch für Strukturierungselemente in für den Nutzer generierten Sichten genutzt wurde und jetzt zusätzlich auch noch im IHE Cookbook mit dem technischen Konstrukt des XDS-Ordners gleichgesetzt ist, wird in der EFA 2.0 Spezifikation zur Wiederherstellung begrifflicher Klarheiten wieder auf den in der ersten EFA Spezifikation benutzten und konzeptionell passendsten Begriff "Partition" zurückgegriffen. Für diese Spezifikation gilt damit grundsätzlich:

- Eine Partition bezeichnet einen Speicherbereich, in dem Dokumente bei einem EFA-Provider verwaltet werden. Die Semantik dieses Speicherbereich bestimmt derjenige, der diesen anlegt und darin von ihm verantwortete Dokumente einstellt. Üblicherweise wird man versuchen, eine Korrespondenz zwischen einer Partition und einer Behandlungsepisode herzustellen. Partitionen sind damit "physikalische" Objekte der EFA.
- Ein Ordner bezeichnet ein Strukturierungselement in für den Nutzer generierten Sichten auf eine Fallakte. Ob diese Strukturierung anhand von Partitionszugehörigkeiten oder Metadaten der in einer Fallakte zusammengefassten Dokumente erfolgt, ist in der EFA-Spezifikation nicht reglementiert. Ordner sind damit rein "logische" Konstrukte für die Visualisierung von Fallakten.

Klasse *Patient*

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01.01}

Jede EFA ist eindeutig einem Patienten zugeordnet und verfolgt einen klar benannten Zweck, z.B. die Unterstützung der Behandlung einer bestimmten Erkrankung des Patienten. Die EFA-Klasse "Patient" ist in der IHE-ACS-Domäne *patient* angesiedelt und bindet alle zur Identifikation des Patienten erforderlichen Informationen sowie die Einwilligungserklärung(en) des Patienten zur Führung einer Fallakte zu einem definierten Zweck.

Klasse *Fallakte (Medizinischer Fall)*

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01.02}

Eine Fallakte bildet einen konkreten Behandlungskontext wie z.B. einer konkrete Erkrankung oder einen bestimmten Versorgungsvertrag zwischen dem Patienten und den behandelnden Einrichtungen auf eine Zweckbindung ab. Der der Fallakte zugrunde liegende medizinische Fall determiniert, welche Arten von Dokumenten über eine Fallakte ausgetauscht werden können. Zusätzlich können in strukturierten Versorgungskontexten ggf. bereits aus dem medizinischen Fall auch Einschränkungen bezüglich der berechtigten EFA-Teilnehmer abgeleitet werden.

Einem Patienten können mehrere Fallakten mit unterschiedlichen Zweckbindungen zugeordnet sein, zu einer konkreten Zweckbindung kann jedoch immer nur eine Fallakte bestehen. Dieses spiegelt die Motivation der Fallakte wider, dass diese den effizienten Austausch von Informationen zwischen allen Personen unterstützen soll, die an der den Zweck abbildenden Behandlung beteiligt sind. Zwei Fallakten zum gleichen Zweck aber mit unterschiedlichen Teilnehmern und Inhalten würden diesem zuwider laufen, da in diesem Fall eben nicht allen Teilnehmern alle fall-relevanten Informationen zur Verfügung stehen würden. Diesem spricht nicht entgegen, dass es z.B. zur Einholung einer Zweitmeinung zwei Fallakten mit inhaltlichen Überschneidungen geben kann; in diesem Fall wäre jedoch eine Akte zum Zweck der Behandlung angelegt und die zweite zum Zweck der Einholung einer Zweitmeinung.

Die Klasse "Fallakte" verbindet die IHE-ACS-Domänen *resource* und *application* und spiegelt damit wider, dass eine Fallakte sowohl Plattform als auch Anwendung ist:

- das generische Konstrukt einer zweckgebundenen Akte ist eine *resource* im Sinne der gleichnamigen IHE-ACS-Domäne.
- eine standardisierte, diagnose-spezifische Ausprägung einer Fallakte (z.B. eine Herz-Akte) ist zusätzlich eine Anwendung (*application*) im Sinne des IHE-ACS-Domänenmodells, da in diesem Fall eine vordefinierte Nutzungssemantik besteht, aus der heraus sich spezifische Anforderungen und Einschränkungen an den Zugang zu der *resource* der Fallakte und deren Inhalte ableiten.

Die hier beschriebene EFA-2.0-Semantik weicht von der Semantik der EFA 1.2 ab, in der mehrere Akten eines Patienten mit der gleichen Zweckbindung möglich waren. Diese "alte" Semantik erlaubte zwar ein flexibleres Berechtigungsmanagement, hatte jedoch zur Folge, dass immer dann implizit parallele Akten aufgebaut wurden, wenn eine Einrichtung in eine Behandlung neu eingebunden wurde und bislang nicht auf eine bereits existierende Akte berechtigt war. In diesem Fall würde aus der Patienteneinwilligung zur EFA heraus von dieser Einrichtung eine neue Akte aufgesetzt, was potenziell jedoch für keinen der Teilnehmer sichtbar wäre. Die "neue" Semantik hat hingegen das fach-semantisch schlüssigere Verhalten, dass in einem solchen Szenario die neue Akte automatisch Bestandteil der bereits zum gleichen Zweck existierenden Akte wird. Will man dennoch explizit zwei parallele Akten im Kontext des gleichen medizinischen Falls (z.B. zur Einholung einer Zweitmeinung) so müssen beide Akten explizit mit unterschiedlichen Zweckbindungen klassifiziert werden.

Verteilung von Fallakten über mehrere EFA-Provider

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01.02.01}

Die hier beschriebene Semantik ist jedoch rechtlich nur innerhalb eines EFA-Providers abbildbar, da ansonsten zwischen Providern abgefragt werden müsste, ob ggf. bei einem anderen Provider schon eine Fallakte zum selben Zweck besteht. Eine solche Abfrage ist durch die Einwilligung des Patienten nicht abgedeckt, da es unmöglich ist, in der Einwilligung alle Provider zu benennen, die angefragt werden. Daher ist eine solche Abfrage nicht zulässig.

Um die konsistente Semantik der engen Korrespondenz von Zweck und Fallakte aufrecht zu erhalten, ohne die Essentials der EFA-Sicherheit zu unterlaufen, wird folgendes Vorgehen für verteilte Fallakten definiert:

- Bei Anlage einer neuen Fallakte bei einem EFA-Provider prüft dieser Provider, ob bereits für diesen Patienten eine Fallakte zum benannten Zweck angelegt ist. Ist dies der Fall, wird die neue Akte der bestehenden Akte als Partition hinzugefügt, sofern dies durch die beiden Einwilligungen abgedeckt ist.
- Eine neue Fallakte wird beim Provider nur angelegt, wenn nicht bereits eine Akte des Patienten zum selben Zweck bei diesem Provider existiert. Eine Anfrage, ob eine solche Akte bei einem anderen Provider existiert, erfolgt nicht.
- In der Konsequenz resultiert dies in zwei Akten bei zwei Providern, die zwar den selben Zweck erfüllen sollen, denen aber unterschiedliche Einwilligungserklärungen zugrunde liegen und für die entsprechend auch unterschiedliche Teilnehmer berechtigt sein können. Dieses ist im Einklang mit den Essentials der EFA-Sicherheit, da hierdurch jeder Provider in der Lage ist, "seine" Einwilligung durchzusetzen. Um jedoch das essentielle Grundkonzept der EFA - nur eine Fallakte pro Zweck - durchzusetzen, muss in einem solchen Szenario eine Zusammenführung der Akten und Einwilligungen erfolgen, da ansonsten keine der beiden "Halb-Akten" seinen medizinischen Mehrwert entfalten kann.

- Um so verteilte, parallel existierende Akten zusammenzuführen, bedarf es der Einwilligung des Patienten, die dieser gegenüber einem Arzt geben muss, der Zugriff auf beide Akten hat (ggf. muss durch eine Änderung der Einwilligung zu einer der Akten dieser Zustand zunächst hergestellt werden). In der Einwilligung sind die zusammenzuführenden Akten sowie die Teilnehmer der so neu entstehenden integrierten Akte zu benennen. Die Inhalte der Einwilligungserklärung müssen an alle beteiligten Provider übermittelt werden ersetzen die jeweils bestehenden Einwilligungen.
- Die betroffenen Provider stellen eine geeignete Verknüpfung zwischen den verteilt vorgehaltenen Teilen der Fallakte her, die es den berechtigten Nutzer ermöglicht, alle in der Akte enthaltenen Daten zu sehen und auf diese zuzugreifen.

Klasse *Partition*

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01.03}

Kliniken und Ärzte nutzen jeweils spezifische Mechanismen zur internen Zusammenführung von medizinischen Daten, z.B. Abrechnungsfälle, Quartale oder Patientenkontakte. Insbesondere in Krankenhäusern mit einer weitgehend automatisierten Steuerung von Datenflüssen kann die Registrierung von Dokumenten an einer EFA vereinfacht werden, wenn sich ein solcher Strukturierungsmechanismus 1:1 auf ein Konstrukt des EFA-Informationsmodells abbilden lässt. In einem solchen Fall können intern freigegebene Dokumente bei ihrer Zuweisung zu einem internen Strukturierungsmechanismus automatisiert an dem korrespondierenden EFA-Konstrukt registriert und damit in die übergeordnete Fallakte eingestellt werden.

Diese skizzierte Rolle übernimmt in der EFA das Konstrukt der Partition. In Analogie zu dem gleichnamigen Konzept des UNIX-Dateisystems ist eine Partition ein eigenständiger Speicherbereich, der einen Teil einer gesamten Datenmenge vorhält aber auch autonom existieren kann.

Die konkrete Semantik einer Partition ist bei der EFA weitgehend frei definierbar, wodurch sie an beliebige bestehende Strukturierungsmechanismen gebunden werden kann. Somit kann eine Fallakte im einfachsten Szenario aus nur einer einzigen Partition bestehen, in die alle EFA-relevanten Daten eingestellt werden. In komplexeren Szenarien können jedoch in einer Fallakte Partitionen für einzelne Klinikaufenthalte und einzelne teilnehmende niedergelassene Ärzte angelegt werden, um eine IT-gesteuerte Filterung und Bereitstellung von Dokumenten aus diesen Einrichtungen zu unterstützen. Die gegebenen Freiheitsgrade erlauben es aber z.B. auch einem niedergelassenen Radiologen eine Partition in einer EFA anzulegen und diese mit einer internen Auftragsnummer zu verknüpfen. Alle Dokumente, die im Rahmen des Auftrags erstellt werden, können so automatisiert der richtigen Fallakte zugeordnet und an dieser registriert werden.

Da Partitionen lediglich ein Konstrukt zur Vereinfachung des Einstellens von Daten in eine Fallakte sind, sind sie auch üblicherweise dem Nutzer gegenüber verborgen.

Die Klasse "Partition" bildet im IHE-ACS-Modell eine Ressource, d.h. sie trägt weder eine Anwendungssemantik noch eigene Berechtigungen. Beides wird von der logisch übergeordneten Fallakte geerbt. Technisch gesehen können Partitionen auch ohne Fallakte existieren, aufgrund der fehlenden Semantik und Teilnehmer-Autorisierungen sind sie dann jedoch nicht als Fallakte nutzbar.

Klasse *Datenobjekt*

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eehä.01.04}`

Datenobjekte bilden die Blätter des EFA-Informationsmodells. Datenobjekte sind atomar und jeweils eindeutig einem Patienten zugeordnet. Jedes Datenobjekt ist mindestens einer Partition zugeordnet. Aktuell werden von der EFA ausschließlich Dokumente als Datenobjekte unterstützt.

Datenobjekte können zueinander in Beziehung stehen. Diese Beziehungen werden explizit festgelegt und sind für EFA-Teilnehmer sichtbar. Die folgenden Beziehungen zwischen Datenobjekten werden von der EFA v2.0 unterstützt:

Ergänzen eines Dokuments
: Ein Dokument stellt eine Ergänzung eines anderen Dokuments dar (z.B. Befund zum Bild).

Ersetzen/Aktualisieren eines Dokuments
: Ein Dokument ersetzt ein benanntes anderes Dokument. Das ersetzte Dokument wird (einschließlich seiner Ergänzungen/Anhänge) invalidiert und beim Abruf von Dokumenten aus einer Fallakte nur für bestimmte Rolleninhaber (z.B. Fallaktenmanager) bereitgestellt. Für alle anderen Teilnehmer ist nur noch das neue Dokument sichtbar. Dieses enthält jedoch einen Verweis auf das ersetzte Dokument.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Lebenszyklus einer Fallakte**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Lebenszyklus einer Fallakte

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eune.01}`

Die elektronische Fallakte dokumentiert einen bestimmten Krankheitsfall. Ist der Patient von dieser Krankheit geheilt oder verstorben, verfällt auch die dazugehörige Fallakte. Diese wird dann vor externen Zugriffen geschützt und deren Inhalte werden gemäß den aktuellen gesetzlichen Bestimmungen archiviert.

Nachdem die eFA vor externen Zugriffen geschützt worden ist, wird die gesperrte Fallakte noch sechs Monate im System vorgehalten (Grace-Periode). In dieser Zeit sind keine Regelzugriffe auf die Fallakte möglich. Diese Grace- Periode dient einzig dem Zweck, dass, sollte der Patient wider Erwarten im gleichen Fall weitere Behandlungen benötigen, der Arzt in diesem Fall die entsprechende eFA durch ein gesondertes Verfahren auf explizite Aufforderung wieder aktivieren kann.

Zustand der elektronischen Fallakte	Beschreibung
Open / Offen	Die Fallakte ist korrekt eingerichtet und kann im täglichen Dienstbetrieb verwendet werden.
Suspended / Gesperrt	Sollte die Behandlung eines Patienten abgeschlossen sein, wird die entsprechende Fallakte zum Behandlungsfall automatisch gesperrt. Beachtenswert ist hierbei, dass eine Behandlung auch mit dem Tod des Patienten enden kann und somit keine weitere Zweckbindung zur Offenhaltung der Fallakte existiert. Eine Fallakte wird weiterhin gesperrt, wenn

	ihre maximale Gültigkeitsdauer überschritten wurde oder sie aus anderen Gründen vor externen Zugriffen geschützt werden muss. Im gesperrten Zustand können lediglich der Case Record Manager und Personen mit datenschutzrechtlichen Kontrollaufgaben über ein gesondertes Verfahren auf die Fallakte zugreifen. Eine Fallakte darf maximal sechs Monate in diesem Zustand verweilen (Grace-Periode).
Retired / Verfallen	Die Fallakte hat die Grace-Periode überschritten oder wurde vom Patienten durch Entzug der Einwilligungserklärung explizit entwertet. Eine verfallene Fallakte ist zeitnah in den Zustand „archiviert“ zu überführen. Auf eine verfallene eFA ist kein Zugriff mehr möglich.
Archived / Langzeitarchiviert	Die Referenzen und Zugriffsrechte/-protokolle der spezifischen eFA sind in einem revisionssicheren Archiv gesichert. Nach erfolgreicher Archivierung ist die verfallene Akte sofort und vollständig zu löschen. Die Archivierungszeit ist institutionsspezifisch festzulegen, beträgt aber mindestens zehn Jahre. Das Risikomanagement der protokollierenden Institution hat hierbei die Aufgabe, die institutionsspezifischen Archivierungsfristen festzulegen. Die Frage, wer wann auf welche Informationen der eFA zugegriffen hat, kann in einem potenziellen Haftungsprozess unter dem Aspekt relevant werden, wer wann von welcher Information Kenntnis hatte bzw. hätte Kenntnis haben müssen bzw. können. Somit bewegen sich die Speicherfristen innerhalb der 30-jährigen Verjährungsfristen für Schadensersatzansprüche, die für die Verletzung von Leib, Leben und körperlicher Unversehrtheit gelten.

Mit dem Verfall einer Akte verfällt auch deren Einwilligungserklärung. Eine zuvor erteilte Einwilligung für bestimmten Fallakte kann nicht auf eine eventuell später zu erstellende Fallakte mit anderer Diagnose übertragen werden.

Sollte ein Patient seine Einwilligungserklärung zu einer Fallakte widerrufen, so endet der Lebenszyklus der Akte ebenso und diese verfällt nach dem oben beschriebenen Muster. Dies findet automatisch statt, der Patient muss den beschriebenen Verfall der Fallakte nicht explizit einfordern.

Zusätzlich ist jede Fallakte beim Eröffnen mit einem Verfallsdatum versehen, welches sich prinzipiell diagnosespezifisch an der Fünf-Jahres-Überlebensrate anlehnt. Sollte dieses Datum erreicht sein, verfällt die Fallakte ebenfalls, es sei denn, der betreffende Patient willigt einer Weiternutzung durch Abgabe einer neuen Einwilligungserklärung ausdrücklich ein. Die Fünf-Jahres-Überlebensrate dient hierbei als Mittel, um eine aus medizinischer Sicht differenzierte maximale Gültigkeitsdauer einer bestimmten Diagnose festzulegen. Abhängig vom Zweck der Fallakte kann jedoch auch eine deutlich kürzere Gültigkeitsdauer festgelegt werden (z.B. bei Anlage einer Fallakte für das Einholen einer Zweitmeinung).

Gesondert wird nochmals darauf hingewiesen, dass die elektronische Fallakte lediglich eine virtuelle Fallakte darstellt, demnach lediglich eine temporäre Zusammenführung aus bereits bestehenden, anderweitig gespeicherten Dokumenten und keine Primärdokumentation repräsentiert. Daraus resultiert, dass im Falle einer Löschung nur die Wurzel der elektronischen Fallakte entfernt wird, die konkreten Dokumente jedoch an ihrem

konkreten Ursprungsort bestehen und gespeichert bleiben. Eine explizite Löschung dieser Dokumente im Primärsystem vor der in §10 Abs. 3 MBO/Ärzte geregelten Aufbewahrungsfrist, in der Regel mindestens zehn Jahre, ist nicht einforderbar.

Querverweise und Referenzen

- EFA-2.0-Spezifikation
- Datenschutzkonzept der EFA Version 1.2

Conceptual Perspective - Computational Dimension

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster der EFA

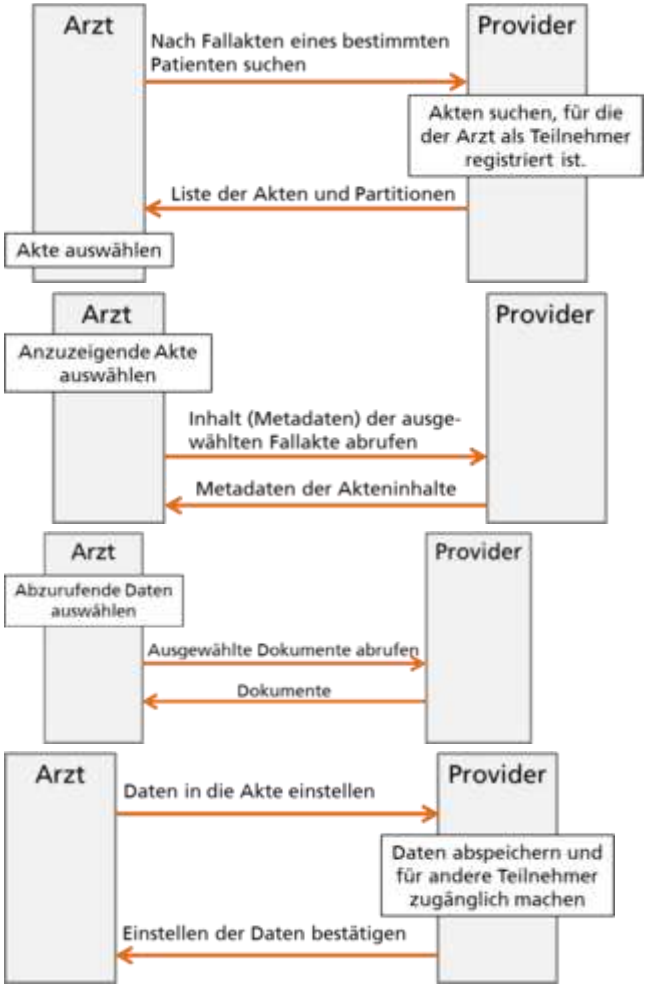
`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Irti.01}`

Arbeiten mit Fallakten

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Irti.01.01}`

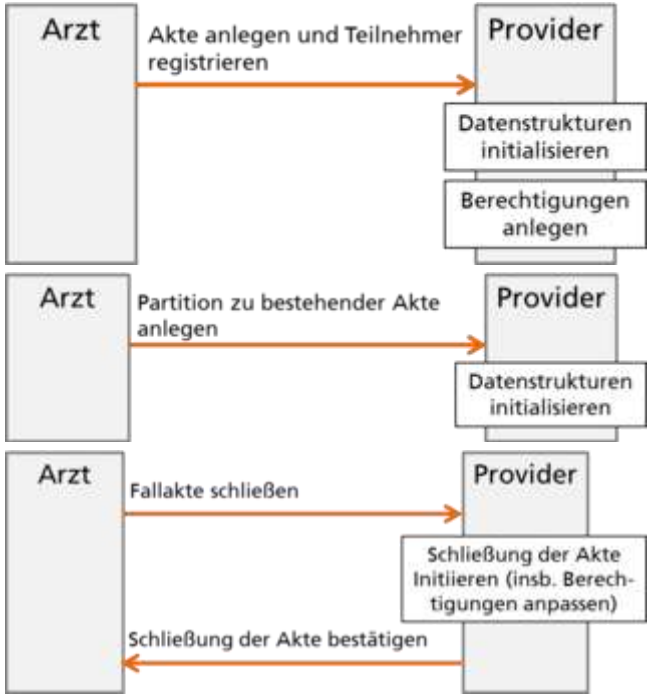
Muster	Kurzbeschreibung	Default-Umsetzung

Auffinden der Fallakten eines Patienten	Das Muster beschreibt wir ein Arzt bei einem EFA-Provider nach Fallakten eines Patienten sucht und eine Akte für die weitere Nutzung auswählt.
Browsing über eine Akte	Das Muster beschreibt, wie ein berechtigter Teilnehmer Informationen zu den in einer Akte verwalteten Dokumenten abrufen kann, so dass diese anschließend in geeigneter Weise in seinem Primärsystem aufbereiten werden können.
Abruf von Datenobjekten	Das Muster beschreibt, wie ausgewählte Dokumente von einem Arzt aus der Fallakte in ein Primärsystem übernommen werden.
Einstellen von Datenobjekten	Das Muster beschreibt, wie berechtigte Teilnehmer in einem Primärsystem erfasste Daten in eine Fallakte einspielen können. Die Daten werden hierdurch für alle anderen berechtigten Teilnehmer der Fallakte zugänglich.
Invalidieren von Datenobjekten	Das Muster beschreibt, wie ein zuvor an einer Fallakte registriertes Datenobjekt invalidiert werden kann, so dass alle anderen Teilnehmer davon in Kenntnis gesetzt sind, dass dieses Objekt nicht weiter verwendet werden soll.



Verwaltung von Fallakten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Irti.01.02}

Muster	Kurzbeschreibung	Default-Umsetzung
Anlegen einer Fallakte	Das Muster beschreibt die Anlage einer Fallakte auf Basis einer Einwilligung des betroffenen Patienten. Varianten des Musters beschrieben, wie zum selben Zweck angelegte Akten integriert werden.	
Anlegen und Registrieren einer Partition	Das Muster beschriebt, wie zu einer bestehenden Fallakte weitere Partitionen - z.B. zur Zusammenfassung der im Rahmen eines stationären Aufenthalts erhobenen Daten - angelegt werden können.	
Schließen einer Fallakte	Das Muster beschriebt das explizite Schließen einer Fallakte, z.B. aufgrund der Rücknahme der Einwilligung durch den Patienten.	
Ändern/Aktualisieren einer Einwilligung	Das Muster beschreibt die Anpassung des Teilnehmerkreises einer EFA aufgrund einer veränderten Behandlungssituation oder einer Änderung der Einwilligung des Patienten. Varianten dieses Musters erlauben auch die Konkretisierung des Zwecks einer EFA sowie die Anpassung des Gültigkeitszeitraums.	
Autorisierung eines weiteren Teilnehmers	Das Muster beschreibt, wie der Patient ergänzend zur bestehenden Einwilligung weitere Ärzte bzw. Einrichtungen zur Teilnahme an einer	

	EFA berechtigen kann (z.B. durch Nutzung eines Offline-Tokens). Varianten dieses Musters erlauben auch die Rücknahme einer solchen Einzelautorisierung.
Zusammenführen von Fallakten	Das Muster beschreibt die Zusammenführung von auf zwei EFA-Peers zum selben Zweck angelegten Akten und stellt eine Ergänzung des Musters "Anlegen einer Fallakte" dar, das nur für Peer-to-Peer vernetzte EFA-Provider relevant ist.

Referenzen und Querverweise

- EFA-2.0-Spezifikation
- Interaktionsmuster: Auffinden der Fallakten eines Patienten
- Interaktionsmuster: Browsing über eine Akte
- Interaktionsmuster: Abruf von Datenobjekten
- Interaktionsmuster: Einstellen von Datenobjekten
- Interaktionsmuster: Invalidieren von Datenobjekten
- Interaktionsmuster: Anlegen einer Fallakte
- Interaktionsmuster: Anlegen und Registrieren einer Partition
- Interaktionsmuster: Schließen einer Fallakte
- Interaktionsmuster: Anpassen des Teilnehmerkreises
- Interaktionsmuster: Zusammenführen von Fallakten (P2P)

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Anlegen einer EFA**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

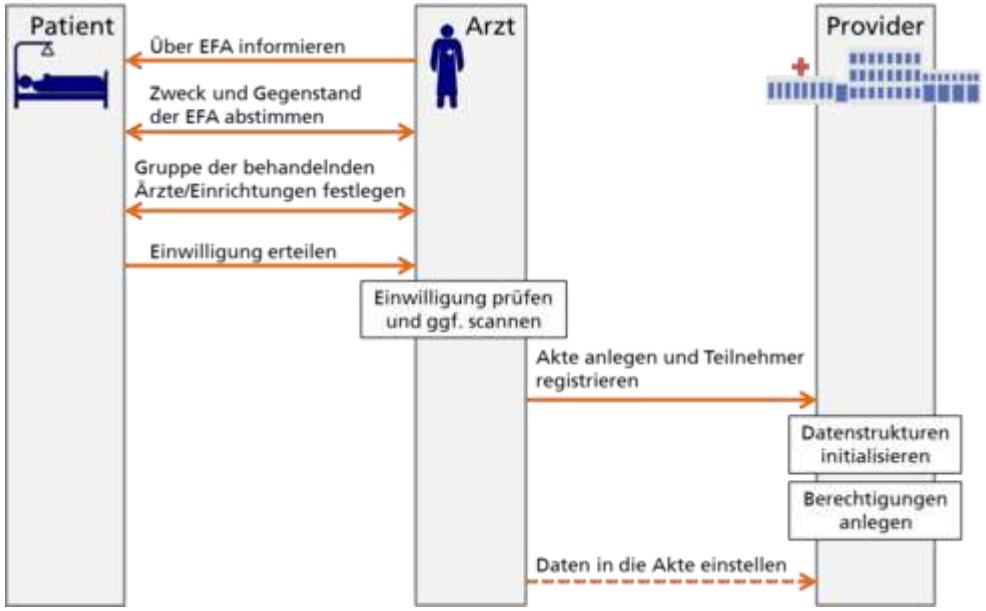
Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht.

Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster zum Anlegen einer EFA

Anwendungsszenario: Anlegen einer Fallakte

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngea.01.01}`



In kooperativen Behandlungsszenarien mit einem Erfordernis eines effizienten Datenaustauschs zwischen den behandelnden Einrichtungen kann eine elektronische Fallakte angelegt werden. Die Anlage einer Fallakte erfolgt in Abstimmung zwischen Patienten und behandelndem Arzt und folgt typischerweise dem folgenden Ablauf:

1. Aufgrund der Diagnose des Patienten bzw. des eingeschlagenen Behandlungspfads wird in einem regionalen Verbund die Nutzung einer Fallakte empfohlen. Sofern noch keine Fallakte für den Patienten besteht, klärt einer der behandelnden Ärzte den Patienten über die Vorteile und Risiken der Nutzung einer Fallakte auf und erklärt, welche Daten zwischen welchen Akteuren über die Fallakte ausgetauscht werden. Insbesondere wird der Patient darauf hingewiesen, dass die Anlage der Fallakte ein freiwilliges Angebot ist und dass er jederzeit die Schließung der Akte verlangen kann ohne dass dieses einen Abbruch der Behandlung zur Folge hätte.
2. Zwischen Arzt und Patient werden im Rahmen der innerhalb des regionalen Verbunds vorgegebenen Konfigurationsspielräume die Modalitäten der Nutzung einer Fallakte zur Behandlungsunterstützung abgestimmt. Insbesondere wird der Zweck der Fallaktennutzung möglichst konkret erfasst und es wird ein Datum festgelegt, zu dem die Fallakte ausläuft (sofern sie nicht vorher verlängert wurde).
3. Der Arzt legt dem Patienten dar, welche Fachdisziplinen und Einrichtungen idealerweise in die Behandlung und damit auch in die Teilnahme an der EFA eingebunden sein sollten. Arzt und Patient verständigen sich auf einen initialen Kreis von behandelnden Ärzten/Einrichtungen.
4. Die getroffenen Vereinbarungen werden in einer Einwilligungserklärung festgehalten. Die Einwilligung wird vom Patienten unterschrieben und an den Arzt übergeben.
5. Sofern die Einwilligung nicht bereits aus einem elektronischen Formular erzeugt worden war, erfasst der Arzt die Daten der Einwilligung in einem elektronischen Formular. Er bestätigt die Richtigkeit der Angaben, die Datenschutzkonformität des Ablaufs der Einwilligungserteilung und das Vorhandensein einer vom Patienten unterschriebenen Kopie.
6. Der Arzt übermittelt die für die Anlage der Akte erforderlichen Informationen einschließlich einer Kopie der Einwilligung an einen EFA-Provider.
7. Der EFA-Provider legt in einem Aktensystem eine Fallakte gemäß den Vorgaben des Arztes an. Die Berechtigungen zum Zugriff auf die Akte werden gemäß den Vorgaben der Einwilligungserklärung aufgesetzt.
8. Der Arzt kann nun die ihm bereits vorliegenden, EFA-relevanten Dokumente in die Akte einstellen.

Varianten des Anwendungsszenarios

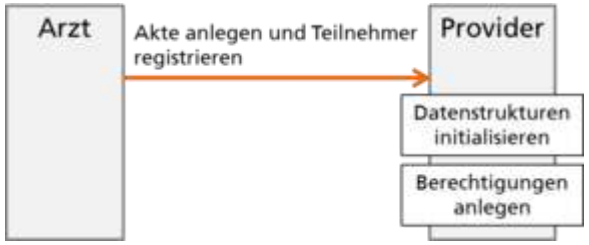
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngea.01.02}

Aktuell sind keine Varianten definiert

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngea.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

	Vorbedingungen:
	• Die Einwilligung des Patienten zur Anlage und Nutzung einer Fallakte liegt vor.
	• Die an der Behandlung teilnehmenden Ärzte und Einrichtungen sind identifiziert.
	• Der Patient ist eindeutig identifiziert und authentisiert (ggf. organisatorisch).
	
	Funktionalität:
	• Eine neue Fallakte wird für einen Patienten zu einem definierten Zweck angelegt.
	• Die an der Behandlung teilnehmenden Ärzte und Einrichtungen werden als EFA-Teilnehmer registriert und autorisiert.
	
	Nachbedingungen:
	• Eine neue Fallakte ist angelegt und kann von den EFA-Teilnehmern genutzt werden.
	• Sofern elektronisch verfügbar, ist die Einwilligung als Dokument aus der Akte abrufbar.
	  ○ Die Einwilligungserklärung und
		Muster **Fallakte anlegen**
		• Bereit gestellte Informationen:
		  ○ Patient (identifizierende Daten)
		  ○ Zweck der Akte
		  ○ Teilnehmer der Akte (identifizierende Daten, Rollen bzw. Autorisierungen)
		  ○ Gültigkeit der Akte
		  ○ elektronisches Einwilligungsdokument oder Bestätigung des Arztes, dass eine solche Einwilligung vorliegt
		• Erforderliche Konfigurationsdaten:
		  ○ EFA Provider

Stammdaten sind ggf. auch zur korrekten Identifikation des Patienten zu nutzen.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Akte auf welcher Basis und in welcher Konfiguration angelegt hat.

Definition der Interaktionsmuster

Interaktionsmuster: Fallakte anlegen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngea.01.04.01}

Motivation	Anlegen einer neuen Fallakte zu einem definierten Zweck.
Akteure und Rollen	Leistungserbringer (LE) Die Anlage einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Basis der von Leistungserbringer angeforderten Aktenkonfiguration ist üblicherweise die informierte, schriftliche Einwilligung des Betroffenen. Wenn keine solche Einwilligung vorliegt, kann eine Akte zwar über dieses Interaktionsmuster angelegt werden, es ist jedoch keine Nutzung der Akte und insbesondere kein Zugriff auf die in der Akte registrierten Daten möglich. EFA-Provider Der EFA-Provider legt die angeforderte Akte gemäß der vom LE vorgegebenen Konfiguration an. Der EFA-Provider stellt sicher, dass Aktenzugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen zugewiesenen Rollen erfolgen können.
Interaktion	Arzt --> (Patientenidentifikation, Zweck der Akte, [Gültigkeit], [EFA-Teilnehmer], [Einwilligungsformular]) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die Anlage einer EFA sind gegeben. Insbesondere ist der Zweck der Akte benennbar.

- Die organisatorischen und rechtlichen Voraussetzungen für die Anlage einer EFA sind gegeben:
  - Der die Akte anlegende LE hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-Datenschutzkonzept definierten Vorgaben entspricht. Sofern es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt werden.
  - Es existiert eine Festlegung zur Besetzung der Rolle des Fallaktenmanagers für die anzulegende Akte.
- Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren.
- Der LE hat den Patienten sicher identifiziert und von diesem Daten erfasst, die auch für andere EFA-Teilnehmer eine eindeutige Identifizierung des Patienten ermöglichen.

Ablauf

1. Der LE übermittelt die zur Anlage der Fallakte erforderlichen Informationen an den EFA-Provider.
2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit.
3. Der EFA-Provider legt eine Fallakte in der gewünschten Konfiguration an.
4. Der EFA-Provider setzt die Berechtigungen der Fallakte analog zu den Rollen der benannten EFA-Teilnehmer. Sofern keine Einwilligung des Patienten vorliegt oder keine EFA-Teilnehmer benannt wurden, wird lediglich ein Schreibrecht für die Organisation des LE vergeben.
5. Sofern im Rahmen der EFA-Anlage eine elektronische Kopie des Einwilligungsformulars übermittelt wurde, wird dieses in der neu aufgesetzten Fallakte abgelegt.

Eingangsinformationen

Patientenidentifikation

Zur Anlage einer Fallakte müssen Angaben zum Patienten übergeben werden, die auch anderen EFA-Teilnehmern die (1) Identifikation des Patienten, (2) die Prüfung der Zuordnung der Akte zum Patienten und (3)das Auffinden der Fallakte anhand von Identitätsinformationen zum Patienten ermöglichen.

Zweck

Der Zweck der Anlage und Nutzung der Fallakte muss möglichst konkret angegeben werden.

Gültigkeit (optional)

Für die anzulegende Fallakte kann eine maximale Gültigkeitsdauer angegeben werden. Diese darf einen beim Provider vorgegebenen Maximalwert nicht überschreiten. Wenn keine Gültigkeitsdauer angegeben ist, wird als Default eine beim Provider vorgegebene Mindest-Gültigkeit angenommen.

EFA-Teilnehmer (optional)

Die Teilnehmer der anzulegenden Fallakte können/sollen bereits bei der Anlage der Akte benannt werden. Zu jedem Teilnehmer sind identifizierende Daten sowie die Rolle im Rahmen der der Fallakte zugrunde liegenden

Behandlung anzugeben. Die identifizierenden Daten müssen geeignet sein, einen authentisierten EFA-Nutzer zuverlässig als EFA-Teilnehmer zu identifizieren. Sofern die genutzten Identitätsdaten keinen Abruf von Informationen zu Name, Adresse etc. des Berechtigten erlauben (bzw. entsprechende Verzeichnisse nicht verfügbar sind), müssen zusätzlich zu jedem EFA-Teilnehmer Daten bereit gestellt werden, die dem Patienten und anderen EFA-Teilnehmern eine Identifizierung dieses Teilnehmers anhand von Name und Anschrift erlauben. Wenn bei der Anlage der EFA keine EFA-Teilnehmer benannt werden, werden lediglich Berechtigungen für den Initiator der Aktenanlage eingerichtet.

Einwilligungsformular (optional)

Eine elektronische Kopie der Einwilligungsformulars kann bei der Anlage der Akte übergeben werden. Dieses wird als Dokument in der Akte abgelegt. Der die Aktenanlage initiierende LE stellt sicher, dass die zur Konfiguration der EFA genutzten Angaben zum Patienten und zu den EFA-Teilnehmern mit den vom Patienten im Rahmen der Einwilligung gemachten Vorgaben übereinstimmen.

Nachbedingungen

- Die Fallakte ist angelegt und für berechtigte EFA-Teilnehmer eindeutig adressierbar. Berechtigte Teilnehmer können Daten in die Akte einstellen und aus dieser auslesen.
- Die Fallakte ist mit einem Patienten und einem Zweck verknüpft. Beide Angaben sind für berechtigte Teilnehmer - und nur für berechtigte Teilnehmer - einsehbar.
- An die Fallakte sind Berechtigungen gebunden, die einen Zugriff auf registriert und autorisierte EFA-Teilnehmer beschränken.
- Sofern eine elektronische Kopie des Einwilligungsformulars bei der EFA-Anlage übergeben wurde, ist diese als Dokument in der Fallakte abrufbar.

Ausnahmeszenarien

- Für den Patienten besteht bei dem angesprochenen EFA-Provider bereits eine Fallakte zu dem angegebenen Zweck.
  - Sofern die Einwilligung den expliziten Zusatz enthält, dass mit der neuen Akte eine ggf. bereits zu dem angegebenen Zweck angelegte Akte in die neue Akte überführt werden kann, wird die neue Akte angelegt. Die Partitionen der bestehenden Akte werden mit der neuen Akte verknüpft. Die neu abgegebene Einwilligung ersetzt alle zuvor abgegebenen Einwilligungen. Dem Arzt wird ein Hinweis angezeigt, dass eine bestehende Akte integriert wurde.
  - Sofern die Einwilligung keinen solchen Zusatz enthält, wird die Operation mit einer Fehlermeldung abgebrochen.
- Für den Patienten besteht bereits bei einem anderen als dem angesprochenen EFA-Provider eine Fallakte zu dem angegebenen Zweck.

- Die Akte wird gemäß des Standardablaufs beim angesprochenen Provider angelegt.
- Ein auf beiden Akten berechtigter Teilnehmer muss über das Muster "Zusammenführen von Fallakten" die Einwilligung des Patienten zur Zusammenführung der beiden Akten einholen und die Zusammenführung der Akten initiieren.

Peer-to-Peer Semantik

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngea.01.05}

Ist ein EFA-Teilnehmer einem EFA-Provider organisatorisch zugehörig, dann legt der EFA-Teilnehmer die neue Fallakte bevorzugt bei diesem EFA-Provider an.

Ansonsten legen EFA-Teilnehmer eine neue Fallakte immer bei dem EFA-Provider an, mit eine entsprechende Vereinbarung über eine Auftragsdatenverarbeitung besteht. Der Patient ist hierüber zu informieren und muss der Auftragsdatenverarbeitung zustimmen (siehe auch Domänenanalyse zur Auftragsdatenverarbeitung).

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Anlegen und Registrieren einer Partition**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster

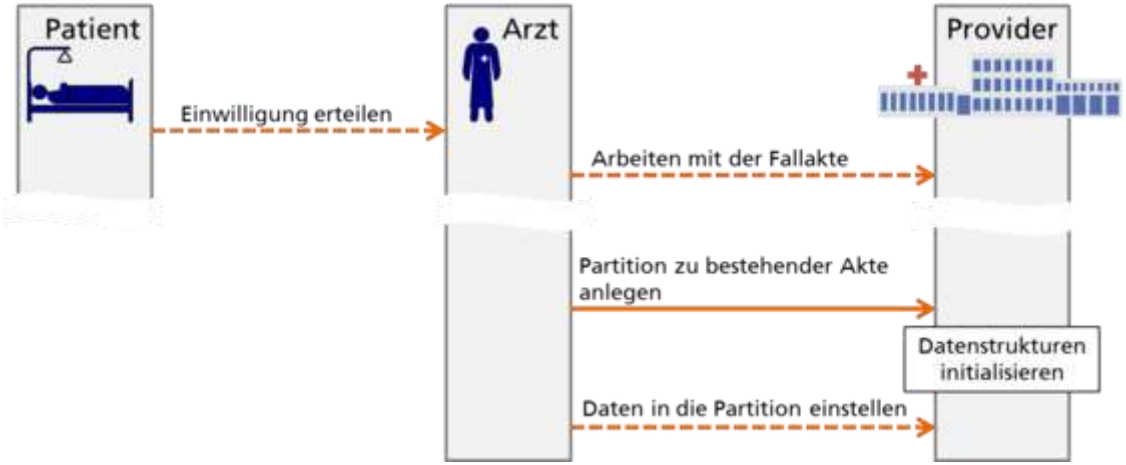
Anwendungsszenario: Anlegen einer Partition zu einer bestehenden Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngei.01.01}

EFA-Teilnehmer können für eine Fallakte relevante Daten entweder in eine bestehende Partition einstellen oder eine neue Partition anlegen, um darüber z.B. eine Verknüpfung mit einem stationären Aufenthalt herzustellen. Auch Strukturierungen auf Daten, die nicht über die Dokumenten-Metadaten herstellbar sind, können über Partitionen realisiert werden (siehe auch Geschäftsobjekt *Partition*).

Aus der Semantik der Fallakte heraus bilden alle zu dem selben Zweck angelegten Partitionen implizit eine Fallakte. Um eine neue Partition (z.B. zu einem stationären Aufenthalt) anzulegen und einer bestehenden Fallakte hinzuzufügen sind die folgenden Ablaufschritte erforderlich:

1. Ein Leistungserbringer ist über die Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert.
2. Der Teilnehmer legt eine neue Partition zu der bestehenden Akte an, um dort Daten zu einem aktuellen stationären Aufenthalt einzustellen und so den anderen EFA-Teilnehmern zugänglich zu machen. Als Zweck der Partition wird der Zweck der Fallakte angegeben. Hiermit ist die neue Partition automatisch mit der bestehenden Akte verknüpft und für alle anderen Teilnehmer der Fallakte zugreifbar.
3. Der Teilnehmer registriert in seinen IT-Systemen erstellte Daten an der neuen Partition.



Varianten des Anwendungsszenarios

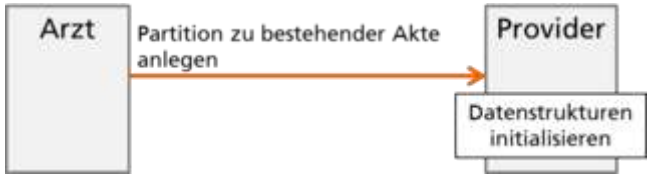
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngei.02}

Aktuell sind keine Varianten definiert.

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngei.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

	Vorbedingungen:
	• Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
	• Der die neue Partition anlegende Arzt ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
		Muster **Partition anlegen**
		• Bereit gestellte Informationen:
		  ○ Zu erweiternde Akte (Identifier, etc.)
		  ○ Titel der Partition

- Der die neue Partition anlegende Arzt besitzt die Berechtigung, bei einem EFA-Provider eine neue Partition zu einer Fallakte anzulegen und dort Daten zu speichern.
- Die neu anzulegende Partition fasst Daten zusammen, die ausschließlich im Rahmen der Zweckbindung der Akte innerhalb des Teilnehmerkreises der Akte kommuniziert werden sollen.

Funktionalität:

- Eine neue Partition wird zu einer bestehenden Fallakte angelegt.
- Zweckbindungen und Teilnehmer/Berechtigungen der Fallakte gelten ohne Änderungen und Ergänzungen auch für die neu angelegte Partition.

Nachbedingungen:

- Eine neue Partition ist mit der Fallakte verknüpft und kann von den EFA-Teilnehmern genutzt werden.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Partition auf welcher Basis und in welcher Konfiguration angelegt hat.

- Erforderliche Konfigurationsdaten:
  - EFA Provider

Definition der Interaktionsmuster

Interaktionsmuster: Partition anlegen und registrieren

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngei.04.01}

Motivation	Anlegen und Registrieren einer neuen Partition zu einer bestehenden Fallakte. Die Partition repräsentiert innerhalb der Fallakte eine einzelne Behandlungsepisode, einen administrativen Fall oder eine andere semantische Klammer um Behandlungsdaten.
Akteure und Rollen	Leistungserbringer (LE) Die Anlage einer Partition zu einer bestehenden Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine Einwilligung durch den Patienten ist nicht erforderlich, da für die Partition alle relevanten Konfigurationsdaten der übergeordneten Fallakte - insbesondere die Zweckbindung und die Berechtigungen - übernommen werden. EFA-Provider Der EFA-Provider legt die angeforderte Partition an und bindet diese an die bei der Anlage angegebene Fallakte. Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die übergeordnete Fallakte zugewiesenen Rollen erfolgen können.
Interaktion	Arzt --> (Aktenidentifikation, Name der Partition, [Anker der Partition], [initiale Dokumente]) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die Anlage einer Partition und deren Verknüpfung mit einer bestehenden Akte sind gegeben. Insbesondere unterstützt die Partition den Zweck der bestehenden Fallakte. • Der LE ist autorisierter Teilnehmer der übergeordneten Fallakte. • Der die Partition anlegende LE hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-Datenschutzkonzept definierten Vorgaben entspricht. Sofern es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt werden. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE hat die Akte, der die Partition zugeordnet werden soll, sicher identifiziert und den Zweck der Akte mit der Motivation zur Anlage der neuen Partition abgeglichen.
Ablauf	1. Der LE übermittelt die zur Anlage der Partition erforderlichen Informationen an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der die Partition anlegende LE in einem vertraglichen Verhältnis zum EFA-

Provider steht, das die Anlage einer Partition ermöglicht.

4. Der EFA-Provider verifiziert, dass der die Partition anlegende LE als Teilnehmer an der übergeordnete Akte registriert ist.
5. Der EFA-Provider verknüpft die angegebene Fallakte und deren Konfiguration (Zweckbindung, Berechtigungen) mit der neuen Partition.

Eingangsinformationen

Aktenidentifikation

Zur Anlage und Verknüpfung einer Partition müssen Angaben zu der übergeordneten Akte übermittelt werden, die dem EFA-Provider die Identifizierung dieser Akte und die Durchsetzung der damit verknüpften Berechtigungen ermöglichen.

Name der Partition

Jede Partition hat einen vom anlegenden LE frei vergebbaren Namen, der beim Browsing über einer Akte angezeigt wird. Der Name sollte so gewählt sein, dass die anderen EFA-Teilnehmer anhand des Namens der Partition eine Vorstellung von den dort verfügbaren Daten haben. Innerhalb eines EFA-Netzwerks können weiter gehende Konventionen zur Vergabe von Partitionsnamen definiert werden.

Anker der Partition (optional)

Wie in der Darstellung der EFA Geschäftsobjekte beschrieben, kann eine Partition mit einem Containerobjekt des EFA-Teilnehmers wie z.B. einem Aufenthalt oder einem Abrechnungsfall verknüpft werden. In diesem Fall kann z.B. ein Kommunikationsserver eine automatisierte Synchronisierung zwischen den Daten in der Partition und dem damit verknüpften internen Container durchführen. Um dieses zu unterstützen kann zu einer Partition ein Anker zu dem damit verknüpften internen Containerobjekt angegeben werden. Dieser Wert ist für den EFA-Provider und die anderen Teilnehmer semantikfrei und transparent.

Initiale Dokumente (optional)

Bei der Anlage einer Partition können initial in diese Partition einzustellende Dokumente angegeben werden.

Nachbedingungen

- Die Partition ist angelegt, mit einer Fallakte verknüpft und damit für berechtigte EFA-Teilnehmer dieser Fallakte sichtbar.
- Berechtigte Teilnehmer können Daten in die Partition einstellen und aus dieser auslesen.
- Sofern bei der Anlage der Partition Patientendaten übergeben wurden, sind diese als Dokumente in der Partition abrufbar.

Ausnahmeszenarien

Aktuell sind keine Ausnahmeszenarien definiert

Peer-to-Peer Semantik

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cngei.05}

Ist ein EFA-Teilnehmer einem EFA-Provider organisatorisch zugehörig, dann legt der EFA-Teilnehmer die neue Partition bevorzugt bei diesem EFA-Provider an.

Ansonsten legen EFA-Teilnehmer eine neue Partition immer bei dem EFA-Provider an, mit eine entsprechende Vereinbarung über eine Auftragsdatenverarbeitung besteht. Der Patient ist hierüber zu informieren und muss der Auftragsdatenverarbeitung zustimmen (siehe auch Domänenanalyse zur Auftragsdatenverarbeitung).

Referenzen und Querverweise

- zurück zur EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Einstellen von Daten in eine Fallakte**.*

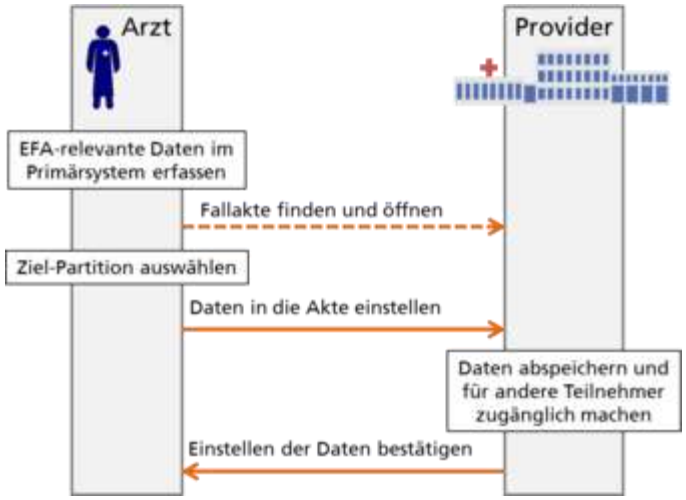
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster zum Einstellen von Daten in eine Fallakte

Anwendungsszenario: Einstellen von Daten in eine Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CiteD.01.01}



Neue Daten zu einer bestehenden Fallakte werden immer in eine vorhandene Partition dieser Akte eingestellt. Welche Partition dies ist, ergibt sich in den meisten Fällen aus dem Kontext der Datenbereitstellung - z.B. weil der zugrunde liegende Krankenhaus-Fall über eine dedizierte Partition an die Fallakte gekoppelt wurde.

Um Daten in eine Partition einzustellen und damit allen berechtigten EFA-Teilnehmern zugänglich zu machen sind die folgenden Ablaufschritte erforderlich:

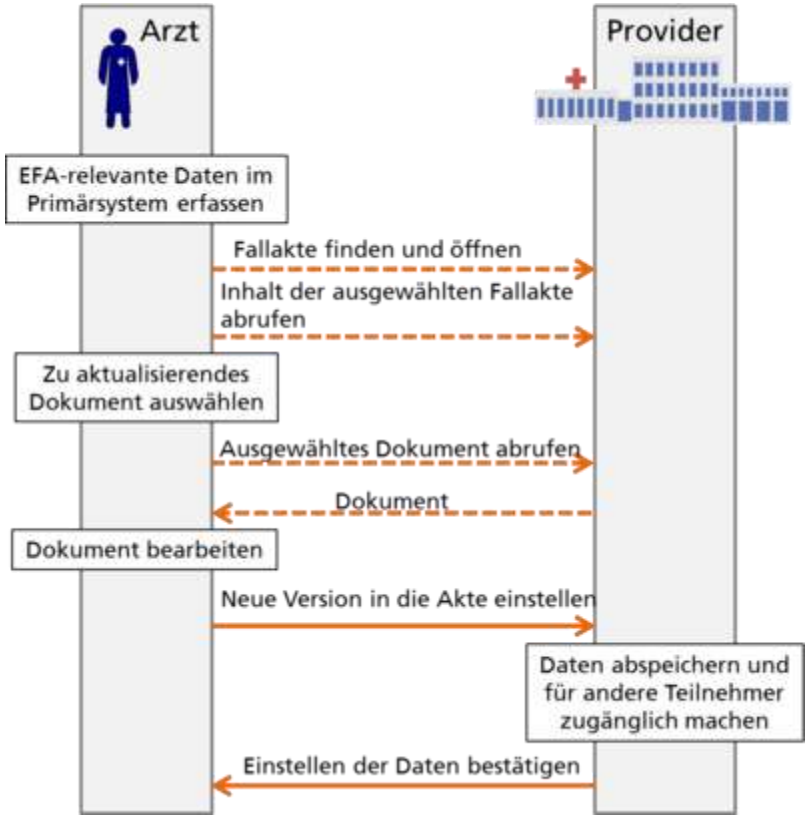
1. Ein Leistungserbringer ist über die Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert. Diese Einwilligung muss im Vorfeld erteilt worden sein.
2. Der Teilnehmer öffnet die gewünschte Fallakte und wählt die Partition aus, in die die neuen Daten eingestellt werden sollen. Die Auswahl der Partition kann dabei auch implizit durch das Teilnehmersystem vorgenommen werden, z.B. aufgrund einer bestehenden Verknüpfung (siehe Interaktionsmuster *Anlegen einer Partition*).
3. Der Teilnehmer sendet in seinen IT-Systemen erstellte Daten an den EFA-Provider und registriert sie an der ausgewählten Partition. Hiermit sind die Daten für alle anderen Teilnehmer der EFA sichtbar und abrufbar.

Varianten des Anwendungsszenarios

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CiteD.01.02}

Neben dem Einstellen orginärer Dokumente in eine Fallakte müssen auch Szenarien des Aktualisierens oder Ergänzens vorhandener Dokumente unterstützt werden.

Aktualisieren eines Dokuments



Ergänzen eines Dokuments

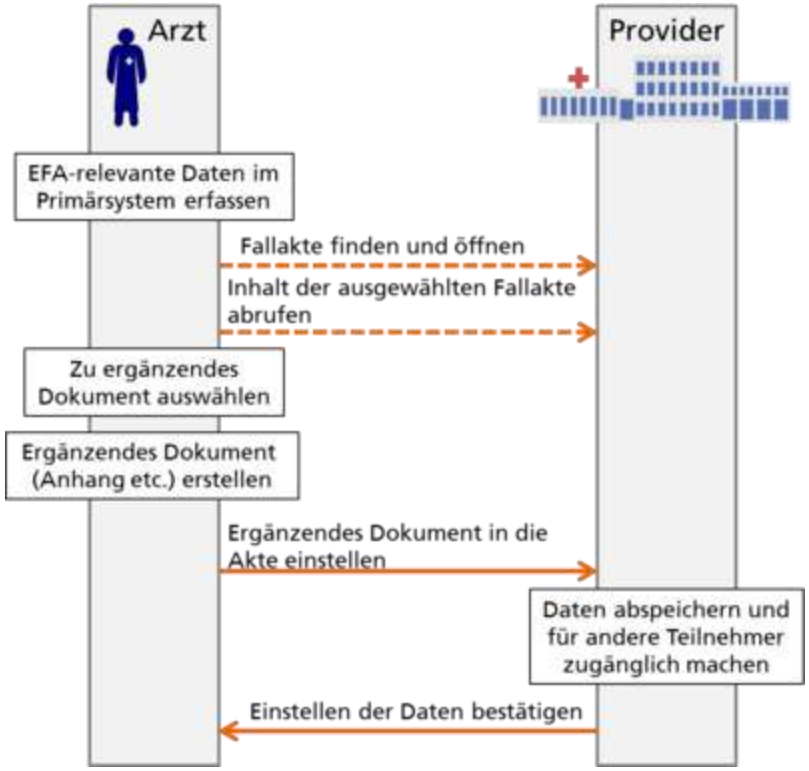
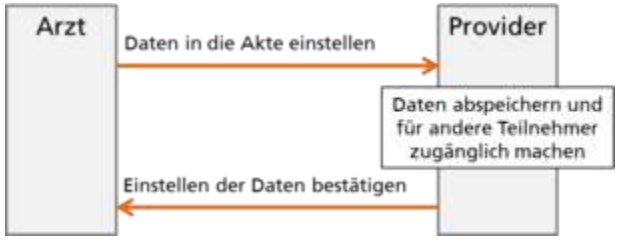


Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CiteD.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster



Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
- Der die Daten einstellende Arzt ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
- Der die Daten einstellende Arzt besitzt die Berechtigung, bei einem EFA-Provider Daten in einer Fallakte zu speichern (d.h. Voraussetzungen für eine Auftragsdatenverarbeitung durch den EFA-Provider sind gegeben).
- Die einzustellenden Daten dienen dem Zweck der ausgewählten Fallakte und werden von den anderen Behandlungsteilnehmern im Kontext derer Tätigkeiten benötigt.

Funktionalität:

- Die übergebenen Daten werden in der angegebenen Partition der Fallakte sicher gespeichert und registriert.
- Zweckbindungen und Teilnehmer/Berechtigungen der Fallakte gelten ohne Änderungen und Ergänzungen auch für die neu hinzu gekommenen Daten.

Nachbedingungen:

- EFA-relevante Daten sind mit der Fallakte

Muster **Daten einstellen**

- Bereit gestellte Informationen:
  - Partition, in der die Daten abgelegt werden sollen
  - Einzustellende Daten und deren Metadaten
- Erforderliche Konfigurationsdaten:
  - EFA Provider

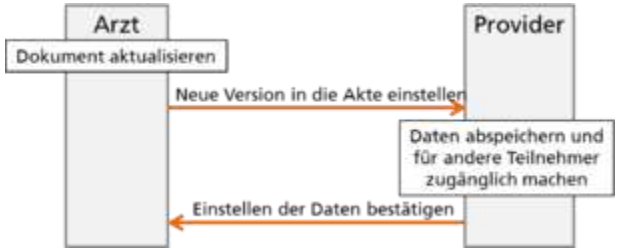
verknüpft und können von den EFA-Teilnehmern genutzt werden.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Daten wann in welche Partition der Akte eingestellt hat.

Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
- Der die Daten einstellende Arzt ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
- Der die Daten einstellende Arzt besitzt die Berechtigung, bei einem EFA-Provider Daten in einer Fallakte zu speichern (d.h. Voraussetzungen für eine Auftragsdatenverarbeitung durch den EFA-Provider sind gegeben).
- Das zu aktualisierende Dokument wurde aus der Fallakte geladen (bzw. aus dem Primärdatenbestand des Teilnehmers übernommen) und aktualisiert.



Funktionalität:

- Die übergebenen Daten werden in der angegebenen Partition der Fallakte sicher gespeichert und registriert.

Muster **Daten einstellen**

- Bereit gestellte Informationen:
  - Partition, in der die Daten abgelegt werden sollen
  - Einzustellende Daten und deren Metadaten
  - Verweis auf das zu aktualisierende Dokument und Hinweis auf Aktualisierung
- Erforderliche Konfigurationsdaten:
  - EFA Provider

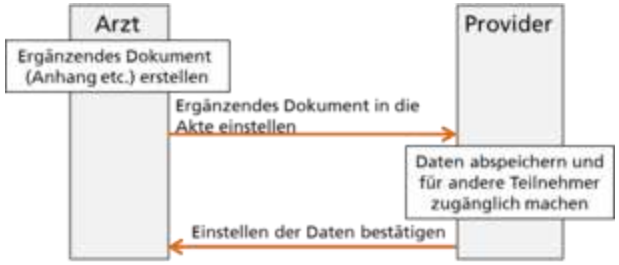
- Das neu eingestellte Dokument ist als Aktualisierung eines bestehenden Dokuments markiert.
- Zweckbindungen und Teilnehmer/Berechtigungen der Fallakte gelten ohne Änderungen und Ergänzungen auch für die neu hinzu gekommenen Daten.

Nachbedingungen:

- EFA-relevante Daten sind mit der Fallakte verknüpft und können von den EFA-Teilnehmern genutzt werden.
- Aktualisierungs-Beziehung ist für alle EFA-Teilnehmer sichtbar und nachvollziehbar.
- Das zuvor aktuelle Dokument ist als veraltet markiert.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Daten wann in welche Partition der Akte eingestellt hat.



Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
- Der die Daten einstellende Arzt ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
- Der die Daten einstellende Arzt besitzt die

Muster **Daten einstellen**

- Bereit gestellte Informationen:
  - Partition, in der die Daten abgelegt werden sollen
  - Einzustellende Daten und deren Metadaten
  - Verweis auf das zu ergänzende

Berechtigung, bei einem EFA-Provider Daten in einer Fallakte zu speichern (d.h. Voraussetzungen für eine Auftragsdatenverarbeitung durch den EFA-Provider sind gegeben).
- Das zu ergänzende Dokument wurde aus der Fallakte geladen (bzw. aus dem Primärdatenbestand des Teilnehmers übernommen) und die Ergänzung wurde als Datenobjekt im Teilnehmersystem angelegt.

Funktionalität:

- Die übergebenen Daten werden in der angegebenen Partition der Fallakte sicher gespeichert und registriert.
- Das neu eingestellte Dokument ist als Ergänzung zu einem bestehenden Dokuments markiert.
- Zweckbindungen und Teilnehmer/Berechtigungen der Fallakte gelten ohne Änderungen und Ergänzungen auch für die neu hinzu gekommenen Daten.

Nachbedingungen:

- EFA-relevante Daten sind mit der Fallakte verknüpft und können von den EFA-Teilnehmern genutzt werden.
- Ergänzungs-Beziehung ist für alle EFA-Teilnehmer sichtbar und nachvollziehbar.

Dokument und Hinweis auf Ergänzung
- Erforderliche Konfigurationsdaten:
  - EFA Provider

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Daten wann in welche Partition der Akte eingestellt hat.

Definition der Interaktionsmuster

Interaktionsmuster: Daten einstellen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CiteD.04.01}

Motivation	Einstellen von Daten in eine bestehenden Partition einer bestehenden Fallakte. Die eingestellten Daten können dabei in einer Beziehung zu bereits vorhandenen Daten stehen (Aktualisierung, Ergänzung).
Akteure und Rollen	Leistungserbringer (LE) Die Bereitstellung von Daten zu einer bestehenden Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine explizite Einwilligung durch den Patienten für diese Einzeltransaktion ist nicht erforderlich, da für die Daten alle relevanten Konfigurationsdaten der übergeordneten Fallakte - insbesondere die Zweckbindung und die Berechtigungen - übernommen werden. EFA-Provider Der EFA-Provider legt Daten in der angegebenen Partition der Fallakte ab und macht sie dadurch den anderen Teilnehmern dieser EFA zugänglich. Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die übergeordnete Fallakte zugewiesenen Rollen erfolgen können. Der EFA-Provider stellt sicher dass ggf. angegebene Beziehungen zu vorhandenen Dokumenten für andere Teilnehmer sichtbar sind.
Interaktion	Arzt --> (Identifikation der Ziel-Partition, Dokumente und Metadaten, Dokumentenbeziehungen) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die Bereitstellung der Daten und deren Verknüpfung mit einer bestehenden Akte sind gegeben. Insbesondere unterstützen die Daten den Zweck der bestehenden Fallakte. • Der LE ist autorisierter Teilnehmer der übergeordneten Fallakte. • Der die Daten einstellende LE hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-

Datenschutzkonzept definierten Vorgaben entspricht. Sofern es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt worden sein.

- Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren.
- Der LE hat die Akte und die Partition, der die Daten zugeordnet werden sollen, sicher identifiziert und den Zweck der Akte mit der Motivation zur Bereitstellung der Daten abgeglichen.
- Sofern bestehende Dokumente aktualisiert oder ergänzt werden sollen, hat der LE diese Dokumente sicher identifiziert und die eindeutigen Objektreferenzen ermittelt.

Ablauf

1. Der LE übermittelt die einzustellenden Daten mitsamt der zur Bereitstellung dieser Daten erforderlichen Informationen an den EFA-Provider. Sofern Beziehungen zu bestehenden Dokumenten bestehen, werden diese explizit durch Art der Beziehung (Aktualisierung, Ergänzung) und Bezugspunkt (bestehendes Dokument) vermerkt.
2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit.
3. Der EFA-Provider verifiziert, dass der die Daten bereitstellende LE in einem vertraglichen Verhältnis zum EFA-Provider steht, das das Einstellen von Daten in eine EFA ermöglicht.
4. Der EFA-Provider verifiziert, dass der die Daten einstellende LE als Teilnehmer an der übergeordnete Akte registriert ist.
5. Der EFA-Provider speichert die übergebenen Daten in der angegebenen Partition.
6. Der EFA-Provider registriert die übergebenen Metadaten, um ein Auffinden der Daten durch Dritte zu ermöglichen.
7. Der EFA-Provider registriert ggf. angegebene Dokumentenbeziehungen, um diese für andere Teilnehmer nachvollziehbar zu machen.

Eingangsinformationen

Identifikation der Ziel-Partition

Zur Ablage und Verknüpfung der Daten in einer Partition müssen Angaben zu dieser Partition übermittelt werden, die dem EFA-Provider die Identifizierung dieser Partition und der übergeordneten Akte sowie die Durchsetzung der damit verknüpften Berechtigungen ermöglichen.

Dokumente und Metadaten

In die benannte Partition einzustellenden Daten. Da die Daten selber (mit wenigen Ausnahmen wie z.B. Einwilligungsinformationen) beim EFA-Provider nicht inhaltlich verarbeitet werden, sind begleitende Metadaten erforderlich, die eine Suche und ein Browsing über dem Datenbestand einer EFA erleichtern.

	Dokumentenbeziehungen Beziehung zwischen neu eingestellten und vorhandenen Dokumenten, wie z.B. Aktualisierung und Ergänzung eines vorhandenen Dokuments durch ein neu eingestelltes Dokument.
Nachbedingungen	• Die Daten sind in einer - mit einer Fallakte verknüpften - Partition abgelegt und damit für berechtigte EFA-Teilnehmer dieser Fallakte sichtbar. • Berechtigte Teilnehmer können die Daten über die Fallakte aus dieser Partition auslesen. Ggf. bestehende Beziehungen zwischen Dokumenten sind sichtbar.
Ausnahmeszenarien	*Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CiteD.01.05}`

Sofern ein EFA-Teilnehmer selber auch als EFA-Provider agiert, werden neue Daten von diesem Teilnehmer bevorzugt in einer vom "eigenen" Provider verwalteten Partition angelegt.

Ansonsten stellen EFA-Teilnehmer neue Daten immer bei einem EFA-Provider ein, mit eine entsprechende Vereinbarung über eine Auftragsdatenverarbeitung besteht. Sofern bei diesem Provider noch keine für die Aufnahme der Daten geeignete Partition für die Akte angelegt wurde, muss vor dem Einstellen der Daten zunächst diese Partition registriert werden. Der Patient ist hierüber zu informieren und muss der Auftragsdatenverarbeitung zustimmen (siehe auch Domänenanalyse zur Auftragsdatenverarbeitung).

Querverweise und Referenzen

- zurück zur EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Auffinden und Öffnen einer Fallakte**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster "Auffinden der Fallakten eines Patienten"

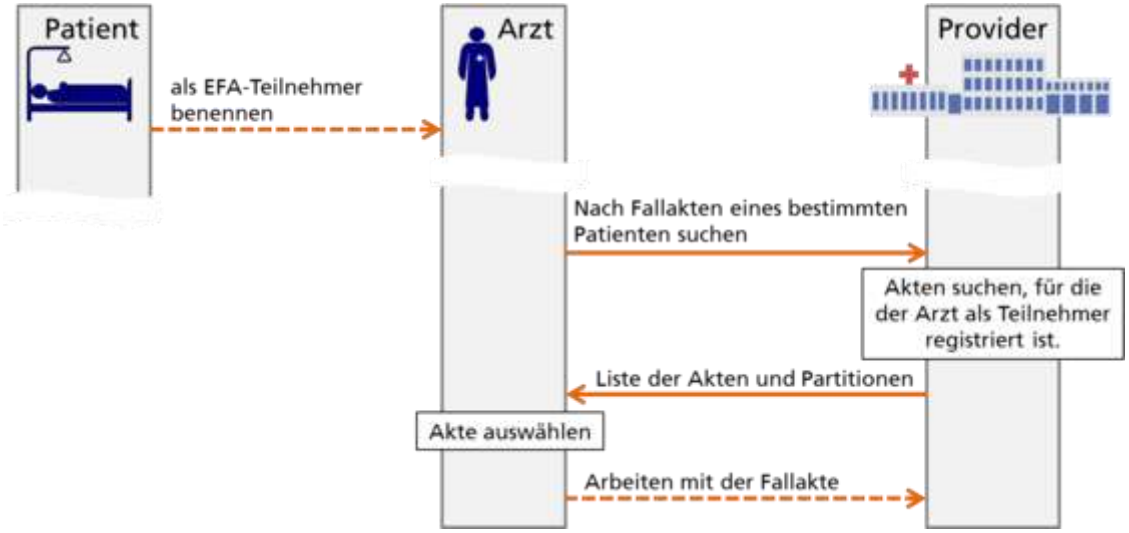
Anwendungsszenario: Auffinden und Öffnen einer Fallakte eines Patienten

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cuina.01.01}`

EFA-Teilnehmer können am EFA-Provider abfragen, zu welchen Fallakten eines Patienten sie Zugang haben und anschließend auf die Daten dieser Akten zugreifen.

Aus der Semantik der Fallakte heraus bilden alle zu dem selben Zweck angelegten Partitionen implizit eine Fallakte. Eine Fallakte zu finden und zu öffnen bedeutet daher, dass ein berechtigter Teilnehmer dieser Akte eine Übersicht aller Partitionen der Akte erhält und über diese Daten abrufen und einstellen können. Hierzu sind die folgenden Ablaufschritte erforderlich:

1. Ein Leistungserbringer ist über die bei der EFA-Anlage abgegebene Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert.
2. Der Teilnehmer sendet eine Anfrage an den EFA-Provider, in der er den Patient angibt, auf dessen Fallakten er zugreifen möchte.
3. Der EFA-Provider prüft, für welche der Fallakten des Patienten der Leistungserbringer als Teilnehmer registriert ist und welche Partitionen diese Akten jeweils aufspannen.
4. Aus den vom EFA-Provider gelieferten Daten zu den relevanten Fallakten und Partitionen bekommt der Leistungserbringer einen Überblick, welche Akten für den Patienten aktiv sind und welche Behandlungsepisoden damit erfasst sind. Auf Basis dieser Übersicht kann er anschließend über der Akte und ihren Partitionen browsen und sich die für seine Tätigkeit erforderlichen Dokumente ansehen.



Varianten des Anwendungsszenarios

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cuina.01.02}

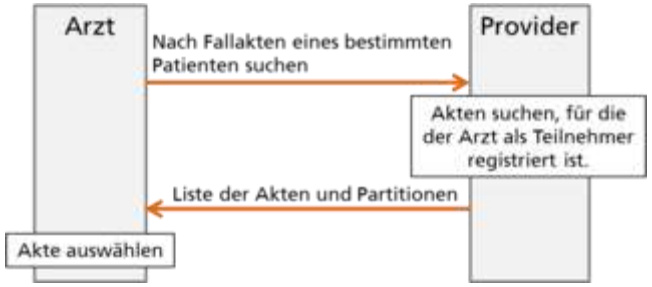
Resource Discovery Token (Offline Token)

tbd

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cuina.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster



Vorbedingungen:

- Der nach Fallakten eines Patienten suchende Arzt besitzt einen Zugang zu einem EFA-Provider.

Funktionalität:

- Suchen nach Fallakten (d.h. medizinischen Fällen eines Patienten) für die der anfragende Arzt als Person oder über seine Organisationszugehörigkeit als berechtigter Teilnehmer registriert ist.

Nachbedingungen:

- Der Leistungserbringer verfügt über alle Informationen, die er zum Arbeiten mit einer ausgewählten Akte benötigt.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person nach Akten welches Patienten gesucht hat.

Muster **Partitionen auflisten**

- Eingangsinformationen:
  - Patient, nach dessen Akten gesucht werden soll
- Ausgangsinformationen
  - Verweise auf die gefundenen Partitionen und die diesen übergeordneten Akten (medizinischen Fälle)
- Erforderliche Konfigurationsdaten:
  - EFA Provider

Definition der Interaktionsmuster

Interaktionsmuster: Partitionen auflisten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cuina.01.04.01}

Motivation	Auffinden und Auswählen einer Fallakte eines Patienten, um diese im Rahmen einer kooperativen Behandlung zu nutzen.
Akteure und Rollen	Leistungserbringer (LE) Nutzer von Fallakten sind die vom Patienten autorisierten Behandlungsteilnehmer. Vor der Nutzung der Akte muss ein Leistungserbringer den Zugang zu dieser Akte erhalten. EFA-Provider Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die übergeordnete Fallakte zugewiesenen Rollen erfolgen können. Eine Leistungserbringer wird ein Zugang nur zu Akten gewährt, für die er als Teilnehmer registriert ist.
Interaktion	Arzt --> (Patientenidentifikation, [Diagnose, etc.]) --> EFA-Provider
Vorbedingungen	• Der Leistungserbringer ist in die Behandlung des Patienten eingebunden. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE kann die Identität des Patienten zu einem im EFA-Verbund genutzten *Patient-Identifier* auflösen.
Ablauf	1. Der LE übermittelt den Patienten-Identifier an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert die Authentizität des Anfragenden. 4. Der EFA-Provider sucht nach Fallakten, für die der LE als Teilnehmer registriert ist. 5. Der EFA-Provider sucht die diesen Fallakten zugeordneten Partitionen. 6. Der EFA-Provider liefert Informationen zu den gefundenen Akten und Partitionen an den LE zurück, die es diesem ermöglichen, auf diese Akten und Partitionen zuzugreifen.
Eingangsinformationen	Patientenidentifikation Zur Suche nach Fallakten muss die Patientenidentifikation angegeben werden, die bei der Anlage der Akte verwendet wurde. Zweck (optional) Die Suche nach Fallakten eines Patienten kann auf Akten eingeschränkt werden, die zu einem bestimmten Zweck angelegt wurden.
Nachbedingungen	• Der Leistungserbringer verfügt über alle Informationen, die es ihm ermöglichen, im Rahmen seiner Berechtigungen auf ausgewählte Akten und Partitionen zuzugreifen.

Ausnahmeszenarien *Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cuina.01.05}`

Innerhalb eines Peer-to-Peer-Netzes von EFA-Providern werden Suchanfragen an alle teilnehmenden Provider weitergereicht. Der ursprünglich aufgerufene Provider führt die Suchergebnisse zusammen und übermittelt sie an den Aufrufer.

Querverweise und Referenzen

- zurück zur EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Browsing über eine Akte oder eine Partition**.*

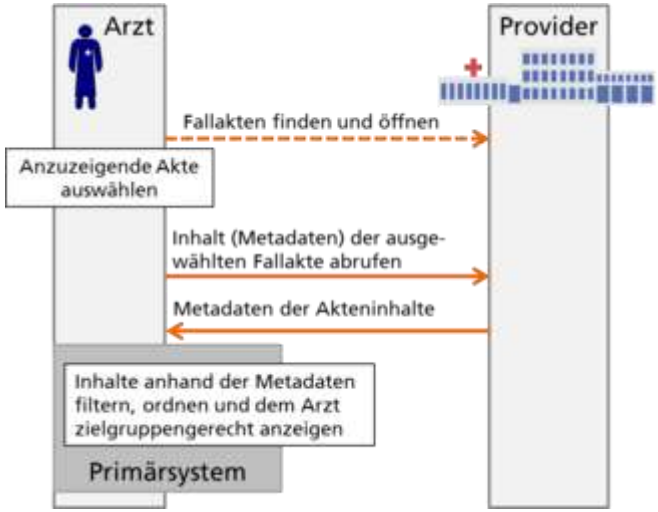
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster "Browsing über einer Fallakte oder einer Partition"

Anwendungsszenario: Browsing über eine Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.01}



Fallakten sind in ihrer Nutzeransicht nach fachlichen Vorgaben strukturiert. Wie diese Struktur konkret aussieht ist Gegenstand von Vereinbarungen in regionalen Netzen, Empfehlungen von Fachgesellschaften und/oder Sortiervorgaben des Nutzers. Beispielsweise können für Akten zu bestimmten Diagnosen fest definierte Ordnungsstrukturen vorgegeben sein, so dass Akten zu dieser Diagnose für Nutzer unabhängig von deren Primärsystem immer identisch strukturiert angezeigt werden. Ebenfalls denkbar ist, dass der Nutzer eine Einordnung der Dokumente einer Akte entlang einer Zeitleiste wünscht, z.B. um sich zunächst die aktuellsten Informationen abrufen zu können.

Um diese Flexibilität zu erreichen, ruft das EFA-Teilnehmersystem nach dem Öffnen einer Akte alle Metadaten der in der Akte enthaltenen Dokumente ab. Anhand dieser Metadaten können die Dokumente anschließend in die vorgegebene Anzeige-Struktur einsortiert oder gemäß Nutzervorgaben sortiert werden. Hiermit ist die Daten-Sicht des Arztes vollkommen von der Speicherstruktur in Partitionen entkoppelt.

Im Einzelnen erfolgt das Browsing über einer vollständigen Fallakte in den folgenden Ablaufschritten:

1. Ein Leistungserbringer ist über die Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert. Der Leistungserbringer hat die gewünschte Akte lokalisiert und geöffnet indem sein Teilnehmersystem die zur Akte gehörigen Partitionen identifiziert hat.
2. Das Teilnehmersystem ruft die beschreibenden Metadaten zu allen an den Partitionen der Fallakte registrierten Dokumente ab.

3. Das Teilnehmersystem stellt die Dokumente anhand der Metadaten in die gewünschte Struktur ein bzw. ordnet diese nach Vorgaben des Nutzers an (z.B. nach Erstellungsdatum) und stellt diese Struktur über eine grafische Benutzeroberfläche dar.

Varianten des Anwendungsszenarios

Suchen und Filtern anhand von definierten Kriterien

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.02.01}

In bestimmten Szenarien können für einen EFA-Teilnehmer nur bestimmte Inhalte einer EFA oder gar nur ein einzelnes spezielles Dokument relevant sein. Ggf. möchte ein Teilnehmer auch nur die Dokumente aufgelistet bekommen, die nach seinem letzten Zugriff auf eine Fallakte neu in diese Akte eingestellt wurden.

Solche Such- und Filter-Funktionen werden bei der EFA clientseitig realisiert. D.h. wie beim Browsing über einer Akte ruft das Teilnehmersystem alle Metadaten der in die Fallakte eingestellten Dokumente ab, und wendet anschließend die Such- und Filter-Kriterien auf diese Metadaten an.

Browsing über einer einzelnen Partition

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.02.02}

Grundsätzlich kann ein Teilnehmersystem dem Nutzer auch in einem ersten Schritt zunächst nur die beim Öffnen der gewünschten Fallakte abgerufenen Informationen zu den verfügbaren Partitionen anzeigen. Insbesondere wenn z.B. in einem regionalen Verbund per Konvention zu jedem stationären Aufenthalt immer eine dedizierte Partition angelegt wird, kann ein Arzt so sehr schnell über diese Partition sehr fokussiert auf die aktuellsten Behandlungsdaten zugreifen.

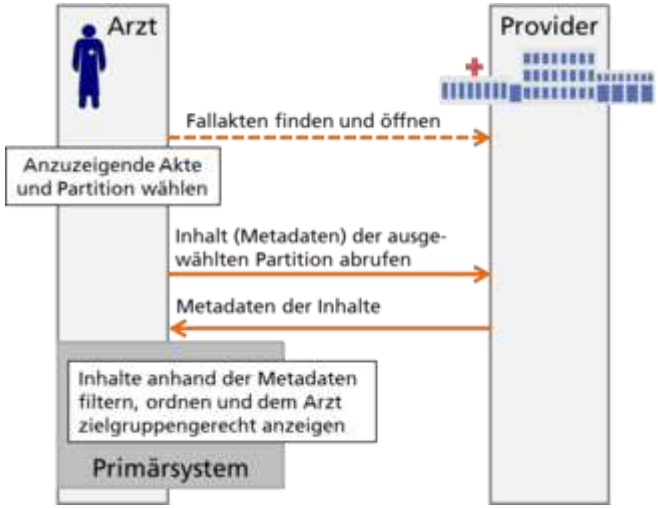
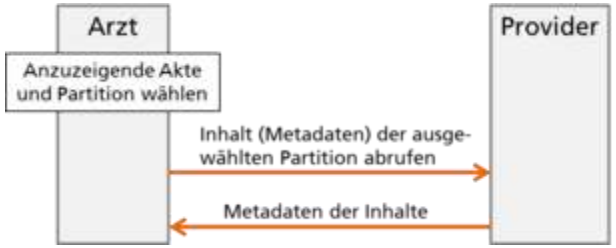


Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

Browsing über einer Partition
 
	Vorbedingungen:
	• Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
	• Der Nutzer ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
	• Der Zugriff auf die Akte und die darin gespeicherten Daten erfolgt im Kontext der Zweckbindung der Fallakte.
	• Der Nutzer hat die Akte und die gewünschte
		Muster **Partition abrufen**
		• Bereit gestellte Informationen:
		  ○ Auszulesende Partition (Identifier, etc.)
		• Erforderliche Konfigurationsdaten:
		  ○ EFA Provider

Partition gefunden und ausgewählt.

Funktionalität:

- Abrufen der Metadaten sämtlicher in der gewählten Partition registrierten Dokumente

Nachbedingungen:

- Die Metadaten der in der Partition registrierten Dokumente sind im Teilnehmersystem des Nutzers verfügbar und können dort für die Visualiserung aufbereitet werden.

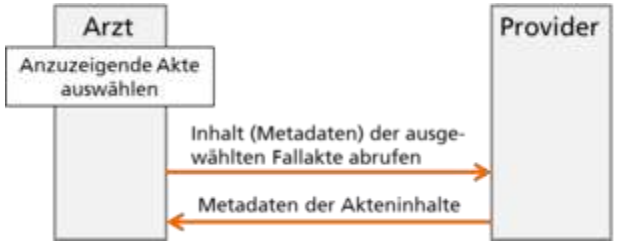
Verpflichtungen:

- Es ist nachvollziehbar, welche Person wann auf die Partition zugegriffen hat.

Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
- Der Nutzer ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
- Der Zugriff auf die Akte und die darin gespeicherten Daten erfolgt im Kontext der Zweckbindung der Fallakte.
- Der Nutzer hat die Akte gefunden und ausgewählt.

Browsing über einer Fallakte



Muster **EFA abrufen**

- Bereit gestellte Informationen:
  - Auszulesende Fallakte (Identifier, etc.)
- Erforderliche Konfigurationsdaten:
  - EFA Provider

Funktionalität:

- Abrufen der Metadaten sämtlicher in der Fallakte registrierten Dokumente

Nachbedingungen:

- Die Metadaten der in der Fallakte registrierten Dokumente sind im Teilnehmersystem des Nutzers verfügbar und können dort für die Visualiserung aufbereitet werden.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person wann auf die Fallakte zugegriffen hat.

Definition der Interaktionsmuster

Interaktionsmuster: Partition abrufen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.04.01}

Motivation	Abrufen der Metadaten der in einer Partition zu einer Fallakte enthaltenen Dokumente. Die Partition repräsentiert innerhalb der Fallakte eine einzelne Behandlungsepisode, einen administrativen Fall oder eine andere semantische Klammer um Behandlungsdaten.
Akteure und Rollen	Leistungserbringer (LE) Der Abruf von Daten aus einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine Einwilligung durch den Patienten ist zu dieser Einzeltransaktion nicht erforderlich, da der Zugriff im Rahmen der vom Patienten eingewilligten Zweckbindung durch einen vom Patienten als Teilnehmer benannten Akteur erfolgt. EFA-Provider

	Der EFA-Provider stellt die angeforderten Metadaten zusammen und liefert sie in strukturierter Form an den Nutzer zurück.
Interaktion	Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die übergeordnete Fallakte zugewiesenen Rollen erfolgen können. Arzt --> (Identifikation der Partition) --> EFA-Provider EFA-Provider --> (Metadaten der Inhalte der Partition) --> Arzt
Vorbedingungen	• Die fachlichen Voraussetzungen für den Zugriff auf Daten der ausgewählten Partition sind gegeben. Insbesondere findet der Zugriff im Rahmen der Zweckbindung der der Partition übergeordneten Akte statt. • Der LE ist autorisierter Teilnehmer der übergeordneten Fallakte. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE hat die Partition, aus der Daten abgerufen werden sollen, sicher identifiziert und ausgewählt.
Ablauf	1. Der LE übermittelt die zum Datenabruf erforderlichen Informationen an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der anfragende LE als Teilnehmer an der übergeordnete Akte registriert ist. 4. Der EFA-Provider stellt die Metadaten aller in der Partition registrierten Dokumente in strukturierter Form zusammen und stellt sie dem LE bereit.
Eingangsinformationen	Identifikation der Partition Identifizierer, mit dem die auszulesende Partition eindeutig innerhalb des Datenbestands des EFA-Providers gefunden und einer übergeordneten Fallakte zugeordnet werden kann.
Nachbedingungen	• Die Metadaten aller an der ausgewählten Partition registrierten Dokumente sind im Teilnehmersystem des LE verfügbar und können für den LE in geeigneter Weise aufbereitet und visualisiert werden.
Ausnahmeszenarien	*Aktuell sind keine Ausnahmeszenarien definiert*

Interaktionsmuster: Fallakte abrufen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.04.02}

Motivation

Abrufen der Metadaten aller in einer Fallakte enthaltenen Dokumente.

Akteure und Rollen

Leistungserbringer (LE)

Der Abruf von Daten aus einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine Einwilligung durch den Patienten ist zu dieser Einzeltransaktion nicht erforderlich, da der Zugriff im Rahmen der vom Patienten eingewilligten Zweckbindung durch einen vom Patienten als Teilnehmer benannten Akteur erfolgt.

EFA-Provider

Der EFA-Provider stellt die angeforderten Metadaten zusammen und liefert sie in strukturierter Form an den Nutzer zurück.

Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die Fallakte zugewiesenen Rollen erfolgen können.

Interaktion

Arzt --> (Aktenidentifikation) --> EFA-Provider

EFA-Provider --> (Metadaten der Akteninhalte) --> Arzt

Vorbedingungen

- Die fachlichen Voraussetzungen für den Zugriff auf Daten der ausgewählten Fallakte sind gegeben. Insbesondere findet der Zugriff im Rahmen der Zweckbindung der Fallakte statt.
- Der LE ist autorisierter Teilnehmer der Fallakte.
- Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren.
- Der LE hat die Fallakte, aus der Daten abgerufen werden sollen, sicher identifiziert und ausgewählt.

Ablauf

1. Der LE übermittelt die zum Datenabruf erforderlichen Informationen an den EFA-Provider.
2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit.
3. Der EFA-Provider verifiziert, dass der anfragende LE als Teilnehmer an der ausgewählten Fallakte registriert ist.
4. Der EFA-Provider stellt die Metadaten aller Dokumente zusammen, die an einer Partition registriert sind, die ihrerseits Bestandteil der ausgewählten Fallakte ist. Der EFA-Provider stellt die Metadaten dem LE in strukturierter Form bereit.

Eingangsinformationen Aktenidentifikation

	Identifizierer, mit dem die auszulesende Fallakte und deren Partitionen eindeutig innerhalb des Datenbestands des EFA-Providers gefunden werden können.
Nachbedingungen	• Die Metadaten aller an Partitionen der ausgewählten Fallakte registrierten Dokumente sind im Teilnehmersystem des LE verfügbar und können für den LE in geeigneter Weise aufbereitet und visualisiert werden.

Ausnahmeszenarien *Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Crsii.01.05}`

Bein Abruf der Dokumente einer Akte müssen alle ggf. über mehrere Peers verteilte Partitionen berücksichtigt werden.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Abruf von Daten aus einer Fallakte**.*

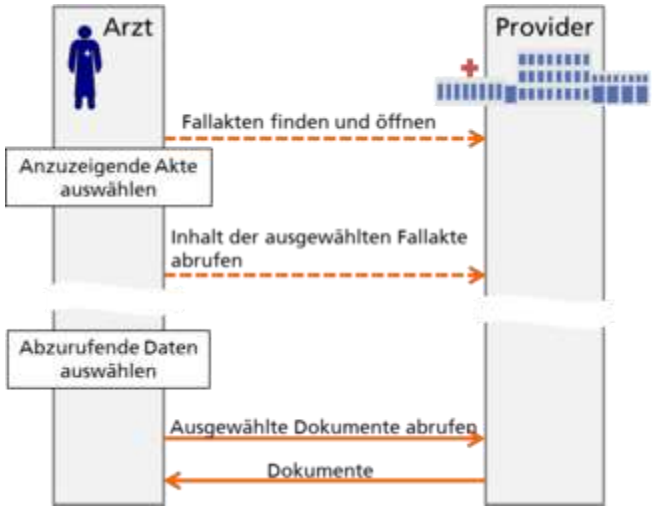
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster "Abruf von Datenobjekten"

Anwendungsszenario: Abruf von Daten aus einer Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cbfuo.01.01}



Die EFA unterstützt den Austausch von medizinischen Daten in einer konkreten, einrichtungsübergreifend angelegten Behandlungssituation. Ein wesentlicher Bestandteil dieses Austauschs ist, dass Daten nicht nur im Sinne einer gemeinsamen Dokumentation der Behandlungsteilnehmer in der Fallakte verwaltet werden, sondern auch zur Nutzung im Rahmen der Behandlung aus der Akte abgerufen und in Primärsysteme der EFA-Teilnehmer übernommen werden können.

Die rechts dargestellte Abbildung stellt den Abruf von Dokumenten im Kontext einer typischen EFA-Nutzungssequenz dar.

Um Daten aus einer Fallakte abzurufen sind die folgenden Ablaufschritte erforderlich:

1. Ein Leistungserbringer ist über die Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert. Diese Einwilligung muss im Vorfeld erteilt worden sein.

2. Der Teilnehmer öffnet die gewünschte Fallakte, ruft die Metadaten der Inhalte ab und wählt die anzuzeigenden bzw. ins Primärsystem zu übernehmenden Dokumente aus.
3. Der Teilnehmer ruft die ausgewählten Dokumente vom EFA-Provider ab und übernimmt sie ggf. in seine Primärdokumentation.

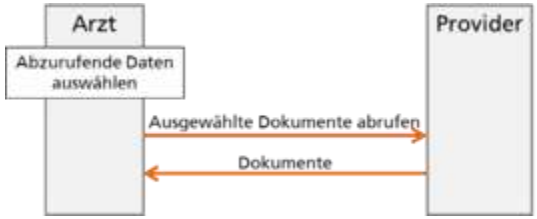
Varianten des Anwendungsszenarios

Aktuell sind keine Varianten definiert.

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cbfuo.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

	Vorbedingungen:
	• Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
	• Der die Daten abrufende Arzt ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
	• Der Arzt hat die Fallakte geöffnet und die benötigten Daten ausgewählt.
	
	Funktionalität:
	• Abruf ausgewählter Daten aus einer Fallakte
	
	Nachbedingungen:
	• Ausgewählte Daten sind aus der Fallakte ausgelesen und können über das Teilnehmersystem angezeigt oder in die Primärdokumentation des Nutzers
		Muster **Daten abrufen**
		• Bereit gestellte Informationen:
		  ○ Identifizierer der abzurufenden Dokumente
		• Erforderliche Konfigurationsdaten:
		  ○ EFA Provider

übernommen werden.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Daten wann abgerufen hat.

Definition der Interaktionsmuster

Interaktionsmuster: Daten abrufen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cbfuo.01.04.01}

Motivation	Abrufen ausgewählter Daten aus einer Fallakte.
Akteure und Rollen	Leistungserbringer (LE) Der Abruf von Daten aus einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine explizite Einwilligung durch den Patienten für diese Einzeltransaktion ist nicht erforderlich, da der Zugriff im Rahmen der vom Patienten eingewilligten Zweckbindung und durch einen vom Patienten benannten EFA-Teilnehmer erfolgt. EFA-Provider Der EFA-Provider verwaltet Daten in Fallakten und stellt sie berechtigten Nutzern zum Abruf zur Verfügung. Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die betroffene Fallakte zugewiesenen Rollen erfolgen können.
Interaktion	Arzt --> (Identifikation der abzurufenden Dokumente) --> EFA-Provider EFA-Provider --> (Dokumente) --> Arzt
Vorbedingungen	• Die fachlichen Voraussetzungen für den Abruf der Daten sind gegeben. Insbesondere unterstützen die ausgewählten Daten den Arzt bei der den Zweck der Akte determinierenden Behandlung des Patienten. • Der LE ist autorisierter Teilnehmer der Fallakte, der die ausgewählten Dokumente zugeordnet sind. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren.

	• Der LE hat die abzurufenden Dokumente sicher identifiziert.
Ablauf	1. Der LE übermittelt die zum Abruf der gewünschten Dokumente erforderlichen Informationen an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der die Daten abrufende LE als Teilnehmer an der Akte registriert ist, der die Dokumente zugeordnet sind. 4. Der EFA-Provider ruft die gewünschten Dokumente aus seiner Datenbank ab, verifiziert deren Integrität und übergibt sie an den LE.
Eingangsinformationen	Identifikation der abzurufenden Dokumente Zum Abruf der Dokumente müssen Angaben zu diesen werden, die dem EFA-Provider die Identifizierung dieser Dokumente und der übergeordneten Akte sowie die Durchsetzung der damit verknüpften Berechtigungen ermöglichen.
Nachbedingungen	• Die angeforderten Dokumente stehen dem LE zur Benutzung und zur weiteren Verarbeitung zur Verfügung.
Ausnahmeszenarien	*Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cbfuo.01.05}`

Ein Abruf von auf mehreren Peers verteilt verwalteten Daten muss möglich sein. Teilnehmersystem und EFA-Provider haben in ihrem Zusammenspiel sicher zu stellen, dass die physische Verteilung der Daten einer Fallakte vor dem Nutzer soweit als möglich verborgen bleibt.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Schließen einer Fallakte**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster "Schließen einer Fallakte"

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01}`

Die Existenz einer Fallakte hängt an der vom Patienten gegebenen Einwilligung. Läuft diese mit Erreichen der maximalen Gültigkeit aus oder wird sie vom Patienten zurückgenommen, so muss die Fallakte geschlossen werden. Während unmittelbar und formal aus einer bestehenden Akte ableitbare Schließungen (z.B. Ablauf der Gültigkeit) vom EFA-Provider mit internen Verfahren realisiert werden, erfordern die durch fachliche Gründe oder den Patientenwunsch motivierten Schließungen eine Interaktion von Patient, Arzt und EFA-Provider.

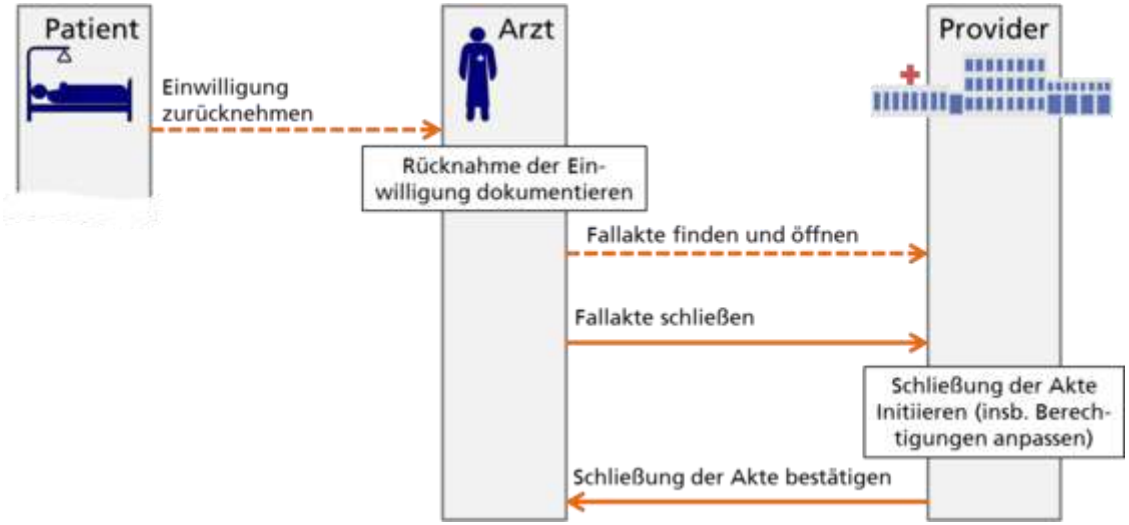
Anwendungsszenario: Rücknahme der Einwilligung durch den Patienten

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01.01}`

Der Patient hat das Recht, seine Einwilligung zur Nutzung einer Akte und zur Bereitstellung seine Daten über eine Akte jederzeit zurückzuziehen. In diesem Fall muss die Akte in einem geregelten Prozess geschlossen werden (siehe auch *Lebenszyklus einer Fallakte*).

Zur Rücknahme einer Einwilligung und der damit verbundenen Schließung einer EFA sind die folgenden Ablaufschritte erforderlich:

1. Der Patient entscheidet sich, die Einwilligung zur Anlage und Nutzung einer Fallakte zurückzunehmen. Er informiert einen der EFA-Teilnehmer über diese Entscheidung.
2. Der Teilnehmer dokumentiert den Patientenwunsch (eine Begründung des Patienten ist nicht erforderlich) und übermittelt eine entsprechende Benachrichtigung an den EFA-Provider.
3. Der EFA-Provider nimmt die Benachrichtigung zur EFA-Schließung entgegen und stößt die erforderlichen Änderungen im Status der Akte und den damit verbundenen Zugriffsberechtigungen an.

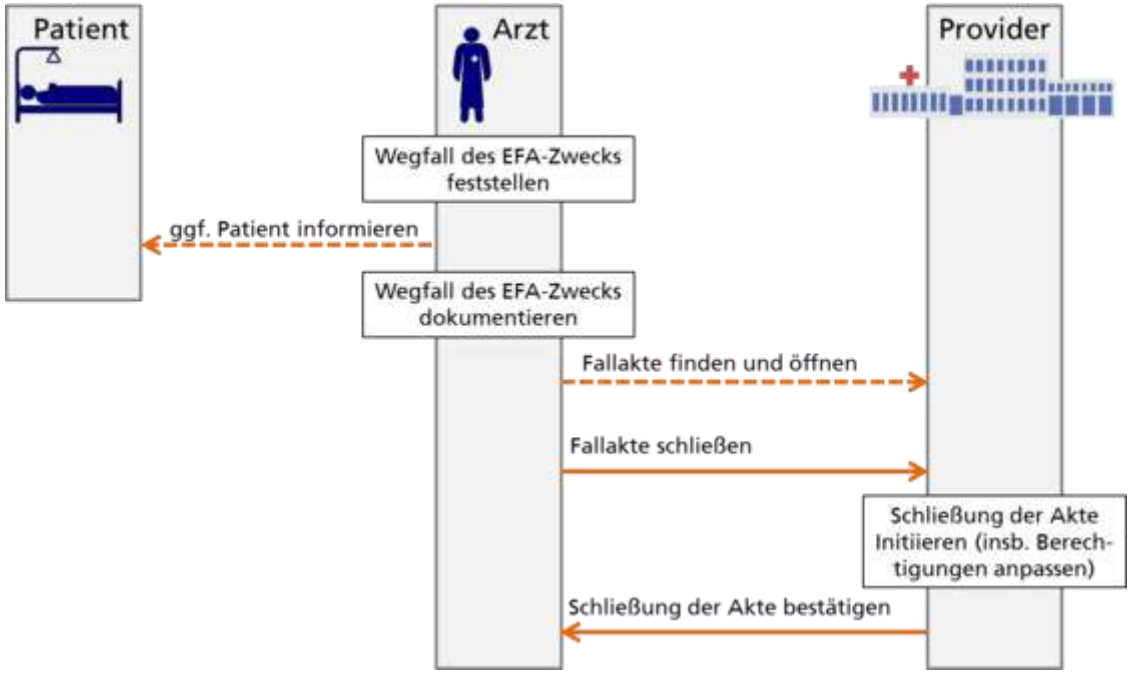


Varianten des Anwendungsszenarios

Wegfall des Zwecks der Akte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01.02.01}

Mit dem Wegfall des Zwecks der Fallakte (z.B. durch Heilung oder Tod des Patienten oder durch gravierende Änderungen in der Diagnose oder der Behandlungsplanung) entfällt auch die an diesen Zweck gebundene Einwilligung. In diesem Fall muss von den beteiligten Leistungserbringern die Schließung der Akte angestoßen werden. Sofern möglich ist der Patient hierüber zu informieren.

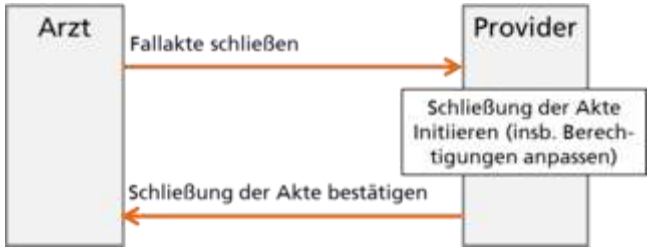


Die IT-gestützten Abläufe dieser Variante sind analog zum Hauptszenario.

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster



Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der zuletzt gegebenen Einwilligung des Patienten nutzbar.
- Der Patient hat den Wunsch zur Rücknahme der Einwilligung gegenüber einem berechtigten Teilnehmer der zu schließenden Akte geäußert.
- Der EFA-Teilnehmer hat den Wunsch des Patienten zur Schließung der Akte schriftlich dokumentiert und sich ggf. vom Patienten unterschreiben lassen.

Funktionalität:

- Entgegennahme der Einwilligungsrücknahme beim EFA-Provider und Dokumentation der Einwilligungsrücknahme in der EFA.
- Schließen der Akte gemäß des Zustandsmodells der EFA.

Nachbedingungen:

- Die Akte wird geschlossen.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Einwilligungsrücknahme dokumentiert und gegenüber dem EFA-Provider angezeigt hat.

Muster **EFA Schließen**

- Bereit gestellte Informationen:
  - Zu schließende Akte (Identifier, etc.)
  - Grund der Schließung ("Patientenwunsch")
- Erforderliche Konfigurationsdaten:
  - EFA Provider

Definition der Interaktionsmuster

Interaktionsmuster: EFA Schließen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01.04.01}

Motivation	Schließen einer bestehenden Fallakte.
Akteure und Rollen	Leistungserbringer (LE) Die Schließung einer bestehenden Fallakte MUSS durch einen berechtigten Leistungserbringer angezeigt werden. EFA-Provider Der EFA-Provider leitet die Schließung der Akte (und aller diese aufspannenden Partitionen) ein und passt die Zugriffsberechtigungen entsprechend an. Ggf. erfolgt eine Information aller Teilnehmer der EFA (nicht Gegenstand der EFA-Spezifikation).
Interaktion	Arzt --> (Aktenidentifikation, Grund der Schließung, [Erklärungen]) --> EFA-Provider
Vorbedingungen	• Die Grundlage zur Führung und Nutzung der Fallakte ist entfallen (z.B. aufgrund einer Rücknahme der Einwilligung durch den Patienten). • Der LE ist autorisierter Teilnehmer der zu schließenden Fallakte. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE hat die zu schließende Akte sicher identifiziert.
Ablauf	1. Der LE übermittelt die Aufforderung zur Schließung der Akte und eine Begründung der Schließung an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der die Akte schließende LE als Teilnehmer an dieser Akte registriert ist. 4. Der EFA-Provider stellt die Begründung zur Schließung der Akte in eine beliebige Partition der Akte ein. 5. Der EFA-Provider ändert den Status der Akte und ihrer Partitionen. 6. Der EFA-Provider passt die Zugriffsberechtigungen der Akte an den neuen Status an. 7. Der EFA-Provider initiiert die weiteren Schritte zur endgültigen Schließung der Akte entlang des definierten Lebenszyklus einer Fallakte.
Eingangsinformationen	Aktenidentifikation Zur Schließung einer Akte müssen Informationen übermittelt werden, die dem EFA-Provider die Identifizierung

	dieser Akte und die Durchsetzung der damit verknüpften Berechtigungen ermöglichen. Grund für die Schließung Der Grund der Schließung (Patientenwunsch, Wegfall des Zwecks, etc.) muss an den EFA-Provider übermittelt und von diesem dokumentiert werden. Erklärungen (optional) Sofern weiter führende Dokumente zur Schließung der Akte elektronisch verfügbar sind, können diese im Sinne einer vollständigen Lebenszylus-Dokumentation noch vor der Schließung in die Akte eingestellt werden.
Nachbedingungen	• Der Prozess zur Schließung der Akte ist beim EFA-Provider angestoßen und wird von diesem ohne weitere Notwendigkeit einer Interaktion mit dem Patienten oder den EFA-Teilnehmern durchgeführt. • Die Zugriffsberechtigungen der Akte sind entsprechend dem veränderten Status der Akte angepasst. • Die Begründung zur Schließung der Akte und ggf. weitere übergebene Dokumente sind für die Archivierung in die EFA eingestellt.
Ausnahmeszenarien	*Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Ccier.01.05}`

Der EFA-Provider leitet die Aufforderung zur Schließung der Akte an alle EFA-Provider weiter, bei denen Partitionen dieser Akte verwaltet werden. Diese leiten die Schließung der bei ihnen verwalteten Partitionen gemäß des Lebenszyklus einer EFA ein.

Jeder dieser Provider stellt das Dokument zur Begründung der Schließung in eine der bei ihm verwalteten Partitionen ein. Ggf. weitere Dokumente werden nur dem EFA-Provider eingestellt, der die Aufforderung zur Schließung entgegen genommen hat. Dieser leitet diese Dokumente auch garnicht erst an die anderen Provider weiter.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

Implementierungsleitfaden ***Interaktionsmuster zum Invalidieren von Daten in einer Fallakte****.*

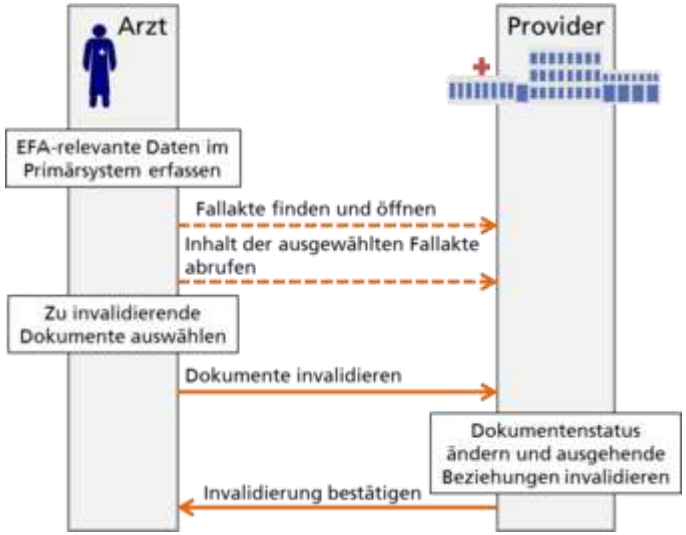
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster zum Invalidieren von Daten in einer Fallakte

Anwendungsszenario: Invalidieren von Daten in einer Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnlio.01.01}



In eine Fallakte eingestellte Daten (siehe Interaktionsmuster Einstellen von Datenobjekten) sind für alle EFA-Teilnehmer sichtbar und abrufbar. Zuweilen kann es passieren, dass ein zuvor in eine EFA eingestelltes Dokument invalidiert werden muss, z.B. da es im Nachhinein als falsch erkannte Informationen enthält oder versehentlich ein falsches Dokument eingestellt wurde (z.B. aufgrund einer intern falsch aufgelösten Patientenidentität).

Das Invalidieren eines Dokuments in einer EFA entfernt dieses Dokument nicht aus der Fallakte, da es ggf. bereits von anderen Teilnehmern abgerufen wurde und daher die Dokumentenreferenz in jedem Fall gültig bleiben muss und das Dokument auch für die Nachvollziehbarkeit der EFA-Nutzung beim Schließen der Akte mitsamt der Akte archiviert werden muss. Statt dessen wird beim Invalidieren der Status des Dokuments so verändert, dass es nur noch für spezielle Rolleninhaber sichtbar ist (z.B. für den Fallaktenmanager). Alle anderen Teilnehmer sehen das Dokument beim Auflisten der EFA-Inhalte nicht mehr und können es daher auch nicht mehr nutzen.

Um Daten zu invalidieren und damit den Dokumentenstatus entsprechend zu ändern sind die folgenden Ablaufschritte erforderlich:

1. Ein Leistungserbringer ist über die Einwilligung des Patienten zur Nutzung einer EFA berechtigt und damit an dieser als Teilnehmer registriert. Diese Einwilligung muss im Vorfeld erteilt worden sein.
2. Der Teilnehmer öffnet die gewünschte Fallakte und listet die enthaltenen Dokumente auf (siehe Interaktionsmuster *Browsing über einer Akte oder Partition*).
3. Der Teilnehmer wählt über sein IT-System das zu invalidierende Dokument aus.

4. Der Teilnehmer sendet eine Nachricht an den EFA-Provider, das ausgewählte Dokument zu invalidieren.

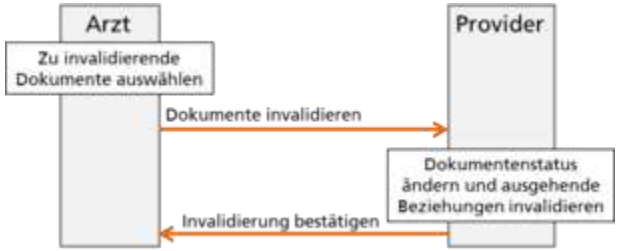
Varianten des Anwendungsszenarios

Aktuell sind keine Varianten definiert

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnlio.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

	Vorbedingungen:
	• Eine Fallakte ist angelegt und gemäß der Einwilligung des Patienten nutzbar.
	• Der Nutzer ist als Teilnehmer an der Fallakte registriert und zum Zugriff auf die Akte berechtigt.
	• Der das Dokument invalidierende Arzt besitzt die Berechtigung, bei einem EFA-Provider Daten in einer Fallakte zu speichern (d.h. Voraussetzungen für eine Auftragsdatenverarbeitung durch den EFA-Provider sind gegeben).
	• Das zu invalidierende Dokument wurde sicher identifiziert.
	• Die fachlichen Gründe für das Invalidieren des Dokuments sind verifiziert und lokal dokumentiert.
	
	Funktionalität:
	• Das identifizierte Dokument wird invalidiert, d.h.
		Muster **Daten invalidieren**
		• Bereit gestellte Informationen:
		  ○ Partition, in der sich das zu invalidierende Dokument befindet
		  ○ Identifier des zu invalidierenden Dokuments
		• Erforderliche Konfigurationsdaten:
		  ○ EFA Provider

in eine Status versetzt, der einen Zugriff nur noch für spezielle Rolleninhaber erlaubt.

Nachbedingungen:

- Mit Ausnahme spezieller Rollen ist das Dokument für EFA-Teilnehmer beim Auflisten der Inhalte einer EFA nicht mehr sichtbar. Dieses gilt auch für an das Dokument geknüpfte Dokumentbeziehungen.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person ein Dokument wann und warum invalidiert hat.

Definition der Interaktionsmuster

Interaktionsmuster: Daten invalidieren

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnlio.01.04.01}

Motivation	Invalidieren eines Dokuments in einer Fallakte.
Akteure und Rollen	Leistungserbringer (LE) Die Invalidierung von Daten in einer bestehenden Fallakte MUSS durch einen Leistungserbringer initiiert werden. Eine explizite Einwilligung durch den Patienten für diese Einzeltransaktion ist nicht erforderlich, da für die Daten alle relevanten Konfigurationsdaten der übergeordneten Fallakte - insbesondere die Zweckbindung und die Berechtigungen - übernommen werden. EFA-Provider Der EFA-Provider nimmt die Invalidierung vor und ändert den Dokumentenstatus entsprechend. Der EFA-Provider stellt sicher, dass Zugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen für die

	übergeordnete Fallakte zugewiesenen Rollen erfolgen können. Der EFA-Provider stellt sicher dass ggf. angegebene Beziehungen zu vorhandenen Dokumenten ebenfalls invalidiert werden.
Interaktion	Arzt --> (Identifikation der Ziel-Partition, Identifikation des zu invalidierenden Dokuments) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die invalidierung des Dokuments sind gegeben und dokumentiert. • Der LE ist autorisierter Teilnehmer der Fallakte, in der sich das zu invalidierende Dokument befindet. • Der die Daten einstellende LE hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-Datenschutzkonzept definierten Vorgaben entspricht. Sofern es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt worden sein. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE hat die Akte und die Partition, der das zu invalidierende Dokument zugeordnet sind, sicher identifiziert. • Der LE hat die zu invalidierenden Dokumente sicher identifiziert und die eindeutigen Objektreferenzen ermittelt.
Ablauf	1. Der LE übermittelt die zur Invalidierung benannter Dokumente erforderlichen Informationen an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der die Daten bereitstellende LE in einem vertraglichen Verhältnis zum EFA-Provider steht, das das Invalidieren von Daten in eine EFA ermöglicht. 4. Der EFA-Provider verifiziert, dass der LE als Teilnehmer an der übergeordnete Akte registriert ist. 5. Der EFA-Provider invalidiert die benannten Dokumente indem er ihren Status entsprechend ändert. 6. Der EFA-Provider invalidiert von den invalidierten Dokumenten ausgehende Dokumentenbeziehungen.
Eingangsinformationen	Identifikation der Ziel-Partition Zur Invalidierung von Dokumenten in einer Partition müssen Angaben zu dieser Partition übermittelt werden, die dem EFA-Provider die Identifizierung dieser Partition und der übergeordneten Akte sowie die Durchsetzung der damit verknüpften Berechtigungen ermöglichen. Identifikation der zu invalidierenden Dokumente Daten, die dem EFA-Provider eine eindeutige Identifizierung der zu invalidierenden Dokumente ermöglichen.
Nachbedingungen	• Der Zustand der benannten Dokumente ist so verändert, dass die Dokumente als invalidiert gelten. • Die invalidierten Dokumente und ihre ausgehenden Dokumentenbeziehungen sind für EFA-Teilnehmer nicht mehr

aubrufbar (Ausnahme: spezielle Nutzerrollen wie z.B. der Fallaktenmanager)

Ausnahmeszenarien *Aktuell sind keine Ausnahmeszenarien definiert*

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnlio.01.05}`

Durch die explizite Benennung der Partition kann der Peer identifiziert werden, auf dem die zu invalidierenden Daten verwaltet werden.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zum Änderung einer Einwilligung**.*

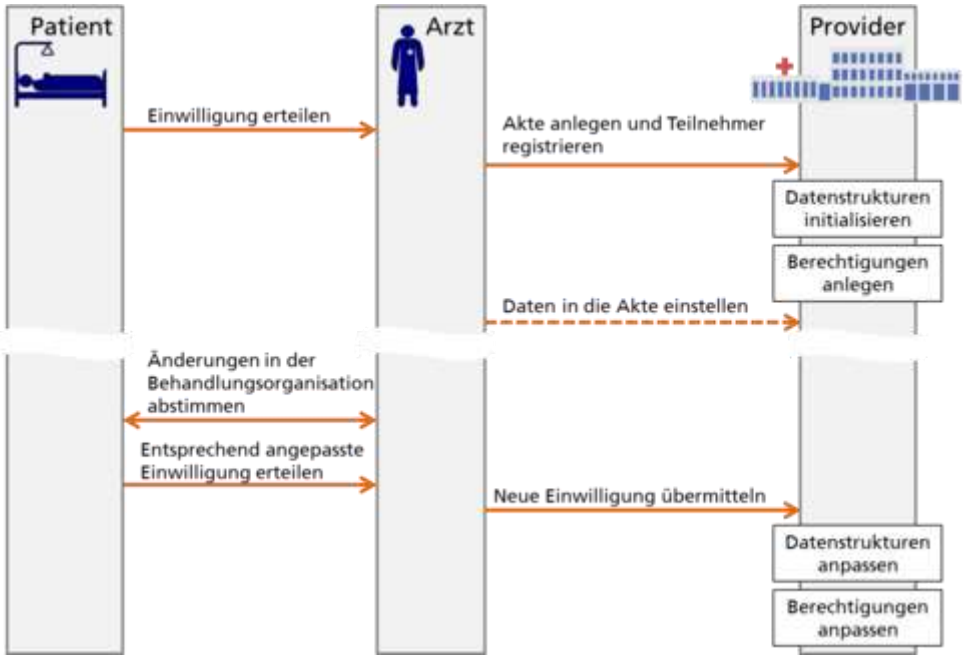
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster zum Anpassen einer EFA

Anwendungsszenario: Anpassen des Teilnehmerkreises

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.01}



In kooperativen Behandlungsszenarien kann von den an der Behandlung teilnehmenden Ärzten eine elektronische Fallakte genutzt werden, um die Effizienz des fall-bezogenen, einrichtungsübergreifenden Datenaustausch zu steigern. Der Teilnehmerkreis der Akte wird vom Patienten bestimmt und entspricht im Normalfall der Gruppe der an der Behandlung teilnehmenden Einrichtungen und Personen. Änderungserfordernisse an der Zusammensetzung des EFA-Teilnehmerkreises können sich ergeben, wenn

- der Patient weitere Leistungserbringer in die Behandlung einbezieht, die einen Zugang zur EFA erhalten sollten
- der Patient einen Arzt auswechselt
- die Behandlungsteilnahme eines Leistungserbringers abgeschlossen ist, bzw. ein neuer Teilnehmer erst in einem fortgeschritteneren Zeitpunkt in die Behandlung einsteigt

Ist eine solche Änderung des Teilnehmerkreises einer EFA erforderlich, gibt des Patient gegenüber einem der teilnehmenden Ärzte eine neue Einwilligung ab, in der der zu berechtigende Teilnehmerkreis benannt ist.

Diese Anpassung einer Fallakte an Änderungen in der Behandlungsorganisation erfolgt in Abstimmung zwischen Patient und behandelndem Arzt und folgt typischerweise dem folgenden Ablauf:

1. Eine Anpassung der Behandlungsorganisation wird erforderlich, da ansonsten die Synchronizität zwischen Behandlungsteilnehmern und EFA-Teilnehmern verloren gehen würde. Dieses Erfordernis wird vom Patienten oder einem der teilnehmenden Ärzte erkannt.
2. Arzt und Patient verständigen sich auf einen dem aktuellen Behandlungsgeschehen optimal angepassten Kreis von behandelnden Ärzten/Einrichtungen.
3. Die getroffenen Vereinbarungen werden in einer Einwilligungserklärung festgehalten. Die Einwilligung wird vom Patienten unterschrieben und an den Arzt übergeben.
4. Sofern die Einwilligung nicht bereits aus einem elektronischen Formular erzeugt worden war, erfasst der Arzt die Daten der Einwilligung in einem elektronischen Formular. Er bestätigt die Richtigkeit der Angaben, die Datenschutzkonformität des Ablaufs der Einwilligungserteilung und das Vorhandensein einer vom Patienten unterschriebenen Kopie.
5. Der Arzt übermittelt die für die Anpassung der Akte erforderlichen Informationen (insb. die neue Liste der zu berechtigenden Behandlungsteilnehme) an den EFA-Provider. Sofern vorliegend, wird auch eine elektronische Kopie der Einwilligung an einen EFA-Provider geschickt.
6. Die Berechtigungen zum Zugriff auf die Akte werden vom EFA-Provider gemäß den Vorgaben der neuen Einwilligungserklärung aufgesetzt.

Es ist zu beachten, dass über dieses Interaktionsmuster ausschließlich EFA-Teilnehmer benannt werden können. Die Belegung der Rolle des Fallaktenmanagers einer EFA kann durch den Patienten nicht geändert werden und ist daher auch über dieses Interaktionsmuster nicht möglich.

Varianten des Anwendungsszenarios

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.02}

Variante: Anpassung der Zweck-Parameter

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.02.01}

Insbesondere wenn die genaue Diagnose vom Patienten benannter Beschwerden schwierig ist und verschiedene Optionen durch unterschiedliche Fachdisziplinen abgeklärt werden müssen, kann die Effizienz dieses Prozesses dadurch erhöht werden, dass eine Fallakte bereits im Rahmen der

Diagnosestellung angelegt und genutzt wird. Eine solche Fallakte wird potenziell zunächst einmal eine recht kurze Laufzeit haben und an einer sehr allgemeinen Beschreibung des "medizinischen Falls" aufgehangen sein.

Soll die Fallakte auch im Rahmen der Behandlung weitergeführt werden, müssen Laufzeit, medizinischer Fall (und alle daran hängenden Konfigurationen) sowie ggf. auch der Kreis der Teilnehmer an die neue Behandlungssituation angepasst werden. Hierzu ist auch eine neue Einwilligung des Patienten erforderlich.

Variante: Verlängerung der Gültigkeit

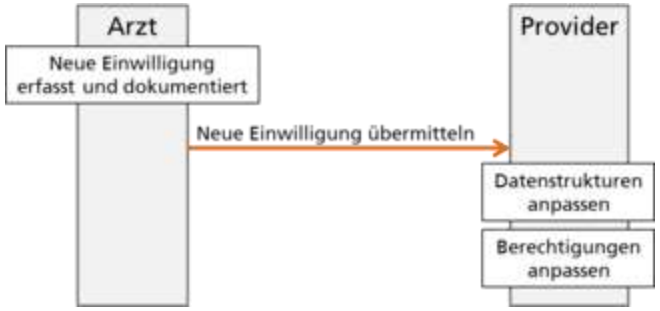
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.02.02}

Bei Neuanlage einer Fallakte wird diese mit einer Gültigkeitsdauer versehen. Mit Ablauf der Gültigkeit werden die bisherige Aktennutzung und die zukünftigen Kommunikationserfordernisse bewertet. Je nach Ergebnis kann dies zur Schließung der Akte mit Ablauf der Gültigkeit oder zu einer Verlängerung der Gültigkeit (ggf. mit Anpassungen an der Aktenkonfiguration) führen.

Soll die Fallakte im Rahmen der Behandlung weitergeführt werden, muss die Gültigkeitsdauer verlängert werden. Hierzu ist auch eine neue Einwilligung des Patienten erforderlich.

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster
	Vorbedingungen: • Eine Fallakte ist angelegt und gemäß der zuletzt gegebenen Einwilligung des Patienten nutzbar. • Ein Anpassung des Teilnehmerkreises, der Konkretisierung des Zwecks oder der	Muster **Fallakte anpassen** • Bereit gestellte Informationen: o zu anzupassende Akte (identifizierende Daten) o angepasster Zweck der Akte o angepasster Teilnehmerkreis der Akte (identifizierende Daten,

Gültigkeit der Fallakte ist erforderlich und zwischen EFA-Teilnehmer und Patient abgestimmt.
- Der EFA-Teilnehmer hat die Absprachen zur Anpassung der Akte schriftlich dokumentiert.
- Ggf. neu in die Behandlung einsteigende Ärzte und Einrichtungen sind identifiziert.
- Eine neue Einwilligung wird anhand der Absprachen erstellt und vom Patienten unterschrieben.

Funktionalität:

- Die neue Einwilligung wird an den EFA-Provider übermittelt.
- Der EFA-Provider richtet die Konfiguration der bestehenden Akte anhand der Einwilligung komplett neu ein.

Nachbedingungen:

- Die Fallakte ist an die neue Behandlungsorganisation angepasst und kann von den EFA-Teilnehmern genutzt werden.
- Sofern elektronisch verfügbar, ist die neue Einwilligung als Dokument aus der Akte abrufbar.

Rollen bzw. Autorisierungen)
    - angepasste Gültigkeit der Akte
    - elektronisches Einwilligungsdokument oder Bestätigung des Arztes, dass eine solche Einwilligung vorliegt
- Erforderliche Konfigurationsdaten:
    - EFA Provider

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Akte auf welcher Basis und wie geändert hat hat.

Definition der Interaktionsmuster

Interaktionsmuster: Fallakte anpassen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.04.01}

Motivation	Anpassen einer Fallakte an eine veränderte Behandlungsorganisation/-situation
Akteure und Rollen	Leistungserbringer (LE) Die Anpassung einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Basis der von Leistungserbringer angeforderten Konfigurationsänderung ist üblicherweise eine informierte, schriftliche Einwilligung des Betroffenen. EFA-Provider Der EFA-Provider passt eine bestehende Akte gemäß der vom LE vorgegebenen Konfiguration an. Der EFA-Provider stellt sicher, dass Aktenzugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen zugewiesenen Rollen erfolgen können.
Interaktion	Arzt --> (Aktenidentifikation, [Zweck der Akte], [Gültigkeit], [EFA-Teilnehmer], [Einwilligungsformular]) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die Anpassung einer EFA an eine veränderte Behandlungsorganisation und/oder -situation sind gegeben. Insbesondere sind Zweck, Teilnehmerkreis und Gültigkeit aus der Behandlungsorganisation ableitbar und konkret benennbar. • Der die Akte anpassende LE hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-Datenschutzkonzept definierten Vorgaben entspricht. Sofern es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt werden. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig

ihre Identität und Authentizität verifizieren.
- Der LE hat den Patienten und die anzupassende Akte sicher identifiziert.

Ablauf

1. Der LE übermittelt die zur Anpassung der Fallakte erforderlichen Informationen an den EFA-Provider.
2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit.
3. Der EFA-Provider passt für die angegebene Fallakte Zweck und Gültigkeitsdauer an.
4. Der EFA-Provider setzt die Berechtigungen der Fallakte analog zu den Rollen der benannten EFA-Teilnehmer. Die zuvor definierten Berechtigungen verlieren damit sämtlich ihre Gültigkeit.
5. Sofern im Rahmen der EFA-Anpassung eine elektronische Kopie des Einwilligungsformulars übermittelt wurde, wird dieses in einer beliebigen Partition der Fallakte abgelegt.

Eingangsinformationen

Patientenidentifikation
: Zur Anlage einer Fallakte müssen Angaben zum Patienten übergeben werden, die auch anderen EFA-Teilnehmern die (1) Identifikation des Patienten, (2) die Prüfung der Zuordnung der Akte zum Patienten und (3)das Auffinden der Fallakte anhand von Identitätsinformationen zum Patienten ermöglichen.

Zweck (optional)
: Der Zweck der Nutzung der Fallakte muss möglichst konkret angegeben werden. Wird kein Zweck angegeben, gilt der bestehende Zweck fort.

Gültigkeit (optional)
: Für die Fallakte kann die maximale Gültigkeitsdauer verändert werden. Diese darf einen beim Provider vorgegebenen Maximalwert nicht überschreiten. Wenn keine Gültigkeitsdauer angegeben ist, gilt die bestehende Gültigkeitsdauer fort.

EFA-Teilnehmer (optional)
: Zu jedem Teilnehmer sind identifizierende Daten sowie die Rolle im Rahmen der der Fallakte zugrunde liegenden Behandlung anzugeben. Die identifizierenden Daten müssen geeignet sein, einen authentisierten EFA-Nutzer zuverlässig als EFA-Teilnehmer zu identifizieren. Sofern die genutzten Identitätsdaten keinen Abruf von Informationen zu Name, Adresse etc. des Berechtigten erlauben (bzw. entsprechende Verzeichnisse nicht verfügbar sind), müssen zusätzlich zu jedem EFA-Teilnehmer Daten bereit gestellt werden, die dem Patienten und anderen EFA-Teilnehmern eine Identifizierung dieses Teilnehmers anhand von Name und Anschrift erlauben. Wenn bei der Anpassung der EFA keine EFA-Teilnehmer benannt werden, gelten die bestehenden Berechtigungen fort.

Einwilligungsformular (optional)

	Eine elektronische Kopie der Einwilligungsformulars kann bei der Anpassung der Akte übergeben werden. Dieses wird als Dokument in der Akte abgelegt. Der die Aktenanpassung initiierende LE stellt sicher, dass die zur Konfiguration der EFA genutzten Angaben zum Patienten und zu den EFA-Teilnehmern mit den vom Patienten im Rahmen der Einwilligung gemachten Vorgaben übereinstimmen.
Nachbedingungen	• Die Fallakte ist angepasst und für berechtigte EFA-Teilnehmer eindeutig adressierbar. Berechtigte Teilnehmer können Daten in die Akte einstellen und aus dieser auslesen. • Die Fallakte ist mit einem Patienten und einem Zweck verknüpft. Beide Angaben sind für berechtigte Teilnehmer - und nur für berechtigte Teilnehmer - einsehbar. • An die Fallakte sind Berechtigungen gebunden, die einen Zugriff auf registriert und autorisierte EFA-Teilnehmer beschränken. • Sofern eine elektronische Kopie der Einwilligung bei der EFA-Anlage übergeben wurde, ist diese als Dokument in der Fallakte abrufbar.

Ausnahmeszenarien	• Für den Patienten besteht bei dem angesprochenen EFA-Provider bereits eine Fallakte zu dem neu angegebenen Zweck.
	  ○ Sofern die Einwilligung den expliziten Zusatz enthält, dass mit der Akte eine ggf. bereits zu dem angegebenen Zweck angelegte Akte in die neue Akte überführt werden kann, werden die Partitionen der bestehenden Akte mit der neuen Akte verknüpft. Die neu abgegebene Einwilligung ersetzt alle zuvor abgegebenen Einwilligungen.
	  ○ Sofern die Einwilligung keinen solchen Zusatz enthält, wird die Operation mit einer Fehlermeldung abgebrochen.
	• Für den Patienten besteht bereits bei einem anderen als dem angesprochenen EFA-Provider eine Fallakte zu dem neu angegebenen Zweck.
	  ○ Die Akte wird gemäß des Standardablaufs beim angesprochenen Provider angepasst.
	  ○ Ein auf beiden Akten berechtigter Teilnehmer muss über das Muster "Zusammenführen von Fallakten" die Einwilligung des Patienten zur Zusammenführung der beiden Akten einholen und die Zusammenführung der Akten initiieren.

Peer-to-Peer Semantik

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Cnssi.01.05}

Sofern ein EFA-Teilnehmer selber auch als EFA-Provider agiert und eine Partition der Akte bei diesem Provider besteht, wird die Anpassung einer Fallakte von diesem Teilnehmer bevorzugt über diesen "eigenen" Provider ausgelöst.

Ansonsten kann die Anpassung der Fallakte über jeden Provider angestoßen werden, bei dem eine Partition der zu verändernden Akte angelegt ist. Der Provider ist verpflichtet, die neuen Konfigurationsdaten der Akte (Zweck, Gültigkeit, Teilnehmer) sowie die ggf. übermittelte Einwilligung an alle EFA-Peers weiter zu reichen, bei denen ebenfalls Partitionen zu der betroffenen Akte angelegt sind.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Interaktionsmuster zur Autorisierung eines weiteren EFA-Teilnehmers**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Interaktionsmuster zur Autorisierung eines weiteren Teilnehmers

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01}`

In kooperativen Behandlungsszenarien kann von den an der Behandlung teilnehmenden Ärzten eine elektronische Fallakte genutzt werden, um die Effizienz des fall-bezogenen, einrichtungsübergreifenden Datenaustausch zu steigern. Der Teilnehmerkreis der Akte wird vom Patienten bestimmt

und entspricht im Normalfall der Gruppe der an der Behandlung teilnehmenden Einrichtungen und Personen. Diese werden in der Einwilligung des Patienten benannt und im EFA-Berechtigungssystem mit ihren jeweiligen Rollen entsprechenden Zugriffsrechten versehen.

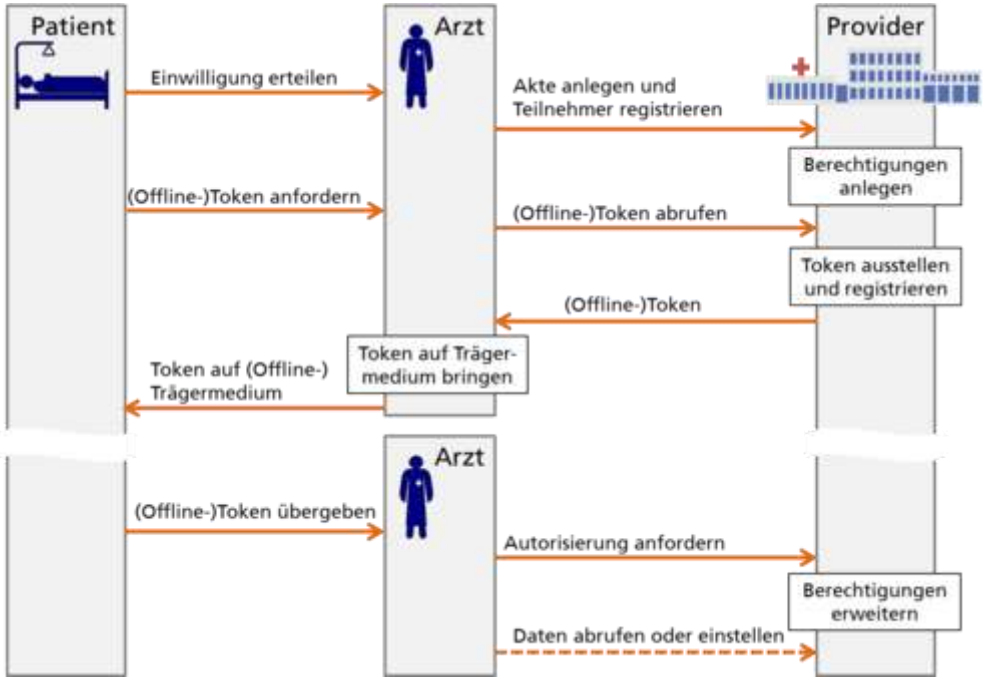
Änderungserfordernisse an der Zusammensetzung des EFA-Teilnehmerkreises können sich ergeben, wenn der Patient weitere Leistungserbringer in die Behandlung einbezieht, die einen Zugang zur EFA erhalten sollten. Hierzu bestehen grundsätzlich drei Optionen:

1. Der Patient gibt gegenüber einem berechtigten Leistungserbringer eine neue Einwilligungserklärung ab
2. Der Patient beauftragt einen berechtigten Leistungserbringer, eine bestehende Einwilligung um einen einzelnen, identifizierten Leistungserbringer (Arzt oder Einrichtung) zu erweitern
3. Der Patient hat (z.B. bei der Anlage der EFA) ein oder mehrere Offline-Token erhalten. Durch Übergabe eines solchen Tokens an einen Leistungserbringer wird diesem eine Berechtigung zur Nutzung der EFA eingerichtet.

Die ersten beiden Optionen werden im Interaktionsmuster zur Änderung einer Einwiligung beschrieben. Die dritte Option wird durch das auf dieser Seite definierte Interaktionsmuster abgedeckt.

Anwendungsszenario: Offline-Token

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.01}



Diese Erweiterung des Nutzerkreises einer Fallakte über ein Offline-Token folgt typischerweise dem folgenden Ablauf:

1. Der Patient fordert bei einem zum Aktenzugriff berechtigten Arzt (z.B. im Zuge der Anlage der Fallakte) ein Offline-Token an.
2. Ein zum Aktenzugriff berechtigter Arzt fordert ein Berechtigungstoken beim EFA-Provider an. Der EFA-Provider stellt das Token in digitaler Form aus und sendet es an den Arzt.
3. Der Arzt bringt das Berechtigungstoken auf ein geeignetes Trägermedium (z.B. als Barcode auf Papier) und übergibt es an den Patienten.
4. Der Patient möchte einen weiteren Arzt zu der EFA hinzuziehen und übergibt ihm ein dazu geeignetes Offline-Token.
5. Der zu berechtigende Arzt liest das Offline-Token ein.
6. Der zu berechtigende Arzt über mittelt Angaben zu seiner Identität sowie die Inhalte des Offline-Tokens an den EFA-Provider.
7. Die Berechtigungen zum Zugriff auf die Akte werden vom EFA-Provider gemäß den Vorgaben im Offline-Token auf den neuen Teilnehmer ausgeweitet.

Es ist zu beachten, dass über dieses Interaktionsmuster ausschließlich weitere EFA-Teilnehmer benannt werden können. Die Belegung der Rolle des Fallaktenmanagers einer EFA kann durch den Patienten nicht geändert werden und ist daher auch über dieses Interaktionsmuster nicht möglich.

Varianten des Anwendungsszenarios

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.02}

Variante: Online-Token

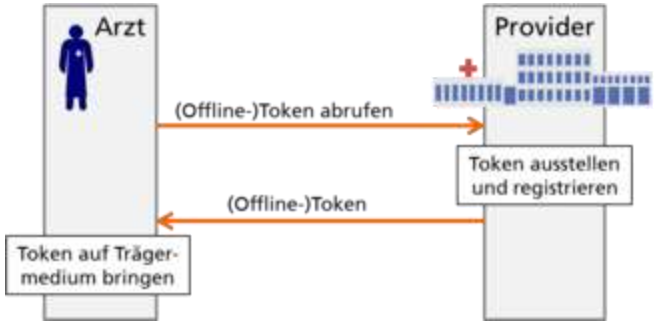
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.02.01}

Das zur Berechtigungserweiterung genutzte Token muss nicht zwingend auf Papier und über den Patienten übermittelt werden. Ebenso sind elektronische Umsetzungen denkbar, die dem neu zu berechtigenden Arzt vom Patienten oder einem bereits berechtigten Arzt über eine sichere Kommunikationsverbindung übermittelt werden. Hierzu kann beispielsweise das KOM-LE Protokoll oder eine ePA-291a genutzt werden.

Abbildung der Szenarien und Varianten auf Interaktionsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.03}

Interaktion	Funktionalität, Vorbedingungen, Nachbedingungen	Muster

	Vorbedingungen:
	• Eine Fallakte ist angelegt und gemäß der zuletzt gegebenen Einwilligung des Patienten nutzbar.
	• Der Arzt hat sich gegenüber seinem EFA-Provider identifiziert und authentifiziert und hat Zugriff auf die Fallakte, zu der ein Berechtigungstoken angefordert
		Muster **Token ausstellen**
		• Bereit gestellte Informationen:
		  ○ Akte, zu der ein Berechtigungstoken ausgestellt werden soll (identifizierende Daten)
		• Erforderliche Konfigurationsdaten:
		  ○ EFA Provider

wird.

Funktionalität:

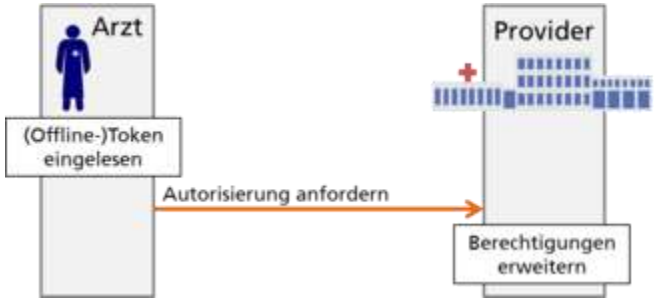
- Der Arzt fordert vom EFA-Provider ein Berechtigungstoken für eine bestehenden Fallakte an.
- Der EFA-Provider stellt ein digitales Token aus und registriert dieses.
- Der EFA-Provider übermittelt das digitale Token an den aufrufenden Arzt.
- Der Arzt bringt das Token auf ein geeignetes Trägermedium auf und übergibt es dem Patienten.

Nachbedingungen:

- Ein Berechtigungstoken ist beim EFA-Provider registriert und für den Patienten verfügbar.

Verpflichtungen:

- Es ist nachvollziehbar, welche Person wann ein Berechtigungstoken für welche Akte angefordert hat.



Vorbedingungen:

- Eine Fallakte ist angelegt und gemäß der zuletzt gegebenen Einwilligung des Patienten nutzbar.
- Dem zusätzlich zu berechtigenden Arzt wurde ein Token zur Berechtigungserweiterung übergeben (offline oder online).
- Der Arzt hat sich gegenüber seinem EFA-Provider identifiziert und wurde von diesem erfolgreich authentifiziert.

Funktionalität:

- Die Identitätsdaten des Arztes und der Inhalt des Berechtigungstokens werden an den EFA-Provider übermittelt.
- Der EFA-Provider legt zu der bestehenden Akte eine weitere Berechtigung an.

Nachbedingungen:

- Die Fallakte ist an die neue Behandlungsorganisation angepasst und kann von dem neuen EFA-Teilnehmer genutzt werden.

Muster **Teilnehmer per Token autorisieren**

- Bereit gestellte Informationen:
  - Akte, zu der der Leistungserbringer Zugang erhalten soll (identifizierende Daten)
  - identifizierende Daten des zu berechtigenden Leistungserbringers
  - Berechtigungstoken (Authentizitätsnachweis, einzurichtende Rolle)
- Erforderliche Konfigurationsdaten:
  - EFA Provider

Verpflichtungen:

- Es ist nachvollziehbar, welche Person die Berechtigungen zum Aktenzugriff wann und wie geändert hat hat.

Definition der Interaktionsmuster

Interaktionsmuster: Token ausstellen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.04.01}

Motivation	Autorisierung eines zusätzlichen Leistungserbringers zur Nutzung einer EFA
Akteure und Rollen	Leistungserbringer (LE) Das Ausstellen eines Berechtigungstokens für eine bestehende Fallakte MUSS durch einen Leistungserbringer initiiert werden. Der Leistungserbringer muss ein über die Einwilligung des Patienten berechtigter Teilnehmer dieser Fallakte sein. EFA-Provider Der EFA-Provider stellt das Berechtigungstoken aus. Der EFA-Provider stellt sicher, dass nur berechtigte Leistungserbringer Berechtigungstoken anfordern können. Er stellt sicher, dass nur Leistungserbringer über das Token autorisiert werden können.
Interaktion	Arzt --> (Anforderung Berechtigungstoken) --> EFA-Provider EFA-Provider --> (Berechtigungstoken) --> Arzt
Vorbedingungen	• Die fachlichen Voraussetzungen für die Einbeziehung weiterer Leistungserbringer in die Behandlungsorganisation und/oder -situation sind gegeben. • Der Leistungserbringer wurde vom Patienten per Einwilligung zur Teilnahme an der Fallakte berechtigt. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig

	ihre Identität und Authentizität verifizieren. • Der LE hat den Patienten und die Akte sicher identifiziert und abgeglichen, die Akte dem Patienten zugeordnet ist.
Ablauf	1. Der LE übermittelt eine Anfrage nach einem Berechtigungstoken an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider verifiziert, dass der Anfragende die Berechtigung zum Erhalt eines Berechtigungstoken besitzt. 4. Der EFA-Provider erstellt ein Berechtigungstoken und legt intern alle Datenstrukturen an, über die ein späteres Einreichen des Tokens geprüft und nachvollziehbar dokumentiert werden können. Alle zuvor definierten Berechtigungen behalten dabei ihre Gültigkeit. 5. Der EFA-Provider sendet das Token in digitaler Form an den anfragenden Leistungserbringer.
Eingangsinformationen	Verweis auf die anzupassende Akte (identifizierende Daten) Der Aktenverweis muss die eindeutige Identifizierung der Akte erlauben, zu der ein Berechtigungstoken ausgestellt werden soll.
Nachbedingungen	• Ein Berechtigungstoken wurde ausgestellt.
Ausnahmeszenarien	-

Interaktionsmuster: Teilnehmer per Token autorisieren

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.04.02}

Motivation	Autorisierung eines zusätzlichen Leistungserbringers zur Nutzung einer EFA
Akteure und Rollen	Leistungserbringer (LE) Die Erweiterung der Berechtigungen auf einer Fallakte MUSS durch einen Leistungserbringer initiiert werden. Basis der von Leistungserbringer angeforderten Berechtigungserweiterung ist ein für den Patienten ausgestelltes Berechtigungstoken. EFA-Provider Der EFA-Provider erweitert die Berechtigungen einer bestehende Akte gemäß der im Berechtigungstoken kodierten Angaben. Der EFA-Provider stellt sicher, dass Aktenzugriffe nur durch autorisierte EFA-Teilnehmer im Rahmen der diesen zugewiesenen Rollen erfolgen können.

Interaktion	Arzt --> (Berechtigungstoken) --> EFA-Provider
Vorbedingungen	• Die fachlichen Voraussetzungen für die Einbeziehung des neu zu berechtigenden Arztes in die Behandlungsorganisation und/oder -situation sind gegeben. Die Hinzuziehung des Arztes erfolgt auf expliziten Wunsch des Patienten, was durch die eigenhändige Übergabe des Berechtigungstokens ausgedrückt wird. • Der neu in die EFA-Nutzung einsteigende Leistungserbringer hat mit dem EFA-Provider eine Vereinbarung geschlossen, die den im EFA-Datenschutzkonzept definierten Vorgaben entspricht. Sofern der Arzt auch Daten in die Akte einstellen können soll und es sich hierbei um eine Datenverarbeitung im Auftrag handelt, muss eine entsprechende Zustimmung des Betroffenen eingeholt werden. • Der LE kann eine sichere Kommunikation mit dem EFA-Provider aufbauen. Beide Akteure können wechselseitig ihre Identität und Authentizität verifizieren. • Der LE hat den Patienten sicher identifiziert und abgeglichen, dass das eingereichte Token dem Patienten zugeordnet ist.
Ablauf	1. Der LE übermittelt das Berechtigungstoken an den EFA-Provider. 2. Der EFA-Provider nimmt die Anfrage entgegen und verifiziert deren Vollständigkeit und Korrektheit. 3. Der EFA-Provider erweitert die Berechtigungen der Fallakte analog zu den Angaben im Berechtigungstoken um den das Token einreichenden Leistungserbringer. Alle zuvor definierten Berechtigungen behalten dabei ihre Gültigkeit.
Eingangsinformationen	Neuer EFA-Teilnehmer (in-band) Die identifizierenden Daten müssen geeignet sein, einen authentisierten EFA-Nutzer zuverlässig als EFA-Teilnehmer zu identifizieren. Sofern die genutzten Identitätsdaten keinen Abruf von Informationen zu Name, Adresse etc. des Berechtigten erlauben (bzw. entsprechende Verzeichnisse nicht verfügbar sind), müssen zusätzlich zu jedem EFA-Teilnehmer Daten bereit gestellt werden, die dem Patienten und anderen EFA-Teilnehmern eine Identifizierung dieses Teilnehmers anhand von Name und Anschrift erlauben. Berechtigungstoken Das Berechtigungstoken enthält einen Verweis auf die Akte, deren Berechtigtenkreis erweitert wird. Zusätzlich können weitere Kontroll- und Konfigurationsdaten enthalten sein.
Nachbedingungen	• Die Berechtigungen auf der Fallakte sind angepasst. Der berechtigte EFA-Teilnehmer kann die Akte eindeutig adressieren sowie Daten in die Akte einstellen und aus dieser auslesen.

Ausnahmeszenarien	• Der Leistungserbringer ist bereits zum Zugriff auf die Akte berechtigt.
	  ◦ Die Operation wird mit einer Fehlermeldung abgebrochen.
	• Die Akte wurde bereits geschlossen.
	  ◦ Die Operation wird mit einer Fehlermeldung abgebrochen.

Peer-to-Peer Semantik

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {CAoug.01.05}`

Sofern ein EFA-Teilnehmer selber auch als EFA-Provider agiert und eine Partition der Akte bei diesem Provider besteht, wird die Anlage einer Berechtigung über diesen "eigenen" Provider ausgelöst.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

cdaefa:CIM Zusammenführen von Fallakten

Logical Perspective - Enterprise Dimension

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Sicherheitsanforderungen**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht.

Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Identifizierung und Authentifizierung von EFA-Teilnehmern

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.01}`

Anforderungen

- Die Identität jedes zugriffsanfragenden Leitungserbringers muss vorab ausreichend sicher authentisiert werden. Die Zusicherung bezüglich der korrekten Identifizierung des Leistungserbringer (und der Stärke des vollzogenen Authentisierungsverfahrens) muss durch den ausstellenden Dienst attestierbar und kommunizierbar gestaltet werden.
- Der austellende Dienst muss neben der Zuweisung der Identität und der Zusicherung über die korrekte Authentisierung des Leistungserbringers auch zusätzliche Attribute liefern, die der datenhaltenden Stelle ermöglichen, informierte und korrekte Zugriffsentscheidungen zu treffen. Der ausstellende Dienst ist zur Bereitstellung der folgenden Informationen verpflichtet:
  - die eindeutige und korrekte Korrelation (Behandlungskontext) zwischen Patient, Daten und die Kombination Leistungserbringer + Organisation ausschließlich anhand der gelieferten Informationen zu ermöglichen
  - Kontextinfomationen über die Natur des Zugriffs zu liefern (Stärke des Authentisierungsverfahrens, Zugriffsart etc.)
  - den ausstellenden und ggf. haftenden Dienst eindeutig und für die datenhaltende Stelle dokumentierbar zu benennen
- Die Identitätsinformationen, inklusive eventuell benötigter zugewiesener Attribute, müssen "in-band", d. h. innerhalb der zu tätigenden Transaktion, übermittelt werden.
- Die datenhaltende Stelle ist verpflichtet, die innerhalb der Transaktion übermittelten Identitätsinformationen vor jeder Datenverarbeitung oder -offenbarung detailliert zu prüfen. Dabei ist es auch zwingend notwendig, neben der Gültigkeit der Identität und der Zusicherung über deren korrekte Zuweisung, auch Kontextinformationen wie beispielsweise die Stärke der Authentisierungsverfahren oder die Stabilität des Vertrauensverhältnis zum austellenden Dienst zu bewerten.
- Der behandelnde Leistungserbringer ist zur korrekten Identifikation und Authentisierung des Patienten verpflichtet. Dies kann in Ermangelung von geeigneten technischen Verfahren ggf. organisatorisch ablaufen und ist mit den durch die Stammdaten und Einwilligungserklärung zugänglichen Identifikationsmerkmalen zu vergleichen.

Autorisierung von EFA-Teilnehmern

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.02}

Anforderungen

- Die fundamentale Erlaubnis, personenbezogene und/oder medizinische Daten eines Patienten zu verarbeiten wird durch die Einwilligungserklärung des Patienten erteilt. Sollte zum Zeitpunkt der Zugriffsanfrage keine gültige Patienteneinwilligung vorliegen und der behandelnde Leistungserbringer nicht vorab berechtigt sein, so ist einen neue Patienteneinwilligung nach dem EFA-üblichen Muster zu erstellen.
- Jegliche legitime Datenverarbeitungen durch die EFA sind durch den Patienten motiviert und müssen ausnahmslos fallbezogen und zum Ziel der Behandlung des Patienten durch einen vorab benannten Leistungserbringer vollzogen werden.
- Die datenverarbeitende Stelle bürgt für die korrekte Identifikation und Authentisierung des Patienten, ggf. auch durch organisatorische Maßnahmen.
- Sowohl die datenverarbeitende Stelle als auch die -haltende Stelle müssen jederzeit in der Lage sein, (Geschäfts-)Rollen und Funktionen geeignet technisch abzubilden und überprüfbar zu kommunizieren.
    - Die Entscheidung unter welcher qualifizierten Rolle der Zugreifende eine Datenoffenbarung erfragt, obliegt der anfragenden Stelle.
    - Die qualifizierte Rolle des Berufstätigen mit qualifizierter Ausbildung (professional role) ist so spezifisch zu fassen, wie es der technische Rahmen und der aktuelle Zugriffskontext zulässt (least privilege).
- Die Entscheidung über die Freigabe der Datenoffenabrung auf Basis der durch die anfragende Stelle gelieferten Informationen obliegt stets der datenhaltenden Stelle.
    - Die Freigabe einer Datenoffenbarung durch die datenhaltende Stelle ist stets erst nach der vollständigen Auswertung aller verfügbarer und durch die datenverarbeitende Stelle gelieferter Informationen und der Anwendung der lokalen Sicherheitsrichtlinie zu entscheiden. Dabei verursachen eventuelle Negativindikatoren zwingend eine negative Zugriffsentscheidung und unterbinden die erfragte Datenoffenbarung.
    - Die datenhaltende Stelle ist dazu verpflichtet eine Datenoffenbarung abzulehnen, wenn die durch die datenverarebitende Stelle gelieferte qualifizierte Rolle nicht dem ausdrücklichen Patientenwunsch innerhalb der Einwilligungserklärung entspricht oder dem durch den aktuellen Behandlungskontext gerechtfertigten Zugriffsnotwendigkeiten widerspricht.
    - Die datenhaltende Stelle ist jederzeit berechtigt und üblicherweise auch dazu verpflichtet, eine Datenoffenbarung abzulehnen, wenn die durch die datenverarbeitende Stelle gelieferte qualifizierte Rolle gemäß der lokalen Sicherheitsrichtlinie ungeeignet ausgestaltet ist.

- Eventuelle Nebenabsprachen zwischen EFA-Partnern, die eine Datenoffenbarung innerhalb vorab definierten Sonderszenarien oder unter besonderen Umständen legitimieren, sind dem Patienten in dessen Einwilligungserklärung vorab mitzuteilen und zu erklären. Sollten die Nebenabsprachen eine den üblichen EFA-Rahmen übersteigene Datenoffenbarung legitimieren oder zusätzliche Informationen zur Erfüllung von Datenanfragen benötigen, so sind auch alle betroffenen EFA-Partner zu informieren.

Vertraulichkeit

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.03}

Anforderungen

- Personenbezogene und/oder medizinische Informationen dürfen ohne vorherige Einwilliung des Patienten keinesfalls gegenüber Dritten offenbart werden, sofern die Offenbarung nicht durch eine vorrangige Rechtsvorschrift vorgeschrieben ist oder es sich um einen geduldeten gesetzlichen Bruch handelt (wie beispielsweise einen Notfallzugriff bei Gefahr für Leib und Leben des Patienten).
- Personenbezogene und/oder medizinische Informationen innerhalb der EFA dürfen ausschließlich an (medizinische) Leistungserbringer und deren benannte Auftragsdatenverarbeiter im Rahmen der Behandlung offenbart werden.
- Personenbezogene und/oder medizinische Informationen dürfen ausschließlich den explizit als berechtigt benannten Stellen offenbart werden. Sollten vorrangige Rechtsvorschriften bestehen, die eine weitere Offenbarung gegenüber Dritten anordenen, so sollte der Patient möglichst über die Grundlage, Art und den Umfang dieser vorgeschriebenen Offenbarung vorab informiert werden.
- Die legitime Verarbeitung von personenbezogene und/oder medizinische Informationen muss lückenlos über den kompletten Lebenszyklus der Fallakte durch den Einsatz geeigneter technischer, organisatorischer und rechtlicher Mittel sichergestellt werden. Der angemessene Einsatz dieser Mittel und die korrekte Umsetzung der Patientenwünsche (dokumentiert in der Patienteneinwilligung) müssen für den Patienten sowie Stellen mit datenschutzrechtlichen Kontrollaufgaben jederzeit und freimütig nachvollziehbar und überprüfbar sein.
- Die zur Übertragung und Speicherung von Daten einer Fallakte benötigten personenbezogenen und/oder medizinische Informationen (beispielsweise innerhalb von Metadaten) sind auf das zwingend notwendige Minimum zu beschränken. Eventuell für Nicht-Berechtigte (d.h. nicht durch den Patienten autorisierte Personen/Einrichtungen) zugängliche Metadaten sind idealerweise so zu gestalten, dass sie keine Rückschlüsse auf die Inhalte der in der Fallakte verwalteten personenbezogenen und/oder medizinische Informationen zulassen. Insbesondere soll kein Bezug zwischen einem für Nicht-Berechtigte identifizierbaren Patienten und einer Erkrankung in den Metadaten kodiert sein.
- Personenbezogene und/oder medizinische Informationen die durch die EFA ausgetauscht werden, müssen stets durch den ursprünglich vereinbarten Zweck gebunden bleiben. Eine eventuelle Neu-Klassifizierung der personenbezogenen und/oder medizinische Informationen muss ausschließlich medizinisch und fallbezogen gerechtfertigt werden und eine zweckfremde Nachnutzung ausschließen.

EFA Secure Channels

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.03.01}

- Die datenhaltende Stelle muss die Kommunikationsendpunkte der am Datenaustausch beteiligten technischen Kommunikationspartner vor jeder Datenoffenbarung gegenseitig authentisieren (Mutual Node Authentication).
- Alle beteiligten Kommunikationspartner müssen besonders abgesicherte, dokumentierbare und zuverlässige technische Verfahren zum einvernehmlichen Datenaustausch einsetzten (Reliable Messaging).
- Spezielle Anforderungen bestehen für alle Kommunikationsprozesse, in denen sich die Daten nicht in der direkten/alleinigen Obhut einer durch den autorisierten Leistungserbinger oder den Patienten kontrollierte Stelle befinden. Hier sind geeignete Maßnahmen zur Herstellung eines vertraulichen Transportkanals zwischen den Kommunikationsendpunkten dieser Datenaustausch-Prozesse umzusetzen:
    - Die innerhalb der EFA durchgeführten Kommunikationsprozesse müssen durch geeignete technische Mittel durchgängig unbelauschbar gestaltet werden.
    - Die innerhalb der EFA durchgeführten Kommunikationsprozesse müssen durch geeignete technische Mittel von anderem Datenverkehr durchgängig isoliert werden.
    - Die innerhalb der EFA durchgeführten Kommunikationsprozesse müssen durch geeignete technische Mittel davor bewahrt werden, Rückschlüsse über die Natur, den Inhalt oder die Betroffenen der Datenübertragung anhand sekundärer Identifikationsmerkmale oder Metadaten der genutzten Kommunikationsmittel zu ermöglichen.

Authentizität und Integrität von EFA Daten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.04}

Anforderungen

- Jeder durch eine EFA vollzogene Datenaustausch muss gesicherte Informationen über die:
    - Urheberschaft der medizinischen Daten (author and/or ownership)
    - Verantwortung und Haftung der Daten (legal authenticator) enthalten.
- Die datenverarbeitende Stelle (datenkonsumierender Leistungserbringer) muss durch die in der Transaktion und EFA enthaltenden Informationen in der Lage versetzt werden, den Datenursprung (Originator Authenticity) und den Grad der Datenautenzität (legal authenticator & data authenticity) selbstständig bewerten und dokumentieren zu können.

- Die Informationen über Datenauthenzität und Datenursprung innerhalb der EFA oder den begleitenden Metadaten dürfen durch die Übertragungsmittel nicht innerhalb des Transfers geändert werden.
- Die innerhalb der EFA enthaltenen medizinischen Daten müssen während des Transfers durch geeignete technische Mittel vor:
  - unabsichtlicher Verfälschung und vorsätzlicher Manipulation,
  - Verlust und Unvollständigkeit geschützt werden.
- Sofern der Datenaustausch zwischen datenhaltenden Stellen und berechtigten Nutzern über Dritte vermittelt wird (beispielsweise P2P-Gateways zur Vernetzung von EFA-Providern), müssen gesicherte Informationen über die Identität der bei einer Datenkommunikation genutzten datenvermittelnden Stellen für alle Kommunikationspartner verfügbar sein.

Digital Signature

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.04.01}

Als future extension, wenn HBA und SMC flächendeckend verfügbar….

Nicht-Abstreitbarkeit, Dokumentation und Audit-Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.05}

Anforderungen

- Jeder durch die EFA vollzogene Datenaustausch muss geeignet dokumentiert werden, so dass eine nachträgliche lückenlose Rekonstruktion der Kommunikation und des Kontexts möglich ist (Nachträglich: nach erfolgtem Zugriff auf einen Fachdienst, Lückenlos: alle Transaktionen auf der EFA-Anwendungsebene sind erfasst).
- Die innerhalb der digitale Beweiskette und dem Audit-Trail abzulegenden Informationen sind manipulations- und revisionssicher abzuspeichern.
- Die digitale Beweiskette und der Audit-Trail müssen geeignet archiviert werden und die Aufbewahrungsfristen sind an den gesetzlichen Gegebenheiten auszurichten. Sollten lediglich Minimalaufbewahrungsfristen gewahrt werden, so sind alle direkt Betroffenen (Patient, EFA-Teilnehmer) über diesen Umstand geeignet zu unterrichten.
- Eine geeignete Beweiskette muss sich aus dem Audit-Trail ergeben, die eventuellen Betroffenen und mit datenschutzrechtlichen Kontrollaufgaben beauftragten Personen eine fallbezogene, umfassende Überprüfung der Legitimität der aktuellen und historischen Fallaktenzugriffe ermöglicht.

- Die digitale Beweiskette und der Audit-Trail darf lediglich die zwingend zur Erfüllung der Dokumentationspflichten personenbezogenen und/oder medizinischen Daten erfassen. Andere Protokolle und -arten, wie beispielsweise Performancelogs, dürfen keinerlei personenbezogenen und/oder medizinischen Daten erfassen.
- Die digitale Beweiskette und der Audit-Trail sind auf Grund der zwingend zur Erfüllung der Dokumentationspflichten enthaltenden personenbezogenen und/oder medizinischen Daten vor Zugriffen unberechtigter Dritter zu schützen und verfügen über den gleichen Schutzbedarf wie die darin enthaltenen Daten.
- Die innerhalb der digitalen Beweiskette und dem Audit-Trail enthaltenden Informationen dürfen lediglich gegenüber dem Patienten und mit datenschutzrechtlichen Kontrollaufgaben betrauten Personen offenbart werden. Reguläre Leistungserbringer haben generell keinen Zugriff auf die digitale Beweiskette und den Audit-Trail. Die digitale Beweiskette und der Audit-Trail dürfen keinesfalls zweckfremd verwendet werden und werden ausschließlich zu Dokumentations- und Nachweiszwecken erfasst. Automatisierte Kontrollsysteme des Audit-Trails sind gesondert zu berechtigen und der Patient ist über den Einsatz derartiger Systeme zu informieren.

Verfügbarkeit von EFA-Teilnehmern und EFA-Daten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierf.06}

Anforderungen

- EFA Partner sind verpflichtet, andere Verbundpartner geeignet über geplante und ungeplante Nicht-Verfügbarkeit durch einen gesonderten Prozess zu unterrichten.
- Die Vollständigkeit und Unversehrtheit der zu übertragenen Daten MUSS während des Transfers durch die gewählten Kommunikationsmittel lückenlos gewährleistet werden.
- Temporäre Fehler in der Datenbereitstellung durch die datenhaltende Stelle müssen geeignet markiert und kommuniziert werden.
    - Eventuelle Providencefehler und/oder Unvollständigkeiten bezüglich der in der Datenübertragung kommunizierten Daten sind stets zu Nachweiszwecken umfänglich von allen beteiligten Kommunikationspartnern eigenständig zu dokumentieren. Dieses kann z.B. im Rahmen der Protokollierung erfolgen, indem auch Fehler- und Warnhinweise zu nicht erfolgten Zugriffen in das Protokoll aufgenommen werden.
    - EFA-Kommunikation ist unter dem "best-attempt" Prinzip zu betreiben und die EFA-Partner sowie der Patient sind über diesen umstand geeignet zu unterrichten. EFA-Daten als solche sind nicht als Primärdokumentation mit den daraus resultierenden Implikationen bezüglich der jederzeit zwingenden Verfügbarkeit zu verstehen.
    - In einer verteilten EFA bewertet die datenverarbeitende als verantwortliche Stelle der Datenkompilation die Bewerting der tatsächlichen Vollständigkeit der emfangenen Datensammlung.

    - Die Entscheidung über die medizinische Nutzbarkeit der unvollständigen Daten kann der datenverarbeitenden Stelle übertragen werden.
- Sofern nicht durch gesonderte Indikatoren angezeigt, gilt eine von der datenhaltenden Stelle freigegebene Datenoffenbarung zum Zeitpunkt der Offenbarung als komplett und unversehrt.
    - Diese Anforderung ist auf die aktuell in der EFA eingestelten Daten zu limitieren und trifft keine Aussage über Art und Umfang der tatsächlich bei der datenhaltenden Stelle vollumfänglich verfügbaren Daten über den betroffenen Patienten.
    - Die Vollständigkeit und Verfügbarkeit der EFA selbst und der darin eingestellten Daten ist durch die Patienteneinwilligung und die lokale Sicherheitsrichtlinie der datenhaltenden Stelle definiert. Dies kann zu Ausblendungen, Zurückhaltung oder Löschung führen, sofern diese durch den Patienten, aktuell gültige Rechtsvorschriften oder die datenhaltende Stelle mandatiert sind.
- Die Existenz einer EFA und den durch diese verfügbar gemachten Daten bedingt keinen Rechtsanspruch bezüglich deren tatsächlicher Nutzung (patientengesteuerte freiwillige Nutzung). Der Patient ist jederzeit berechtigt situationsbezogen entscheiden, ob und wie die EFA in dessen Behandlungskontext durch die Leistungserbringer genutzt wird.
    - Die tatsächliche Verfügbarkeit einer EFA und den in diese eingestellen Daten kann nicht über die gesamte Dauer des Behandlungskontext garantiert werden. Der Patient hat jederzeit das Recht die Einwilligung der EFA zurückzuziehen und damit auch vorab durch die EFA zuängliche oder kommunizierte Daten unverfügbar zu machen. Dieser Umstand ist insbesondere bei datenverarbeitenden Stellen geeignet zu adressieren, um stets eine angemessen vollständige lokale Behandlungsdokumentation gewährleisten zu können.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Logical Perspective - Information Dimension

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Informationsmodell der EFA Geschäftsobjekte**.*

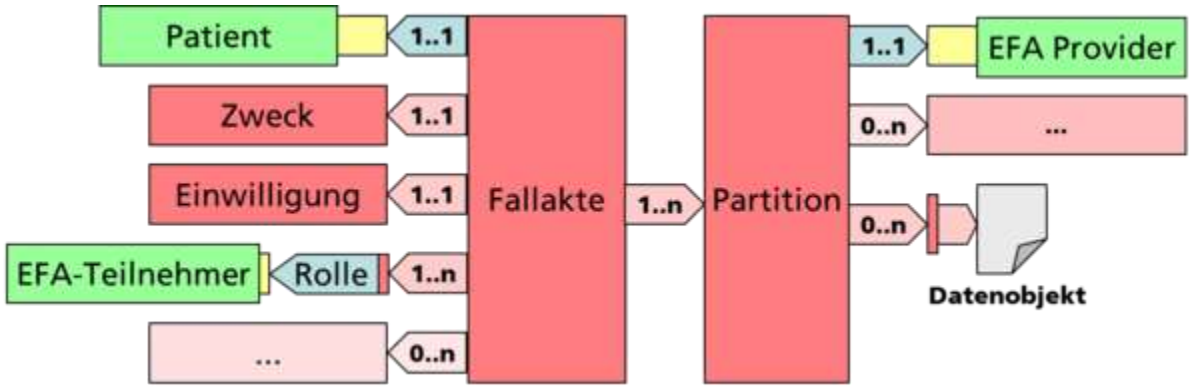
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Informationsmodell

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.01}`

Die folgende Abbildung zeigt das aus der Definition der EFA-Geschäftsobjekte abgeleitete und über HL7 RIM Klassen ausgedrückte Informationsmodell des EFA-Konstrukts.



Prinzipiell schreibt die EFA-Spezifikation keine bestimmte interne Umsetzung dieses Informationsmodells vor, d.h. ein Hersteller kann dieses über beliebige Technologien abbilden. Normative Vorgaben bestehen jedoch bezüglich der Aussen-Semantik und der über Operationen der EFA-Dienste ausgetauschten Instanzen (von Ausschnitten) dieses Informationsmodells. Dieses spiegelt sich vor allem in der nachfolgend beschriebenen Abbildung der EFA Geschäftsobjekte auf ihre korrespondierenden logischen Objekte im Informationsmodell wider.

Patient

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.01.01}

Die funktional-logische Spezifikation der EFA korrespondiert mit der Sichtweise auf ein EFA-Netzwerk als eine Versorgungsdomäne. Auf der Sicht einer Affinity Domain angesiedelte Problemstellungen bezüglich der Repräsentation des Patienten durch in den einzelnen EFA-Peers unterschiedliche Patienten-IDs müssen daher außerhalb der EFA gelöst werden. Hierzu sind die u.a. im IHE Cookbook beschriebenen, von der EFA unabhängig umsetzbaren Verfahren eines Master Patient Index oder einer domänenübergreifend gültigen ID zu nutzen.

Konkret bedeutet dies: Eine von einem EFA-Teilnehmersystem beim Aufruf eines EFA-Dienstes genutzte Patienten-ID muss immer in der Affinity Domain des EFA-Providers bekannt sein, d.h. das Clientsystem des EFA-Teilnehmers muss ggf. vor dem Dienstaufruf eine Abbildung der lokal genutzten Patienten-ID auf die Patienten-ID der Domäne des EFA-Providers vornehmen. Analog hierzu gilt auch in einer aus mehreren Affinity Domains bestehenden Versorgungsdomäne die Regel "Sender does it right", d.h. bevor eine Anfrage von einem EFA-Provider an einen anderen weitergeleitet wird, muss der initierende Peer die Überführung der Patienten-ID in die Domäne des Ziel-Peers vornehmen.

Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.01.02}

Die folgenden Aussagen prägen das Außen-Verhalten eines logischen Objekts der Klasse "Fallakte":

- Jede Fallakte ist genau einem Patienten zugeordnet. Diese Beziehung ist für Berechtigte bidirektional auflösbar, d.h. zu einem Patienten können die zugehörigen Fallakten und zu einer gegebenen Fallakte der betroffene Patient ermittelt werden.
- Jede Fallakte dient genau einem klar abgrenzbaren Zweck. Pro Patient und Zweck kann es nur eine Fallakte geben.
- Zu jeder Fallakte gibt es zu jeder Zeit genau eine gültige Einwilligung des betroffenen Patienten. Die Fallakte ist von der Einwilligung abhängig, d.h. eine Rücknahme der Einwilligung bedingt das Schließen der Fallakte.
- Zu jeder Fallakte sind berechtigte EFA-Teilnehmer benannt, deren Berechtigungen sich aus ihren definierten Rollen der EFA-Nutzung ableiten.

Partition

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.01.03}

Die folgenden Aussagen prägen das Außen-Verhalten eines logischen Objekts der Klasse "Partition":

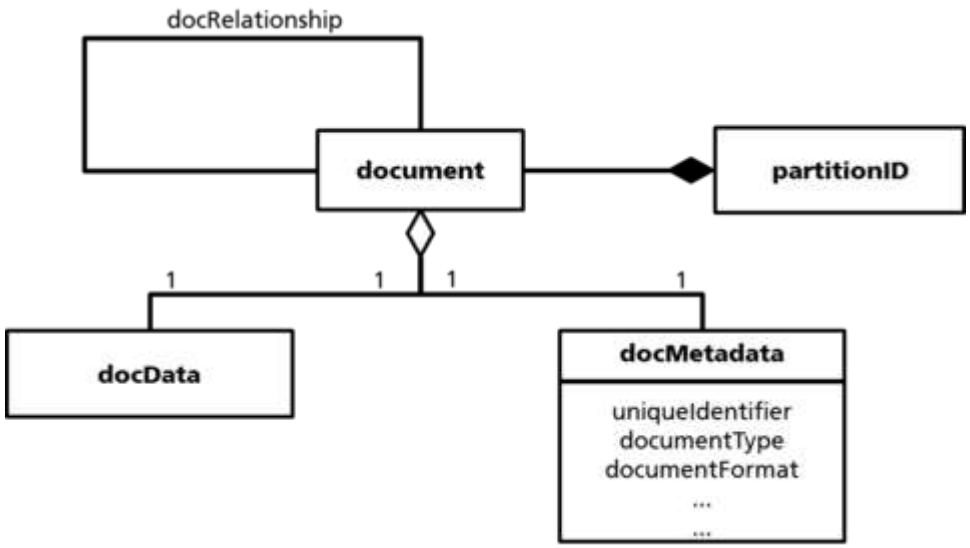
- Eine Fallakte besteht aus einer oder mehr Partitionen. Jede Partition ist genau einer Fallakte zugeordnet. Auch hier besteht eine Abhängigkeitsbeziehung; mit Schließen der Fallakte werden auch die abhängigen Partitionen geschlossen und sind nicht mehr zugreifbar.
- Jede Partition wird bei einem EFA-Provider angelegt und verwaltet. Dieser ist für die sichere Speicherung der daran hängenden Daten sowie die Durchsetzung der definierten Berechtigungen bei Zugriffen auf die Partition verantwortlich.

document

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.10}

Datenobjekte der EFA werden in Partitionen verwaltet. Ein Datenobjekt kann mehreren Partitionen zugeordnet sein, sofern diese beim selben EFA-Provider angelegt sind. Aktuell werden lediglich (medizinische) Dokumente als Datenobjekte der EFA unterstützt.

Für die EFA-v2.0-Spezifikation wird davon ausgegangen, dass die Inhalte von Dokumenten nur für einige wenige definierte Dokumentklassen (z.B. consentInfo) maschinell verarbeitet werden können. Dies bedeutet, dass alle für das Einstellen, die Auswahl, den Abruf, die Strukturierung/Suche und die Anzeige von Dokumenten relevanten Attribute eines Dokuments explizit außerhalb des Dokuments verfügbar sein müssen.



Die Klasse *document* bildet hierbei die Klammer über alle Bestandteile eines Dokuments, die explizit über Klassen gekapselt und hierdurch potenziell für eine maschinelle Verarbeitung verfügbar sind:

partitionID
: Jedes Dokument ist eindeutig einer Partition zugeordnet, die ihrerseits eindeutig einer Fallakte zugeordnet ist. Die für diese Fallakte definierten Zugriffsrechte werden auf deren Partitionen und damit auch die darin enthaltenen Dokumente vererbt.

docMetadata
: Jedem Dokument sind beschreibene Metadaten (z.B. Dokumenttyp und Dokumentformat) zugeordnet, um die automatisierte Filterung und Strukturierung zur Anzeige von EFA-Inhalten gegenüber einem EFA-Teilnehmer zu unterstützen.

docData
: Das eigentliche Dokument ist aus Sicht der EFA (von wenigen Ausnahmen abgesehen) ein BLOB, der nicht weiter maschinell verarbeitet wird.

docRelationship
: Dokumente können zueinander in Beziehung stehen. Neben in Dokumenten kodierten Verweisen können diese Beziehungen auch über eigenständige Objekte explizit gemacht werden.

PIM Data Structures

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02}

Die nachfolgend beschriebenen Objektklassen beschreiben die über Operationen der EFA-Dienste ausgetauschten Instanzen (von Ausschnitten) des EFA-Informationsmodells. Diese Klassen werden nachfolgend in der Abstraktionsstufe des *EFA Service Functional Model* unabhängig von einer konkreten technischen Umsetzung definiert.

patientID

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.01}

Die *patientID* ist ein eindeutiger Identifizierer eines Patienten innerhalb einer von einem EFA-Provider realisierten Affinity Domain. Sie bildet damit in der IHE-Semantik die "XAD-PID" ab (siehe IHE Cookbook).

Wenn eine *patientID* bei einem Operationsaufruf von einem EFA-Teilnehmer an einen EFA-Dienst übergeben wird, muss diese ID in der Affinity Domain des EFA-Providers registriert sein, d.h. das Clientsystem des EFA-Teilnehmers muss ggf. vor dem Dienstaufruf eine Abbildung der lokal genutzten Patienten-ID auf die EFA *patientID* der Domäne des EFA-Providers vornehmen.

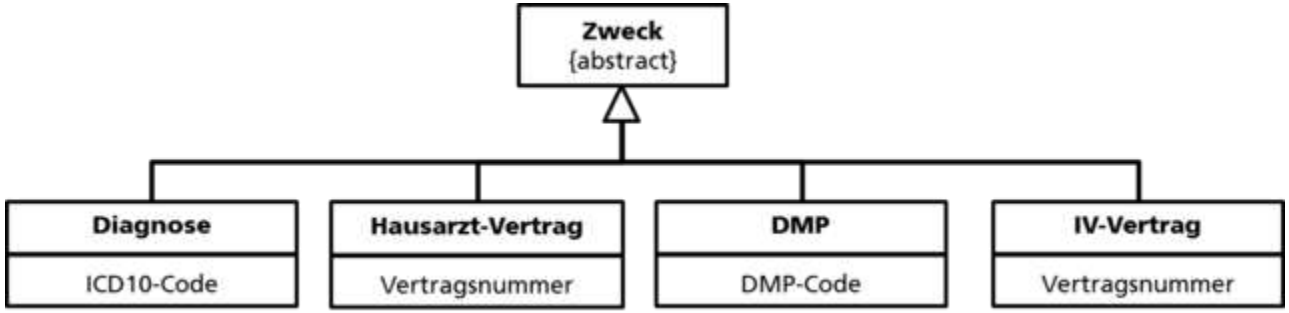
Im Fall von in einem Peer-to-Peer-Verbund verteilt verwalteten Fallakten ist es nicht unwahrscheinlich, dass jeder Provider den selben Patienten unter einer anderen *patientID* führt. Um eine sichere Verknüpfung der verteilt verwalteten Partitionen einer Fallakte realisieren zu können, muss jeder Provider bei einer verteilten Akte eine Abbildung der von ihm genutzten *patientID* auf die von sämtlichen anderen beteiligten Providern genutzten *patientID*s realisieren können. Analog zu der Nutzung der *patientID* in einem Single-Peer-Szenario gilt auch hier die Regel "Sender does it right", d.h. bevor eine Anfrage von einem Peer an einen anderen weitergeleitet wird, muss der initierende Peer die Überführung der *patientID* in die Domäne des Ziel-Peers vornehmen.

Da jede Fallakte eindeutig einem Patienten zugeordnet ist und jede Partition zu genau einer Fallakte gehört, ist auch jede Partition eindeutig einem Patienten zugeordnet. D.h. aus Sicht des Informationsmodells spielt es keine Rolle, ob eine EFA-Umsetzung die Patientenzuordnung ausschließlich auf Ebene der Fallakten verwaltet oder auch auf die Ebene der Partitionen herunter zieht.

purpose

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.02}

Die Klasse *purpose* kodiert den Zweck einer Fallakte und referenziert damit eindeutig auf einen "medizinischen Fall" des Patienten. Die Kodierung des Zwecks kann entweder über einen standardisierten Diagnosecode (z.B. ICD-10) oder die Referenzierung eines Vertrags (DMP, IV, etc.) erfolgen. Instanzen der Klasse *purpose* müssen den Zweck einer Akte ausschließlich über kodierte Werte aus einem vorab innerhalb einer Versorgungdomäne definierten Vokabular verwenden.



Da jede Fallakte eindeutig einem Zweck dient und jede Partition zu genau einer Fallakte gehört, ist auch jede Partition eindeutig einem Zweck zugeordnet. D.h. aus Sicht des Informationsmodells spielt es keine Rolle, ob eine EFA-Umsetzung die Zweckbindung ausschließlich auf Ebene der Fallakten verwaltet oder auch auf die Ebene der Partitionen herunter zieht.

ecrInfo

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.03}

Die Klasse *ecrInfo* umfasst die Metadaten zu einer Fallakte.

Attribut	Beschreibung	Verwendung
patientID (mandatory)	Eindeutiger Identifier des Patienten, dem die EFA zugeordnet ist	Jede Fallakte ist genau einem Patienten zugeordnet. Die *patientID* ist ein eindeutiger Identifizierer dieses Patienten innerhalb einer von einem EFA-Provider realisierten Affinity Domain.
purpose	Zweck der Fallakte	Jede Fallakte eines Patienten wird zu genau einem Zweck geführt, der den der EFA zugrunde

(mandatory)		liegenden "medizinischen Fall" des Patienten repräsentiert.
ecrStatus (mandatory)	Status der Fallakte	Der Status einer Fallakte spiegelt den Lebenszyklus der Fallakte wider. Änderungen des Status erfolgen insbesondere beim Ablauf der Gültigkeit einer Akte sowie bei Änderungen an der vom Patienten gegebenen Einwilligung.

Jede Fallakte ist durch die Kombination aus patientID und purpose eindeutig identifizierbar. Beide Attribute zusammen bilden die ID einer Fallakte (ecrRef).

Gängige Aktenstandards wie IHE XDS unterstützen keine logischen Konstrukte oberhalb weitgehend semantikfreier Ordner, d.h. der Container für Metadaten einer Fallakte muss entweder als proprietäre Ergänzung realisiert werden oder es muss eine Abbildung der EFA-Metadaten auf Ordner erfolgen. Um die zweite Option einfach realisieren zu können, wurde in der EFAv2.0 im Vergleich zur EFA-1.2-Spezifikation das Konstrukt der Partitionen deutlich gestärkt und auch die Funktionalität stärker auf dieses Konstrukt fokussiert:

- In der EFA-v2.0-Spezifikation ist eine Fallakte implizit als Summe der unter einer Patienteneinwilligung gefassten, zum gleichen Patienten und Zweck angelegten Partitionen definiert. "Einwilligung" (consentInfo), "Partition" (partitionID) sowie "Patient und Zweck" (ecrRef) sind hierbei eigenständig verwaltete und verknüpfte Objekte, die sofern im Rahmen eines Operationsaufrufs erforderlich auch explizit als Argumente übergeben werden. Hiermit werden implizit auch die EFA-Metadaten patientID und purpose auf der Ebene der Partitionen realisiert.
- Die EFA-v2.0-Spezifikation besitzt mit Ausnahme der Operationen zur Steuerung des Lebenszyklus (createECR, closeECR, registerConsent) keine Operationen auf Fallakten, sondern realisiert Funktionen zum Lesen und Schreiben ausschließlich auf Ebene der Partitionen. Insbesondere gibt es im *Service Functional Model* keine Operationen zum Suchen, Öffnen oder Auslesen von Fallakten, für die administrative oder gar medizinische Metadaten einer Fallakte erforderlich wären.

consentInfo

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.04}`

Die Klasse *consentInfo* bildet den Inhalt einer Patienteneinwilligung in so weit maschinenlesbar ab, als dass darüber eine automatische Konfiguration einer Fallakte und ihrer Zugriffsrechte möglich ist. *consentInfo* ist ein EFA-2.0-Profil auf dem im Domänenmodell "Einwilligung zur zweckgebundenen Kommunikation" definierten Konzeptmodell und dem daraus abgeleiteten Informationsmodell einer Einwilligungserklärung. Im Einzelnen umfasst dieses Profil die folgenden Einschränkungen zu dem im Leitfaden "Einwilligung" definierten Informationsmodell:

- Die Kodierung des Zwecks unterliegt den im Abschnitt zur Klasse "purpose" definierten Vorgaben. Es müssen die im EFA-2.0-XDS-Binding festgelegten Codesysteme verwendet werden.
- Die maschinenlesbare Darstellung einer Einwilligung muss eine Umsetzung der im Interaktionsmuster "Fallakte anlegen" beschriebenen Ausnahmeszenarien erlauben. Dies bedeutet, dass per Konvention oder per expliziter Aussage erkennbar sein muss, wie die Anlage einer Akte realisiert wird, wenn bereits eine Akte zu den benannten Zweck besteht.

Die technischen Umsetzung der Klasse *consentInfo* kann über jedes Binding erfolgen, dass den Leitfaden "Einwilligung" umsetzt. Hierbei sind die benannten Einschränkungen aus dem Informationsmodell in das Binding zu übernehmen.

Es kann zu jedem Zeitpunkt nur eine aktuelle gültige Einwilligung geben, d.h. mit dem Einstellen eines validen *consentInfo*-Objekts in eine Fallakte werden automatisch alle zuvor eingestellten *consentInfo*-Objekte ungültig.

consentDoc

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.05}

Die Klasse *consentDoc* ist eine Spezialisierung der Klasse *document* und umfasst ein vom EFA-Provider inhaltlich nicht weiter verarbeitetes Dokument, dessen Gegenstand eine Patienteneinwilligung ist.

Es kann zu jedem Zeitpunkt nur eine aktuelle gültige Einwilligung geben, die dem EFA-Provider gegenüber über die Klasse *consentInfo dargestellt wird. Zusammen mit der Bekanntmachung einer Einwilligung über ein* consentInfo-*Objekt kann eine Instanz der Klasse* consentDoc *als menschenlesbares Pendant in die betroffene Akte eingestellt werden. Das* consentDoc-*Objekt wird dabei als Ergänzung des* consentInfo-*Objekts deklariert.*

Ein Einstellen eines *consentInfo*-Objekts ohne korrespondierendes *consentDoc*-Objekt ist möglich. Das Einstellen eines *consentDoc*-Objekts ist nur möglich, wenn dieses über eine Ergänzt-Beziehung mit einem *consentInfo*-Objekt verknüpft ist.

partitionID

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.06}

Die Klasse *partitionID* beschreibt eine eindeutige Referenz auf eine Partition einer Fallakte. Bestandteil der Referenz sind

- ein Verweis auf den EFA-Provider, der die Partition verwaltet, sowie
- ein von diesem Provider eindeutig auflösbarer Identifizierer.

partitionList

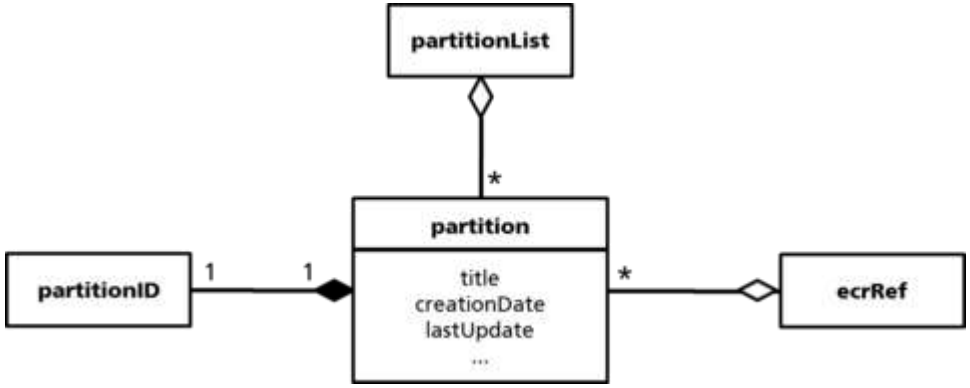
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.07}

Die Klasse *partitionList* beschreibt eine Menge von Partitionen, die Fallakten des selben Patienten zugeordnet sind. Jede Partition wird durch ein *partition*-Objekt repräsentiert. Mit diesem Objekt müssen vom EFA-Provider im Rahmen der Operation listPartitions die folgenden Informationen zu einer Partition verknüpft sein:

partitionID
: Identifizierer der Partition, über den diese Partition eindeutig referenziert werden kann. Eine solche Referenzierung ist vor allem zum Einstellen von Daten in eine Partition und zum Auslesen einer Partition erforderlich.

ecrRef
: Verweis auf die Fallakte, der die Partition zugeordnet ist. Jede Partition ist genau einer Fallakte zugeordnet.

Metadaten der Partition
: Die genaue Festlegung der von einem EFA-Provider zu einer Partition verwalteten Metadaten ist vom konkreten Binding abhängig. Jedes Binding muss aber mindestens die in der Klasse *partitionInfo* enthaltenen Angaben unterstützen und als Teil des eine Partition repräsentierenden *partition*-Objekts bei der Abfrage der Partitionen einer Fallakte an den Aufrufer zurück liefern.



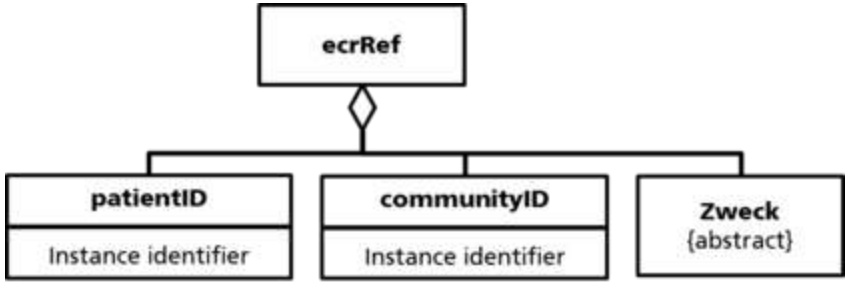
ecrRef

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.08}

In der EFA-2.0-Spezifikation ist kein orginärer Identifier für Fallakten definiert. Wie schon im Zusammenhang mit der Klasse *ecrInfo* beschrieben, wird durch die Möglichkeit eines vollständigen Verzichts auf ein manifestiertes Fallakten-Objekt eine flexiblere und einfachere Umsetzung der EFA-Spezifikation über bestehende Standards unterstützt.

Um dennoch Fallakten eindeutig referenzieren zu können, wird die Tatsache ausgenutzt, dass pro Patient (*patientID*) und Zweck (*purpose*) per Definition nur eine Fallakte existieren darf. Hiermit bilden die in der Klasse *ecrRef* zusammengefassten Angaben zu Patient und Zweck zusammen eine innerhalb einer Affinity Domain eindeutige Referenz auf eine Fallakte.

Bei einer Peer-to-Peer-Vernetzung, in der Daten einer Fallakte über mehrere Affinity Domains verteilt vorgehalten werden, kann jede Affinity Domain potenziell eine eigene patientID für den selben Patienten vergeben. Daher ist eine Fallakten-Referenz aus patientID und Zweck immer relativ, d.h. kann nur in der Affinity Domain verarbeitet werden, in der diese Referenz zur Verarbeitung der in dieser Domain verwalteten Partitionen der Fallakte erzeugt wurde. Um Fallakten über Affinity Domains hinweg zu vernetzen und insbesondere auch Zugriffe auf verteilte Fallakten zu ermöglichen, wird daher zusätzlich eine communityID als dritter Bestandteil einer Fallakten-Referenz benötigt, die angibt, in welcher Affinity Domain die Referenz gültig ist.



partitionInfo

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.09}

Der Zugriff auf die Inhalte einer Fallakte erfolgt durch Auflisten der Partitionen der Akte und anschließendes Browsing bzw. Suchen/Filtern über den in den einzelnen Partitionen enthaltenen Daten. Damit die IT-Systeme der EFA-Teilnehmer diesen Ablauf optimieren und an verschiedene Zugriffsmetaphern (z.B. Anzeigen seit dem letzten Zugriff neu hinzugekommener Daten) anpassen können, werden Partitionen mit Metadaten versehen. Hierbei muss ein Binding zumindest die folgenden Metadaten unterstützen:

Attribut	Beschreibung	Verwendung
partitionID (mandatory)	Eindeutiger Identifizierer der Partition	Die ID der Partition wird beim Anlegen einer Partition abhängig vom genutzten Binding durch den EFA-Teilnehmer oder den EFA-Provider festgelegt. Sie muss beim Auslesen der Partitionsdaten vom EFA-Provider zurück geliefert werden. Die ID der Partition wird zum Abruf von Daten aus einer Partition und zum Einstellen von Daten in eine Partition benötigt.
Titel (mandatory)	Für den EFA-Teilnehmer verständliche Bezeichnung der Partition, aus der hervorgeht, welche Daten in der Partition zu erwarten sind (z.B. "Nachsorge nach Bypass-Operation"). Aus Datenschutzgründen darf dieser Titel keine identifizierenden Angaben zum Patient enthalten.	Der Titel wird beim Anlegen einer Partition gesetzt und unverändert beim Auslesen der Partitionsdaten vom EFA-Provider zurück geliefert. Dieses Attribut kann z.B. genutzt werden, um einem EFA-Teilnehmer beim Browsing über einer Akte zunächst die verfügbaren Partitionen anzuzeigen und nur Daten aus vom Teilnehmer als für die aktuelle Behandlungssituation relevant markierten Partitionen abzurufen.
Klassifizierung (optional)	In Ergänzung zum Titel kann eine Partition auch eine maschinenlesbare Klassifizierung enthalten. Beispiele hierfür finden sind administrative Informationen, z.B. ob es sich um Daten zu einem Krankenhausaufenthalt handelt.	Klassifizierungen müssen beim Anlegen einer Partition gesetzt und vom EFA-Provider unverändert beim Auslesen der Partitionsdaten vom EFA-Provider zurück geliefert werden.
Erfasster Behandlungszeitraum (mandatory)	Zeitraum der über die Partition unterstützten Behandlungsepisode. Hierbei werden das Anfangsdatum der Episode sowie das Datum der letzten Änderung der Inhalte der Partition verwaltet.	Das Anfangsdatum der Episode wird beim beim Anlegen einer Partition gesetzt. Fehlt diese Angabe, wird das Datum der Anlage der Partition als Anfang der begleiteten Episode angenommen. Das Datum der letzten Änderung wird vom EFA-Provider bei jeder Einstellen von Daten in die Partition neu

		gesetzt und beim Auslesen der Partitionsdaten mitgegeben. Ein EFA-Teilnehmersystem kann Partitionen anhand dieser Angaben in eine chronologische Reihenfolge bringen oder effizient nach den aktuellsten Daten durchsuchen.
Verantwortliche Organisation (optional)	Bezeichner der Organisation, die für die Anlage der Partition und die Pflege der darin enthaltenen Inhalte verantwortlich ist.	Sofern diese Information nicht beim Anlegen einer Partition gesetzt wird, gilt die Organisation des die Partition anlegenden Leistungserbringers als für die Partition verantwortlich. Diese Information muss beim Auslesen der Partitionsdaten bereit gestellt werden.
Anker (optional)	Bei der Anlage der Partition gesetzter Wert, der von der für die Partition verantwortlichen Einrichtung für interne Zwecke genutzt werden kann.	Wie in der Darstellung der EFA Geschäftsobjekte beschrieben, kann eine Partition mit einem Containerobjekt des EFA-Teilnehmers wie z.B. einem Aufenthalt oder einem Abrechnungsfall verknüpft werden. In diesem Fall kann z.B. ein Kommunikationsserver eine automatisierte Synchronisierung zwischen den Daten in der Partition und dem damit verknüpften internen Container durchführen. Um dieses zu unterstützen kann zu einer Partition ein Anker zu dem damit verknüpften internen Containerobjekt angegeben werden. Dieser Wert ist für den EFA-Provider und die anderen Teilnehmer semantikfrei und transparent.

Ein EFA-Binding kann weitere Attribute für Partitionen definieren. Diese müssen jedoch von einem clientseitigen Teilnehmersystem nicht zwingend verarbeitet werden.

docMetadata

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.11}

Die Interaktionsmuster der EFA-v2.0 sehen vor, dass ein Teilnehmersystem nach dem Öffnen einer Fallakte zunächst die Metadaten dieser Akte abruft und in einer dem Nutzungsszenario angemessenen Struktur anzeigt. Hierbei können auch Filter genutzt werden, um nicht relevante Daten auszublenden. Gezielte Suchen nach bestimmten Dokumenten setzen auf dem selben Muster auf, auch hier ruft das Teilnehmersystem zunächst die Metadaten der Inhalte der Fallakte ab und führt anschließend eine Suche auch diesen Daten durch.

Damit die IT-Systeme der EFA-Teilnehmer diesen Ablauf optimieren und an verschiedene Zugriffsmetaphern (z.B. Anzeigen seit dem letzten Zugriff neu hinzugekommener Daten) anpassen können, werden umfangreiche Metadaten zu jedem Dokument benötigt:

Attribut	Beschreibung	Verwendung
documentID (mandatory)	Eindeutiger Identifizierer des Dokuments	Die ID eines Dokuments wird beim Einstellen von Daten in eine Partition abhängig vom genutzten Binding durch den EFA-Teilnehmer oder den EFA-Provider festgelegt. Sie muss beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert werden. Die documentID wird beim Abruf eines Dokuments, zum Invalidieren eines Dokuments sowie zum Setzen von Dokumentenbeziehungen benötigt. Die ID eines Dokuments ist eine Instanz der Klasse documentID.
Titel (mandatory)	Für den EFA-Teilnehmer verständliche Bezeichnung des Dokuments (z.B. "OP-Bericht zu Bypass-Operation"). Aus Datenschutzgründen darf dieser Titel keine identifizierenden Angaben zum Patient enthalten.	Der Titel wird beim Einstellen eines Dokuments in eine Partition gesetzt und unverändert beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Dieses Attribut kann z.B. genutzt werden, um einen EFA-Teilnehmer beim gezielten Abruf benötigter Informationen zu unterstützen.
Dokumentklasse (mandatory)	Grobgranulare Klassifizierung des Dokuments in einer über Versorgungsdomänen hinweg einheitlichen Nomenklatur.	Die Dokumentklasse wird beim Einstellen eines Dokuments in eine Partition gesetzt und unverändert beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Dieses Attribut kann z.B. genutzt werden, um einen EFA-Teilnehmer beim gezielten Abruf benötigter Informationen zu unterstützen.
Dokumenttyp (mandatory)	Feingranulare Klassifizierung des Dokuments in einer in der aktuellen Versorgungsdomäne definierten Nomenklatur.	Der Dokumenttyp wird beim Einstellen eines Dokuments in eine Partition gesetzt und unverändert beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Dieses Attribut kann z.B. genutzt werden, um einen EFA-Teilnehmer beim gezielten Abruf benötigter Informationen zu unterstützen.

Dokumentformat (mandatory)	Kodierte Angabe zum Format des Dokuments (z.B. PDF)	Das Dokumentformat wird beim Einstellen eines Dokuments in eine Partition gesetzt und unverändert beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Ein EFA-Provider kann zum Schutz vor Angriffen und Viren bestimmte Dokumentformate ablehnen bzw. vor der Übernahme in seine Datenbank prüfen, ob ein eingestelltes Dokument dem angegebenen Format entspricht.
Zeitpunkt der Bereitstellung (mandatory)	Datum des Einstellens des Dokuments in die Fallakte.	Das Einstellungsdatum eines Dokuments wird beim Einstellen eines Dokuments in eine Partition durch den EFA-Provider gesetzt, sofern es nicht in den bereitgestellten Metadaten enthalten ist. Das Einstellungsdatum wird beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Dieses Attribut soll die gezielte Suche nach neu in eine Akte eingestellten Dokumenten unterstützen.
Zeitliche Einordnung (optional)	Zeitraum der über das Dokument beschriebenen Handlung. Sofern dieser Zeitraum nicht bekannt, nicht eingrenzbar oder nicht medizinisch relevant ist, muss diese Angabe weggelassen werden; insbesondere darf hier nicht das Datum des Einstellens des Dokuments in die Akte als Default-Wert eingesetzt werden.	Die zeitliche Einordnung eines Dokuments wird beim Einstellen eines Dokuments in eine Partition gesetzt. Die festgesetzte zeitliche Einordnung wird beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Dieses Attribut soll die chronologische Sortierung von EFA-Inhalten entlang eines Behandlungsverlaufs unterstützen.
Verantwortliche Organisation (optional)	Bezeichner der Organisation, die für das Einstellen des Dokuments und die Richtigkeit der darin enthaltenen Inhalte verantwortlich ist.	Sofern diese Information nicht beim Einstellen eines Dokuments in eine Partition gesetzt wird, gilt die Organisation des die Daten in die Akte einstellenden Leistungserbringers als für das Dokument verantwortlich. Diese Information muss beim Auflisten der Dokumente einer Partition bereit gestellt werden.
Dateigröße (optional)	Dateigröße des Dokuments	Die Dateigröße eines Dokuments wird vom EFA-Provider ermittelt und beim Auflisten der Dokumente einer Partition übermittelt. Dieses Attribut kann vom EFA-Teilnehmersystem genutzt werden, um z.B. sehr große Dokumente parallel zu laufenden Nutzerinteraktionen im Hintergrund zu laden.

Fehlererkennender Code (conditional, mandatory)	Informationen zur Prüfung der Integrität des Dokuments. Dieses Attribut kann entfallen, wenn das Dokument mit einer digitalen Signatur versehen ist (s.u.).	Ein fehlererkennender Code (z.B. Hashwert) wird idealerweise bereits beim Einstellen eines Dokuments in eine Partition berechnet und unverändert beim Auflisten der Dokumente einer Partition vom EFA-Provider zurück geliefert. Hierdurch kann der Nutzer eines Dokuments sicher sein, dass ein Dokument während der Übertragung und Speicherung nicht verfälscht wurde.
Signatur (optional)	Digitale Signatur zur Sicherung der Authentizität (und Integrität)	Idealerweise werden nur vom Ersteller digital signierte Dokumente in eine Fallakte eingestellt, um ein sehr hohes Maß an Integritäts- und Authentizitätsschutz zu realisieren. Da die hierzu benötigten Mechanismen jedoch erst mit der flächendeckenden Einführung von Heilberufsausweisen und zugehörigen Prüfdiensten verfügbar sind, ist die Nutzung von Signaturen zunächst optional.

Ein EFA-Binding kann weitere Attribute für Dokumente definieren. Diese müssen jedoch von einem clientseitigen Teilnehmersystem nicht zwingend verarbeitet werden.

docRelationship

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.12}

Beziehungen zwischen Dokumenten können sowohl innerhalb von Dokumenten als auch als eigenständige Objekte kodiert werden. Die Klasse *docRelationship* beschreibt ausschließlich außerhalb von Dokumenten definierte Beziehungen zwischen Dokumenten. Hierbei muss ein Binding die beiden folgenden Beziehungen unterstützen:

- Replace: Ein Dokument ersetzt ein anderes Dokument
- Append: Ein Dokument ergänzt ein anderes Dokument

Die nachfolgende Tabelle stellt dar, wie hierbei die auf der konzeptionellen Ebene definierten Dokumentbeziehungen umzusetzen sind.

Dokumentbeziehung	**Semantik**	**Umsetzung**	**Anmerkungen**

Ergänzen eines Dokuments	Ein Dokument stellte eine Ergänzung eines anderen Dokuments dar (z.B. Befund zum Bild).	Append	Diese Beziehung wird u.a. im Rahmen der Verwaltung von Einwilligungen genutzt, um ein consentDoc-Objekt an ein consentInfo-Objekt zu binden.
Ersetzen eines Dokuments	Ein Dokument ersetzt ein benanntes anderes Dokument mitsamt seiner Anhänge/Ergänzungen. Das ersetzte Dokument wird invalidiert und beim Abruf von Dokumenten aus einer Fallakte nur für bestimmte Rolleninhaber (z.B. Fallaktenmanager) bereitgestellt. Für alle anderen Teilnehmer ist nur noch das neue Dokument sichtbar. Dieses enthält jedoch einen Verweis auf das ersetzte Dokument.	Replace	Das ersetzte Dokument muss durch den EFA-Provider im Register als "deaktiviert" markiert werden. Das Ersetzen eines Dokuments mit einem leeren Dokument entspricht der Semantik des Invalidieren dieses Dokuments.

documentID

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.13}

Die Klasse *documentID* beschreibt eine eindeutige Referenz auf ein Dokument. Bestandteil der Referenz sind

- ein Verweis auf das EFA Document Repository, in dem das Dokument verfügbar ist, sowie
- ein von diesem Repository eindeutig auflösbarer Identifizierer.

communityID

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {BnsIi.02.14}

Die Klasse *communityID* beschreibt eine eindeutige Referenz auf eine Affinity Domain und damit auf den für diese Domain verantwortlichen EFA-Provider.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

Implementierungsleitfaden ***Informationsmodell der EFA Sicherheitsobjekte****.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Sicherheitskontext

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.01}`

Alle Aufrufe einer EFA-Funktionalität erfolgen innerhalb eines definierten Sicherheitskontextes, der über den EFA Context Manager aufgebaut und verwaltet wird.

Grundsätzlich macht diese Spezifikation nur wenige Vorgaben, welche Sicherheitsobjekte im Sicherheitskontext abgelegt sind und wie diese Objekte in den Sicherheitskontext gelangen. Hierdurch entkoppelt der über ein context-Objekt gekapselte Sicherheitskontext die EFA-Anwendungsarchitektur von der darunter liegenden Sicherheitsarchitektur. EFA-Dienste erhalten mit jedem Operationsaufruf eine Kopie des lokalen context-Objekts und können anhand der darin enthaltenen Informationen die eigenen Sicherheitsdienste zur Authentisierung und Autorisierung ausführen.

PIM Data Structures

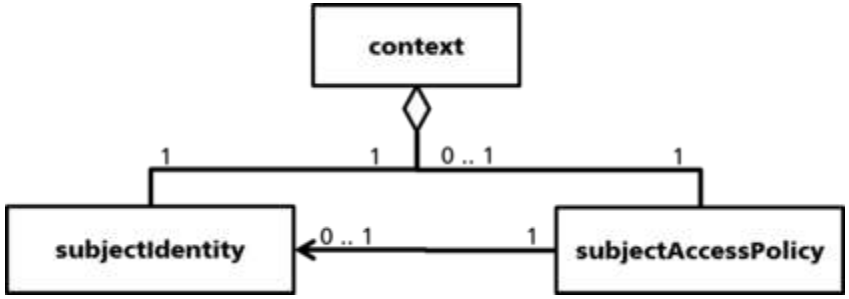
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.02}

Die nachfolgend beschriebenen Objektklassen werden im Rahmen des *EFA Service Functional Model* verwendet und bilden das Informationsmodel des *Platform Independent Model* der EFA Sicherheitsarchitektur.

context

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.02.01}

Die Klasse *context* entkoppelt Anwendungs- und Sicherheitsarchitektur der EFA. Jeder Aufruf einer EFA-Operation enthält eine Kopie des im lokalen EFA Context Manager des EFA-Clients verwalteten context-Objekts.



Während in der EFA-1.2-Spezifikation noch vier Sicherheitsnachweise über die Klasse *context* gekapselt wurden, sind in der EFA-2.0-Spezifikation zunächst nur zwei Nachweise normativ spezifiziert. Weitere Sicherheitsnachweise können für Ergänzungen dieser Spezifikation bzw. auch für einzelne Umsetzungen der EFA 2.0 definiert werden. Wesentlich ist lediglich, dass hierbei das logische Konstrukt des *context* zur Verwaltung und

zum Austausch dieser Nachweise genutzt wird. Hierdurch sind die Interoperabilität auf der logischen Ebene sowie die grundsätzliche Migrationsfähigkeit in die Telematikinfrastruktur sichergestellt.

Die nebenstehende Abbildung stellt den Aufbau der context-Klasse dar:

- eine subjectIdentity kapselt die Identität des EFA-Teilnehmers und sichert bei Dienstaufrufen die Authentizität des EFA-Teilnehmers ab.
- eine subjectAccessPolicy beschreibt die Zugriffsberechtigungen des über die *subjectIdentity* identifizierten EFA-Teilnehmers.

In jedem Sicherheitskontext muss genau ein *subjectIdentity*-Objekt vorhanden sein. Dieses wird durch den EFA Context Manager im Rahmen der Identifizierung und Authentifizierung des EFA-Teilnehmers von einem Identity Provider ausgestellt. Die Umsetzung des Identity Providers kann flexibel ausgestaltet werden, wodurch nicht nur ein Single Sign-On aus einem Primärsystem heraus sondern auch eine Nutzung der Sicherheitsobjekte und -mechanismen der Telematikinfrastruktur unterstützt werden (siehe Optionen zur Authentifizierung von EFA-Teilnhemern).

Eine *subjectAccessPolicy* ist nur bei Verwendung eines *Policy-Push* Verfahrens Bestandteil des Sicherheitskontextes. Ansonsten erfolgt der Abruf von Berechtigungsregeln on demand über den EFA-Dienst, der die angefragte Ressource verwaltete.

Sofern weitere Sicherheitsnachweise über ein *context*-Objekt verwaltet und ausgetauscht werden sollen, müssen diese direkt oder indirekt an das *subjectIdentity*-Objekt gebunden sein, da nur so eine integre und authentische Nachweis-Kette aufgebaut werden kann.

subjectIdentity

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.02.02}

Dieses Sicherheitsobjekt fasst Informationen zu einem EFA-Teilnehmer zusammen. Es wird mit jeder Anfrage an einen EFA-Dienst übermittelt und soll es dem aufgerufenen Dienst ermöglichen, den Aufrufer zu authentisieren und dessen Berechtigungen anhand der verfügbar gemachten Informationen auszuwerten und durchzusetzen.

In einem *subjectIdentity* Nachweis müssen mindestens die folgenden Informationen enthalten sein:

ID des EFA-Teilnehmers

Bei der Abbildung einer Patienteneinwilligung auf Berechtigungsregeln werden EFA-Teilnehmer durch eine eindeutige ID repräsentiert. In der subjectIdentity muss ein eindeutiger Identifier des EFA-Teilnehmers enthalten sein, der zu der aus der Einwilligung abgeleiteten ID des Teilnehmers korrespondiert (bzw. idealerweise sogar identisch ist).

Name des EFA-Teilnehmers

Anhand der im Audit Trail zu Datenschutzzwecken protokollierten Aktenzugriffe muss der Patient Information darüber erhalten können, wer wann und wieso auf welche Daten des Patienten zugegriffen hat. In der subjectIdentity muss der Klartextname des EFA-Teilnehmers (als Person) enthalten sein, da diese Information für das Schreiben eines auch für den Patienten nachvollziehbaren Zugriffsprotokoll benötigt wird.

Art der Authentifizierung und authentifizierende Stelle

Jeder EFA-Provider ist für den Schutz der bei ihm verwalteten Daten verantwortlich (siehe EFA Sicherheitsprinzipien). Hierzu gehört, dass der Provider die Vertrauenswürdigkeit einer ggf. an anderer Stelle vorgenommenen Authentifizierung bewerten können muss. Aus diesem Grund muss die subjectIdentity sichtbar machen, wie sich der EFA-Teilnehmer authentifiziert hat und welche Stelle die Richtigkeit und Sicherheit dieser Authentifizierung abgesichert hat.

Prüfdaten zur Feststellung der Authentizität des EFA-Teilnehmers

Ein EFA-Provider muss verifizieren können, dass die einen Dienst aufrufende Person der EFA-Teilnehmer ist, für den er/sie sich ausgibt. Entsprechende Prüfdaten müssen fest an die subjectIdentity gebunden sein.

Prüfdaten zur Feststellung der Authentizität und Integrität der *subjectIdentity*

Eine Verifizierbarkeit der Daten eines subjectIdentity ist nur gegeben, wenn die subjectIdentity selbst integer und authentisch ist. Daher muss jede subjectIdentity von der ausstellenden Stelle signiert werden.

Hier besteht noch eine Inkonsistenz zum *IHE Cookbook*. Das Cookbook verlangt, dass eine Identity Assertion einen Verweis auf den Patienten enthält, um so bestehende Schwachstellen von IHE XDS auffangen zu können. Die EFA 2.0 Spezifikation schließt einen solchen Verweis zwar nicht aus, sieht diesen aber auch nicht als verpflichtenden Bestandteil einer *subjectIdentity* (logisches Pendant zur Identity Assertion). Die Gründe hierfür sind:

- auf der logischen Ebene repräsentiert die *subjectIdentity* die *Subject Domain* des IHE 5-Domänen-Modells, die Beziehung zum Patienten ist jedoch Bestandteil der *Context Domain* und sollte daher - analog z.B. zu epSOS - in einer diese Domain abbildenden separaten Assertion erfasst werden.
- EFA zielt auf eine bestmögliche Unterstützung eines Single Sign-On ab. Ein Arzt soll in der Lage sein, innerhalb eines definierten Zeitraums mit einer einmal ausgestellten *subjectIdentity* auf Daten und Anwendungen zu verschiedenen Patienten zugreifen zu können.
- Sowohl EFA 2.0 als auch das IHE Cookbook binden Berechtigungen nicht an Patienten, sondern an Ordner bzw. mit Ordnern verknüpfte Attribute (EFA: Patient + Zweck-Codes). Da diese Daten im Registry verwaltet werden, muss in jedem Fall auch beim

Aufruf der RetrieveDocument Transaktion ein Registry-Zugriff erfolgen, d.h. es gibt keinen Effizienzgewinn (dieser wäre auch bei Bindung der Rechte an den Patienten nicht zu erzielen, da auch hier gegen das Registry geprüft werden müsste, ob das Dokument überhaupt dem fraglichen Patienten zugeordnet ist).

Sofern in der EFA-Einwilligung eines Patienten Organisationen bzw. Organisationseinheiten als EFA-Teilnehmer benannt sind, muss der subjectIdentity-Nachweis weiter Informationen enthalten, anhand derer eine einer Organisation zugehörige Person die für diese Person vergebenen Rechte instantiieren kann:

Organisations-ID
: Bei der Abbildung einer Patienteneinwilligung auf Berechtigungsregeln werden EFA-Teilnehmer durch eine eindeutige ID repräsentiert. Wenn der in der Einwilligung benannte berechtigte Teilnehmer eine Organisation(seinheit) ist, muss in der subjectIdentity ein eindeutiger Identifier der Organisation enthalten sein, der der Aufrufer angehört. Sofern sich diese IDs eindeutig aufeinander abbilden lassen (bzw. identisch sind) kann der Aufrufer die für seine Organisation(seinheit) definierten Rechte in Anspruch nehmen.

Point of Care
: Zur Nachvollziehbarkeit der Instantiierung von an Organisationen vergebenen Berechtigungen muss in dem subjectIdentity Nachweis benannt sein, von wo aus der Zugriff auf Patientendaten erfolgt.

Ein subjectIdentity Nachweis kann weitere Nutzerattribute enthalten. Diese müssen jedoch - im Gegensatz zu den oben aufgeführten Informationen - von dem angefragten Dienst nicht verarbeitet werden.

subjectAccessPolicy

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.02.03}

Dieses Sicherheitsobjekt fasst Informationen zu den Berechtigungen eines EFA-Teilnehmers zusammen. Sofern für eine EFA-Umsetzung ein Policy-Push Verfahren genutzt wird, erfolgen Abruf und Austausch dieses Sicherheitsobjekts in folgender Sequenz:

1. ein EFA-Provider oder ein EFA-Dienst gibt in seiner Schnittstellenbeschreibung an, dass die zum Zugriff zu überprüfenden Berechtigungen von einem dedizierten Sicherheitsdienst (EFA Policy Provider) verwaltet werden und als Teil des Dienstaufrufs vom EFA-Teilnehmer bereitgestellt werden müssen

2. der Context Manager des EFA-Clients ruft die als *subjectAccessPolicy* kodierten Berechtigungen des über eine *subjectIdentity* identifizierten und authentisierten EFA-Teilnehmers vom EFA Policy Provider ab
3. der Context Manager fügt jedem Dienstaufruf die *subjectAccessPolicy* bei.
4. der aufgerufene Dienst wertet die *subjectAccessPolicy* unter Nutzung von Attributen der Ressource und des Nutzers (*subjectIdentity*) aus und setzt sie durch.

In einem subjectAccessPolicy Sicherheitsnachweis müssen mindestens die folgenden Informationen enthalten sein:

Bindung an eine *subjectIdentity*
: Eine *subjectAccessPolicy* ist immer für einen bestimmten EFA-Teilnehmer gültig und kann auch nur von diesem für selbst veranlasste Zugriffe genutzt werden. Durch Bindung einer *subjectAccessPolicy* an eine *subjectIdentity* kann der aufgerufene Dienste verifizieren, dass die *subjectAccessPolicy* auch wirklich für den Aufrufer ausgestellt wurde und von diesem eingebracht wird.

Prüfdaten zur Feststellung der Authentizität und Integrität der subjectAccessPolicy
: Eine Verifizierbarkeit der Daten einer subjectAccessPolicy ist nur gegeben, wenn die subjectAccessPolicy selbst integer und authentisch ist. Daher muss jede subjectAccessPolicy von der ausstellenden Stelle signiert werden.

Zusätzlich enthält die subjectAccessPolicy die **Berechtigungen des EFA-Teilnehmers**. Analog zum GDD Referenzmodell können diese Berechtigungen auf der Ebene der Anwendung oder auf der Ebene der Ressource definiert sein:

- Anwendungsberechtigungen: Die *subjectAccessPolicy* definiert die Berechtigungen eines Leistungserbringers im Kontext eines EFA-Providers. Hierzu zählen z.B. Berechtigungen zur Anlage von Fallakten, zum Einstellen von Daten bei diesem Provider oder zur Besetzung bestimmter Rollen (z.B. Berechtigung, als Fallaktenmanager zu agieren). Die Berechtigungen spiegeln damit die vertraglichen und organisatorischen Bindungen zwischen dem Leistungserbringer und einem EFA-Provider wider.
- Ressourceberechtigungen: Die *subjectAccessPolicy* definiert die Berechtigungen eines Leistungserbringers im Kontext einer konkreten Fallakte. Hierzu zählen insbesondere die aus der Einwilligung des Betroffenen abgeleiteten Zugriffsrechte auf dieser Fallakte. Die Berechtigungen spiegeln damit die vertraglichen Vereinbarungen zwischen dem Leistungserbringer und einem Patienten wider.

Grundsätzlich können beide Arten von Berechtigungen auch in einem Regelwerk kombiniert werden.

accessToken

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eecim.02.04}

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Fehlermeldungen und Warnungen (logische Spezifikation)**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Fehler und Warnungen

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Feeln.01}`

Analog zu den Spezifikationen der Dienste und Operationen werden in der EFA 2.0 Spezifikation auch Fehler und Warnungen auf zwei Ebenen definiert:

- auf der logischen Ebene sind Fehler und Warnungen definiert, die in direktem Zusammenhang mit den anderen Artefakten dieser Ebene - insbesondere Kommunikationsmustern, *Service Functional Models* und Informationsmodellen - stehen. Logische Fehler und Warnungen beschreiben eine Ausnahmesituation und geben ggf. Hinweise zu deren Auflösung.
- eine Belegung der logischen Fehler und Warnungen mit Fehlercodes und Fehlermeldungen ist Teil des Bindings der Operationen, in denen der Fehler ausgelöst werden kann. Werden die EFA-Operationen z.B. an IHE XDS/XDR gebunden, so müssen auch die logischen EFA-Fehler und -Warnungen an die für XDS/XDR definierten Fehlermechanismen, -codes und -meldungen gebunden werden.

In diesem Abschnitt werden alle von einem konkreten technischen Binding unabhängigen Fehler und Warnungen aufgelistet und beschrieben. Hierbei wird zwischen Ausnahmesituationen im Zusammenhang mit der sicheren Kommunikation zwischen logischen EFA-Bausteinen und mit einzelnen Argumenten eines Operationsaufrufs zusammenhängenden Problemen unterschieden. Fehlern und Warnungen, die spezifisch für eine einzelne Operation sind, werden an dieser Stelle nicht aufgeführt, sondern im Kontext der logischen Spezifikation der entsprechenden Operationen beschrieben.

Sicherheit(skontext)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Feeln.01.01}

Schutzziel	Fehler bzw. Warnung	Betroffene Dienste
Identifizierung und Authentifizierung von EFA-Teilnehmern	**Fault: Invalid Subject-ID** Die Identität eines EFA-Teilnehmers ist für einen EFA-Dienste nicht verifizierbar. Dieser Fehler kann z.B. auftreten, wenn ein EFA-Teilnehmer im Rahmen der Identifizierung/Authentifizierung durch eine ID repräsentiert wird, die einer ID-Domäne entnommen wurde, die dem EFA-Provider nicht bekannt ist bzw. von diesem nicht unterstützt wird. **Fault: Weak Authentication** Das zur Authentifizierung des EFA-Teilnehmers genutzte Verfahren wird von einem EFA-Dienste nicht akzeptiert bzw. der die Authentifizierung bestätigende Dienst wird nicht als vertrauenswürdig anerkannt. Beispielsweise kann ein EFA-Provider festlegen, dass eine alleinige Authentisierung über User-ID/Passwort für einen Zugriff auf EFA-Daten nicht ausreichend ist. **Fault: Insufficient Attributes** Die zum EFA-Teilnehmer verfügbaren Attribute sind unvollständig oder unzureichend. Dieser Fehlerfall liegt insbesondere dann vor, wenn die bereitgestellten Angaben zum Nutzer nicht ausreichen, um eine Zugriffskontrollentscheidung zu	Angaben zur Identität und Authentizität von EFA-Teilnehmern werden über Sicherheitsnachweise als Sicherheitskontext gekapselt und als Teil eines Operationsaufrufs übertragen. Da alle EFA-Dienste einen solchen Sicherheitskontext erfordert, müssen die hier aufgeführten Fehlerfälle von allen EFA-Diensten geprüft und ggf. angezeigt werden.

	treffen oder einen den Sicherheitsanforderungen genügenden Audit Trail zu schreiben.	
Autorisierung von EFA-Teilnehmern	**Fault: Insufficient Permissions** Der EFA-Teilnehmer ist zwar grundsätzlich zum Zugang zu einer Fallakte berechtigt, verfügt aber nicht über die konkreten Rechte zur Durchführung der angeforderten Operation. Dieser Fehlerfall kann vor allem in Zusammenhang mit Sonderrollen der EFA auftreten. **Fault: Policy Mismatch** Die in dem Identitätsnachweis genutzten Kodierungen der Nutzer-Attribute (z.B. zu Rollen und Organisationszugehörigkeiten) können nicht eindeutig auf die in den Berechtigungsregeln einer EFA genutzten Attribute abgebildet werden. **Fault: Grace Period** Die zum EFA-Teilnehmer verfügbaren Attribute sind unvollständig oder unzureichend. Dieser Fehlerfall liegt insbesondere dann vor, wenn die bereitgestellten Angaben zum Nutzer nicht ausreichen, um eine Zugriffskontrollentscheidung zu treffen oder einen den Sicherheitsanforderungen genügenden Audit Trail zu schreiben.	Bei der Prüfung von Zugriffsrechten werden die in einer Einwilligung definierten Berechtigungen mit den im aktuellen Sicherheitskontext gekapselten Nutzerattributen abgeglichen. Da alle Operationen der EFA einer Berechtigungsprüfung unterliegen, müssen die hier aufgeführten Fehlerfälle von allen EFA-Diensten geprüft und ggf. angezeigt werden.
Vertraulichkeit	**Fault: No Channel** Der zur Übertragung von Daten benötigte sichere Kommunikationskanal kann nicht aufgebaut werden.	Dieser Fehlerfall betrifft vorrangig den EFA-Client, der für den Aufbau sicherer Kommunikationskanäle zu allen genutzten EFA-Diensten verantwortlich ist.
Authentizität und Integrität von EFA-Daten	**Fault: Integrity Violation** Die Integrität übermittelter medizinischer Daten und/oder zugehöriger Metadaten ist nicht gegeben bzw. kann nicht in dem erforderlichen Maß verifiziert werden. **Fault: No Originator Authenticity** In übertragenen Daten oder Metadaten fehlen ausreichend abgesicherte Angaben zu der für diese Daten verantwortlichen Person bzw. Organisation.	Diese Fehlerfälle betreffen alle Operationen, in denen Dokumente oder Metadaten übertragen werden.

Nicht-Abstreitbarkeit, Dokumentation und Audit-Trail	**Fault: Audit Trail Failure** Ein Audit Trail Eintrag kann nicht geschrieben werden, so dass die angeforderte Operation nicht ausgeführt werden kann.	Dieser Fehlerfall alle EFA-Dienste. Jeder Dienst muss vor Ausführung einer Operation sicherstellen, dass der zugehörige Audit Trail Eintrag geschrieben werden kann.
Verfügbarkeit von EFA-Teilnehmern und EFA-Daten	**Fault: Unknown Service Provider** Ein EFA-Dienst kann nicht lokalisiert werden bzw. die verfügbaren Informationen erlauben es nicht, eine Kommunikation mit diesem Dienst aufzubauen. **Fault: Service Not Available** Ein angeforderter EFA-Dienst ist nicht verfügbar.	Dieser Fehlerfall betrifft vorrangig den EFA-Client, der für den Aufbau sicherer Kommunikationskanäle zu allen genutzten EFA-Diensten verantwortlich ist.

Operationsaufruf -und abwicklung

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Feeln.01.02}

In diesem Abschnitt werden Fehlerfälle beschrieben, die durch fehlerhafte Angaben in den Argumenten eines Operationsaufrufs ausgelöst werden. Prinzipiell können diese Fehlerfälle damit bei allen Operationen auftreten, die das angegebene Argument als Eingabe erwarten. Die in der Tabelle angegebene Kurznamen der einzelnen Fehler und Warnungen dienen lediglich der besseren Referenzierbarkeit innerhalb dieses Spezifikationsdokuments und müssen in einem konkreten Binding der EFA-Operationen auf die im entsprechenden Standard definierte Fehlermeldungen und -codes abgebildet werden.

Argument	Fehler bzw. Warnung	betroffene Operationen
patientID	**Fault: Invalid PID** Die bei einem Operationsaufruf angegeben Patienten-ID kann nicht aufgelöst werden. Dieser Fehler tritt auf, wenn der aufrufende Akteur eine Patienten-ID verwendet, die nicht im EFA-Netzwerk bzw. beim EFA-Provider registriert ist. Bei dieser Registrierung ist es nicht erforderlich, dass die Identität der Person des Patienten offengelegt wird; wesentlich ist lediglich, dass für EFA-Teilnehmer eine Möglichkeit besteht, eine Abbildung intern verwendeter IDs auf eine in einem EFA-Netzwerk einheitliche ID herzustellen. Anmerkung: Dieser Fehler kann nicht auftreten, wenn in einem EFA-Netzwerk ein von der EFA vollständig unabhängige Verwaltung von einheitlichen Patienten-IDs realisiert ist und keine über dieses Netzwerk	createECR listPartitions

	hinausgehende Verknüpfung von Patientendaten stattfindet. In diesem Fall müssen EFA-Anwendungsdienste übermittelte Patienten-IDs als valide akzeptieren.	
purpose	**Fault: Invalid Purpose** Die für eine Fallakte festzusetzende Zweckbindung ist ungültig. Dieser Fehler tritt auf, wenn bei der Anlage einer Fallakte oder im Rahmen einer Änderung einer Einwilligung eine Fallakte mit einem Zweck verknüpft werden soll, der entweder falsch/unvollständig kodiert ist oder undefinierte Festsetzungen (Codes) enthält. **Fault: Prohibited Purpose** Die für eine Fallakte festzusetzende Zweckbindung ist unzulässig. Dieser Fehler tritt auf, wenn bei der Anlage einer Fallakte oder im Rahmen einer Änderung einer Einwilligung eine Fallakte mit einem Zweck verknüpft werden soll, der zu grobgranular ist oder vom angesprochenen EFA-Provider explizit nicht unterstützt wird. Ein Beispiel für die letzte Konstellation ist ein EFA-Provider, der sich auf Fallakten zu bestimmten DMPs spezialisiert hat und keine Anlage von Fallakten zu anderen Diagnosen erlaubt.	createECR listPartitions
consentInfo	**Fault: Unidentifiable Participant** Eine oder mehrere der im *consentInfo* benannten zu berechtigenden Personen bzw. Organisationen • können nicht identifiziert werden, d.h. sind nicht in einem für den EFA-Provider zugänglichen Teilnehmerverzeichnis registriert oder • können anhand der angegebenen Informationen nicht eindeutig identifiziert werden. **Fault: Prohibited Role-Assignment** Eine im *consentInfo* beschriebene Rollenbelegung ist nach den Regularien des EFA-Netzwerks nicht zulässig. Beispielsweise kann ein EFA-Verbund festlegen, dass nur Personen mit einer entsprechenden Schulung die Rolle des Fallaktenmanager ausfüllen dürfen. **Fault: Inconsistent PID** Bei bestehender Akte: Der im *consentInfo* benannte Patient kann nicht auf die an die bestehende Akten gebundene patientID abgebildet werden. **Fault: Prohibited Lifespan** Die angegebene Gültigkeitdauer der Einwilligung (und damit der daran hängenden Akte) ist nicht gültig, da sie im EFA-Netzwerk definierte Vorgaben über- oder unterschreitet. **Fault: Inconsistent Consent** Im *consentInfo* enthaltene Angaben sind inkonsistent oder gar widersprüchlich zu anderen Argumenten des Operationsaufrufs.	createECR registerConsent closeECR

partitionID	**Fault: Invalid Partition** Die angegeben Partitions-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der übergeordneten Akte auszuführen.	listData provideData registerData
ecrRef	**Fault: Invalid ECR** Die angegeben EFA-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der Akte auszuführen.	createPartition closeECR registerConsent
document	**Warning: Integrity Violation** Bei einem mit einem Integritäts- und/oder Authentizitätsschutz versehenen Dokument wurde eine mögliche	createECR
consentDoc	Verletzung der Integritär/Authentizität festgestellt. Das betroffene Dokument wurde nicht in die Akte eingestellt, der Operationsaufruf aber ansonsten bearbeitet.	createPartition closeECR registerConsent
	Warning: Security Check Failure Ein in die Akte einzustellendes Dokument hat die Sicherheitsfilter des Repository nicht passiert (z.B. da angegebenes Format und erkanntes Format nicht übereinstimmen). Das betroffene Dokument wurde nicht in die Akte eingestellt, der Operationsaufruf aber ansonsten bearbeitet.	provideData
docMetadata	**Warning: Inappropriate Metadata** Die zu einem Dokument bereitgestellten Metadaten sind unvollständig, falsch kodiert oder nicht konsistent. Das betroffene Dokument wurde nicht in die Akte eingestellt, der Operationsaufruf aber ansonsten bearbeitet.	provideData registerData
	Warning: Prohibited Document Type Dokumente mit den in den Metadaten beschriebenen Eigenschaften dürfen nicht in die benannte Fallakte eingestellt werden. Die betroffenen Dokumente wurden nicht in die Akte eingestellt, der Operationsaufruf aber ansonsten bearbeitet. Dieser Fehler kann seine Ursache sowohl in Vorgaben des EFA-Providers (z.B. Festlegung einer maximalen Dateigröße) als auch des EFA-Netzwerks haben (z.B. Ausschluss von Dokumenten mit sehr hohem Schutzbedarf oder Einschränkung bestimmter Aktenausprägungen auf vorab definierte Dokumenttypen).	
docRelationship	**Warning: Invalid Association Target** Die zu einem Dokument benannten Beziehungen referenzieren auf Dokument-IDs, die nicht auflösbar sind bzw. Dokumente in einer anderen Fallakte referenzieren. Die betroffenen Dokumentenbeziehungen wurden verworfen, das Dokument aber in die Akte eingestellt.	provideData registerData
	Warning: Consent Association Corrected	createPartition

	Wenn bei der Registrierung einer Einwilligung (bzw. der Rücknahme einer Einwilligung) neben einem die Einwilligung beschreibenden consentInfo-Objekt auch ein (gescanntes) Dokument (consentDoc) eingestellt wird, muss das Dokument in einer "Append"-Beziehung zu dem consentInfo-Dokument stehen. Falls diese Beziehung nicht oder falsch gesetzt ist, wird sie vom EFA-Provider gesetzt bzw. korrigiert. In diesem Fall wird eine Warnung ausgegeben, dass die Dokumentenbeziehungen durch den Provider verändert wurden.	closeECR registerConsent

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Logical Perspective = Computational Dimension

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Dienste**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Technische Akteure der EFA

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eist.01}`

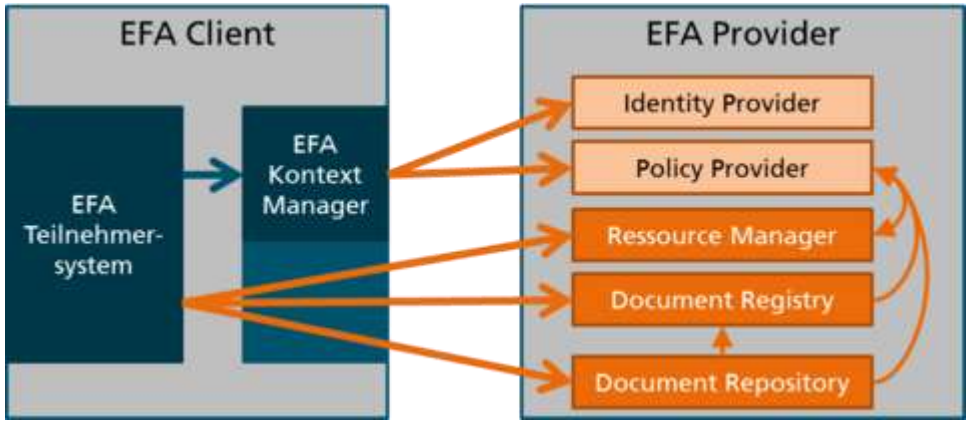
Die logische Anwendungsebene einer Fallakten-Infrastruktur besteht im einfachsten Fall aus fünf Klassen von Akteuren:

- Ein EFA-Kontext-Manager (**eCR Context Manager**) baut den Sicherheitskontext zur Nutzung von Fallakten auf und verwaltet die darin bereit gestellten Sicherheitsnachweise des EFA-Teilnehmers.
- Ein EFA-Ressource-Manager(**eCR Resource Manager**) stellt ein Verzeichnis zur Verwaltung von Fallakten und EFA-Partitionen bereit. Mit dem selben Patienten und dem selben Zweck verbundene Partitionen bilden eine Fallakte.
- Ein EFA-Daten-Register (**eCR Document Registry**) stellt ein Verzeichnis zur Verwaltung von Dokumenten bereit. In einem regionalen Gesundheitsnetz kann ein einzelner EFA-Provider das EFA-Register für das gesamte Netzwerk anbieten.
- Ein EFA-Speichersystem (**eCR Repository**) hält die registrierten Dokumente vor und stellt sie für berechtigte Nutzer zum Abruf bereit. Jeder EFA-Provider kann ein eigenes EFA-Speichersystem bereitstellen und an das EFA-Register anbinden.
- Ein EFA-Teilnehmersystem (**eCR Consumer**) bildet eine Nutzerschnittstelle ab, über die ein Arzt Behandlungsdaten anderer Ärzte aus an einem EFA-Daten-Register registrierten Speichersystemen abrufen kann bzw. in einem Speichersystem verwaltete Behandlungsdaten am EFA-Register registrieren kann.

Hinzu kommen zwei Klassen von Sicherheitstoken-Diensten, die jeweils Sicherheitsnachweise zum Aufbau eines zwischen EFA-Teilnehmersystem und EFA-Fachdienst (Register bzw. Speichersystem) geteilten Sicherheitskontextes bereit stellen:

- Ein **Identity Provider** stellt einen von allen anderen EFA-Akteuren als vertrauenswürdig akzeptierten Identitätsnachweis für authentifizierte Nutzer aus. Der Identity Provider unterstützt potenziell beliebige Verfahren der Authentifizierung (z. B. mittels Passwort, HBA oder SMC-B).
- Ein **Policy Provider** liefert die für den aufrufenden Nutzer gültigen Berechtigungsregeln (Policy) auf einer spezifischen Fallakte.

Der Aufruf der Sicherheitstoken-Dienste und die Verwaltung der von diesen abgerufenen Sicherheitsnachweise wird gegenüber dem EFA-Teilnehmersystem über den EFA-Kontext-Manager gekapselt.



Querverweise und Referenzen

- EFA Kommunikationsmuster
- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Kommunikationsmuster**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Kommunikationsmuster

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01}

Kommunikationsmuster bilden die Ende-zu-Ende definierten EFA Interaktionsmuster auf einzelne logische Transaktionen zwischen technischen Akteuren ab. Sie sind ebenfalls funktional ausgerichtet und beschreiben, wie ein technischer Anwendungsfall über zwischen EFA Diensten definierte Ablaufsequenzen realisiert wird. Sie stellen damit das über den EFA Diensten definierte Protokoll dar.

Die nachfolgende Tabelle stellt die Umsetzung der Interaktionsmuster über die hier definierten Kommunikationsmuster dar.

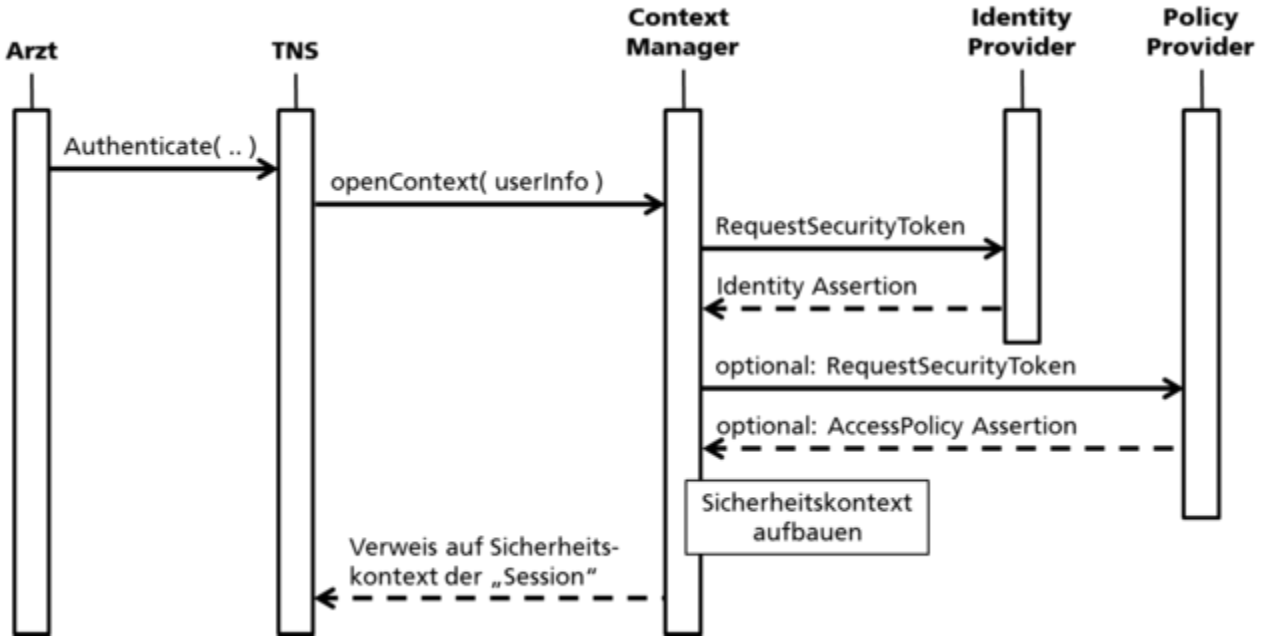
Interaktionsmuster	Kommunikationsmuster	Anmerkungen
Auffinden der Fallakten eines Patienten	Auflisten von Partitionen	Mit dem Kommunikationsmuster werden alle mit einem angegebenen Patienten verknüpften EFA-Partitionen ermittelt, zu denen der Aufrufer zugangsberechtigt ist (d.h. diese Partitionen sind Bestandteil von Fallakten zu denen der Aufrufer vom Patient als Behandlungsteilnehmer benannt wurde). Die Sortierung der Partitionen zu Fallakten anhand des jeweils mit den Partitionen verbundenen Zwecks erfolgt im Teilnehmersystem.
Browsing über eine Akte	Auflisten von Dokumenten	Das Kommunikationsmuster ruft die Metadaten aller in einer angegeben Partition enthaltenen Dokumente ab. Das Teilnehmersystem kann anhand dieser Daten eine nach beliebigen Kriterien strukturierte Ansicht für den Nutzer erzeugen, über die der EFA-Teilnehmer anschließend navigieren kann. Soll die Ansicht die gesamte Akte umfassen, müssen zunächst mit dem Kommunikationsmuster Auffinden der Fallakten eines Patienten alle Partitionen der Akte ermittelt werden. Anschließend muss das Kommunikationsmuster Auflisten von Dokumenten für jede einzelne dieser Partitionen abgespult werden.
Abruf von Datenobjekten	Abrufen von Dokumenten	Der Abruf eines Dokuments erfordert die Angabe der Dokumenten-ID, die zuvor über das Kommunikationsmuster Auflisten von Dokumenten ermittelt werden muss.
Einstellen von Datenobjekten	Einstellen von Dokumenten	Die im Interaktionsmuster beschriebenen Varianten (Ersetzen, Aktualisieren, Verknüpfen von Dokumenten) werden über das Kommunikationsmuster unterstützt.
Invalidieren von Datenobjekten	Einstellen von Dokumenten	Datenobjekte werden invalidiert, indem sie durch ein (potenziell leeres) Dokument eines speziellen Typs ersetzt werden. Dieses Verhalten soll für alle im IHE Cookbook beschriebenen Aktentypen gleichermaßen definiert werden. Die konkrete Spezifikation des "Invalidierungsdokuments" und seiner Metadaten ist daher Gegenstand des IHE Cookbooks.

Anlegen einer Fallakte	Anlegen einer Fallakte	Das Kommunikationsmuster ist eine 1:1 Abbildung des Interaktionsmusters und seiner Varianten/Ausnahmeszenarien.
Anlegen und Registrieren einer Partition	Anlegen einer Partition	Die im Interaktionsmuster explizit benannten Registrierung einer neuen Partition an einer Fallakte ist auf Ebene des Kommunikationsmusters nur implizit, da alle zum gleichen Patienten und Zweck angelegten Partitionen implizit zu einer Fallakte zusammengefasst sind. Eine explizite Registrierung ist daher auf Ebene der technischen Anwendungsfälle nicht erforderlich.
Schließen einer Fallakte	Schließen einer Fallakte	Das Kommunikationsmuster ist eine 1:1 Abbildung des Interaktionsmusters und seiner Varianten/Ausnahmeszenarien.
Änderung einer Einwilligung	Registrierung einer neuen Einwilligung	Anpassungen des Teilnehmerkreises einer EFA erfordern eine neue Einwilligung des Patienten. Das Kommunikationsmuster übermittelt diese an den EFA-Provider, der die angegebenen Änderungen in der Konfiguration einer Fallakte und ihrer definierten Zugriffsrechte vornimmt.
Autorisierung eines weiteren Teilnehmers	Anfordern eines Berechtigungstoken	Der Patient kann einer EFA weitere Teilnehmer über (Offline-)Token hinzufügen. Dieses Kommunikationsmuster beschreibt die Anforderung eines solchen Tokens durch einen bereits berechtigten EFA-Teilnehmer.
	Einlösen eines Berechtigungstoken	Der Patient kann einer EFA weitere Teilnehmer über (Offline-)Token hinzufügen. Dieses Kommunikationsmuster beschreibt, wie ein Leistungserbringer mit Hilfe eines solchen Tokens als Teilnehmer einer EFA autorisiert wird.
Zusammenführen von Fallakten	Registrierung einer neuen Einwilligung	Die Zusammenführung von zwei oder mehr Fallakten erfordert eine entsprechende Einwilligung des Patienten, in der insbesondere der Zweck und der Teilnehmerkreis der zusammengeführten Akte explizit benannt sind. Das Kommunikationsmuster übermittelt diese an den EFA-Provider, der die angegebenen Änderungen in der Konfiguration einer Fallakte und ihrer definierten Zugriffsrechte vornimmt.
-	Aufbau des Sicherheitskontextes	Dieses Kommunikationsmuster bildet einen technischen Anwendungsfall ab, der im Idealfall keine Nutzerinteraktion beinhaltet und zu dem von daher auch kein Interaktionsmuster existiert. Der Aufbau eines Sicherheitskontextes ist Grundlage aller anderen Kommunikationsmuster und stellt sicher, dass den beim EFA-Provider angesiedelten Diensten alle Informationen authentisch und vollständig zur Verfügung stehen, die für die Prüfung und Durchsetzung der aus der Einwilligung abgeleiteten Berechtigungsregeln sowie zur datenschutzkonformen Protokollierung benötigt werden.

Aufbau des Sicherheitskontextes

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.01}

Die nachfolgende Abbildung stellt das Kommunikationsmuster zum Aufbau des Sicherheitskontextes im Überblick dar. Jeder nachfolgende Aufruf eines EFA-Dienstes erfordert, dass der im EFA-Kontext-Manager verwaltete Sicherheitskontext in Form von authentischen Sicherheitsnachweisen an den aufgerufenen Dienst übergeben wird. Dieser wird so in die Lage versetzt, den Sicherheitskontext des Aufrufers zu rekonstruieren und dadurch den Aufruf innerhalb dieses Kontextes gegen die geltenden Sicherheitsregeln zu verifizieren.



1. Der EFA-Teilnehmer authentisiert sich gegenüber dem EFA-Teilnehmersystem. Die EFA Spezifikation macht hierzu keine normativen technischen Vorgaben, Umsetzungen müssen jedoch die Regularien des EFA Sicherheitskonzepts berücksichtigen.

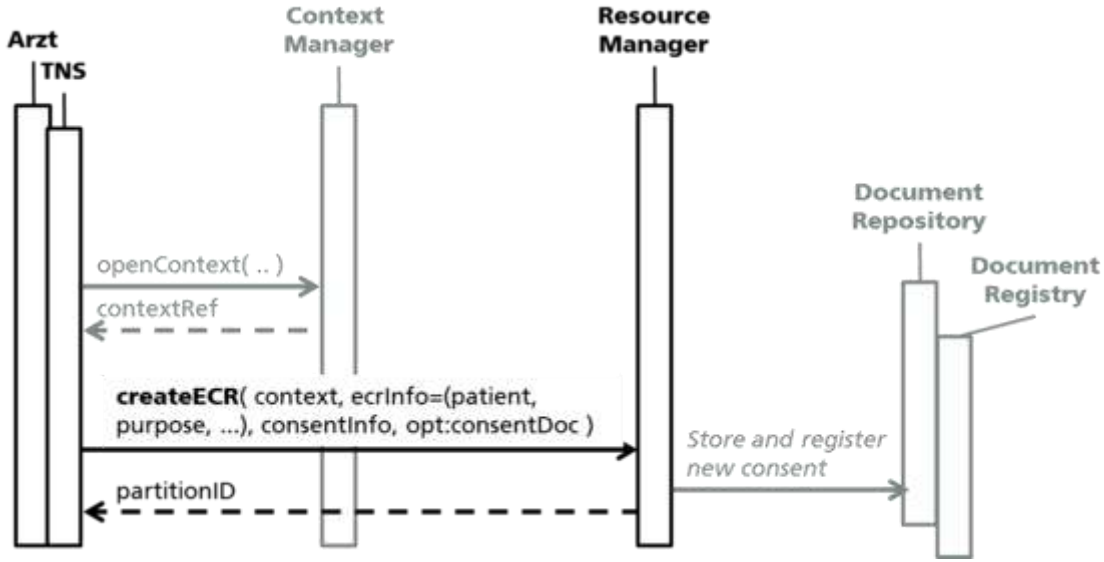
2. Das EFA-Teilnehmersystem (TNS) erfasst die für die EFA-Nutzung wichtigen Informationen zum EFA-Teilnehmer und übermittelt sie an den EFA-Kontext-Manager. Hierzu wird die funktionale Schnittstelle *openContext* des EFA-Kontext-Managers verwendet.
3. Der EFA-Kontext-Manager nutzt die übergebenen Informationen, um für den EFA-Teilnehmer von den EFA-Sicherheitsdiensten Sicherheitsnachweise abzurufen, die von den EFA-Fachdiensten prüfbar sind. Welche Dienste aufgerufen werden, hängt von der konkreten Sicherheitspolitik eines EFA-Netzwerks ab. Eine typische Konfiguration umfasst den Aufruf des *Identity Providers* zum Abruf eines netzweit gültigen Identitäts- und Authentisierungsnachweises. Optional können auch Teile der für den Teilnehmer geltenden Zugriffspolitik bereits vor dem Aufruf der EFA-Fachdienste von einem *EFA Policy Provider* abgefragt werden.
4. Der EFA-Kontext-Manager verknüpft die abgerufenen Sicherheitsnachweise mit der aktuellen Nutzersitzung und liefert einen Verweis auf den so gebildeten Sicherheitskontext an das EFA-Teilnehmersystem zurück.

Anlegen einer Fallakte

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.02}`

Eine neue Fallakte wird angelegt, indem im EFA-Ressource-Manager eines EFA-Providers für den betroffenen Patienten eine neue Partition angelegt wird, die sowohl mit einem Zweck als auch einer Einwilligung verbunden ist:

- Gemäß der Vorgaben des Interaktionsmusters *Anlegen einer Fallakte* erteilt der Patient eine informierte, schriftliche Einwilligung über die Nutzung einer Fallakte zur Unterstützung einer Behandlung. Die vom Patienten benannten Teilnehmer der Behandlung sind die zugriffsberechtigten Teilnehmer der Fallakte.
- Der Arzt baut über sein EFA-Teilnehmersystem den zur Anlage einer EFA erforderlichen Sicherheitskontext auf (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
- Der Arzt fordert beim von seinem EFA-Provider bereit gestellten *EFA-Ressource-Manager* die Anlage einer neuen Fallakte an. Hierbei benennt der den Zweck der Akte sowie die als Teilnehmer zu berechtigenden Personen und Organisationen. Mit der Anlage einer Fallakte ist implizit die Anlage einer Partition verknüpft.



- Der EFA-Provider prüft, ob bei ihm für den Patienten bereits eine Fallakte existiert, die mit dem angegebenen Zweck assoziiert ist. Im Ergebnis dieser Prüfung müssen zwei Konstellationen unterschieden werden:
  - Es besteht noch keine Fallakte für den benannten Patienten und den benannten Zweck bei diesem EFA-Provider: Eine neue, aus einer einzigen Partition bestehende Fallakte wird angelegt
  - Es besteht bereits eine Fallakte für den benannten Patienten und den benannten Zweck bei diesem EFA-Provider: Sofern dies durch die Einwilligung vom Patienten legitimiert/angefordert ist, wird die bestehende Akte in eine neu anzulegende Fallakte überführt. Hierzu werden alle Partitionen der bestehenden Akte mit der neuen Akte verknüpft. Der Teilnehmerkreis (und damit die Zugriffsrechte) werden wie in der neuen Einwilligung angegeben für die gesamte Akte festgeschrieben. Alle für Akten zu dem angegebenen Zweck von Patienten zuvor gegebenen Einwilligungen werden damit durch die neu gegebene Einwilligung außer Kraft gesetzt.

Die nachfolgenden Abschnitte definieren das Verhalten des EFA-Providers in diesen beiden Konstellationen.

Neu-Anlage einer Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.02.01}

- Im EFA-Berechtigungsmanagement des EFA-Providers wird eine neue Berechtigungsregel registriert, die den für die Aktenanlage angegebenen Zweck und die Patientenidentität mit den in der Patienteneinwilligung angegebenen Vorgaben zu den EFA-Teilnehmern und der Gültigkeit der Fallakte verknüpft.
    - (Patient, Zweck) -> (Teilnehmer, Gültigkeit)
- Der EFA-Provider legt zu der Akte eine initiale Partition als Container-Objekt an, mit dem Dokumente verknüpft werden können.
- Sofern die Einwilligung des Patienten als (gescanntes) Dokument vorliegt, wird diese als Dokument in die neu angelegte Partition eingestellt.

Fusion mit einer bestehenden Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.02.02}

- Im EFA-Berechtigungsmanagement des EFA-Providers wird die Patienteneinwilligung (Berechtigungsregel) für die bestehende Fallakte darauf hin geprüft, ob
    - die zu der bestehenden Akte registrierte Einwilligung eine Erweiterung der Berechtigungen durch den die Aktenneuanlage initiierenden Arzt zulässt, d.h. dieser dort bereits als Teilnehmer registriert ist. Ist dies nicht der Fall, wird der Vorgang abgebrochen und eine Fehlermeldung ausgegeben.
    - die vom Patienten für die neue Akte gegebene Einwilligung die Übernahme einer eventuell bereits bestehenden Akte autorisiert. Ist dies nicht der Fall, wird der Vorgang abgebrochen und eine Fehlermeldung ausgegeben. Um die neue Akte dennoch anlegen zu können, muss eine entsprechend erweiterte Einwilligung des Patienten vorliegen.
- Die neue Akte wird angelegt (s.o)
- Die Partitionen der bestehenden Akte werden mit der neuen Akte verknüpft. Die "alte" Akte wird aufgelöst und alle in deren Kontext gegebenen Einwilligungen verlieren ihre Gültigkeit.

Aktenfusion vs. Änderung der Einwilligung

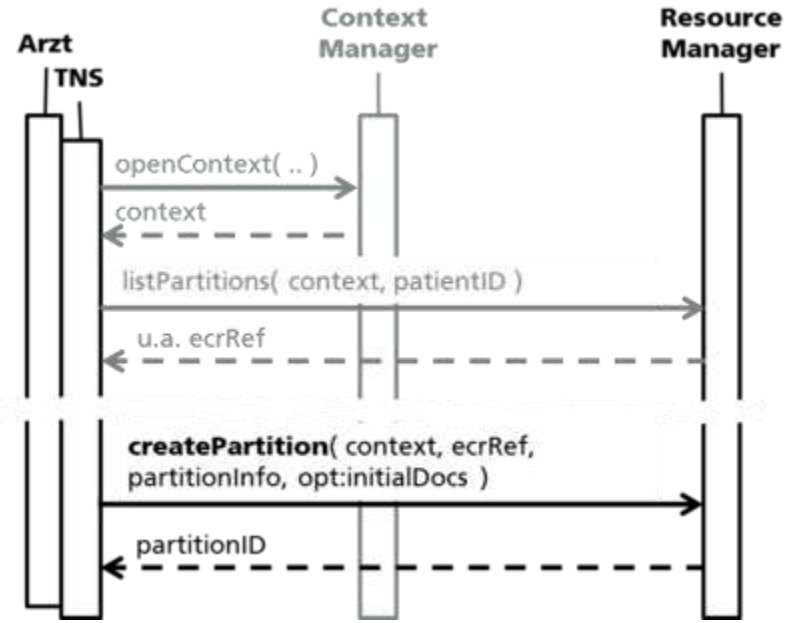
Der Zustand der Fallakte nach Ablauf dieses Kommunikationsmusters entspricht weitestgehend einem Zustand, der auch über das Kommunikationsmuster Registrierung einer neuen Einwilligung hergestellt werden kann. Die Aktenfusion findet jedoch immer im Rahmen einer Akten-Neuanlage statt, d.h. es wird davon ausgegangen, dass im nächsten Ablaufschritte Daten in diese Akte eingestellt werden. Daher wird bei der Akten-Neuanlage - und damit auch der Aktenfusion - immer auch eine neue Partition angelegt und ein Verweis auf diese Partition an den Aufrufer zurückgeliefert.

Damit entspricht eine Aktenfusion einer Sequenz der Kommunikationsmuster Registrierung einer neuen Einwilligung und Anlegen einer Partition.

Anlegen einer Partition zu einer bestehenden Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.03}

Zur Teilnahme an einer EFA berechtigte Teilnehmer können dieser Akte weitere Partitionen - z.B. zur Zusammenfassung der im Kontext eines Klinikaufenthalts erhobenen Daten - hinzufügen. Die Anlage einer neuen Partition muss innerhalb eines gültigen EFA-Sicherheitskontextes erfolgen und erfordert neben der Angabe einiger Daten zu der Partition selbst (Titel, etc.) vor allem eine Referenz auf die Akte, der die Partition hinzugefügt werden soll. Mit der Anlage der Partition können bereits in die Partition einzustellende Dokumente übergeben werden.



Die Anlage einer Partition erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Auffinden und Öffnen der Fallakte, der die Partition hinzugefügt werden soll. Hierzu werden Metadaten der die Akte repräsentierenden Partitionen abgerufen, in denen u.a. die eindeutige Referenz auf die Akte kodiert ist (siehe Kommunikationsmuster Auflisten von Partitionen).
3. Anlegen der neuen Partition innerhalb des Sicherheitskontextes durch Angabe der Referenz auf die übergeordnete Akte, der Metadaten zur Partition sowie (optional) in die Partition einzustellender Dokumente.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die Akte berechtigt ist. Falls dies nicht der Fall sein sollte wird die Operation mit einer Fehlermeldung abgebrochen.
    2. Der EFA-Provider legt die internen Strukturen der Partition an und verknüpft diese mit den Zuordnungsdaten der Fallakte (Patientenidentität und Zweckbezeichnung der Fallakte). Hierdurch ist die neue Partition Bestandteil der Akte und es gelten die für die Akte definierten Zugriffsrechte.
    3. Der EFA-Provider verknüpft die ggf. übergebenen Dokumente mit der neuen Partition.
4. Über interne Mechanismen wie z.B. einen Kommunikationsserver kann der Teilnehmer die neue Partition mit einer internen ID (z.B. Fall-ID der aktuellen Behandlungsepisode) verknüpfen um das Einstellen intern mit dieser ID verknüpfter Daten in die EFA zu vereinfachen.

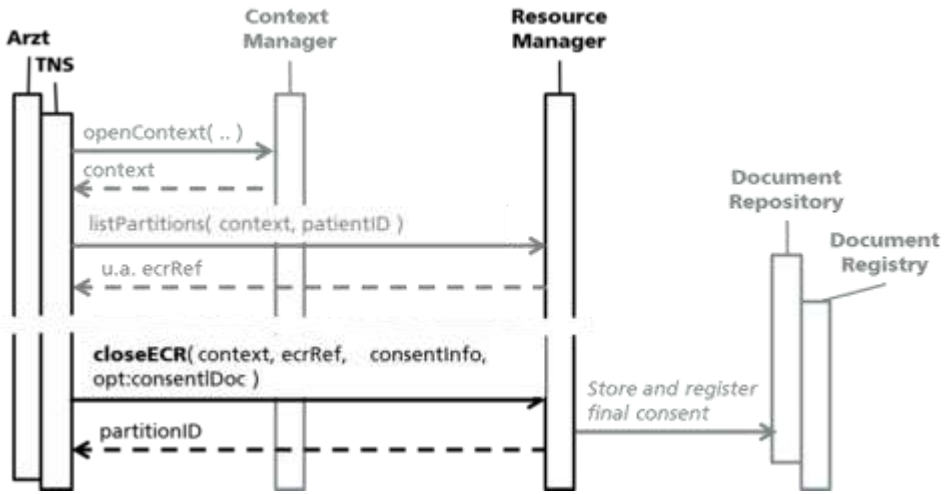
Schließen einer Fallakte

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.04}

Eine Fallakte wird durch den EFA-Provider geschlossen, wenn die vom betroffenen Patienten gegebene Einwilligung ihre Gültigkeit verliert (siehe auch Zustandsdiagramme zu den EFA-Geschäftsobjekten).

Die Gültigkeit der Einwilligung erlischt implizit mit Erreichen des in der Einwilligung angegebenen Gültigkeitsdatums. Hier ist es Verantwortung des EFA-Providers, den entsprechenden Zustandsübergang anzustoßen und die Zugriffsrechte auf die Akten entsprechend anzupassen. Darüber hinaus erlischt die Einwilligung, wenn sie entweder explizit vom Patienten zurückgenommen wird oder wenn der Zweck der EFA nicht mehr gegeben ist. In diesen Fällen greift das Interaktionsmuster "EFA Schließen".

Das Kommunikationsmuster "Schließen einer Fallakte" entspricht weitgehend dem gleichnamigen Interaktionsmuster und besteht im wesentlichen in der Übermittlung der Aufforderung zur Schließung der Akte an den EFA-Provider.



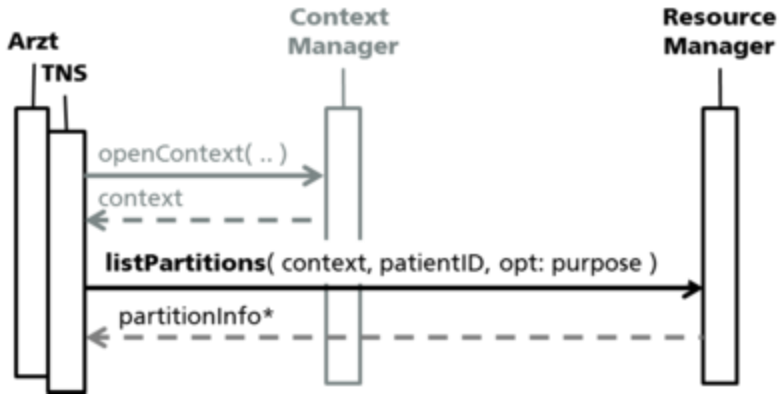
Im Einzelnen werden die folgenden Schritte durchlaufen:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Auffinden und Öffnen der Fallakte, die geschlossen werden soll. Hierzu werden Metadaten der die Akte repräsentierenden Partitionen abgerufen, in denen u.a. die eindeutige Referenz auf die Akte kodiert ist (siehe Kommunikationsmuster Auflisten von Partitionen). Dieser Schritt ist erforderlich, da Angaben zum Grund der Aktenschließung als Dokument in der Akte abgelegt werden und damit die Voraussetzungen für diesen Schreibzugriff hergestellt werden müssen.
3. Schließen der Akte innerhalb des Sicherheitskontextes durch Angabe der Referenz auf diese Akte sowie der Begründung zur Schließung der Akte.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die Akte berechtigt ist. Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
    2. Der EFA-Provider verknüpft die Begründung zur Aktenschließung und die ggf. übergebenen Dokumente mit einer bestehenden Partition der Akte.
    3. Der EFA-Provider leitet die Schließung der Akte ein, indem er den Status der Akte und die Zugriffsberechtigungen gemäß des Lebenszyklus einer EFA ändert.

Auflisten von Partitionen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.05}

Eine Fallakte ist ein Verbund von Partitionen, die mit dem selben Patienten und dem selben Zweck verknüpft sind. Um auf eine Fallakte zuzugreifen müssen in einem ersten Schritt Informationen zu den zugehörigen Partitionen abgerufen werden. Anhand der so ermittelten Aktenreferenz (ecrRef) und Partitions-Identifier (partitionID) können anschließend Daten aus der Akte ausgelesen und in die Akte eingestellt werden.



Das Auflisten der Partitionen der für den anfragenden Nutzer zugreifbaren Fallakten erfolgt in den folgenden Schritten:

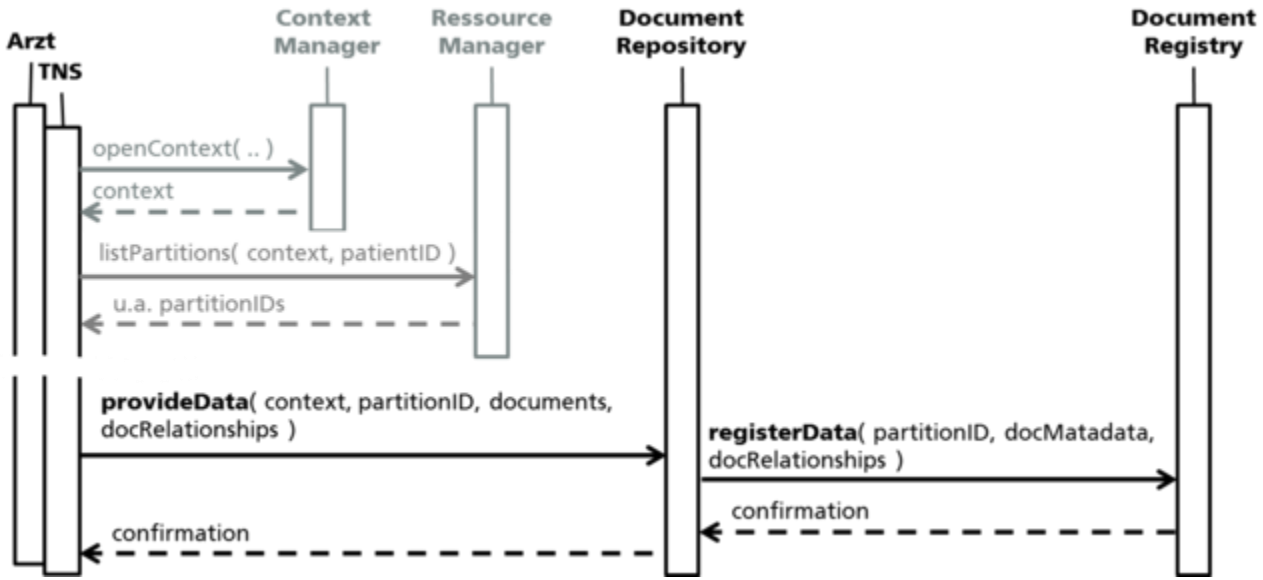
1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Senden der ID des Patienten, dessen EFAs gefunden und genutzt werden sollen, an den EFA-Provider.
    1. Der EFA-Provider sucht nach Aktenreferenzen (Patienten-ID und Zweck) an die eine Zugangsberechtigung für den anfragenden Arzt gebunden ist.
    2. Der EFA-Provider sucht nach Partitionen, die mit den gefundenen Aktenreferenzen verknüpft sind und sendet die Metadaten dieser Partitionen an den Aufrufer zurück
3. Das Teilnehmersystem (Primärsystem) zeigt dem Aufrufer die gefundenen Akten und zugehörigen Partitionen an

Einstellen von Dokumenten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.06}

Daten zu einer Fallakte werden immer in eine an diese Akte gekoppelte Partition eingestellt. Das Einstellen von Daten erfolgt innerhalb eines gültigen EFA-Sicherheitskontexts und bedingt, dass der die Daten einstellende Nutzer ein berechtigter Teilnehmer der Fallakte ist, zu der er Daten hinzufügen möchte.

Die Benennung der Ziel-Partition erfolgt über eine *partitionID*. Sofern diese nicht bereits im Primärsystem des Nutzers bekannt ist (z.B. aufgrund einer statischen Verknüpfung eines internen Fall-Identifiers mit dieser Partiton), muss dieser Identifier zunächst durch Öffnen der Fallakte - d.h. Auflisten der zugängigen Partitionen - ermittelt werden. Beziehungen zwischen Daten (z.B. Aktualisierung oder Ergänzung eines bestehenden Dokuments) müssen explizit benannt werden.



Das Einstellen von Daten in eine Partition erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Ermitteln der *partitionID*, mittels der die Ziel-Partition und deren übergeordnete Fallakte eindeutig identifizierbar sind. Sofern diese ID nicht bereits bekannt ist, muss sie über das Kommunikationsmuster *Auflisten von Partitionen* ermittelt werden.

3. Sofern die eingestellten Dokumente eine Aktualisierung oder Ergänzung in der EFA bereits vorhandener Daten darstellen: Ermitteln der documentIDs der zu aktualisierenden bzw. zu ergänzenden Dokumente (z.B. über das Kommunikationsmuster Auflisten von Dokumenten)
4. Senden der partitionID und der in diese Partition einzustellenden Daten an das Document Repository des EFA-Providers (siehe auch Hinweisbox weiter unten). Ggf. anzulegende Dokumentenbeziehungen müssen dabei explizit angegeben werden.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die der Partition übergeordneten Akte berechtigt ist. Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
    2. Der EFA-Provider prüft, ob der Teilnehmer berechtigt ist, bei diesem Provider Daten abzulegen (siehe auch Infobox weiter unten). Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
    3. Der EFA-Provider legt die übergebenen Daten zur sicheren Speicherung im Document Repository ab
    4. Das Document Repository sendet die Benennung der Ziel-Partition, die Metadaten der empfangenen Dokumente sowie ggf. benannte Dokumentenbeziehungen zur Registrierung an das Document Registry des EFA-Providers
    5. Der EFA-Provider verknüpft die übergebenen Dokumente im Document Registry mit der angegebenen Partition und speichert die Metadaten und Dokumentenbeziehungen sicher ab
    6. Sofern benannte Dokumentenbeziehungen die Ersetzung bestehender Dokumente anzeigen, wird der Status dieser Dokumente entsprechend geändert.
5. Der EFA-Provider meldet dem Teilnehmer die erfolgreiche Bereitstellung der übergebenen Dokumente zurück.

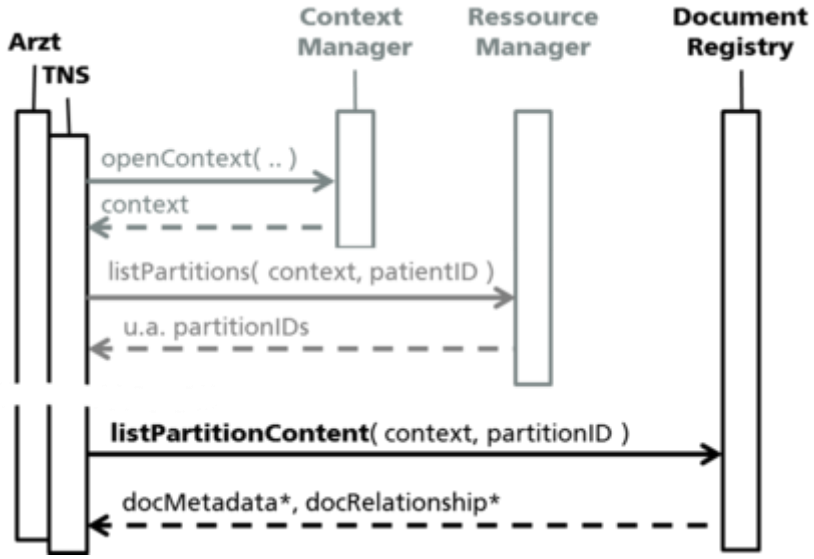
Zuordnung von Teilnehmern zu Providern
Jeder EFA-Teilnehmer ist immer einer oder mehreren Affinity-Domains zugeordnet. Jede Affinity-Domain wird durch einen EFA-Provider realisiert. Zwischen EFA-Teilnehmer und EFA-Provider besteht eine vertragliche Beziehung, die u.a. auch die Vorhaltung von Daten des Teilnehmers durch den Provider regelt. Wenn im Zusammenhang mit dem Einstellen von Daten somit von einem "EFA-Provider" die Rede ist, ist damit implizit immer ein EFA-Provider gemeint, mit dem der EFA-Teilnehmer eine vertragliche Beziehung hat, die ihm das Einstellen von EFA-Daten bei diesem Provider ermöglicht. Analog ist auch der Begriff "Document Repository" auf das Document Repository dieses Providers eingeschränkt, das dieser für die Daten des Teilnehmers vorgesehen hat. Ein Sonderfall ist die Konstellation, wenn ein Teilnehmer gleichzeitig Provider ist. In diesem Fall erfolgt die Datenvorhaltung analog zu den bestehenden Regularien für die Datenspeicherung innerhalb dieser Einrichtung.

Auflisten von Dokumenten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.07}

Daten zu einer Fallakte werden immer in an diese Akte gekoppelten Partition verwaltet. Das Auflisten der verwalteten Daten erfolgt immer auf Ebene dieser Partitionen, d.h. um alle mit einer Fallakte verknüpften Daten aufzulisten müssen alle Partitionen "angefasst" werden.

Die Benennung der auszulesenden Partition erfolgt über eine *partitionID*, die im Rahmen des Öffnens einer Fallakte beim Auflisten der zugängigen Partitionen ermittelt werden kann. Das Auflisten der Daten einer Partition liefert die Metadaten aller in der Partition enthaltenen Dokumente sowie die Beziehungen, die zwischen diesen Dokumenten und Dokumenten in dieser oder anderen Partitionen bestehen.



Das Auslesen der Metadaten zu allen an einer vorgegebenen Partition registrierten Dokumenten erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Ermitteln der *partitionID*, mittels der die auszulesende Partition und deren übergeordnete Fallakte eindeutig identifizierbar sind. Sofern diese ID nicht bereits bekannt ist, muss sie über das Kommunikationsmuster *Auflisten von Partitionen* ermittelt werden.
3. Senden der partitionID an das Document Registry des EFA-Providers.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die der Partition übergeordneten Akte berechtigt ist. Falls dies nicht der Fall sein sollte wird die Operation mit einer Fehlermeldung abgebrochen.

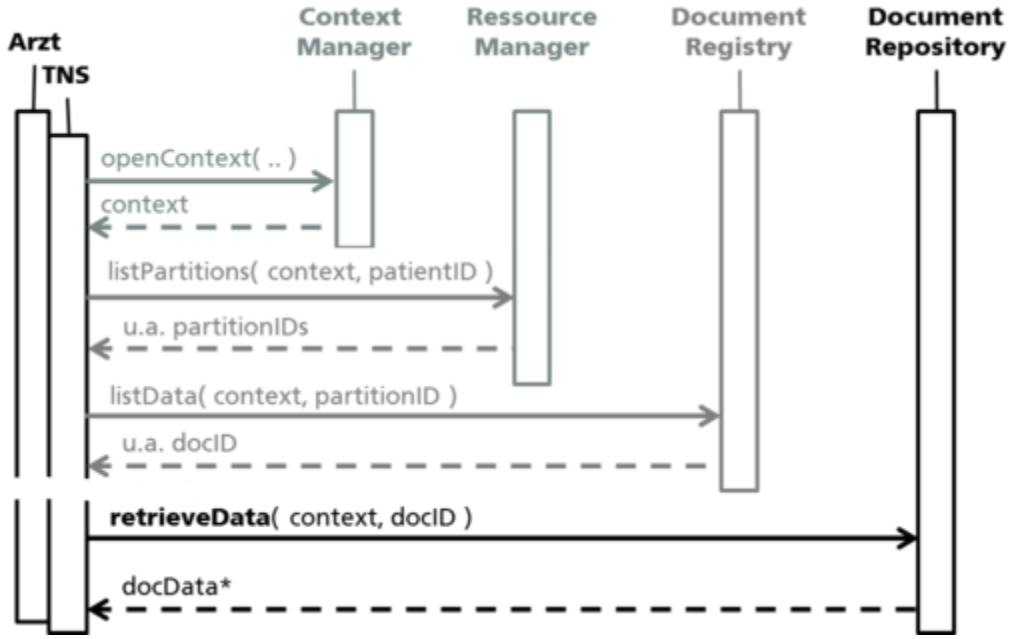
2. Im Document Registry werden die mit der Partition verknüpften Dokumente ermittelt und deren Metadaten zu einer Antwortnachricht zusammengestellt.
3. Die ausgehenden Beziehungen der gefundenen Dokumente zu anderen Dokumenten werden ermittelt und der Antwortnachricht hinzugefügt.

4. Der EFA-Provider übermittelt dem Teilnehmer die Metadaten und Dokumentenbeziehungen der in der Partition registrierten Dokumente zurück.

Abrufen von Dokumenten

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.08}

Der Abruf von Dokumenten aus einer Fallakte erfolgt über deren eindeutige Dokumenten-ID (*documentID*), die beim Auflisten der Inhalte einer Partition als Teil der Dokumenten-Metadaten bereitgestellt wird.



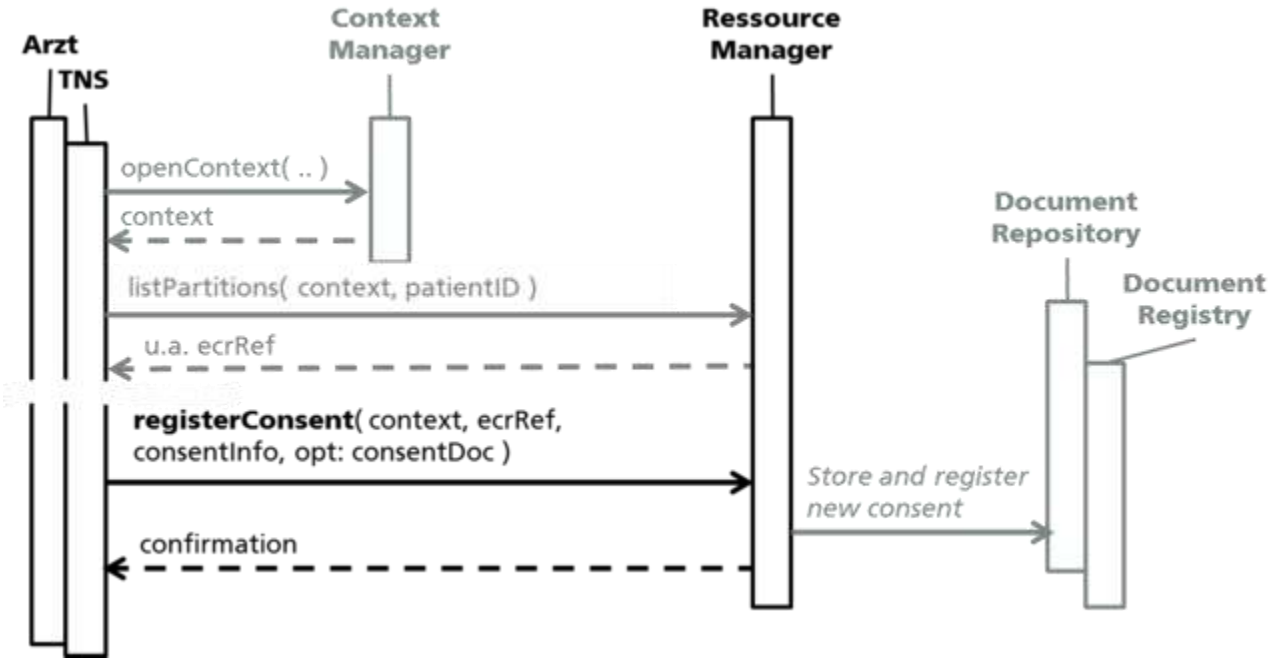
Das Abrufen von Dokumenten aus einer Fallakte erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Auflisten der Partitionen einer Fallakte und Auflisten der darin enthaltenen Dokumente.
3. Senden der *documentIDs* der abzurufenden Dokumente an das Document Repository des EFA-Providers, der die Partition verwaltet, in dem sich die angeforderten Dokumente befinden.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die den Dokumenten übergeordnete Akte berechtigt ist. Falls dies nicht der Fall sein sollte wird die Operation mit einer Fehlermeldung abgebrochen.
4. Der EFA-Provider übermittelt dem Teilnehmer die angefragten Dokumente zurück.

Registrierung einer neuen Einwilligung

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.09}

Die Registrierung einer neuen Einwilligung erfolgt innerhalb eines gültigen EFA-Sicherheitskontexts und bedingt, dass der die Einwilligung registrierende Nutzer ein berechtigter Teilnehmer der Fallakte ist.



Das Registrieren einer neuen Einwilligung erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Ermitteln der *ecrRef*, mittels der die Fallakte eindeutig identifizierbar sind, auf die sich die neue Einwilligung bezieht. Sofern diese ID nicht bereits bekannt ist, muss sie über das Kommunikationsmuster *Auflisten von Partitionen* ermittelt werden.
3. Senden des Aktenverweises, der Angaben zur neuen Einwilligung sowie eine ggf. verfügbare elektronische Version des vom Patienten unterschriebenen Einwilligungsdokuments an den Ressource Manager des EFA-Providers.
    1. Der EFA-Provider prüft, ob der Teilnehmer zum Zugriff auf die Akte berechtigt ist und für diese Akte Änderungen an den Zugriffsrechten initiieren darf. Falls dies nicht der Fall sein sollte wird die Operation mit einer Fehlermeldung abgebrochen.
    2. Sofern in der Einwilligung ein konkretisierter Zweck benannt ist: Der EFA-Provider prüft, ob für den Patienten bereits eine Akte zu dem konkretisierten Zweck besteht. Ist dies der Fall, wird die Operation mit einer Fehlermeldung abgebrochen. Der Nutzer sollte in

diesem Fall zunächst prüfen, ob eine Integration mit der bestehenden Akte sinnvoll ist und dann ggf. das Interaktionsmuster "Zusammenführen von Fallakten" ausführen.

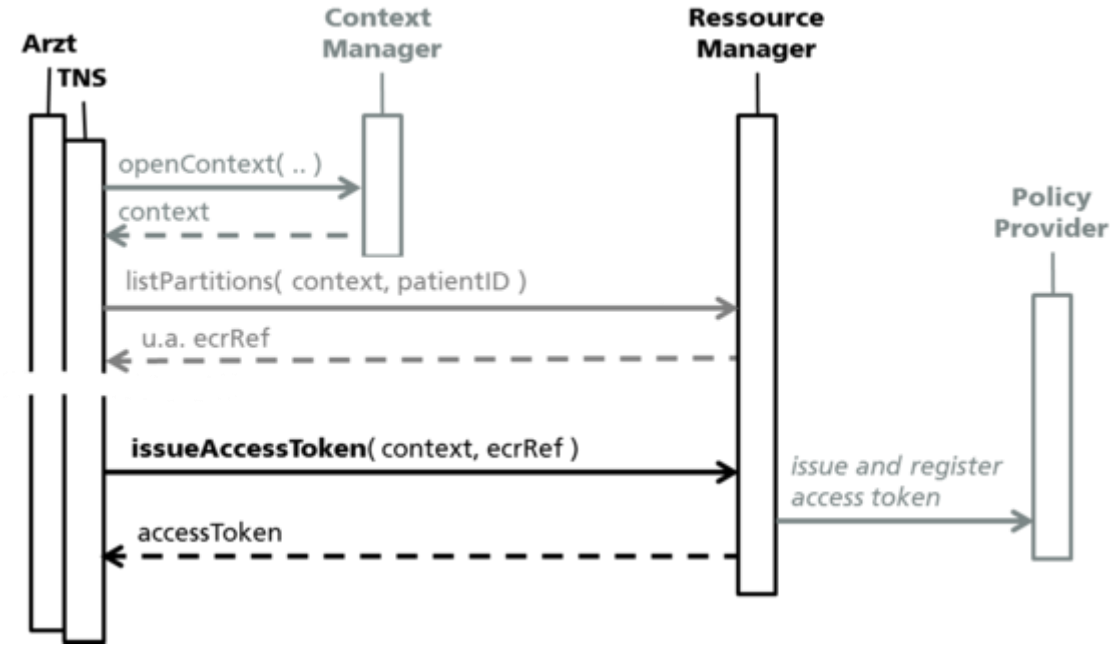
3. Der EFA-Provider prüft die Angaben zur Einwilligung und stellt sicher, dass er diese in seinem Berechtigungsmanagement abbilden kann:
    1. Die Angaben zur Identität der Teilnehmer ermöglichen eine sichere Identifizierung der Teilnehmer.
    2. Die Angaben zu den Rollen der Teilnehmer ermöglichen eine Zuordnung der Teilnehmer zu mit konkreten Zugriffsrechten hinterlegten EFA-Rollen.
    3. Die Angaben zur Gültigkeit der Einwilligung entsprechen den Vorgaben des Providers (z.B. in Bezug auf die maximale Gültigkeitsdauer von Fallakten)
4. Der EFA-Provider identifiziert die aktuell gültige Einwilligung und stellt eine Verknüpfung der neuen Einwilligung zu der bestehenden Einwilligung her, aus der ersichtlich ist, dass die neue Einwilligung die bestehenden Einwilligung ersetzt.
5. Sofern in der Einwilligung ein konkretisierter Zweck benannt ist: Der EFA-Provider ändert die Zweckbezeichnung aller Partitionen der Akte.
6. Der EFA-Provider bildet den in der Einwilligung benannten Teilnehmerkreis in seinem internen Berechtigungsmanagement so ab, dass die Teilnehmer ihrer Rolle entsprechenden Zugriffsrechte auf der Akte erhalten.
7. Der EFA-Provider legt die übergebenen Daten (Angaben zur Einwilligung, ggf. Einwilligungsdokument) zur sicheren Speicherung im Document Repository ab. Hierzu verfährt er analog zum Kommunikationsmuster Einstellen von Dokumenten

4. Der EFA-Provider meldet dem Teilnehmer die erfolgreiche Anpassung der Fallakte an die neue Einwilligung.

Anfordern eines Berechtigungstoken

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.10}

Das Anfordern eines durch einen Dritten einlösbaren Berechtigungstoken erfolgt innerhalb eines gültigen EFA-Sicherheitskontexts und bedingt, dass der das Token anfordernde Nutzer ein berechtigter Teilnehmer der Fallakte ist.



Die Anforderung und Bereitstellung eines Berechtigungstoken erfolgt in den folgenden Schritten:

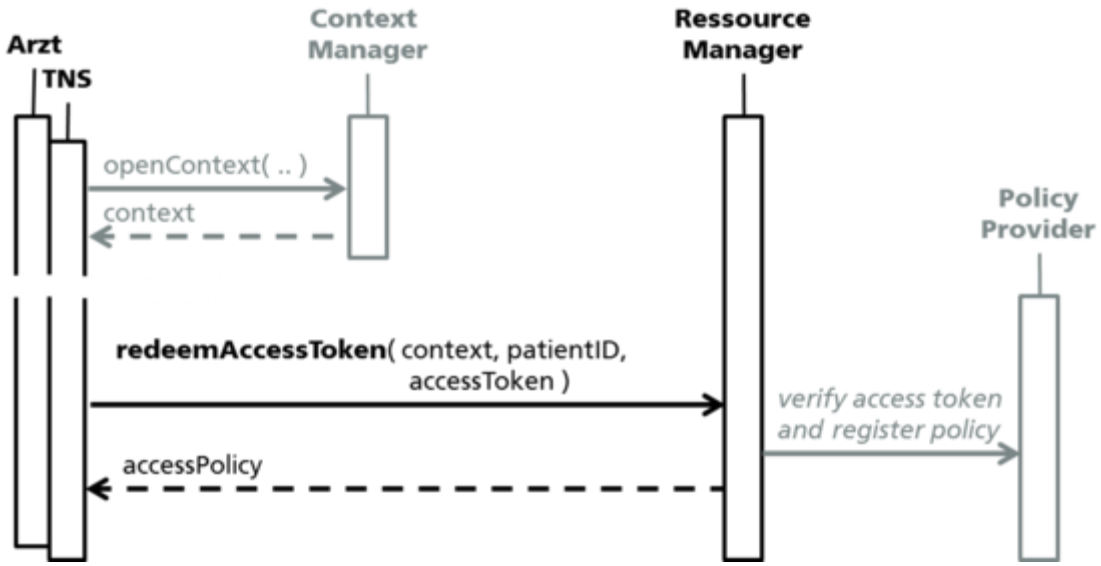
1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des Teilnehmers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Ermitteln der *ecrRef*, mittels der die Fallakte eindeutig identifizierbar sind, für die ein Berechtigungstoken ausgestellt werden soll. Sofern diese ID nicht bereits bekannt ist, muss sie über das Kommunikationsmuster *Auflisten von Partitionen* ermittelt werden.
3. Senden des Aktenverweises an den Ressource Manager des EFA-Providers.
    1. Der EFA-Provider prüft, ob der Teilnehmer für diese Akte Berechtigungstoken anfordern und ausgeben darf. Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
    2. Der EFA-Provider prüft, ob die bestehende Einwilligung die Ausstellung von Berechtigungstoken zulässt. Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
    3. Der EFA-Provider stellt ein Berechtigungstoken für die Akte aus und registriert dieses beim Policy Provider.
4. Der EFA-Provider sendet dem Teilnehmer das Berechtigungstoken (accessToken-Object) zu.

Das Berechtigungstoken liegt beim Teilnehmer nun in digitaler Form vor und kann auf einen beliebigen Träger aufgebracht und an den Patienten übergeben werden.

Einlösen eines Berechtigungstoken

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eouns.01.11}`

Das Einlösen eines Berechtigungstoken erfolgt innerhalb eines gültigen EFA-Sicherheitskontexts. Durch das Einlösen eines Berechtigungstoken wird der einreichende Arzt berechtigter Teilnehmer der Fallakte, für die das Token ausgestellt wurde.



Das Einlösen eines Berechtigungstoken erfolgt in den folgenden Schritten:

1. Aufbau eines Sicherheitskontextes, der dem EFA-Provider die sichere Identifizierung und Authentifizierung des als Teilnehmer zu registrierenden Leistungserbringers ermöglicht (siehe Kommunikationsmuster Aufbau des Sicherheitskontextes).
2. Senden des Berechtigungstoken (accessToken-Object) an den Resource Manager des EFA-Providers.

1. Der EFA-Provider extrahiert aus dem Berechtigungstoken die *ecrRef*, mittels der die Fallakte eindeutig identifizierbar ist, für die ein Berechtigungstoken eingelöst werden soll.
2. Der EFA-Provider prüft, ob das Token authentisch und durch den einreichenden Leistungserbringer einlösbar ist. Falls dies nicht der Fall sein sollte, wird die Operation mit einer Fehlermeldung abgebrochen.
3. Der EFA-Provider stellt für den Teilnehmer eine Berechtigungspolicy für die Akte aus. Sofern die Berechtigung mehrfach oder dauerhaft gültig ist, registriert der Policy Provider die Policy an seinem internen Berechtigungsmanagement.

3. Der EFA-Provider sendet dem Teilnehmer die Berechtigungspolicy (subjectAccessPolicy-Objekt) zu.

Die Berechtigungspolicy kann von dem Teilnehmer über das Client-Policy-Push Verfahren unmittelbar zum Zugriff auf die Akte genutzt werden.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Anwendungsdienste (logische Spezifikation)**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

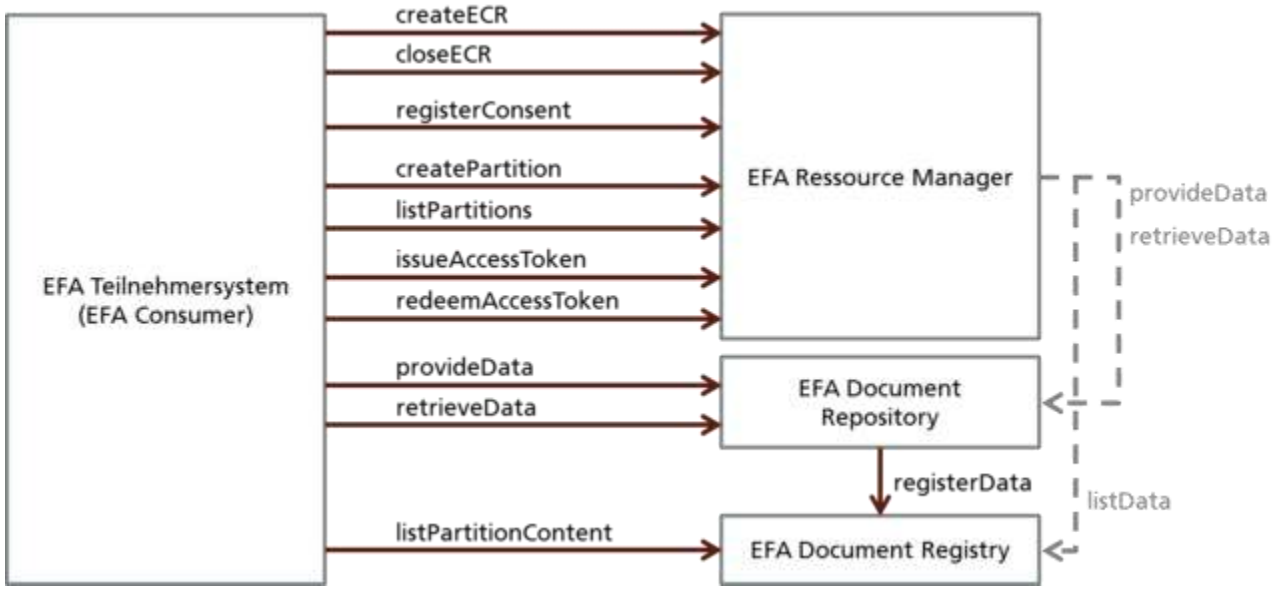
EFA Anwendungsarchitektur: Service Functional Model

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01}

Die nachfolgende Tabelle listet zu den EFA-Kommunikationsmustern die zu deren Umsetzung benötigten Operationen auf. Die Gesamtheit dieser Operationen bildet das *Service Functional Model* der EFA-Anwendungsarchitektur, d.h. liefert eine vollständige plattformunabhängige Beschreibung der technisch umzusetzenden EFA-Funktionalität.

Kommunikationsmuster	Operation (logisch)	Umsetzender Dienst (logisch)
Anlegen einer Fallakte	createECR	EFA Ressource Manager
Anlegen einer Partition zu einer bestehenden Fallakte	createPartition	EFA Ressource Manager
Schließen einer Fallakte	closeECR	EFA Ressource Manager
Auflisten von Partitionen	listPartitions	EFA Ressource Manager
Registrierung einer neuen Einwilligung	registerConsent	EFA Ressource Manager
Anfordern eines Berechtigungstoken	issueAccessToken	EFA Ressource Manager
Einlösen eines Berechtigungstoken	redeemAccessToken	EFA Ressource Manager
Einstellen von Dokumenten	provideData	EFA Document Repository
	registerData	EFA Document Registry
Auflisten von Dokumenten (einer Partition)	listPartitionContent	EFA Document Registry
Abrufen von Dokumenten	retrieveData	EFA Document Repository

Das Zusammenspiel von Diensten und Operationen ist in der folgenden Darstellung noch einmal im Überblick dargestellt.



Die gestrichelt dargestellten internen Operationsaufrufe vom Ressource Manager zu den anderen Diensten sind optional in dem Sinne als dass die geforderte Funktionalität der Speicherung und Registrierung von Einwilligungen und Einwilligungsdokumenten auch über interne Mechanismen des EFA-Providers erfolgen kann.

Operationen des EFA Ressource Manager

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01}`

In den folgenden Abschnitten werden die Operationen des EFA Ressource Managers plattform-unabhängig als *Service Functional Model* spezifiziert. Die folgenden Vorbedingungen müssen für alle Aufrufe an den Ressource Manager erfüllt sein und werden:

- Das aufrufende Teilnehmersystem kann den EFA Ressource Manager lokalisieren und sicher authentifiziern.
- Der vom Teilnehmersystem übermittelte Sicherheitskontext ist gültig, vollständig, authentisch und wurde von einer vertrauenswürdigen Stelle für Aufrufer ausgestellt.
- Der Ressource Manager kann den Aufrufer anhand der im context übermittelten Daten sicher identifizieren und authentifizieren.

- Der Ressource Manager ist technisch in der Lage, einen Audit Trail Eintrag zu schreiben
- Der Ressource Manager verfügt über eine Möglichkeit, mit dem Operationsaufruf ggf. übergebene Daten im Document Repository abzulegen und im Document Registry zu registrieren.

createECR

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.01}

Operation	**createECR**	
Funktionalität	Mit der Operation *createECR* wird eine neue Fallakte für einen Patienten angelegt. Sofern bereits eine Fallakte zu dem benannten Zweck existiert, wird keine neue Akte angelegt, sondern stattdessen die bestehende Akte um eine Partition erweitert. In diesem Fall wird die bestehende Einwilligung invalidiert und durch die übergebene Einwilligung ersetzt.	
Eingabe	context	Die Anlage einer Fallakte muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die EFA-Neuanlage initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter *context* wird der vorab über die Operation *openContext* des EFA Kontext Managers erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	ecrInfo	Identifizierende und beschreibende Daten zur anzulegenden Fallakte. patientID Eindeutige Identifizierung des Patienten für den eine Fallakte angelegt werden soll. Hierzu muss eine ID verwendet werden, die bereits beim EFA-Provider für den Patienten registriert ist. Ggf. muss eine Abfrage an einen MPI dieser Operation vorgeschaltet werden, um diese ID anhand demografischer Daten des Patienten zu ermitteln (siehe IHE Cookbook für die Abfrage einer XAD-PID). purpose Festlegung des Zwecks zu dem die Fallakte angelegt werden soll. Bei einem EFA-Provider kann für jeden Patienten zu einem Zweck nur eine Fallakte existieren. status muss bei der Neuanlage einer EFA immer "offen" sein.
	consentInfo	Informationen zu der vom Patienten gegebenen Einwilligung einschließlich der Gültigkeitsdauer der Akte und

		der Angabe der als EFA-Teilnehmer zum Zugriff auf die Akte zu berechtigenden Personen und Organisationen.
Rückgabe	consentDoc (optional)	Sofern die Einwilligungserklärung des Patienten als (gescanntes) elektronisches Dokument vorliegt, kann diese bei der Anlage der Akte direkt in die Akte eingestellt werden.
	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
	partitionID	Eindeutige ID der initial zu der neuen Akte angelegten Partition. Mit Hilfe dieser ID kann der EFA-Teilnehmer weitere Operationen, wie z.B. das Einstellen von Dokumenten in die Fallakte, durchführen.

Vorbedingungen

- Der Aufrufer ist berechtigt, beim angesprochenen EFA-Provider neue Fallakten anzulegen.
- Die übergebene Patienten-ID ist gültig und mit einer natürlichen Person verknüpft.
- Die übergebene Zweckbenennung ist gültig und als EFA-Zweck gemäß der Regularien des Providers zulässig.
- Das übergebene consentInfo Dokument ist konsistent:
  - Die Angaben zum betroffenen Patient stimmen mit den verfügbaren Informationen zum Besitzer der übergebenen Patienten-ID überein.
  - Sofern ein Zweck benannt ist, stimmt dieser mit dem bei der EFA-Anlage benannten Zweck überein.
  - Es ist ein Gültigkeitsdatum benannt und dieses ist gemäß der Vorgaben des EFA-Providers zulässig.
  - Die EFA Teilnehmer sind benannt. Die Angaben zur Identität der Teilnehmer ermöglichen eine sichere Identifizierung der Teilnehmer.
  - Sofern im *consentInfo* ein Fallaktenmanager identifiziert ist, stimmt dieser mit der im EFA-Netzwerk für diese Rolle benannten Person überein (die Festlegung des Fallaktenmanagers erfolgt nicht durch den Patienten und muss daher nicht zwingend in den kodierten Informationen zur Einwilligung enthalten sein).

Ablaufsequenz (logisch)

Der Ressource Manager ...

1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind.
2. ... erzeugt aus Patientenidentifikation und Zweckbenennung ein ecrRef-Objekt für die neu anzulegende Fallakte
3. ... prüft, ob ein identisches ecrRef-Objekt bereits existiert und mit Partitionen und Berechtigungen verknüpft ist. Sollte dies der Fall sein, prüft der Ressource Manager, ob die bestehende und die neu übergebene Einwilligung eine Überführung der bestehenden Akte in die neue anzulegende Akte erlauben. Ist dies nicht der Fall, wird die Operation mit einer Fehlermeldung abgebrochen.
4. ... legt eine neue Partition an und verknüpft diese mit dem ecrRef-Objekt.
5. ... bildet den Inhalt der Einwilligung auf ein Berechtigungsregelwerk ab und verknüpft dieses mit dem ecrRef-Objekt.

6. ... stellt die Angaben zur Einwilligung und ein ggf. übergebenes Einwilligungsformular als Dokumente in die neu erzeugte Partition ein.
7. bei Überführung einer bestehenden Akte: ... lokalisiert die Partitionen der zu überführenden Akte und verknüpft diese mit dem neuen ecrRef-Objekt.
8. bei Überführung einer bestehenden Akte: ... erzeugt eine "Ersetzt"-Verknüpfung zwischen der neuen Einwilligung und der für die bestehende Akte zuletzt gültigen Einwilligung.
9. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation
10. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation sowie eine Referenz auf die neu angelegte Partition an das aufrufende System zurück

Fehler und Warnungen

Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert:

- Der Aufrufer hat keine für die Anlage von Fallakten ausreichende vertragliche Vereinbarung mit dem EFA-Provider.
- Eine neue Akte kann nicht angelegt werden, da bereits eine Akte zum angegebenen Patienten und Zweck besteht.
- Die angegeben Patienten-ID kann nicht aufgelöst werden.
- Eine oder mehrere der in der consentInfo angegebenen Identitäten zu berechtigender Teilnehmer kann nicht aufgelöst werden.
- Die übergebene consentInfo ist nicht konsistent zu anderen Angaben.

Darüber hinaus sind die folgenden Warnungen definiert:

- Eine bestehende Fallakte wurde in die neu angelegte Akte überführt. Der Aufrufer sollte ggf. verifizieren, dass die damit übernommenen Dokumente noch dem Zweck der Akte dienen. Veraltete Dokumente sollten invalidiert werden.

createPartition

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.02}

Operation	**createPartition**

Funktionalität	Anlegen einer neuen Partition zu einer bestehenden Fallakte.	
Eingabe	context	Die Anlage einer Partition muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anlage der Partition initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	ecrRef	Eindeutige Identifizierung der Fallakte, zu der die Partition hinzugefügt werden soll.
	partitionInfo	Metadaten zu der neu anzulegenden Partition (Titel, etc.)
	initialDoc (optional)	Bei der Anlage einer Partition können initial in diese Partition einzustellende Dokumente mit übergeben werden.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
	partitionID	Eindeutige ID der neu angelegten Partition. Mit Hilfe dieser ID kann der EFA-Teilnehmer weitere Operationen, wie z.B. das Einstellen von Dokumenten in diese Partition, durchführen.
Vorbedingungen	• Der Aufrufer ist berechtigt, beim angesprochenen EFA-Provider Partitionen zu bestehenden Fallakten anzulegen. • Die übergebene EFA-Referenz ist valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf dieser Akte, um die angeforderte Aktion durchzuführen. • Die übergebenen Metadaten der anzulegenden Partition sind vollständig und valide. • Die Konfiguration der angesprochenen Akte erlaubt das Einstellen der ggf. übergebenen Dokumente.	
Ablaufsequenz (logisch)	Der Ressource Manager ... 1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind. 2. ... legt eine neue Partition an und verknüpft diese mit dem übergebenen ecrRef-Objekt. 3. ... stellt die ggf. übergebenen Dokumente in die neu erzeugte Partition ein. 4. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation 5. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation sowie eine Referenz auf die neu angelegte Partition an das aufrufende System zurück	
Fehler und	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus sind für diese Operation die folgenden	

Warnungen	spezifischen Fehlermeldungen definiert: • Der Aufrufer hat keine für die Anlage von Partitionen ausreichende vertragliche Vereinbarung mit dem EFA-Provider. • Die angegeben Fallakten-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf dieser Akte auszuführen. • Die übergebene partitionInfo ist nicht vollständig oder nicht konsistent zu anderen Angaben. Darüber hinaus sind die folgenden Warnungen definiert: • Eines oder mehrere der übergebenen Dokumente konnte nicht in der Partition abgelegt werden.	

closeECR

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.03}

Operation	**closeECR**	
Funktionalität	Schließen einer bestehenden Fallakte. Die Fallakte geht damit in den "Grace"-Status über.	
Eingabe	context	Das Schließen einer Fallakte muss innerhalb eines Sicherheitskontextes erfolgen, in dem der diese Operation initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	ecrRef	Eindeutige Identifizierung der Fallakte, die geschlossen werden soll.
	consentInfo	Angaben zum Grund für das Schließen der Fallakte (z.B. Rücknahme der Einwilligung durch den Patienten).
	consentDoc (optional)	Sofern die Schließung der Akte auf eine Änderung der Einwilligung zurückzuführen ist, kann eine elektronische Version des entsprechenden Dokuments mit übergeben werden. Hierdurch ist auch nach dem Schließen der Akte der Grund für diese Operation noch nachvollziehbar.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung

potenziell relevante Warnungen)

Vorbedingungen	• Die übergebene EFA-Referenz ist valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf dieser Akte, um die angeforderte Aktion durchzuführen. • Das übergebene consentInfo Dokument ist konsistent: ○ Die Angaben zum benannten Patient stimmen mit den verfügbaren Informationen zum Betroffenen der Akte überein.
Ablaufsequenz	Der Ressource Manager ... 1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind. 2. ... ändert die auf der Akte definierten Zugriffsrechte sowie den internen Status der Akte entsprechend der Vorgaben in der Rücknahme der Einwilligung und unter Berücksichtigung des definierten EFA-Lebenszyklus 3. ... stellt die Angaben zur Einwilligungsrücknahme und ein ggf. übergebenes Einwilligungsformular als Dokumente in eine Partition der Akte ein. 4. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation 5. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation an das aufrufende System zurück
Fehler und Warnungen	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert: • Die angegeben Fallakten-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf dieser Akte auszuführen. • Die übergebene consentInfo ist nicht vollständig oder nicht konsistent zu anderen Angaben. • Eines oder mehrere der übergebenen Dokumente konnten nicht in der Akte abgelegt werden.

listPartitions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.04}

Operation	**listPartitions**

Funktionalität	Mit der Operation *listPartitions* werden Informationen zu allen Partitionen (und deren übergeordneten Fallakte) aufgelistet, zu denen der Aufrufer über die vom betroffenen Patienten gegebenen Einwilligungen zugangsberechtigt ist.	
Eingabe	context	Die Suche nach Fallakten und Partitionen muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anfrage initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter *context* wird der vorab über die Operation *openContext* des EFA Kontext Managers erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	patientID	Eindeutige Identifizierung des Patienten nach dessen Fallakten und Partitionen gesucht werden soll. Hierzu muss eine ID angegeben werden, die bereits beim EFA-Provider für den Patienten registriert ist und die bei der Anlage der EFA verwendet wurde. Ggf. muss eine Abfrage an einen MPI dieser Operation vorgeschaltet werden, um diese ID anhand demografischer Daten des Patienten zu ermitteln (siehe IHE Cookbook für die Abfrage einer XAD-PID).
	purpose (optional)	Einschränkung der Suche auf Akten und Partitionen, die zu einem bestimmten Zweck angelegt wurden.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
	partitionList	Liste von nach übergeordneten Fallakten strukturierten Partitionen des Patienten, die im Ergebnis der Suchanfrage gefunden wurden.
Vorbedingungen	• Die übergebene Patienten-ID ist gültig und mit einer natürlichen Person verknüpft. • Eine ggf. übergebene Zweckbenennung ist gültig und als EFA-Zweck gemäß der Regularien des Providers zulässig.	
Ablaufsequenz (logisch)	Der Ressource Manager ... 1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind. 2. ... lokalisiert alle Partitionen, die mit dem angegebenen Patienten verknüpft sind und identifiziert die jeweils übergeordneten Fallakten. 3. ... prüft für jede der gefundenen Fallakten, ob der Aufrufer ein berechtigter Teilnehmer der Akte ist. 4. ... stellt die Metadaten der Partitionen dieser Akten zur Ergebnisstruktur dieser Operation zusammen. 5. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation 6. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation sowie die Metadaten der gefundenen Partitionen	

	an das aufrufende System zurück	
Fehler und Warnungen	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert: • Die angegeben Patienten-ID kann nicht aufgelöst werden.	

registerConsent

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.05}`

Operation	**registerConsent**	
Funktionalität	Registrierung einer neuen Patienteneinwilligung zu einer bestehenden Fallakte. Zweck, Gültigkeitsdauer und Teilnehmerkreis der Akte werden gemäß der neuen Einwilligung festgesetzt. Alle vorher gegebenen Einwilligungen verlieren damit ihre Gültigkeit, sind aber nach wie vor über die Akte nachvollziehbar.	
Eingabe	context	Das Registrieren einer neuen Einwilligung muss innerhalb eines Sicherheitskontextes erfolgen, in dem der diese Operation initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	ecrRef	Eindeutige Identifizierung der Fallakte, zu der eine neue Einwilligung vorliegt.
	consentInfo	Angaben zur neuen Einwilligung auf deren Basis Zweck, Gültigkeitsdauer und Teilnehmerkreis der Akte an Änderungen in der Behandlungsorganisation oder der Behandlungssituation angepasst werden sollen.
	consentDoc (optional)	Eine ggf. verfügbare elektronische Version des Einwilligungsdokuments kann im Rahmen dieser Operation zur Ablage in der Akte übergeben werden.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
Vorbedingungen	• Das übergebene consentInfo Dokument ist konsistent: ○ Die Angaben zum betroffenen Patient stimmen mit den verfügbaren Informationen zum Betroffenen der	

angegeben Akte überein.
    - Sofern ein Zweck benannt ist, ist dieser valide und zulässig.
    - Es ist ein Gültigkeitsdatum benannt und dieses ist gemäß der Vorgaben des EFA-Providers zulässig.
    - Die EFA Teilnehmer sind benannt. Die Angaben zur Identität der Teilnehmer ermöglichen eine sichere Identifizierung der Teilnehmer.

Ablaufsequenz (logisch)

Der Ressource Manager ...

1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind.
2. ... bildet den Inhalt der Einwilligung auf ein Berechtigungsregelwerk ab und verknüpft dieses mit dem ecrRef-Objekt.
3. ... lokalisiert die Partitionen der referenzierten Akte
4. ... prüft ob die Zweckbenennung über die neue Einwilligung verändert wird. Falls dies der Fall ist, prüft der Ressource Manager, ob bereits eine Akte des Patienten zu dem neuen Zweck besteht. Existiert eine solche Akte, wird die Operation mit einer Fehlermeldung abgebrochen. Ansonsten wird die neue Zweckbindung im ecrRef-Objekt vermerkt.
5. ... stellt die Angaben zur Einwilligung und ein ggf. übergebenes Einwilligungsformular als Dokumente in eine Partition der referenzierten Akte ein.
6. ... erzeugt eine "Ersetzt"-Verknüpfung zwischen der neuen Einwilligung und der für die bestehende Akte zuletzt gültigen Einwilligung.
7. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation
8. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation an das aufrufende System zurück

Fehler und Warnungen

Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert:

- Der Aufrufer hat keine für die Anpassung von Fallakten ausreichende vertragliche Vereinbarung mit dem EFA-Provider.
- Die angegeben Fallakten-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf dieser Akte auszuführen.
- Der Zweck der Akte kann nicht geändert werden, da bereits eine Akte zum angegebenen Patienten und Zweck besteht.
- Eine oder mehrere der in der consentInfo angegebenen Identitäten zu berechtigender Teilnehmer kann nicht aufgelöst werden.
- Die übergebene consentInfo ist nicht konsistent zu anderen Angaben.

issueAccessToken

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.06}

Operation	**issueAccessToken**	
Funktionalität	Abrufen eines Berechtigungstoken, über das ein Patient einen weiteren Arzt als Teilnehmer zur Nutzung einer bestehenden Fallakte berechtigen kann. Erteilte Einwilligung, Zweck und Gültigkeit der Akte werden von dieser Operation nicht berührt.	
Eingabe	context	Das Abrufen eines Berechtigungstoken muss innerhalb eines Sicherheitskontextes erfolgen, in dem der diese Operation initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	ecrRef	Eindeutige Identifizierung der Fallakte, zu der ein Berechtigungstoken abgerufen werden soll.
Rückgabe	accessToken	Berechtigungstoken, dessen Einlösung den einlösenden Leistungserbringer zum Zugriff auf eine Fallakte berechtigt.
Vorbedingungen	• Der Aufrufer ist berechtigter Teilnehmer der Fallakte und zum Abruf von Berechtigungstoken berechtigt. • Die bestehende Einwilligung der Fallakte lässt die Nutzung von Berechtigungstoken zu. • Der Aufrufer kann vom EFA Ressource Manager identifiziert und in seiner Authentizität verifiziert werden.	
Ablaufsequenz (logisch)	Der Ressource Manager ... 1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind. 2. ... generiert einen Proof-Schlüssel (Geheimnis, etc.) anhand dessen beim Einreichen des Berechtigungstoken die Authentizität des Token validiert werden kann 3. ... erzeugt ggf. eine Token-Redeem-Policy, die definiert, wer (Rolle, Fachbereich, etc.) das Token einreichen darf 4. ... erzeugt eine Token-Access-Policy, die definiert, welche Berechtigungen an den Einreicher des Tokens vergeben werden 5. ... kapselt Informationen zur Fallakte und Proof-Schlüssel in einem Berechtigungstoken (accessToken-Objekt) 6. ... registriert das erzeugte accessToken mitsamt Proof-Schlüssel und zugehörigen Poicies (z.B. im Policy Provider) 7. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation	

8. ... liefert ein Berechtigungstoken an das aufrufende System zurück

Fehler und Warnungen	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert: • Die angegeben Fallakten-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf dieser Akte auszuführen. • Die Einwilligung zu der Fallakte lässt keine Ad-Hoc-Autorisierungen über Berechtigungstoken zu.

redeemAccessToken

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.01.07}`

Operation	**redeemAccessToken**	
Funktionalität	Einlösen eines Berechtigungstoken, über das ein Patient einen weiteren Arzt als Teilnehmer zur Nutzung einer bestehenden Fallakte berechtigen kann. Erteilte Einwilligung, Zweck und Gültigkeit der Akte werden von dieser Operation nicht berührt.	
Eingabe	context	Das Einlösen eines Berechtigungstoken muss innerhalb eines Sicherheitskontextes erfolgen, in dem der diese Operation initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	patientID	ID des Patienten in der Affinity Domain des Arztes, der das Token einreicht.
	accessToken	Über die Operation issueAccessToken ausgestelltes Berechtigungstoken, mit dem der Einreicher als Teilnehmer an der im Token kodierten Fallakte registriert werden soll.
Rückgabe	subjectAccessPolicy	Berechtigungspolicy für den neuen EFA-Teilnehmer. Die Berechtigungspolicy kann von dem Teilnehmer über das Client-Policy-Push Verfahren unmittelbar zum Zugriff auf die Akte genutzt werden.
Vorbedingungen	• Der Aufrufer kann vom EFA Ressource Manager identifiziert und in seiner Authentizität verifiziert werden. • Die Fallakte ist im Zustand "offen". • Der Aufrufer verfügt über ein gültiges accessToken	

- Der Patient wurde in der Affinity Domain des Arztes eindeutig identifiziert und die in der Affinity Domain bekannte patientID des Patienten liegt vor.

Ablaufsequenz (logisch)

Der Ressource Manager ...

1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind.
2. ... validiert den im Token kodierten Proof-Schlüssel (Geheimnis, etc.) um die Authentizität des Tokens sicherzustellen
3. ... validiert die Identitätsdaten des Einreichers gegen eine ggf. erzeugte Redeem-Policy, um sicherzustellen, dass der Einreicher dieses Token einlösen darf
4. ... verknüpft Fallakte und ID des Einreichers mit der hinterlegten Token-Access-Policy, die definiert, welche Berechtigungen an den Einreicher des Tokens vergeben werden
5. ... registriert die erzeugte Policy am Policy Provider
6. ... ruft vom Policy Provider die gültige subjectAccessPolicy des Einreichers ab
7. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation
8. ... liefert die subjectAccessPolicy an das aufrufende System zurück

Fehler und Warnungen

Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert:

- Die im Token kodierte Fallakten-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf dieser Akte auszuführen.
- Die Einwilligung zu der Fallakte lässt keine Ad-Hoc-Autorisierungen über Berechtigungstoken zu.
- Die Redeem-Policy schließt den Einreicher von der Einlösung des Berechtigungstoken aus.

Operationen des EFA Document Registry

```
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.02}
```

In den folgenden Abschnitten werden die Operationen des EFA Document Registry plattform-unabhängig als *Service Functional Model* spezifiziert. Die folgenden Vorbedingungen müssen für alle Aufrufe an das Document Registry erfüllt sein und werden:

- Das aufrufende Teilnehmersystem kann das EFA Document Registry lokalisieren und sicher authentifizieren.
- Ein aufrufendes Document Repository kann das EFA Document Registry lokalisieren und sicher authentifizieren.
- Der vom Teilnehmersystem übermittelte Sicherheitskontext ist gültig, vollständig, authentisch und wurde von einer vertrauenswürdigen Stelle für den Aufrufer ausgestellt.
- Das Document Registry kann den Aufrufer anhand der im context übermittelten Daten sicher identifizieren und authentifizieren.
- Das Document Registry ist technisch in der Lage, einen Audit Trail Eintrag zu schreiben.

registerData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.02.01}

Operation	**registerData**	
Funktionalität	Registrieren von Daten an einer bestehenden Partition einer Fallakte. *Dies ist eine EFA-Provider interne Funktion, die ausschließlich vom EFA Document Repository aufgerufen wird. Die Absicherung der Kommunikation durch einen zwischen beiden Diensten gespannten Sicherheitskontext ist Aufgabe des EFA-Providers und kann mit EFA-unabhängigen Mechanismen realisiert werden.*	
Eingabe	context	Das Einstellen von Daten in eine Partition muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anlage der Partition initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	partitionID	Eindeutige Identifizierung der Partition, an der die Daten registriert werden sollen.
	docMetadata[1..*]	Metadaten der bereits im Document Repository abgelegten Daten, die am Document Registry registriert werden sollen.
	docRelationship[0..*]	Beziehungen der neu zu registrierenden Daten zu bestehenden Dokumenten. Diese müssen so registriert werden, dass sie bei der Auflistung von Dokumenten mit bereit gestellt werden können.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
Vorbedingungen	• Der Aufrufer ist berechtigt, beim angesprochenen EFA-Provider Daten zu bestehenden Fallakten anzulegen. • Die übergebene Partitons-Referenz ist valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf der übergeordneten Akte, um die angeforderte Aktion durchzuführen.	

- Die übergebenen Metadaten der einzustellenden Daten sind vollständig und valide.
- Die Konfiguration der angesprochenen Akte erlaubt das Einstellen der übergebenen Dokumente.
- Die angegebenen Dokumentbeziehungen sind valide und referenzieren ausschließlich zu der selben Akte gehörige Dokumente.

Ablaufsequenz

Das Document Registry ...

1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind.
2. ... registriert die Metadaten und Dokumentbeziehungen an der angegebenen Partition.
3. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation
4. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation zurück

Fehler und Warnungen

Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert:

- Der Aufrufer hat keine für das Einstellen von Daten in Fallakten ausreichende vertragliche Vereinbarung mit dem EFA-Provider.
- Die angegeben Partitions-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der übergeordneten Akte auszuführen.

Zusätzlich sind die folgenden Warnungen definiert:

- Eine oder mehrere der übergebenen Dokument-Beziehungen konnte nicht aufgelöst werden oder ist nicht zulässig.

listPartitionContent

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.02.02}

Operation	**listPartitionContent**
Funktionalität	Abruf der Metadaten zu den an einer Partition einer Fallakte registrierten Dokumenten.

Eingabe	context	Das Auflisten von Daten einer Partition muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anlage der Partition initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	partitionID	Eindeutige Identifizierung der Partition, deren Inhalte ausgelesen werden sollen.
Rückgabe	docMetadata[0..*]	Metadaten der an der ausgewählten Partition registrierten Dokumente
	docRelationship[0..*]	Beziehungen zwischen den Dokumenten der zu listenden Partition und Dokumenten dieser und anderer Partitionen.
Vorbedingungen	• Die übergebene Partitons-Referenz ist valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf der übergeordneten Akte, um die angeforderte Aktion durchzuführen.	
Ablaufsequenz	Das Document Registry ... 1. ... verifiziert, dass die Vorbedingungen zur Ausführung der Operation erfüllt sind. 2. ... überführt die Metadaten der an der angegebenen Partition registrierten Dokumente in das im Binding dieser Operation definierte Format. Hierbei werden nur Dokumente berücksichtigt, die für den Aufrufer gemäß seiner Rolle zugreifbar sind (siehe insbesondere die mäglichen Sonderrollen von EFA-Teilnehmern) 3. ... schreibt einen Audit Trail Eintrag über die erfolgreiche Durchführung der Operation 4. ... liefert einen Statuscode zur erfolgreichen Ausführung der Operation sowie die Metadaten der an der Partition registrierten Dokumente zurück	
Fehler und Warnungen	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert: • Die angegeben Partitions-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der übergeordneten Akte auszuführen.	

Operationen des EFA Document Repository

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.03}

In den folgenden Abschnitten werden die Operationen des EFA Document Repository plattform-unabhängig als *Service Functional Model* spezifiziert. Die folgenden Vorbedingungen müssen für alle Aufrufe an das Document Repository erfüllt sein und werden:

- Das aufrufende Teilnehmersystem kann das EFA Document Repository lokalisieren und sicher authentifizieren.
- Der Document Repository ist ein Document Registry zugeordnet. Das Document Repository kann dieses Document Registry lokalisieren und sicher authentifizieren.
- Der vom Teilnehmersystem übermittelte Sicherheitskontext ist gültig, vollständig, authentisch und wurde von einer vertrauenswürdigen Stelle für den Aufrufer ausgestellt.
- Das Document Repository kann den Aufrufer anhand der im context übermittelten Daten sicher identifizieren und authentifizieren.
- Das Document Repository ist technisch in der Lage, einen Audit Trail Eintrag zu schreiben

provideData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.03.01}

Operation	**provideData**	
Funktionalität	Einstellen von Daten in eine bestehende Partition einer Fallakte.	
Eingabe	context	Das Einstellen von Daten in eine Partition muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anlage der Partition initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	partitionID	Eindeutige Identifizierung der Partition, in die die Daten eingestellt werden sollen.
	document[1..*]	In die Partition einzustellende Dokumente mitsamt ihrer Metadaten.
	docRelationship[0..*]	Beziehungen der neu zu registrierenden Daten zu bestehenden Dokumenten.
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
Vorbedingungen	• Die übergebene Partitons-Referenz ist valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf der übergeordneten Akte, um die angeforderte Aktion durchzuführen.	

- Die übergebenen Metadaten der einzustellenden Daten sind vollständig und valide.
- Die Konfiguration der angesprochenen Akte erlaubt das Einstellen der übergebenen Dokumente.
- Die angegebenen Dokumentbeziehungen sind valide und referenzieren ausschließlich zu der selben Akte gehörige Dokumente.

Ablaufsequenz

Das Document Repository

1. ... stellt sicher, dass die Vorbedingungen erfüllt sind.
2. ... legt alle übergebenen Dokumente in einem sicheren Dokumentenspeicher ab.
3. ... initiert die registerData Operation mit den übergebenen Metadaten und Beziehungen beim Document Registry.
4. ... schreibt einen Audit Trail Eintrag über die Ausführung der Operation.
5. ... sendet eine Information zum Ausführungsstatus der Operation an den Nutzer zurück.

Fehler und Warnungen

Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert:

- Der Aufrufer hat keine für das Einstellen von Daten in Fallakten ausreichende vertragliche Vereinbarung mit dem EFA-Provider.
- Die angegeben Partitions-Referenz kann nicht aufgelöst werden bzw. der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der übergeordneten Akte auszuführen.

Zusätzlich sind die folgenden Warnungen definiert:

- Eine oder mehrere der übergebenen Dokument-Beziehungen konnte nicht aufgelöst werden oder ist nicht zulässig.

retrieveData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Enndn.01.03.02}

Operation	**retrieveData**

Funktionalität	Abrufen von Daten aus einer Fallakte.	
Eingabe	context	Das Abrufen von Daten muss innerhalb eines Sicherheitskontextes erfolgen, in dem der die Anlage der Partition initierende Arzt identifizierbar und in seiner Authentizität überprüfbar ist. Mit dem Parameter context wird der vorab über die Operation *openContext* des *EFA Kontext Managers* erstellte Sicherheitskontext so an den EFA-Provider übergeben, dass dieser den Kontext provider-seitig zur Prüfung der Berechtigungen des Aufrufers innerhalb des Aufrufkontextes rekonstruieren kann.
	documentID	Eindeutige Identifizierung der abzurufenden Dokumente
Rückgabe	statusInfo	Informationen zur Durchführung der Operation (z.B. aufgetretene Fehler oder für die weitere EFA-Nutzung potenziell relevante Warnungen)
	docData[0..n]	angeforderte Dokumente
Vorbedingungen	• Die übergebenen Dokument-Referenzen sind valide und der Aufrufer hat die erforderlichen Zugriffsrechte auf der übergeordneten Akte, um die angeforderte Aktion durchzuführen. • Die angefragten Dokumente sind der selben Fallakte zugeordnet.	
Ablaufsequenz	Das Document Repository 1. ... stellt sicher, dass die Vorbedingungen erfüllt sind. 2. ... ruft die angefragten Dokumente aus dem sicheren Dokumentenspeicher ab. 3. ... schreibt einen Audit Trail Eintrag über die Ausführung der Operation. 4. ... sendet eine Information zum Ausführungsstatus der Operation sie wie die angefragten Dokumente an den Nutzer zurück.	
Fehler und Warnungen	Über die in Fehlermeldungen und Warnungen definierten Ausnahmesituationen hinaus, sind für diese Operation die folgenden spezifischen Fehlermeldungen definiert: • Der Aufrufer hat keine (ausreichenden) Berechtigungen, die angeforderte Operation auf der übergeordneten Akte auszuführen. Zusätzlich sind die folgenden Warnungen definiert:	

- Eine oder mehrere der übergebenen Dokument-Referenzen konnten nicht aufgelöst werden.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Sicherheitsdienste (logische Spezifikation)**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Sicherheitstoken und Sicherheitstokendienste

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierz.01}`

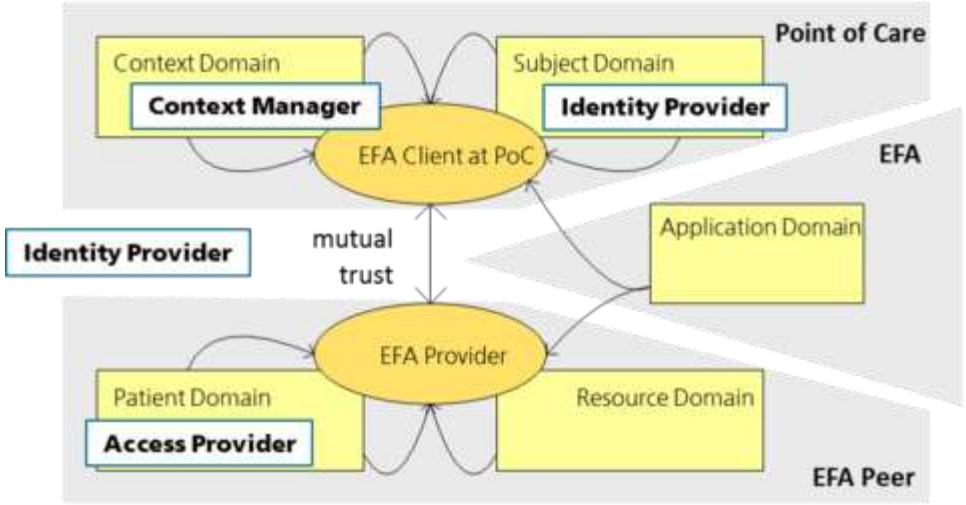
Jeder EFA-Anwendungsdienst und jeder EFA-Sicherheitsdienst besitzt eine Sicherheitspolitik, in der u. a. definiert ist, wie der Sicherheitskontext aussehen muss, aus dem heraus der Dienst aufgerufen werden kann. Hierdurch „weiß“ ein EFA-Client, welches Sicherheitstoken er von welchem GDD-Sicherheitsdienst abrufen und in den Ablaufkontext laden muss, bevor der gewünschte Dienst aufgerufen werden kann. Dadurch dass auch Sicherheitsdienste Sicherheitspolitiken besitzen, lässt sich die komplette Ablaufsteuerung über den Sicherheitsdiensten deklarativ abbilden. Beispielsweise kann ein EFA-Anwendungsdienst für den Zugriff auf eine Ressource ein Sicherheitstoken verlangen, über das die entsprechende

Berechtigung des Nutzers verifizierbar ist. Der dieses Token ausstellende Autorisierungsdienst wiederum kann eine Politik definieren, dass Berechtigungsnachweise nur ausgestellt werden, wenn der Nutzer über ein entsprechendes Token seine Authentizität nachweist, d.h. vor dem Autorisierungsdienst ein Authentifizierungsdienst aufgerufen wurde.

Im Rahmen des *IHE Cookbook* und der EFA-2.0 Spezifikation werden verschiedene Sicherheitstokendienste (föderierte Authentifizierung, Pseudonymisierung, Zugang zu Anwendungen, Autorisierung auf Ressourcen) spezifiziert, die nach dem oben skizzierten Prinzip von allen Aktendiensten genutzt werden können. Welche Sicherheitsdienste ein Aktendienst in Anspruch nimmt, definiert er über seine Sicherheitspolitk, die im Fachmodul in Aufrufe an die Sicherheitstokendienste übersetzt wird.

EFA Sicherheits(token)dienste

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eierz.02}



EFA Identity Provider

Der EFA Identity Provider ist ein Sicherheitstoken-Dienst. Er wird vom EFA-Teilnehmersystem aufgerufen und stellt einen Identitätsnachweis für authentifizierte Nutzer aus. Dieser Nachweis kann neben Angaben zu Rollen und Gruppenzugehörigkeiten des Nutzers je nach Sicherheitspolitik auch ein *Proof-of-Possession* Merkmal enthalten, über der Provider die Authentizität des Nutzers

unmittelbar verifizieren kann (im Gegensatz hierzu wird bei einer mittelbaren Authentizitätsprüfung die Nutzer-Authentizitätsprüfung eines als authentisch geprüften Clientsystems akzeptiert).

Der EFA Identity Provider unterstützt potenziell beliebige Verfahren der Authentifizierung (z.B. mittels Passwort, HBA oder SMC-B). Bei einer Authentifizierung mittels HBA werden die Nutzerattribute aus dem HBA-Zertifikat in den Identitätsnachweis übernommen. Zusätzlich wird anhand der genutzten SMC-B die Organisationszugehörigkeit eingetragen. Bei der Authentifizierung mittels SMC-B hat sich der Nutzer bereits innerhalb seiner Organisation sicher authentisiert. Auch alle Attribute wurden bereits durch die Organisation zugewiesen. Beim Aufruf des EFA Identity Providers bestätigt die Organisation die durchgeführte Authentifizierung und die Authentizität der Attribute in Form eines selbst ausgestellten, von der SMC-B signierten Identitätsnachweises (Guarantor Assertion). Dieser Nachweis wird vom EFA Identity Provider geprüft und in einen für EFA-Anwendungs- und EFA-Sicherheitsdienste nutzbaren Authentifizierungsnachweis überführt.

EFA Policy Provider

Der EFA Policy Provider ist ein Sicherheitstoken-Dienst. Er wird vom EFA-Client oder einem EFA-Anwendungsdienst aufgerufen und liefert einen Verweis auf die für den aufrufenden Nutzer gültigen Berechtigungsregeln (Policy) zu einer Anwendungsinstanz (z. B. einer spezifischen eFA) oder die zum Verweis gehörende Policy. Diese Verweise sind transparent, d. h. sie können sowohl selber bereits eine Semantik tragen (z. B. gemäß IHE BPPC) oder eine Policy-Datei referenzieren. Um auch ein "Policy Pull" zu erlauben (siehe IHE White Paper on Access Control), wird auch ein Aufruf des Policy Provider durch einen EFA-Anwendungsdienst unterstützt.

Dienst	Aufgaben	Datenhaltung
EFA Identity Provider	Authentifiziert einen EFA-Teilnehmer durch Verifikation seiner Credentials. Der Dienst bietet verschiedene Authentifizierungsmethoden an: • Direktes Vertrauen: Authentifiziert einen EFA-Teilnehmer per X.509 Zertifikat oder Benutzername/Passwort-Kombination • Vermitteltes Vertrauen: Authentifiziert einen EFA-Teilnehmer durch Verifikation einer übermittelten signierten Guarantor Assertion (lokaler Identitätsnachweis eines EFA-Teilnehmers aus einer Organisation).	Weitere Attribute können über einen mit dem EFA Identity Provider gruppierten Verzeichnisdienst abgerufen werden. Der Dienst enthält einen Identity Store, wo die verwalteten Identitäten sowie die Credentials für die Authentifizierung gespeichert sind.
EFA Policy Provider	Gibt eine Policy zu einem bestimmten (Behandlungs-)Zweck heraus. Je nach Autorisierungsmodell ("Policy Push"/"Policy Pull") kann eine explizite Access Control Policy oder ein Verweis (mit impliziter Semantik) die Autorisierung eines Benutzers (oder seiner Rolle) zu einer Fallakte bzw. dem festgelegten	Policies, welche jeweils den konsentierten Kreis der Behandelnden zu einem Zweck definieren.

Zweck beschreiben.

Querverweise und Referenzen

- EFA-2.0-Spezifikation
- Normative Spezifikation: EFA Identity Provider Service Functional Model
- Normative Spezifikation: EFA Policy Provider Service Functional Model

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Context Manager Service Functional Model**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Context Manager

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eoexr.01}`

Die EFA nutzt einen vom Client aufgebauten und mit dem EFA-Provider geteilten Sicherheitskontext. Wesentlicher Bestandteil dieses Sicherheitskontextes sind authentische Nachweise zur Identität des EFA-Teilnehmern, die auf Seiten des EFA-Providers zur Berechtigungsprüfung benötigt werden.

Der erste Schritt jeder EFA-Nutzung ist der Aufbau eines initialen Sicherheitskontextes, da dieser bei jedem Aufruf eines EFA-Dienstes mitgegeben werden muss. Der initiale Sicherheitskontext kann durch Nutzung verschiedener Sicherheitsdienste ausgeweitet werden. Die entsprechenden Anforderungen werden vom EFA-Provider formuliert, der für jeden EFA-Dienst angeben kann, welche Sicherheitsnachweise der zum Aufruf des Dienstes erforderliche Sicherheitskontext enthalten muss.

Auf Seiten des EFA-Clients kapselt der (logische) Dienst des EFA ContextManagers den Aufbau und die Verwaltung des Sicherheitskontextes. Alle clientseitigen Aufrufe von EFA-Sicherheitsdiensten werden durch den EFA ContextManager ausgeführt, der die von diesen Diensten für den EFA-Teilnehmer ausgestellten Sicherheitsnachweise in den bestehenden Sicherheitskontext integriert.

Authentisierung eines EFA-Teilnehmers

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eoexr.02}

Die EFA macht keine Vorgaben, wie eine Authentifizierung eines EFA-Teilnehmers erfolgen muss. Verpflichtend ist in Bezug auf das Authentifizierungsverfahren und die eingesetzten Objekte und Mechanismen lediglich die Einhaltung der geltenden regionalen und nationalen Vorgaben zur Stärke der Authentifizierung sowie deren technischer und organisatorischer Absicherung.

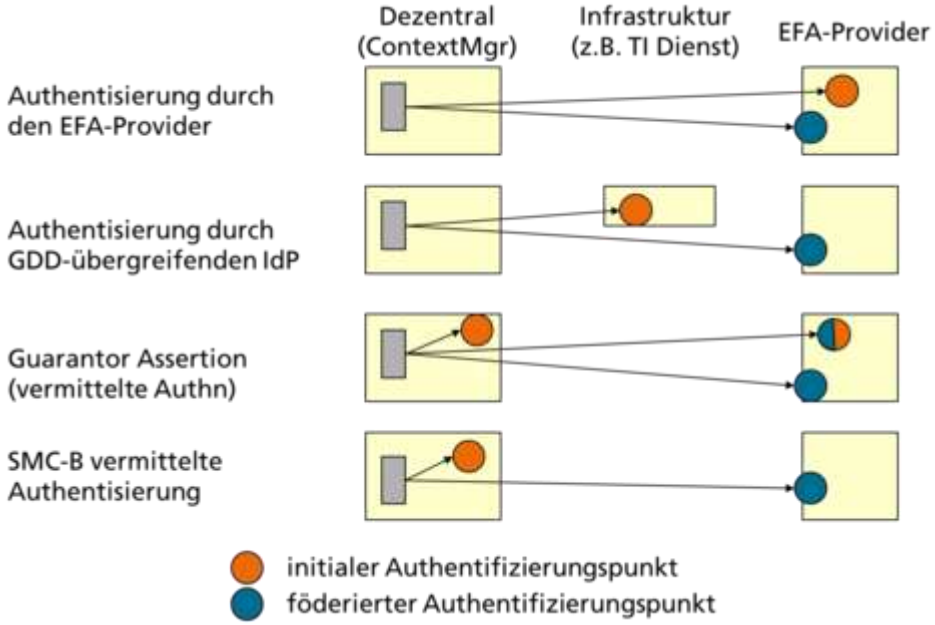
Wesentlich für die über den ContextManager gesteuerte Authentisierung ist lediglich, dass in deren Ergebnis eine authentischer Identitätsnachweis des EFA-Teilnehmers vorliegt. Dieser Nachweis muss einem vorgegebenen Format genügen und bestimmte Identitätsinformationen kodieren, so dass jeder EFA-Dienst dieses Nachweis verarbeiten und semantisch gleichartig interpretieren kann.

Optionen zur Authentisierung von EFA-Teilnehmern (nicht-normativ)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eoexr.02.01}

Die Identifizierung und Authentifizierung von EFA-Teilnehmern gegenüber den EFA-Diensten erfolgt in zwei Stufen; an einem initialen Authentisierungspunkt erfolgt die Prüfung des Authentizitätsnachweises und die Erstellung eines Identitätsnachweises, in dem die Identität des EFA-Teilnehmers über Attribute (z. B. Rollen und Organisationszugehörigkeiten) beschrieben ist. Jeder EFA-Dienst umfasst einen föderierten Authentisierungspunkt, an dem die Authentizität von Identitätsnachweisen verifiziert werden kann. Dieses zweistufige Verfahren erlaubt die Dezentralisierung der initialen Authentifizierung und die Einbringung von beim Leistungerbringer verwalteten Nutzerattributen (z. B. Funktionsrollen). Darüber hinaus bleiben so die technischen Besonderheiten verschiedener und potenziell parallel genutzter Authentifizierungsmechanismen (HBA, Mitarbeiterausweise einer Klinik, Username/Passwort, etc.) vor den EFA-Diensten verborgen.

Die nachfolgende Grafik stellt verschiedene Optionen zur Umsetzung eines initialen Authentisierungspunkts dar. Wesentlich hierbei ist, dass der Aufruf des initialen Authentisierungspunkts logisch über den ContextManager gekapselt wird, d.h. client-seitige Funktionalitäten der EFA-Nutzung und die beim EFA-Provider angesiedelten EFA-Dienste von konkreten Umsetzungen der initialen Authentisierung unabhängig sind. Einen Sonderfall stellt die Nutzung einer Guarantor Assertion dar, die dezentral ausgestellt wird und anschließend an einem Identity Provider in einen für den EFA-Dienste verarbeitbaren Identitätsnachweis überführt wird. Hierbei prüft der Identity Provider die Authentizität der Guarantor Assertion (föderierter Authentisierungspunkt) und stellt mit den Angaben aus der Guarantor Assertion und ggf. weiteren Informationen eines Verzeichnisdienstes einen neuen, für den EFA-Dienst validierbaren Nachweis aus (initialer Authentisierungspunkt aus Sicht des EFA-Dienstes).



Operation: OpenContext

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eoexr.02.02}

Method	openContext(credential Object) : ContextIdentifer fault AuthenticationFailedException	
Description	This method establishes a security context for a user that wants to get access to an eCR peer. The security context holds the Identity Assertion [SAML2.0core] necessary for invoking service operations from business services. A credential MUST be passed.	
Input Parameters	credential	Object which MAY be a username/password combination, a subject identifier, a health card handle, or a SAML assertion that guarantees for an authentication.
Return Value	context	The identifier used to refer to the security context when issuing EFA activities within that context
Preconditions	1. Credentials (i.e., username/password) are present. 2. No previously established security context with the same credentials is present.	
Sequence (Main success scenario)	1. If a username/password combination is passed, the connector/ECRRequestor constructs a UsernameToken [WSSUsername] and invokes the RequestSecurityToken [WSTrust] operation of the eCR Identity Provider [eCR SecArch 1.2] for issuing an Identity Assertion. 2. If a subject identifier is passed and a local Guarantor Token Service is configured, a local au-thentication assertion is issued and forwarded to the eCR Identity Provider. 3. If the credential is already an Authentication Assertion, it will be forwarded as a security token to the eCR Identity Provider. 4. If the authentication was successful, the Identity Assertion is stored in the session context within the eCR-Connector for later use. Otherwise an exception is thrown.	
Exception	AuthenticationFailedException	Authentication failed due to wrong credentials.

Referenzen und Querverweise

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Identity Provider Service Functional Model**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Identity Provider

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Edtie.01}`

Die Authentisierung ist der initiale Schritt eines Clients (EFA-Teilnehmer), um einen EFA Sicherheitskontext zwischen Client und EFA-Provider aufzubauen. Ein Client, der sich gegenüber einen EFA Identity Provider (über die OpenContext-Operation) authentisiert, muss dazu Credentials für seine behauptete Identität vorlegen, welche serverseitig überprüft werden.

Der EFA Identity Provider bietet als Schnittstelle zum Client nur eine Operation zur Authentifizierung an. Da der EFA Identity Provider ist als Sicherheitstokendienst deployt ist, erstellt er bei positiver Authentifizierung einen Nachweis als Sicherheitstoken, nämlich die HP Identity Assertion. Die EFA 2.0 Spezifikation macht keine spezifischen Vorgaben, wie das Protokoll ausgestaltet ist. Als Vorgabe gilt hingegen das IHE-Profil Cross-Enterprise User Assertion (XUA), welches ein Binding auf das SAML- oder WS-Tust-Protokoll spezifiziert (siehe EFA XUA Binding). Der Authentifizierungsnachweis kann weitere Attribute eines EFA-Teilnehmers aus einem Healthcare Provider Directory (HPD) enthalten, welche später für eine Zugriffskontrolle genutzt werden.

Method	**requestHPIdentityAssertion()(credential Object) :**

	HPIdentityAssertion fault AuthenticationFailedException	
Description	This method authenticates a user by means of an EFA Identity Provider. If necessary the EFA Identity Provider calls more user attributes from a HPD. A credential MUST be passed.	
Input Parameters	credential	Object which MAY be a username/password combination, a subject identifier, a health card handle, or a SAML assertion that guarantees for an authentication.
Return Value	HP Identity Assertion	The assertion confirms the successful authentication.
Preconditions	1. Credentials (i.e., username/password) are present. 2. The user is already registered in the identity store of the EFA Identity Provider (i.e., the identity is established).	
Sequence (Main success scenario)	1. The EFA Identity Provider detects whether a username password combination [WSSUsername], SAML assertion (i.e, a locally issued Guarantor Assertion), or a X.509 certificate is passed. 2. Depending on the given credentials, the EFA Identity Provider authenticates the user using the identity store. 3. If the authentication was successful, the Identity Assertion is issued. Otherwise an exception is thrown.	
Exception	AuthenticationFailedException	Authentication failed due to wrong credentials.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Policy Provider Service Functional Model**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem

Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert. Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Policy Provider

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocye.01}`

Der EFA Policy Provider ist für die Verwaltung der Berechtigungen in Form von Policies in einem Policy Repository zuständig. Berechtigungen sind an einen bestimmten Zweck gebunden und steuern den Zugriff von EFA-Teilnehmern auf eine Fallakte.

requestPolicy

Zur Umsetzung des Policy Push Verfahrens muss der EFA Policy Provider eine Schnittstelle zum Abruf der für einen Nutzerkontext und eine zu verarbeitende Fallakte gültigen Policy bereitstellen.

Operation	**requestPolicy**	
Funktionalität	Stellt eine für einen angegebenen Nutzer zum Zugriff auf eine benannte Fallakte gültige Policy in Form eines Berechtigungsregelwerks bereit.	
Eingabe	context	Nutzerkontext, der eine [[cdaefa:EFA_Security_Informationsmodell#subjectIdentity|subjectIdentity] zur Identifizierung des Nutzers enthält, dessen Berechtigungen auf der angegebenen Fallakte abgerufen werden sollen.
	ecrRef	Eindeutige Identifizierung der Fallakte, für die Berechtigungen abgefragt werden sollen.
	consentInfo (optional)	Informationen zu einer vom Patienten gegebenen Einwilligung. *Dieses Argument wird für Ad-Hoc-Berechtigungen und Additive Berechtigungen benötigt und näher ausspezifiziert, wenn die entsprechenden Verfahren im Detail definiert sind.*
Rückgabe	subjectAccessPolicy	Für den aktuellen Kontext und die angegebene Fallakte gültigen Berechtigungsregeln.
Vorbedingungen	1. Der EFA-Teilnehmer hat sich authentisiert und ein Nachweis liegt vor	

	2. Policies für die angefragte Fallakte sind beim Policy Provider registriert	
Ablaufsequenz	1. Überprüfe die Authentizität des Authentisierungsnachweises 2. Ermittle die zu verwendende Access Policy anhand der Eingabedaten 3. Liefere Access Policy an den Aufrufer zurück	
Mögliche Fehler	MissingAttributes	Für die Auswahl der zu verwendenden Policy erforderliche Angaben zum EFA-Teilnehmer fehlen.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **Gruppierung von Anwendungs- und Sicherheitsdiensten**.*

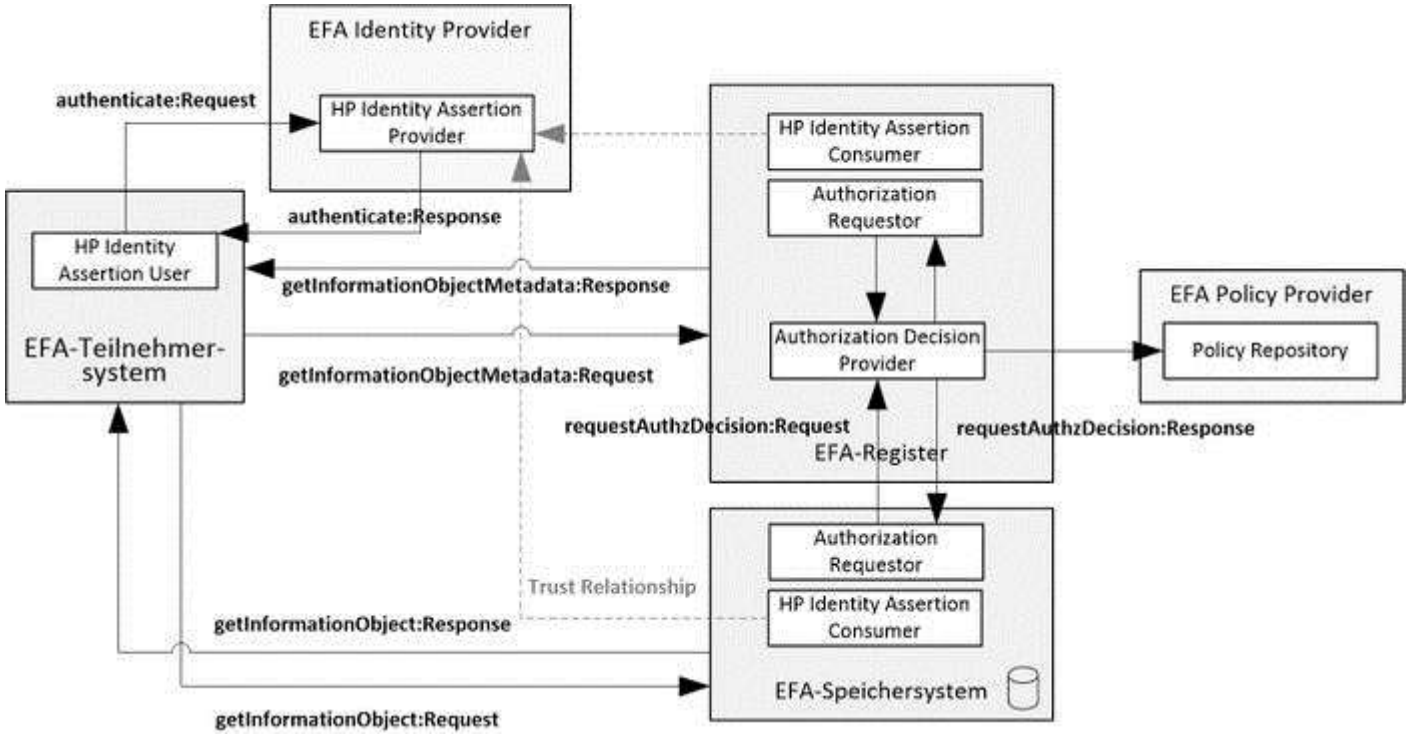
Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Gruppierung von Anwendungs- und Sicherheitsdiensten

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Gpruw.01}`

Die EFA Anwendungs- und Sicherheitsarchitektur ist über eine spezielle Gruppierung von Akteuren miteinander verzahnt. Die nachfolgende Grafik stellt die Beziehungen im Überblick dar.



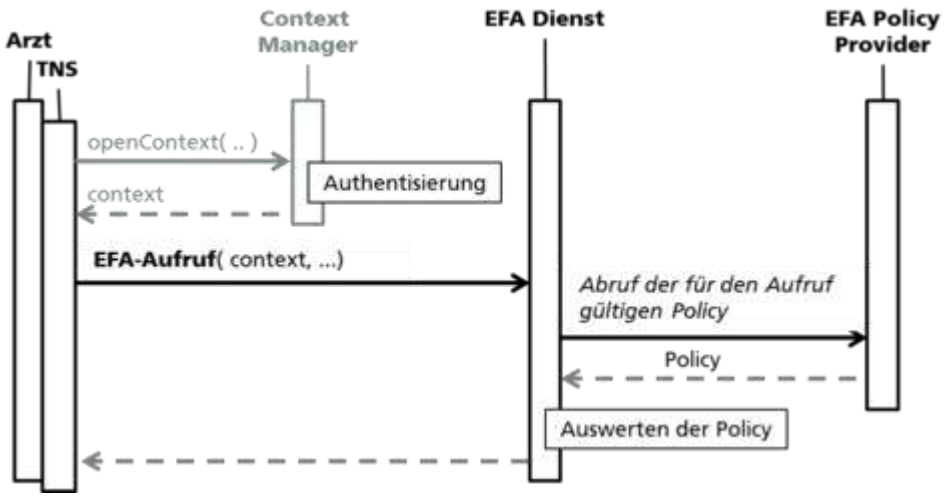
Aus der Grafik sind die folgenden Gruppierungen ersichtlich:

Anwendungsdienst bzw. Akteur	Sicherheitsdienst bzw. Akteur	Beschreibung
EFA-Teilnehmersystem	HP Identity Assertion User	Das EFA-Teilnehmersystem bzw. der Arzt authentisiert sich bei einem konfigurierten EFA Identity Provider, welcher eine HP Identity Assertion als Authentifizierungsnachweis ausstellt.
EFA-Register	HP Identity Assertion Consumer	Die HP Identity Assertion ist für die Nutzung des EFA-Registers notwendig. Die Inhalte des Nachweises werden für eine Zugriffskontrollprüfung durch den Authorization Requestor Akteur

		verwendet.
EFA-Speichersystem	Authorization Requestor	Der Authorization Requestor Akteur stellt eine Autorisierungsanfrage an den Authorization Decision Provider.
	Authorization Decision Provider	Der Authorization Decision Provider Akteur wird mit dem EFA-Register gruppiert, da keine standardisierte Schnittstelle vorgesehen ist, über die effizient alle für die Zugriffsentscheidung notwendigen Dokumentenmetadaten transportiert werden können.
	HP Identity Assertion Consumer	Die HP Identity Assertion ist für die Nutzung des EFA-Speichersystems notwendig.
	Authorization Requestor	Für eine Zugriffsentscheidung zur Herausgabe eines Dokuments wird über den Authorization Requestor Akteur eine Autorisierungsanfrage an den Authorization Decision Provider Akteur des EFA-Registers gestellt.

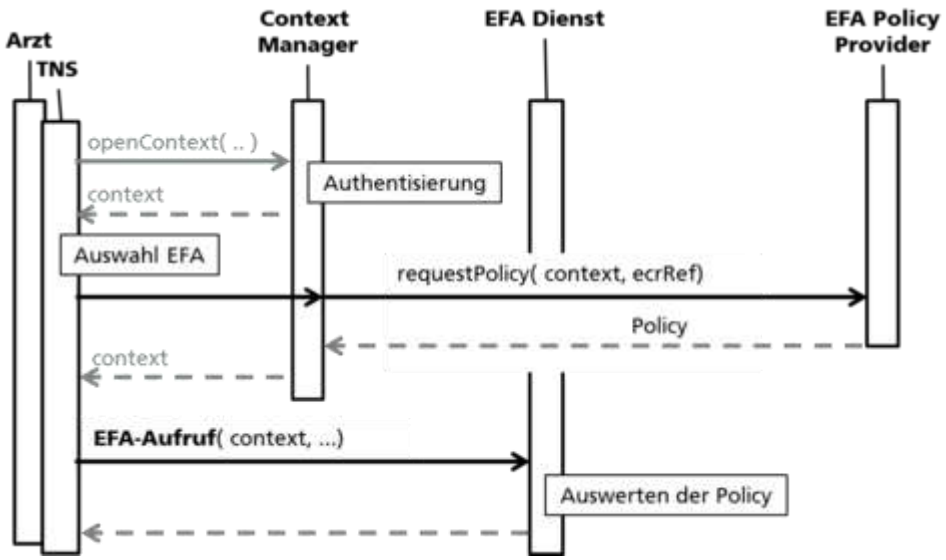
Policy Pull

Jeder EFA-Provider muss das im IHE Cookbook beschriebene Verfahren des Policy Pull unterstützen. Hierbei wird vom EFA-Dienst für jede Anfrage die gültige Policy (Berechtigungsregelwerk) ermittelt und ausgewertet. Der EFA Policy Provider zur Verwaltung und Bereitstellung von Berechtigungsregeln ist hierbei ein logischer Dienst, dessen konkrete Umsetzung nicht näher reglementiert ist. Insbesondere ist es dem Hersteller der EFA-Aktendienste überlassen, wie er eine Einwilligungserklärung in eine Policy übersetzt und wie er diese bei einem Aktenaufruf ermittelt und auswertet.



Client Policy Push

Optional kann ein EFA-Provider das in der EFAv1.2 bevorzugt genutzte Policy Push Verfahren unterstützen. Hierbei ruft der Client die für den aktuellen Nutzer gültige Policy für eine zu öffnende Fallakte vom EFA Policy Provider ab. Die Policy wird als Teil des EFA-Nutzerkontextes im Context Manager verwaltet und bei jedem Aufruf eines EFA-Dienstes in Form einer subjectAccessPolicy mitgegeben.



Querverweise und Referenzen

- EFA-2.0-Spezifikation

Implementable Perspective - Enterprise Dimension

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Verwendete Standards: Sicherheit

Security Assertion Markup Language (SAML)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eeenn.01.01}

Die Security Assertion Markup Language (SAML) spezifiziert einen Rahmen, in dem vertrauenswürdige Aussagen zu Identitäten dargestellt und ausgetauscht werden können. Die primären Anwendungsszenarien, in denen SAML eingesetzt wird, sind Single Sign-On sowie Identity Federation (Verknüpfung und Austausch von Identitätsinformationen über Organisationsgrenzen hinweg).

Den zentralen Bestandteil des Standards bilden die abstrakten Nachweise (Assertions) und Protokolle.[1] Während die Assertions vertrauenswürdige Aussagen zur Authentifizierung und Autorisierung einer Identität sowie einer Identität zugeordnete Attribute kapseln, erlauben es die Protokolle, solche Assertions anzufragen und zu transportieren.

SAML Core

Organisation	OASIS
Version	2.0 (März 2005)
Zweck	Abstrakte, XML-basierte Darstellung von vertrauenswürdigen Aussagen in Form von SAML Assertions Abstrakte Protokolle für den Transport der SAML Assertions

Die SAML-Protokolle und deren Nachrichten werden in [1] zunächst abstrakt spezifiziert. Wie die Protokolle an ein konkretes Nachrichten- oder Transportprotokoll, beispielsweise SOAP oder HTTP, gebunden werden, wird in [2] spezifiziert. Abhängig vom mit SAML umzusetzenden Anwendungsszenario können Assertions und Protokolle zusätzlich in Form einer Profilierung konkretisiert werden. Für typische Anwendungsszenarien gibt der SAML-Standard bereits Profilierungen in [3] vor. Diese umfassen u.a. Single Sign-On-Szenarien für Web Browser und für erweiterte Clients sowie Identity-Federation-Szenarien in verschiedenen Varianten.

Die EFA 2.0 Spezifikation verwendet SAML Assertions als Sicherheitstoken, welche von speziellen Sicherheitstokendiensten ausgestellt werden. Die Assertions erlauben die Kodierung von Identitäts- und Authentifizierungsnachweisen.

Weitere Informationen zu diesem Standard sind im IHE Cookbook zu finden.

eXtensible Access Control Markup Language (XACML)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eeenn.01.02}

XACML[4] erlaubt die XML-basierte Beschreibung von Regeln für den Zugriff auf Ressourcen und spezifiziert Protokolle, mit denen Autorisierungsentscheidungen angefordert und ausgegeben werden können. Der Standard verfolgt einen generischen Ansatz, sodass mit XACML verschiedenartige Ansätze für Berechtigungssysteme (z.B. rollenbasierte Berechtigungen) realisiert werden können.

	XACML
Organisation	OASIS
Version	2.0 (Februar 2005)
	Autorisierung
Zweck	Beschreibung von Zugriffsregeln
	Protokoll zur Anforderung und Herausgabe von Autorisierungsentscheidungen

Der Standard besteht in seinem Kern aus den Systembausteinen Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP) sowie Policy Administration Point (PAP). Diese Systembausteine werden durch weitere periphere Informationssysteme (z.B. Verzeichnisdienste) unterstützt. Weitere von OASIS herausgegebene Profile adressieren das Zusammenspiel mit anderen Standards (z.B. SAML) oder die Implementierung spezifischer Berechtigungsmodelle über die Konstrukte von XACML.

XACML spezifiziert – wie SAML auch – zunächst lediglich die Schemata für Protokollnachrichten. Der Transport dieser Nachrichten wird vom Standard nicht adressiert und ist Gegenstand einer Profilierung. In der EFA 2.0 Spezifikation wird XACML für die Kodierung von Autorisierungsnachweisen verwendet.

Weitere Informationen zu diesem Standard sind im IHE Cookbook zu finden.

Web Service Security (WS-Security)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eeenn.01.03}

WS-Security [5] erlaubt es, SOAP-Nachrichten auf der Nachrichtenebene zu signieren und zu verschlüsseln. Es bietet außerdem einen Rahmen, in dem verschiedene Sicherheitstoken übertragen werden können. Der Standard wird daher von weiteren Token-Profilen begleitet, die etwa die Nutzung von X.509-basierten Zertifikaten, SAML-Token oder Kerberos-Tickets als Sicherheitstoken spezifizieren.

WS-Security	
Organisation	OASIS
Version	1.1 (Februar 2006)
Zweck	Nachrichtensicherheit auf Nachrichtenebene, Bereitstellung von Mechanismen für höhere Sicherheitsprotokolle
Erweiterungen Tokenprofile:	Username Token Profile 1.1 X.509 Token Profile 1.1 SAML Token Profile 1.1 Kerberos Token Profile 1.1

Im Rahmen der EFA-Sicherheitsarchitektur wird WS-Security genutzt, um Sicherheitstoken zwischen EFA-Teilnehmersystem und EFA-Anwendung- und Sicherheitsdiensten auszutauschen.

Web Services Trust Language (WS-Trust)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eeenn.01.04}

WS-Trust [6] erweitert WS-Security um ein nachrichtenbasiertes Protokoll, das das Anfragen und Ausstellen von Sicherheitstoken sowie die Delegation von Vertrauensbeziehungen erlaubt. WS-Trust führt dazu ein aus drei Rollen bestehendes Modell ein, in dem ein Webservice-Nutzer bei einem Sicherheitstokendienst ein Sicherheitstoken anfragt, welches dieser anschließend bei einem Webservice-Anbieter einlösen kann. Die vom Webservice-Nutzer so vorgelegten Behauptungen zur Nutzeridentität sind durch die Vertrauensbeziehung zwischen Webservice-Anbieter und Sicherheitstokendienst mithilfe von kryptographischen Methoden verifizierbar.

WS-Trust ist funktional dem SAML 2.0 Protokoll sehr ähnlich, wobei SAML eher in browserbasierten Lösungen zum Einsatz kommt, während WS-Trust vorwiegend in Fat-Client-Umgebungen genutzt wird, bei denen auch über eine rein textbasierte HTTP-Kommunikation hinausgehende

Protokolle wie z.B. SOAP zur Kommunikation zwischen Systemkomponenten genutzt werden. Hersteller von Identitäts- und Berechtigungsmanagement-Lösungen unterstützen üblicherweise beide Protokolle.

WS-Trust

Organisation	OASIS
Version	1.3 (März 2007)
Zweck	Anfragen und Ausstellen von Sicherheitstoken (z. B. SAML Assertions), Konzept des direkt vermittelten Vertrauens

Der EFA Identity Provider ist ein WS-Trust 1.3 Sicherheitstokendienst. Er erlaubt einen Abruf von EFA Identity Assertions über das WS-Trust-Protokoll. Weitere Informationen im IHE Cookbook.

Referenzen

1. ↑ [1,0](#) [1,1](#) S. Cantor et al. (2005), Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.
2. ↑ S. Cantor et al. (2005), Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0.
3. ↑ J. Hughes et al. (2005), Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.
4. ↑ T. Moses (2005), eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS.
5. ↑ A. Nadalin et al. (2006), Web Service Security: SOAP Message Security 1.1. OASIS.
6. ↑ A. Nadalin et al. (2007), WS-Trust 1.3. OASIS.

- zurück zur EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Used Namespaces**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

ECR Namespace Prefixes

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Esams.01}`

XML namespace prefixes are used in this specification to stand for their respective namespaces as follows:

Prefix	Namespace
ecr	urn:efa:v2:2013
soapenv	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
saml	urn:oasis:names:tc:SAML:2.0:assertion
xacml	urn:oasis:names:tc:xacml:2.0:policy:schema:os
xacml-saml	urn:oasis:names:tc:xacml:2.0:saml:assertion:schema:os
hl7v2	urn:hl7-org:v2
hl7v3	urn:hl7-org:v3
xds	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance
rimext	urn:ihe:iti:xds-ebrim:extensions:2010
query	urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0
rim	urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0

rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0

Implementable Perspective - Information Dimension

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Information Model IHE XD* Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Mapping of Core Information Model Classes

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {MdaBs.01}`

For the linkage of XDS compliant components with eCR components the following mapping of business objects MUST be implemented:

Electronic Case Record	**IHE XDS**
Patient	Patient
eCR CaseRecord	Set of XDS Folders that have values of XDSFolder.patientID and XDSFolder.codeList in common

eCR Partition	XDS Folder
no correspondence	XDS Submission Set
eCR Medical Data Object	XDS Document Entry (document metadata) Repository Object (document data)

Mapping of PIM Classes

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {MdaBs.01}

Instances of ECR PIM Classes are shared through XD* transactions and within XD* metadata. The following table shows the respective binding of these classes to IHE XD* message arguments and ebRS metadata slots/elements.

ECR PIM Class	IHE XD*	Comments
patientID	XDSDocumentEntry.patientId XDSFolder.patientID	-
communityID	XDSDocumentEntry.homeCommunityId XDSFolder.homeCommunityID	-
purpose	XDSFolder.codeList	see XDS Folder Metadata
ecrInfo	see below	As there is no correspondence to a case record object with IHE XD* this class is mapped onto folder metadata. This implies that the ecrInfo fraction of all folder's belonging to the same eCR shall be identical and synchronized.
consentInfo	-	ECR consentInfo objects are represented as structured, coded documents. See "Leitfaden Patienteneinwilligung" for details. The binding of consentInfo is not subject to the EFA Specification. An EFA domain must agree on a specific binding. Implementation Guide for CDA®, Release 2: Consent Directives, Release 1 MAY be used.
consentDoc	-	Consent documents are represented as documents of a format that is to be agreed by each ECR domain (e.g. PDF/A).

partitionID	XDSFolder.uniqueID	see IHE ITI TF Vol3 section 4.1.9.1 for details
partitionList	set of XDSFolder objects	-
ecrRef	XDSFolder.patientID and XDSFolder.codeList and XDSFolder.homeCommunityID	All folders classified with the same patient ID and purpose codes set up a unique case record. The homeCommunityID signals the XDS Affinity Domain where the reference is valid.
partitionInfo	XDSFolder object	see XDS Folder Metadata for details
docMetadata	XDSDocument registry object	see XDS Document Metadata for details
docRelationship	XDS Association object	see IHE ITI TF Vol3 section 4.1.6 for details
documentID	XDSDocument.uniqueID XDSDocument.repositoryUniqueID	shall be used for document retrieval (retrieveDocument transaction).
	XDSDocument.entryUUID	shall be used for document referral (associations between registry entries)

ecrInfo

Attribute	Description	Mapping onto IHE XD* metadata
patientID (mandatory)	Identifier of the patient who is subject to the eCR	All XDS folders representing the partitions of an eCR instance shall be assigned the same *patientID* attribute (see IHE ITI TF Volume 3, Section 4.2.3.1.3).
purpose (mandatory)	purpose for maintaining the eCR	All XDS folders representing the partitions of an eCR instance shall be classified with the same purpose (see folder metadata *codeList* element).
ecrStatus (mandatory)	Status of an eCR instance	The status of en eCR is implemented through the eCR access policy and the avaibalility status of the XDS folders that represent the partitions of the ecR.

status	XDS folder availabilityStatus	eCR Access Policy
open	approved	access policy reflects the patient's consent
suspended	approved	access policy only allows access to the case record manager and to privacy commissionars
retired	approved	deny-all access policy assigned to the eCR.

archived	-	all eCR data and metadata have been deleted from the XDS registry and repository


According to IHE ITI TF volume 3, the deprecation of Folders is not allowed. Therefore this value shall always be Approved. Nevertheless eCR takes this attribute into account as future versions of the ITI technical framework may allow for further options.

Querverweise und Referenzen

- EFA-2.0-Spezifikation


Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS Folder Metadata Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Folder Metadata

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDold.01}`

Instances of the partitionInfo ECR PIM Class are shared through XD* transactions and within XDS folder metadata. The following table shows the respective binding of the partitionInfo subelements to IHE XDS Folder ebRS metadata slots/elements.

partitionInfo	IHE XDS Folder Metadata	Comments
partitionID	XDSFolder.uniqueID	see IHE ITI TF Vol3 section 4.1.9.1 for details
title	XDSFolder.title	see IHE ITI TF Vol3 section 4.2.3.4.8 for details on the encoding of folder titles. ECR partition (XDS folder) titles SHALL NOT contain the name of the patient.
classification (purpose)	XDSFolder.codeList	see additional profiling for eCR purpose codes below
time.startTime	-	This eCR partitionInfo element cannot be mapped to IHE XDS Folder Metadata. Client-side implementations of the partitionInfo data structure SHALL allow for NULL-Values for this element.
time.endTime	XDSFolder.lastUpdateTime	As this element is mainly used for sorting partitions, the last update time of the corresponding folder is considered a good indicator for this purpose.
organization	XDSFolder.comments	This eCR partitionInfo element cannot be mapped to "regular" IHE XDS Folder Metadata. Client-side implementations of the partitionInfo data structure SHALL allow for NULL-Values for this element.
anchor	XDSFolder.codeList	The creator of a XDS folder may add further classifications to the corresponding eCR partition. Beside the purpose-clasification, eCR participants SHALL NOT process classifications that were defined by other participants.

Folder metadata which are not profiled in the table MUST be used as defined in table 4.1-7 of [IHE ITI TF Vol3 v9.0]. Further constraints MAY apply for EFA national profiles.

codeList

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDold.01.01}

The linkage of a folder to a case record is implemented through the *codeList* classification of that folder. Each folder SHALL contain at least 2 event codes:

1. a single event code that denotes the folder as part of a case record. The respective classification is done by assigning an event code of (code="ECR", codeSystem="IHE-D-Cookbook-FolderClassCode") to the folder.
2. one or more event codes that indicate the purpose of the case record. These event codes can be a diagnosis code, a contract type, etc. Folders that are assigned to multiple case records SHALL be classified with multiple of such event codes (at least one per case record). Only the code systems and codes as listed in the following table SHALL be used.

Purpose	Code System Name	Code System OID	Value(s)
Diagnosis	ICD-10-GM	1.2.276.0.76.5.311	see http://www.dimdi.de/static/de/klassi/icd-10-gm/kodesuche/onlinefassungen/htmlgm2013/index.htm
Disease Management Contract (DMP)	S_KBV_DMP	1.2.276.0.76.5.223	see http://www.kbv.de/keytabs/ita/schluesseltabellen.asp?page=S_KBV_DMP_V1.01.htm
Integrated Care Contract (*IV Vertrag*)	S_VDX_VERTRAGSART	1.2.276.0.76.5.257	09 This code just signales that this folder is linked with a case record that serves an integrated care contract. Information about the contract SHALL be given with the display name of this code.
GP managed care (*Hausarztzentrierte Versorgung*)	S_VDX_VERTRAGSART	1.2.276.0.76.5.257	07 This code just signales that this folder is linked with a case record that serves a GP managed care contract. Information about the contract SHALL be given with the display name of this code.

Example: Diagnosis (ICD-10)

```
<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
```

```
   nodeRepresentation="ECR">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>IHE-D-Cookbook-FolderClassCode</rim:Value>
       </rim:ValueList>
   </rim:Slot>
   <rim:Name>
       <rim:LocalizedString xml:lang="de" charset="UTF-8" value="Elektronische Fallakte"/>
   </rim:Name>
</rim:Classification>

<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
   nodeRepresentation="I21.0">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>1.2.276.0.76.5.311</rim:Value>
       </rim:ValueList>
   </rim:Slot>
   <rim:Name>
       <rim:LocalizedString xml:lang="de" charset="UTF-8" value="Akuter transmuraler Myokardinfarkt der Vorderwand"/>
   </rim:Name>
</rim:Classification>
```

Example: DMP

```
<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
```

```
   nodeRepresentation="ECR">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>IHE-D-Cookbook-FolderClassCode</rim:Value>
       </rim:ValueList>
   </rim:Slot>
   <rim:Name>
       <rim:LocalizedString xml:lang="de" charset="UTF-8" value="Elektronische Fallakte"/>
   </rim:Name>
</rim:Classification>

<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
   nodeRepresentation="6">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>1.2.276.0.76.5.223</rim:Value>
       </rim:ValueList>
   </rim:Slot>
   <rim:Name>
       <rim:LocalizedString xml:lang="de" charset="UTF-8" value="COPD"/>
   </rim:Name>
</rim:Classification>
```

Example: IV Vertrag

```
<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
   nodeRepresentation="ECR">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
```

```
            <rim:Value>IHE-D-Cookbook-FolderClassCode</rim:Value>
        </rim:ValueList>
    </rim:Slot>
    <rim:Name>
        <rim:LocalizedString xml:lang="de" charset="UTF-8" value="Elektronische Fallakte"/>
    </rim:Name>
</rim:Classification>

<rim:Classification
    id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
    lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
    objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
    classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4"
    classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
    nodeRepresentation="09">
    <rim:Slot name="codingScheme">
        <rim:ValueList>
            <rim:Value>1.2.276.0.76.5.257</rim:Value>
        </rim:ValueList>
    </rim:Slot>
    <rim:Name>
        <rim:LocalizedString xml:lang="de" charset="UTF-8" value="IV Vertrag Darmkrebs"/>
    </rim:Name>
</rim:Classification>
```

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS Document Metadata Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Document Metadata

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.01}`

Unless stated otherwise in the following sub-sections, document metadata MUST be used as defined in table 4.1-5 of [IHE ITI TF Vol3 v9.0]. This as well holds for cardinalities and optionalities of document metadata elements. Further constraints MAY apply for EFA national profiles (see below for the German profile).

classCode

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.01.01}`

The document class shall be taken from a national catalogue. The national catalogue should be a value set on top of LOINC as a reference terminology.

typeCode

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.01.02}`

The document type shall be provided as a LOINC code. Document types shall be more specific than document classes. They may be defined per Care Domain.

Example:

```
<rim:Classification
   id="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   lid="urn:uuid:c33ca26a-29b4-45be-a9b9-de60adca4c64"
   objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
   classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
   classifiedObject="urn:uuid:fbf2ea29-3aa3-4bc5-9187-01d7b6b0f481"
   nodeRepresentation="11520-4">
   <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>2.16.840.1.113883.6.1</rim:Value>
       </rim:ValueList>
   </rim:Slot>
   <rim:Name>
       <rim:LocalizedString xml:lang="de" charset="UTF-8" value="EKG Befund"/>
   </rim:Name>
</rim:Classification>
```

Comments

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.01.03}

This slot is optional. If given, it SHALL hold a summary of the document content.

Example:

```
<rim:Description>
   <rim:LocalizedString xml:lang="de" charset="UTF-8" value = "Befund zur Magenspiegelung vom 3.3.13"/>
</rim:Description>
```

German Profile

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.02}

For using EFA within the German national healthcare IT infrastructure (*Telematikinfrastruktur*) the constraints listed below MUST be considered.

Author Institution

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.02.01}

For the German healthcare system the following identification schemes MUST be used. If multiple schemes are available for an organization, the order in the table denotes the order of preference.

Organization	Scheme	Code System OID
Practice	Telematik ID This ID scheme MUST be preferred only if the Telematik ID is recorded within the SMC-B AUT certificate of the practice.	*not defined yet*
Practice	ID of the SMC-B AUT Certificate	1.2.276.0.76.4.77
Practice	»Institutskennzeichen (IK)« acc. to § 293 SGB V	1.2.276.0.76.4.5
Practice	KBV »Arztnummer Praxis«	1.2.276.0.76.4.10
Practice	Any internal identification scheme that guarantees a unique identification within the scope of the affinity domain. Identifiers SHALL be resolvable to all EFA participants through public directory services (e.g. HPD, see IHE-Cookbook).	*local code system*
Hospital department or faculty	Telematik ID This ID scheme MUST be preferred only if the Telematik ID is recorded within the SMC-B AUT certificate of the department/faculty.	*not defined yet*
Hospital department or faculty	ID of the SMC-B AUT Certificate	1.2.276.0.76.4.77
Hospital department or faculty	Any internal identification scheme that guarantees a unique identification within the scope of the affinity domain. Identifiers SHALL be resolvable to all EFA participants through public directory services (e.g. HPD, see IHE-Cookbook).	*local code system*
Hospital	Telematik ID This ID scheme MUST be preferred only if the Telematik ID is recorded within the SMC-B AUT certificate of the hospital.	*not defined yet*

Hospital	ID of the SMC-B AUT Certificate	1.2.276.0.76.4.77
Hospital	»Institutskennzeichen (IK)« acc. to § 293 SGB V	1.2.276.0.76.4.5
Hospital	Any internal identification scheme that guarantees a unique identification within the scope of the affinity domain. Identifiers SHALL be resolvable to all EFA participants through public directory services (e.g. HPD, see IHE-Cookbook).	*local code system*

Telematik ID and SMC-B certificates will only be available with the Telematik-Infrastruktur. Before the final roll-out of the Telematik-Infrastruktur identifiers based on Telematik ID and SMC-B SHOULD NOT be used.

Example:

A resident practice with the *Institutskennzeichen* 260326822 would be encoded as:

```
<rim:Slot name="authorInstitution">
  <rim:ValueList>
    <rim:Value>Name der Praxis^^^^^&amp;1.2.276.0.76.4.5&amp;ISO^^^^260326822</rim:Value>
  </rim:ValueList>
</rim:Slot>
```

Author Person

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.02.02}

For the German healthcare system the following identification schemes MUST be used. If multiple schemes are available for an author's ID, the order in the table denotes the order of preference. If multiple IDs are known, at least two SHOULD be provided (considering the order of preference). An author identifier SHALL NOT be used without additionally providing the full name of the author.

Person Role	Scheme	Code System OID
Physician	Telematik ID This ID scheme MUST be preferred only if the Telematik ID is recorded within the HBA AUT certificate of the physician.	*not defined yet*
Physician	ID of the HBA AUT Certificate	1.2.276.0.76.4.75

Physician	Lebenslange Arztnummer KV	1.2.276.0.76.4.16
Physician Hospital Staff Practice Staff	Any internal identification scheme that guarantees a unique identification within the scope of the identified organization. The <authorInstitution> and an <id> for this organization MUST be recorded.	*local code system*

Telematik ID and HBA certificates will only be available with the Telematik-Infrastruktur. Before the final roll-out of the Telematik-Infrastruktur identifiers based on Telematik ID and HBA SHOULD NOT be used.

Example:

A physician with the *Arztnummer* 12345678 would be encoded as:

```
<rim:Slot name="authorPerson">
  <rim:ValueList>
    <rim:Value>Name des Arztes^^^^^&1.2.276.0.76.4.16&ISO^^^^12345678</rim:Value>
  </rim:ValueList>
</rim:Slot>
```

HealthcareFacilityTypeCode

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.02.03}

The healthcare facility type code SHALL be encoded as a coded value acc to the *KBV Schlüsseltabelle S_VDX_PRAXISTYP* ([1]). The root OID 1.2.276.0.76.3.1.1.5.1.4 SHALL be used.

Example:

A hospital facility type would be encoded as:

```
<rim:Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
                    classifiedObject="theDocument" id=”ID_050"
                    objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:Classification"
                    nodeRepresentation="50">
    <rim:Name>
```

```
        <rim:LocalizedString xml:lang="de" value="Krankenhaus"/>
    </rim:Name>
    <rim:Slot name="codingScheme">
       <rim:ValueList>
           <rim:Value>1.2.276.0.76.3.1.1.5.1.4</rim:Value>
       </rim:ValueList>
    </rim:Slot>
</rim:Classification>
```

sourcePatientInfo

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDoct.02.04}

For reasons of protecting the confidentiality of personal medical information this slot SHALL NOT be used. For the identifing the patient the sourcePatientId element SHALL be provided for all documents metadata.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Security Object Bindings**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt

und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Security Object Bindings

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eeris.01}`

EFA security objects are encapsulated through SAML assertions so as the following mapping of security objects MUST be implemented:

Electronic Case Record	SAML
Authentication Token / HP Identity Assertion	EFA Identity Assertion SAML2 Binding
Authorization Token / Access Policy	EFA Policy Assertion SAML2 Binding

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Identity Assertion SAML2 Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die unter den einzelnen Überschriften in geschweiften Klammern angegebenen Kürzel dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt

und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

SAML 2.0 Profile for ECR Identity Assertions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01}

Assertion Element	Opt	Usage Convention
@Version	R	MUST be “2.0”
@ID	R	URN encoded unique identifier (UUID) of the assertion
@IssueInstant	R	time instant of issuance in UTC
Issuer	R	address URI that identifies the endpoint of the issuing service
Subject	R	This element defines the subject confirmation method of the user in order to use the Identity Assertion as a protection token. Moreover, it defines the subject name identifier that accords with the user identity.
NameID	R	Identifier of the HP encoded as an X.509 subject name, an e-Mail address or as a string value (unspecified format). Only identifiers must be used that can be long-term tracked back to an individual person.
@Format	R	MUST be *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified* or *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName* or *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress* For providing an OID as a subject identifier the *unspecified* format must be used. The OID must be provided as a string encoded in ISO format.
SubjectConfirmation	R	
@Method	R	This element MUST hold a URI reference that identifies a protocol to be used to authenticate the subject.[SAML2.0core] The value of this element MUST be set to *urn:oasis:names:tc:SAML:2.0:cm:holder-of-key* or *urn:oasis:names:tc:SAML:2.0:cm:bearer*

		If the bearer method is used, the EFA Identity Assertion SHALL only be exchanged over secure channels with trusted endpoints in order to maintain confidentiality and message integrity.
SubjectConfirmationData	R	
ds:KeyInfo	R	The XML Signature [XMLSignature] element MUST embed a cryptographic key that is only held by the user. This can be the user's public key (ds:KeyValue/ds:RSAKeyValue), the complete user's X.509 certificate (ds:X509Data/ds:X509Certificate), or an encrypted symmetric key (xenc:EncryptedKey [XMLEncryption]). This symmetric key MUST be encrypted by using the public key of the consumer service's certificate [eFA PKI 1.2].
Conditions	R	
@NotBefore	R	time instant from which the assertion is useable. This condition MUST be assessed by the assertion consumer to proof the validity of the assertion.
@NotOnOrAfter	R	time instant at which the assertion expires. This condition MUST be assessed by the assertion consumer to proof the validity of the assertion. The maximum validity timespan for an HCP Identity Assertion MUST NOT be more than 4 hours.
AuthnStatement	R	
@AuthnInstant	R	time instant of HP authentication in UTC
@SessionNotOnOrAfter	O	Time instant of the expiration of the session
AuthnContext	R	
AuthnContextClassRef	R	A URI reference that specifies the type of authentication that took place (see SAML 2.0).
AttributeStatement	R	HP identity attributes and permissions (see section below for details)
ds:Signature	R	Enveloped XML signature of the issuer of the HCP Identity Assertion (see section below for details).

German Profile

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01.05}

The subject must refer to a health professional. The subject identifier must be provided as an OID. Only the following identitification schemes must be used. The order of the table denotes the order of preference.

Person Role	Scheme	Code System OID

Physician	Telematik ID This ID scheme MUST be preferred only if the Telematik ID is recorded within the HBA AUT certificate of the physician.	*not defined yet*
Physician	ID of the HBA AUT Certificate	1.2.276.0.76.4.75
Physician	Lebenslange Arztnummer KV	1.2.276.0.76.4.16
Physician Hospital Staff Practice Staff	Any internal identification scheme that guarantees a unique identification within the scope of the identified organization. The <representedOrganization> and an <id> for this organization MUST be recorded.	*local code system*

Telematik ID and HBA certificates will only be available with the Telematik-Infrastruktur. Before the final roll-out of the Telematik-Infrastruktur identifiers based on Telematik ID and HBA SHOULD NOT be used.

Assertion Signature

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01.01}

Every HP Identity Assertion MUST be signed by its issuer. The XML signature MUST be applied by using the *saml:Assertion/ds:Signature* element as defined below.

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be *http://www.w3.org/2001/10/xml-exc-c14n#*
Transformation	Enveloped signature transform acc. to section 6.6.4 of [W3C XMLDSig] SHOULD be used (*http://www.w3.org/2000/09/xmldsig#enveloped-signature*). In addition, exclusive canonicalization SHOULD be defined as transformation (*http://www.w3.org/2001/10/xml-exc-c14n#*, acc. [W3C XMLDSig] and [W3C XML-EXC 1.0]). As inclusive namespaces other prefixes than the ones defined in *EFA Namespaces* MUST NOT be used.
SignatureMethod	For signing assertions the signature method *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256* or *http://www.w3.org/2000/09/xmldsig#rsa-sha1* SHOULD be used. An assertion consumer MAY reject signatures that use SHA-1 for digesting.
DigestMethod	For signing assertions the digest method

	http://www.w3.org/2000/09/xmldsig#sha1 or *http://www.w3.org/2001/04/xmlenc#sha256* SHOULD be used. An assertion consumer MAY reject SHA-1 digests.
KeyInfo	This element MUST either contain a wsse:SecurityTokenReference element which references the X.509 certificate of the assertion's issuer by using a subject key identifier OR contain a ds:X509Data element which contains the X.509 certificate of the assertion issuer.

HCP Identity Attributes

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01.02}

An identity assertion can carry an arbitrary number of attributes on the authenticated entity. Each attribute MUST be encoded using a SAML attribute element.

For ECR the following attribute names and catalogues are defined.

HP Identifier

FriendlyName	XSPA Subject
Name	urn:oasis:names:tc:xacml:1.0:subject:subject-id
Values	Human readable name of the HP
Type	String
Optionality	Mandatory
Description	This attribute MUST contain the full name of the HP.

Structural Role of the HCP

FriendlyName	XSPA Role
Name	urn:oasis:names:tc:xacml:2.0:subject:role
Values	See ASTM E1986-98 (2005). Only the ASTM structural roles "dentist", "nurse" "pharmacist", "physician", "nurse midwife", "admission clerk", "ancillary services" and "clinical services" MUST be used.

Type	String
Optionality	Mandatory

Delegated Rights

FriendlyName	OnBehalfOf
Name	urn:epsos:names:wp3.4:subject:on-behalf-of
Values	See ASTM E1986-98 (2005). Only the ASTM structural roles “dentist”, “pharmacist”, “physician” and “nurse midwife” MUST be used.
Type	String
Optionality	Mandatory if a structural role of “ancillary services” or “clinical services” is presented. For all other structural roles this attribute is optional
Description	If a person is acting on behalf of another person the role of this person MAY be provided with this attribute. If this attribute is included with a HCP identity assertion, the issuer of the assertion MUST be able to track back the delefation to the two natural persons involved. Only valid roles as defined for HCP structural roles MUST be used. An assertion consumer MAY decide not to accept delegated access rights by just ignoring this attribute.

Healthcare Professional Organisation

FriendlyName	XSPA Organization
Name	urn:oasis:names:tc:xspa:1.0:subject:organization
Values	Name of the Healthcare Professional Organisation
Type	String
Optionality	Optional
Description	This value SHOULD only be provided if different from the point of care (e.g. in cases where a hospital organization runs multiple points of care or where a hospital just provides a professional environment for otherwise independent care providers)

Healthcare Professional Organisation ID

FriendlyName	XSPA Organization Id
Name	urn:oasis:names:tc:xspa:1.0:subject:organization-id
Values	URN encoded OID of the Healthcare Professional Organisation
Type	URI

Optionality	Mandatory

Purpose of Use

FriendlyName	XSPA Purpose of Use
Name	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse
Values	MUST be *TREATMENT*
Optionality	Optional
Description	ECR access is only granted for treatment purposes.

Point of Care

Attribute Name	XSPA Locality
Name	urn:oasis:names:tc:xspa:1.0:environment:locality
Values	String
Optionality	Optional
Description	Name of the hospital or medical facility where patient care takes place.

ECR regional networks MAY agree on further attributes. Any attributes not listed in this list MAY be ignored by the assertion consumer.

German Extensions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01.03}

Speciality of the HP

FriendlyName	Clinical Speciality
Name	**TO BE DEFINED**
Values	**HIER MUSS NOCH DIE PASSENDE KBV SCHLÜSSELTABELLE RAUSGESUCHT WERDEN**
Type	URI
Optionality	Optional
Description	Clinical speciality of the HP as expressed in her Health Professional Card (HBA)

HBA attributes will only be available with the Telematik-Infrastruktur. Before the final roll-out of the Telematik-Infrastruktur identifiers based on HBA SHOULD NOT be used.

Example Assertion

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {ItyAn.01.04}

```
 <soap12:Envelope … >
 <soap12:Header … >
  <wsse:Security … >
   <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                   ID="_2c356d70-1215-42f9-93a0-fc6fab1c966e"
                   IssueInstant="2009-09-21T12:03:28.788Z" Version="2.0">
   <saml:Issuer>urn:de:berlin:hp:idp</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:SignedInfo>
      <ds:CanonicalizationMethod
       Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
       <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
       <ds:Reference URI="#urn:uuid:7102AC72154DCFD1F51253534608780">
        <ds:Transforms>
         <ds:Transform
          Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
         <ds:Transform
          Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ec:InclusiveNamespaces
           xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
           PrefixList="ds saml xs" />
         </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>A1LyLvFHRrYaOJ28YVFd3MfKGSI=</ds:DigestValue>
       </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>cH+lCY … </ds:SignatureValue>
      <ds:KeyInfo>
       <ds:X509Data>
```

```
      <ds:X509Certificate> … </ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </ds:Signature>
   <saml:Subject>
    <saml:NameID
     Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
     ...
    </saml:NameID>
    <saml:SubjectConfirmation
     Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
     <saml:SubjectConfirmationData>
       <ds:KeyInfo>
         <ds:X509Data>
           <ds:X509Certificate> … </ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
      </saml:SubjectConfirmationData/>
    </saml:SubjectConfirmation>
   </saml:Subject>
   <saml:Conditions
    NotBefore="2012-09-21T12:03:28.788Z"
    NotOnOrAfter="2012-09-21T16:03:28.788Z">
  </saml:Conditions>
  <saml:AuthnStatement
   AuthnInstant="2012-09-21T12:03:28.788Z"
   SessionNotOnOrAfter="2012-09-21T16:03:28.788Z">
   <saml:AuthnContext>
   <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:X509
   </saml:AuthnContextClassRef>
   </saml:AuthnContext>
  </saml:AuthnStatement>
 <saml:AttributeStatement>
 <saml:Attribute
  FriendlyName="XSPA Subject"
  Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">Dr. Peter Meier
 </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
 FriendlyName="XSPA Organization"
 Name="urn:oasis:names:tc:xspa:1.0:subject:organization"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
 <saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">Kreiskrankenhaus Neustadt
 </saml:AttributeValue>
</saml:Attribute>
</saml:Attribute>
<saml:Attribute
 FriendlyName="XSPA Role"
 Name="urn:oasis:names:tc:xacml:2.0:subject:role"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
 <saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">physician
 </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
 FriendlyName="XSPA Purpose of Use"
 Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
 <saml:AttributeValue
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">TREATMENT
 </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
 FriendlyName="XSPA Locality"
 Name="urn:oasis:names:tc:xspa:1.0:environment:locality"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
 <saml:AttributeValue
```

```
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:type="xs:string">Kreiskrankenhaus Neustadt
    </saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
 </saml:Assertion>
</wsse:Security>
</pre>
```

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA Policy Assertion SAML2 Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

SAML 2.0 Profile for ECR Policy Assertions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01}

This profile applies to scenarios where the eCR Context Manager requests an Access Policy Assertion from the eCR Policy Provider and thus implements a policy push authorization model. There is no specification in the case that the Authorization Decision Provider requests policies from the eCR Policy Provider.

Assertion Element	Opt	Usage Convention
@Version	R	MUST be “2.0”
@ID	R	URN encoded unique identifier (UUID) of the assertion
@IssueInstant	R	Time instant of issuance in UTC
Issuer	R	Address URI that identifies the endpoint of the issuing service
Subject	R	This element defines the subject confirmation method of the user in order to use the Policy Assertion as a supporting token. Moreover, it defines the subject name identifier that accords with the user identity from an Identity Assertion.
NameID	R	Identifier of the HP given in the Identity Asstertion encoded as an X.509 subject name, an e-Mail address or as a string value (unspecified format). Only identifiers must be used that can be long-term tracked back to an individual person.
@Format	R	MUST be *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified* or *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName* or *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress* For providing an OID as a subject identifier the *unspecified* format must be used. The OID must be provided as a string encoded in ISO format.
SubjectConfirmation	R	
@Method	R	This element MUST hold a URI reference that identifies a protocol to be used to authenticate the subject.[SAML2.0core] The value of this element MUST be set to *urn:oasis:names:tc:SAML:2.0:cm:holder-of-key*
SubjectConfirmationData	R	
ds:KeyInfo	R	The XML Signature [XMLSignature] element MUST embed a cryptographic key that is only held by the user. This can be the user’s public key (ds:KeyValue/ds:RSAKeyValue), the complete user’s X.509 certificate (ds:X509Data/ds:X509Certificate), or an encrypted symmetric key (xenc:EncryptedKey [XMLEncryption]). This

		symmetric key MUST be encrypted by using the public key of the consumer service's certificate [eFA PKI 1.2].
Conditions	R	
@NotBefore	R	time instant from which the assertion is useable. This condition MUST be assessed by the assertion consumer to proof the validity of the assertion.
@NotOnOrAfter	R	Time instant at which the assertion expires. This condition MUST be assessed by the assertion consumer to proof the validity of the assertion. The maximum validity timespan for a Policy Assertion MUST NOT be more than 4 hours.
XACMLPolicyStatement	R	
PolicySet	R	PolicySet that expresses the given authorization (see section below for details).
ds:Signature	R	Enveloped XML signature of the issuer of the Policy Assertion (see section below for details).

PolicySet Profile

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01.01}

The ECR 2.0 specification differentiates three kinds of an authorization statement as it is described logically in the security token services section for the Policy Provider. These are:

- Reference without semantics (policyId) to an access policy which contains the valid authorization rules for an eCR Consumer
- Access policy which contains the valid authorization rules for an eCR Consumer

In order to implement such differentiations the <*PolicySet*> element has different sub-elements.

Policy Assignment

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01.02}

PolicySet Element	Opt	Usage Convention
@PolicySetId	R	UUID or OID of the policy set. The value MUST NOT be URN encoded.
@PolicyCombiningAlgId	R	This attribute is REQUIRED. Its value is a predefined identifier of the policy-combining algorithm for this

		policy set (see Appendix C and section B.10 in [XACML2.0Core]). The identifier *urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides* MUST be used.
Target	R	This element is used to specify the resource match (i.e., purpose)
Subjects	R	This element contains at least one *xacml:Subject* element.
Subject	R	It contains one *xacml:SubjectMatch* element.
SubjectMatch	R	It defines matches of the subject attributes.
		Its value specifies the matching function. The identifier refers to the subject nameID format of the Identity Assertion. The following list defines the used matching functions (see Section 7.5 in [XACML2.0Core]): • *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified -> urn:oasis:names:tc:xacml:1.0:function:string-equal* • *urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName -> urn:oasis:names:tc:xacml:1.0:function:x500Name-equal* • *urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress -> urn:oasis:names:tc:xacml:1.0:function:rfc822Name-equal*
@MatchId	R	Alternatively, the following HCP attributes MAY be used: • *urn:oasis:names:tc:xacml:1.0:subject:subject-id -> urn:oasis:names:tc:xacml:1.0:function:string-equal* • *urn:oasis:names:tc:xacml:2.0:subject:role -> urn:oasis:names:tc:xacml:1.0:function:string-equal* • *urn:oasis:names:tc:xspa:1.0:subject:organization -> urn:oasis:names:tc:xacml:1.0:function:string-equal* • *urn:oasis:names:tc:xspa:1.0:subject:organization-id -> urn:oasis:names:tc:xacml:1.0:function:string-equal* • *urn:oasis:names:tc:xspa:1.0:environment:locality -> urn:oasis:names:tc:xacml:1.0:function:string-equal*
AttributeValue	R	It defines the subject value for matching depending on the subject match id format.
@DataType	R	Its value is either *http://www.w3.org/2001/XMLSchema#string*, *urn:oasis:names:tc:xacml:1.0:data-type:x500Name*, or *urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name* that corresponds to the subject

		match.
SubjectAttributeDesignator	R	It defines the designator of a resource attribute.
@SubjectCategory	O	It specifies the categorized subject from which to match named subject attributes. If set, it MUST have the value *urn:oasis:names:tc:xacml:1.0:subject-category:access-subject*.
@AttributeId	R	If the nameID is provided for the XACML subject, then the value of this attribute is set to *urn:oasis:names:tc:xacml:1.0:subject:subject-id*. Otherwhise the following attribute IDs SHALL be used: • *urn:oasis:names:tc:xacml:1.0:subject:subject-id* • *urn:oasis:names:tc:xacml:2.0:subject:role* • *urn:oasis:names:tc:xspa:1.0:subject:organization* • *urn:oasis:names:tc:xspa:1.0:subject:organization-id* • *urn:oasis:names:tc:xspa:1.0:environment:locality*
@DataType	R	Its value is either *http://www.w3.org/2001/XMLSchema#string*, *urn:oasis:names:tc:xacml:1.0:data-type:x500Name*, or *urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name* that corresponds to the subject match.
Resources	R	This element contains one *xacml:Resource* element.
Resource	R	It contains one *xacml:ResourceMatch* element.
ResourceMatch	R	It defines matches of the resource attributes.
@MatchId	R	Its value specifies the matching function. The identifier *urn:oasis:names:tc:xacml:2.0:function:anyURI-regexp-match* is defined to use regular expressions (see A.3.13 in [XACML2.0Core]).
AttributeValue	R	It defines the regular expression for matching.
@DataType	R	Its value is *http://www.w3.org/2001/XMLSchema#string* to indicate that the attribute value is of *string* simple type.
ResourceAttributeDesignator	R	It defines the designator of a resource attribute.
@AttributeId	R	It specifies the identifier of the attribute that is used for matching. The value of this attribute is set to *urn:ihe:iti:xds-b:2007:folder:code*.
@DataType	R	It specifies the type of the values that the resource attribute designator returns. The value of this attribute is set to *urn:hl7-org:v3#CV* (HL7v3 "Coded Value" data type, see HL7v3 Abstract Data Type Specification -

		ANSI/HL7 V3 DT, R1-2004 11/29/2004; section 2.9). This custom data type holds a code and its associated code system using the following format: code@code-system. Example: <CodedValue code="ECR" codeSystem="IHE-D-Cookbook-FolderClassCode" /> is mapped to "ECR@IHE-D-Cookbook-FolderClassCode".
PolicySetIdReference	R	Its value either references an assigned access policy that is expressed in a separate XACML *PolicySet* or already expresses the given authorization.

Policy Attachment

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01.03}

The ECR's lifecycle is represented by means of interaction patterns and communication patterns. These patterns are bound to XACML actions. The following XACML Action element SHALL be used in a separate XACML Policy which shares the definition of the Policy Assignment.

Policy Element	Opt	Usage Convention
Target	R	This element is used to specify the resource match (i.e., purpose)
Subjects	R	see Policy Assignment
Resources	R	see Policy Assignment
Actions	R	This element contains at least one *xacml:Action* element.
Action	R	It contains one *xacml:ActionMatch* element.
ActionMatch	R	It defines matches of the action attributes.
@MatchId	R	Its value specifies the matching function. The following matching function SHALL be used: *urn:oasis:names:tc:xacml:1.0:function:string-equal*
AttributeValue	R	It defines the action value for matching depending on the action match id format. The action value refers to the EFA transaction as defined in EFA Audit Trail Binding.
@DataType	R	The value of this attribute is set to *urn:hl7-org:v3#CV* (HL7v3 "Coded Value" data type, see HL7v3 Abstract Data Type Specification - ANSI/HL7 V3 DT, R1-2004 11/29/2004; section 2.9). This custom data type holds a code and its associated code system name using the following format: code@code-system-name. Example: <CodedValue code="EFA-01" codeSystem="EFAv2 Transaction" /> is mapped to "ECR-01@EFAv2

		Transaction".
ActionAttributeDesignator	R	It defines the designator of a resource attribute.
@AttributeId	R	The following attribute ID SHALL be used: *urn:oasis:names:tc:xacml:1.0:action:action-id*
@DataType	R	Its value is *http://www.w3.org/2001/XMLSchema#string* that corresponds to the action match.

Assertion Signature

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01.04}

Every Policy Assertion MUST be signed by its issuer. The XML signature MUST be applied by using the *saml:Assertion/ds:Signature* element as defined below.

Signature Parameter	Usage Convention
CanonicalizationMethod	SHOULD be *http://www.w3.org/2001/10/xml-exc-c14n#*
Transformation	Enveloped signature transform acc. to section 6.6.4 of [W3C XMLDSig] SHOULD be used (*http://www.w3.org/2000/09/xmldsig#enveloped-signature*). In addition, exclusive canonicalization SHOULD be defined as transformation (*http://www.w3.org/2001/10/xml-exc-c14n#*, acc. [W3C XMLDSig] and [W3C XML-EXC 1.0]). As inclusive namespaces other prefixes than the ones defined in *EFA Namespaces* MUST NOT be used.
SignatureMethod	For signing assertions the signature method *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256* or *http://www.w3.org/2000/09/xmldsig#rsa-sha1* SHOULD be used. An assertion consumer MAY reject signatures that use SHA-1 for digesting.
DigestMethod	For signing assertions the digest method *http://www.w3.org/2000/09/xmldsig#sha1* or *http://www.w3.org/2001/04/xmlenc#sha256* SHOULD be used. An assertion consumer MAY reject SHA-1 digests.

KeyInfo	This element MUST either contain a wsse:SecurityTokenReference element which references the X.509 certificate of the assertion's issuer by using a subject key identifier OR contain a ds:X509Data element which contains the X.509 certificate of the assertion issuer.

Example Assertion

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {Eocyo.01.05}

```
<soap12:Envelope … >
<soap12:Header … >
 <wsse:Security … >
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="uuid-6dbb391c-20d3-4568-8c04-ff9d91d049c1"
    IssueInstant="2013-04-05T08:14:28.788Z" Version="2.0">
  <saml:Issuer>urn:de:berlin:hp:pap</saml:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
     <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#urn:uuid:7102AC72154DCFD1F51253534608780">
       <ds:Transforms>
        <ds:Transform
         Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform
         Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
         <ec:InclusiveNamespaces
          xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
          PrefixList="ds saml xs" />
        </ds:Transform>
       </ds:Transforms>
       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
       <ds:DigestValue>A1LyLvFHRrYaOJ28YVFd3MfKGSI=</ds:DigestValue>
      </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue>ggyn … LQ==</ds:SignatureValue>
     <ds:KeyInfo>
```

```
   <ds:X509Data>
    <ds:X509Certificate> … </ds:X509Certificate>
   </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <saml:Subject>
  <saml:NameID
   Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
   ...
  </saml:NameID>
  <saml:SubjectConfirmation
   Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
   <saml:SubjectConfirmationData>
     <ds:KeyInfo>
       <ds:X509Data>
         <ds:X509Certificate> … </ds:X509Certificate>
       </ds:X509Data>
     </ds:KeyInfo>
    </saml:SubjectConfirmationData/>
  </saml:SubjectConfirmation>
 </saml:Subject>
 <saml:Conditions
  NotBefore="2013-04-05T08:14:28.788Z"
  NotOnOrAfter="2013-04-05T12:14:28.788Z">
</saml:Conditions>
<xacml-saml:XACMLPolicyStatement>
  <xacml:PolicySet>
    <xacml:Target>
      <xacml:Subjects>
         <xacml:Subject>
           <xacml:SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:x500Name-equal">
             <xacml:AttributeValue
               DataType="http://www.w3.org/2001/XMLSchema#string">CN= ...</AttributeValue>
             <xacml:SubjectAttributeDesignator
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
               DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"/>
           </xacml:SubjectMatch>
         </xacml:Subject>
       </xacml:Subjects>
       <xacml:Resources>
```

```
            <xacml:Resource>
              <xacml:ResourceMatch MatchId="urn:oasis:names:tc:xacml:2.0:function:anyURI-regexp-match">
                <xacml:AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">...</AttributeValue>
                <xacml:ResourceAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                  DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
              </xacml:ResourceMatch>
            </xacml:Resource>
          </xacml:Resources>
        </xacml:Target>
        <xacml:PolicySetIdReference>urn:ecr:names:xacml:2.0:default:policyid:permit-all</xacml:PolicySetIdReference>
      </xacml:PolicySet>
    </xacml-saml:XACMLPolicyStatement>
 </saml:Assertion>
</wsse:Security>
</soap12:Header>
<soap12:Body/>
</soap12:Envelope>
```

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA RFC3881 Audit Trail Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht.

Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Audit Trail Binding for XDS-based Transactions

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EAiai.01}` For transactions implemented by the EFA Resource Manager, EFA Document Registry and EFA Document Repository an Audit Trail shall be written as defined for the underlying XDS transactions. Extensions and exceptions to this rule are defined in the following sections.

Event Identification

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EAiai.01.01}` Each audit trail entry written as an obligation to the processing of an EFA transaction shall contain an *eventID* element as specified for the underlying IHE XDS transaction. In addition each entry shall contain an *eventTypeCode* element for the logical EFA operation that is implemented through the XDS transaction. The following table lists the respective codes and display names.

EFA Service	eventTypeCode.codeSystemName	eventTypeCode.code	eventTypeCode.displayName
createECR	EFAv2 Transaction	EFA-01	createECR
createPartition	EFAv2 Transaction	EFA-02	createPartition
closeECR	EFAv2 Transaction	EFA-03	closeECR
listPartitions	EFAv2 Transaction	EFA-04	listPartitions
registerConsent	EFAv2 Transaction	EFA-05	registerConsent
issueAccessToken	EFAv2 Transaction	EFA-06	issueAccessToken
redeemAccessToken	EFAv2 Transaction	EFA-07	redeemAccessToken
registerData	EFAv2 Transaction	EFA-08	registerData
listPartitionContent	EFAv2 Transaction	EFA-09	listPartitionContent
ProvideData	EFAv2 Transaction	EFA-10	provideData

retrieveData	EFAv2 Transaction	EFA-11	retrieveData

Encoding of the User Identifier

The HP identifier entry MUST be taken from the subject field of the identity assertion that is transmitted together with a request. For conformance with IHE XUA++ the following encoding MUST be used:

```
SPProvidedID<saml:SubjectNameID@saml:Issuer>
```

The SPProvidedID is needed because there are situations where identity federation is in place. The SPProvidedID is a name identifier established by a service provider or affiliation of providers for the entity in the NameID different from the primary name identifier given in the content of the element. cdaefa:EFA Error Codes and Warning Codes

Implementable Perspective - Computational Dimension

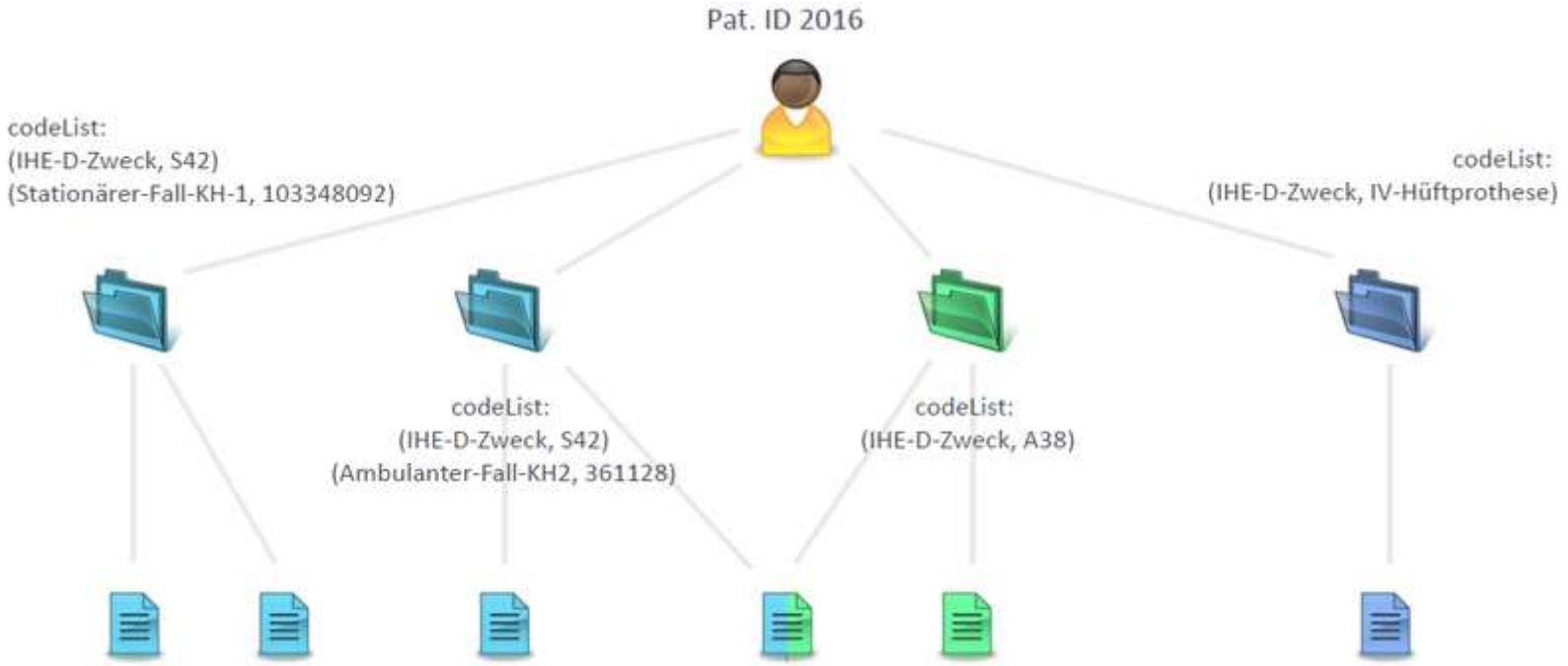
Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Setup

```
Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EHetw.01}
```

In IHE XDS wird eine Fallakte durch die Summe aller Ordner mit dem gleichen Zweck (im Sinne einer allgemeinen Zweckgebundenen Akte) abgebildet. Der Zweck wird in der XDSFolder.codeList gespeichert. Als code wird dabei ein 3-stelliger ICD-10 Wert verwendet, der Name oder die Nummer eines IV Vertrags oder ein beliebiges anderes Kennzeichen. Als codingScheme wird dabei ein fixer, zu standardisierender Wert angenommen, unabhängig davon ob der code aus dem ICD-10 Katalog stammt oder einen IV-Vertrag referenziert.

Um als Fallakte zu gelten, muss es für einen Patienten mindestens einen XDSFolder mit einem Zweck geben, d.h. mit einem Eintrag in der codeList dessen codingScheme dem festgelegten Wert entspricht. Zwei XDSFolder mit dem gleichen Zweck gelten als zwei „Ordner“ einer gemeinsamen Fallakte. Ein XDSFolder darf immer nur einen Zweck haben, da ansonsten der zweite Zweck code fälschlicherweise lesbar ist. XDSFolder mit Zweck können beliebige zusätzliche codes verwenden. Zum Beispiel kann durch Hinzufügen der administrativen Fall ID in die codeList ein XDSFolder mit Zweck auch als „Ordner“ genutzt werden.



Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS/XDR Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA XDR/XDS Binding

`Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDXDg.01}`

Within EFA the actors and transactions of the IHE XDS/XDR integration profiles are mapped onto EFA logical services and operations as follows:

Role	EFA Service Functional Model	IHE XDS/XDR	Binding
Actor	EFA Client	Document Source (for createECR, createPartition, closeECR, registerConsent, provideData) Document Consumer (for listPartitions, retrieveData)	-
Actor	EFA Resource Manager	Document Repository implementing Document Recipient (for createECR, createPartition, closeECR, registerConsent) Document Registry (for listPartitions)	-
Actor	EFA Document Registry	XDS Document Registry	-
Actor	EFA Document Repository	XDS Document Repository (implementing Document Recipient for provideData)	-

Transaction createECR	Provide and Register Document Set ITI-41	createECR
Transaction createPartition	Provide and Register Document Set ITI-41	createPartition
Transaction closeECR	Provide and Register Document Set ITI-41	closeECR
Transaction listPartitions	Registry Stored Query ITI-18	listPartitions
Transaction registerConsent	Provide and Register Document Set ITI-41	registerConsent
Transaction registerData	Register Document Set ITI-42	registerData
Transaction listData	Registry Stored Query ITI-18	listData
Transaction provideData	Provide and Register Document Set ITI-41	provideData
Transaction retrieveData	Retrieve Document Set ITI-43	retrieveData

Constraints and Triggers

The IHE ITI-41 and ITI-18 transactions are profiled by multiple EFA logical operations. The following table defines how an XDS/XDR document repository (document recipient) or document registry can decide by an incoming message which EFA operations binding is addressed.

Transaction	Flavour	Trigger	EFA behavior
ITI-41	-	provided documents are not associated with a folder	The EFA document repository/recipient SHALL respond with an error. This request is not defined for EFA as each provided document shall be associated with a folder (partition).
ITI-41	-	documents provided are associated with a folder. The folder codeList does not signal an EFA folder.	EFA document repository/recipient SHALL respond with an error. This request is not defined for EFA as non-EFA folders are not covered by the EFA access control model.
ITI-41	-	a consent (consentInfo) is included within the set of provided documents	depending on the type of consent the createECR, closeECR or registerConsent binding shall be enforced. closeECR and registerConsent require that the provided folder codeList signals an existing EFA instance.
ITI-41	-	The folder associated to the provided documents does not exist	The document repository/recipient shall enforce the createPartiton binding
ITI-41	-	any other condition	The document repository/recipient shall enforce the provideData binding

ITI-18	FindFolder	-	The document registry shall enforce the listPartitons binding
ITI-18	GetFolderAndContents	-	The document registry shall enforce the listData binding
ITI-18	any other flavor	-	the document registry shall respond with an error as other flavors than FindFolder and GetFolderAndContents shall not be implemented by an EFA compliant document registry.

Hybrid EFA/non-EFA systems should verify that a request is an EFA request prior to processing it with EFA semantics. Non-EFA requests MUST be rejected with an error message if processed with EFA semantics.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS/XDR Resource Manager Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Resource Manager XDR/XDS Binding

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.01}

Within EFA the actors and transactions of the IHE XDS integration profile are mapped onto EFA Resource Manager actors and operations as follows:

Role	EFA Resource Manager Service	IHE XDS	Binding
Actor	EFA Consumer	Document Source (for createECR, createPartition, closeECR, registerConsent) Document Consumer (for listPartitions)	-
Actor	EFA Resource Manager	Document Repository (for createECR, createPartition, closeECR, registerConsent) Document Registry (for listPartitions)	-
Transaction	createECR	Provide and Register Document Set ITI-41	createECR
Transaction	createPartition	Provide and Register Document Set ITI-41	createPartition
Transaction	closeECR	Provide and Register Document Set ITI-41	closeECR
Transaction	listPartitions	Registry Stored Query ITI-18	listPartitions
Transaction	registerConsent	Provide and Register Document Set ITI-41	registerConsent

EFA XDS/XDR Binding: createECR

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02}

The initialization of a new ECR is performed by creating a new XDS folder for the patient. The folder is classified by the ECR purpose codes and as such implicitly linked to all other folders (ECR: partitions) which are assigned to the same purpose.

This EFA binding introduces the following extensions and restrictions on the IHE XDR actor and transaction definitions in order to properly cover the EFA createECR operation and to align with the EFA security framework:

- A new folder shall be created and purpose codes shall be provided for the newly created folder as codeList.
- A consent information document containing the list of authorized subjects shall be provided through BPPC. A scanned consent document may be additionaly provided.
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements

- Documents cannot be copied by reference (Permissions are assigned to folders and therefore there is no easy way for an EFA Provider to verify the legitimacy for linking a document with another case record)
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.01}

The createECR request message implements the IHE Provide And Register DocumentSet transaction (ITI-41) request message as profiled in [IHE ITI TF-2b]

The following table shows how the createECR SFM is mapped onto the ITI-41 transaction:

createECR	ITI-41	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
patientID	XDS Folder Attribute: patientID XDS Document Attribute: patientID	The same patient identifier SHALL be used throughout all metadata
purpose	XDS Folder Attribute: codeList	see EFA XDS Folder Metadata Binding for details
ecrInfo	XDS Folder Attribute: title XDS Folder Attribute: uniqueID	Further elements of the ecrInfo structure MAY be set by the EFA provider.
consentInfo	XDS Document	
consentDoc (optional)	XDS Document	Scaned documents SHALL be provided acc. to the XDS SD Integration Profile.

Following this, implementations SHALL consider the following constraints:

- All provided documents SHALL be associated with a newly created XDS folder. Folder metadata SHALL be used as specified in the EFA XDS Folder Metadata Binding.
- The request carries one or more documents. One of these documents SHALL be a consent information document.
- All document metadata SHALL be provided as specified in the EFA XDS Document Metadata Binding.
- The requestor (EFA Client) SHOULD provide documents embraced by a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- The EFA Provider SHOULD ignore the submission set grouping and MUST ignore all associations between documents and submission sets.
- All metadata of the submission set MUST NOT have EFA semantics. The EFA Provider MUST solely rely on the document metadata and contents.
- The EFA Provider MUST NOT register documents that are provided by reference.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.02}

The XDS Document Repository SHALL respond to an ProvideAndRegisterDocument request message with the ProvideAndRegisterDocument response message containing a success indicator.

The XDS Document Repository MUST verify that the requesting service user has sufficient rights to setup a new ECR at this EFA Provider. This includes that the service user is registered with the provider and familiar with using ECRs. Additionaly the EFA Provider SHALL verify the completeness and consistency of the provided *consentInfo* document. It SHALL verify that all named ECR participants are either registered with the provider or identifiable through a shared healthcare provider directory.

The EFA Provider SHALL check if an ECR for the given patient and purpose already has been registered with this provider.

If no ECR with the given purpose exists for the given patient, the EFA Provider SHALL

- setup a folder as specified in the request message
- translate the provided *consentInfo* document into an access control policy which can be automatically enforced for each request to the newly setup ECR
- store the provided documents within the XDS Document Repository
- forward the metadata of the received documents to the XDS Document Registry for registration

If an ECR with the given purpose already exists for the given patient, the EFA Provider SHALL

- verify that EFA participant is allowed to modify the consent of the ECR. If this access is denied an error status SHALL be returned.
- setup a folder as specified in the request message
- extract the identified ECR participants from the provided *consentInfo* document and add them as authorized users to the existing access control policy.
- store the provided documents within the XDS Document Repository
- forward the metadata of the received documents to the XDS Document Registry for registration

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the EFA Resource Manager MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.03}

If the XDS Document Registry is able to decode the received message and to properly initialize the new ECR and its initial partition it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

If the XDS Document Registry wants to respond with further information on the processing of the transmitted data or with a non-critical warning it SHOULD include an additional <RegistryErrorList> element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”:

```
<rs:RegistryResponse
         status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
   <rs:RegistryErrorList>
     <rs:RegistryError
         severity=”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”
         errorCode=”....”
         codeContext=”Partition linked with existing ECR”
         location="" />
   </rs:RegistryErrorList>
 </rs:RegistryResponse>
```

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
Request was received but not processed; e.g. because a manual intervention by the EFA Provider is required to initalize a new ECR	Processing deferred	2201	None
An ECR with the given purpose already exists for the patient. Instead of initalizing a new ECR a partition has been added to the existing ECR.	Partition linked with existing ECR	2202	None

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.04}

If the XDS Document Repository is able to decode the received message but the processing of the request failed, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

The instantiation of an ECR is an All-or-Nothing operation. Therefore in any case of failure the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure".

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for EFA:

Condition and Severity	Location	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The EFA Provider only accepts *consentInfo* documents if they are digitally signed by an HP.	OID of the consentInfo	No Signature	4704	If possible, the EFA Client SHOULD re-issue the request with the data signed by an HP.

(ERROR)	document			
The requestor has not sufficient permission to perform the requested operation (ERROR)	-	No Consent	4701	The request MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.
An ECR of the given purpose already exists for the patient. The requestor does not have sufficient permissions to create a new partiton and to register new participants (ERROR)	-	No Consent	4701	The request MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent for the existing ECR.
The EFA Provider is unable to identify one or more of the participants that are listed in the consentInfo document (ERROR)	OID of the participant that cannot be identified	Unknown HP Identity	4111	The request MUST NOT be processed by the service provider. The requestor SHOULD first resolve the participants' identities into identifiers which are resolvable to the EFA Provider.

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.05}

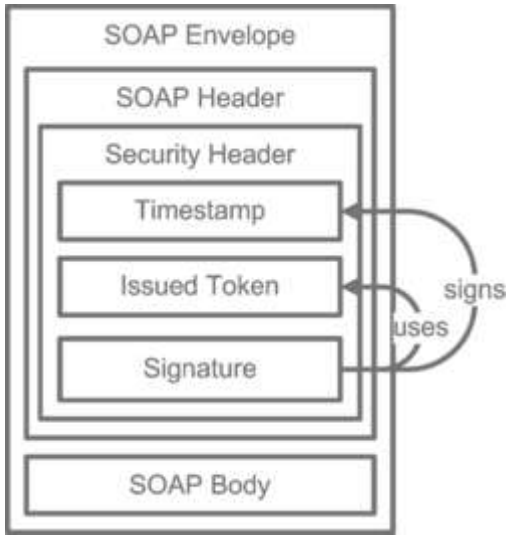
Message Protection

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.05.01}

The ECR requester MUST apply means to achieve message authenticity, message integrity and message confidentiality. The EFA Resource Manager MUST approve at least one of the following mechanisms.

Transport Layer Security with SAML Issued Endorsing Token

The request message and the response message are sent over an EFA Resource Manager authenticated TLS-channel. In the SOAP Security Header the EFA client provides an EFA Identity Assertion and a wsu:timestamp element. If the SAML subject confirmation method is set to holder-of-key the wsu:timestamp element MUST be signed with the Subject-Confirmation-Key. If the SAML subject confirmation method is set to bearer the TLS-channel MUST be mutually authenticated.



WS-Security-Policy Example

```
<wsp:Policy wsu:Id="ServicePortBindingPolicy">
    <sp:TransportBinding>
        <wsp:Policy>
            <sp:TransportToken>
                <wsp:Policy>
                    <sp:HttpsToken RequireClientCertificate="false" />
                </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
                <wsp:Policy>
                    <sp:Basic256Sha256 />
                </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:IncludeTimestamp />
            <sp:Layout>
                <wsp:Policy>
                    <sp:Strict />
                </wsp:Policy>
            </sp:Layout>
```

```
        </wsp:Policy>
    </sp:TransportBinding>
    <sp:Wss11>
        <wsp:Policy />
    </sp:Wss11>
    <wsam:Addressing />
</wsp:Policy>
<wsp:Policy wsu:Id="Input_Policy">
    <sp:EndorsingSupportingTokens>
        <wsp:Policy>
            <sp:IssuedToken
                sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeTokenAlwaysToRecipient">
                <sp:RequestSecurityTokenTemplate>
                    <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
                    <wst:KeySize>2048</wst:KeySize>
                </sp:RequestSecurityTokenTemplate>
                <wsp:Policy></wsp:Policy>
            </sp:IssuedToken>
        </wsp:Policy>
    </sp:EndorsingSupportingTokens>
</wsp:Policy>
```

Asymmetric Message Protection

The request message and the response message are signed and encrypted. The ECR requester uses the key material corresponding with the Subject-Confirmation-Key provided with the issued EFA Identity Assertion. The EFA Provider uses its service certificate and key. The wsu:timestamp element, all WS-Addressing elements and the SOAP-Body element MUST be signed. The SOAP-Body element MUST be encrypted.

WS-Security-Policy Example

```
<wsp:Policy wsu:Id="ServicePortBindingPolicy">
    <sp:AsymmetricBinding>
        <wsp:Policy>
            <sp:InitiatorToken>
                <wsp:Policy>
                    <sp:IssuedToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
```

```
                        <sp:RequestSecurityTokenTemplate>
                            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</wst:TokenType>
                            <wst:KeySize>2048</wst:KeySize>
                        </sp:RequestSecurityTokenTemplate>
                        <wsp:Policy></wsp:Policy>
                    </sp:IssuedToken>
                </wsp:Policy>
            </sp:InitiatorToken>
            <sp:RecipientToken>
                <wsp:Policy>
                    <sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToInitiator">
                        <wsp:Policy><sp:WssX509V3Token10 /></wsp:Policy>
                    </sp:X509Token>
                </wsp:Policy>
            </sp:RecipientToken>
            <sp:AlgorithmSuite><wsp:Policy><sp:Basic256 /></wsp:Policy></sp:AlgorithmSuite>
            <sp:Layout><wsp:Policy><sp:Strict /></wsp:Policy></sp:Layout>
            <sp:IncludeTimestamp />
            <sp:OnlySignEntireHeadersAndBody />
        </wsp:Policy>
    </sp:AsymmetricBinding>
    <sp:Wss11><wsp:Policy></wsp:Policy></sp:Wss11>
    <sp:Trust10>
        <wsp:Policy><sp:MustSupportIssuedTokens /></wsp:Policy>
    </sp:Trust10>
    <wsap10:UsingAddressing />
</wsp:Policy>
```

WS-SecureConversation bootstrapped with SAML Issued Token

The request message and the response message are signed and encrypted. Both the ECR requester and the EFA Provider use a symmetric Secure-Conversation-Token key. The Secure-Conversation-Token MUST reference the issued EFA Identity Assertion. The wsu:timestamp element, all WS-Addressing elements and the SOAP-Body element MUST be signed. The SOAP-Body element MUST be encrypted.

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.02.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS/XDR Binding: createPartition

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03}

The linkage of a new partition to an existing ECR is performed by creating a new XDS folder for the patient. The folder is classified by the ECR purpose codes of the existing ECR and as such implicitly linked to all other folders (ECR: partitions) which are already assigned to the same ECR.

This EFA binding introduces the following extensions and restrictions on the IHE XDR actor and transaction definitions in order to properly cover the EFA createPartition operation and to align with the EFA security framework:

- A new folder shall be created and purpose codes shall be provided for the newly created folder as codeList
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.01}

The createPartition request message implements the IHE Provide And Register DocumentSet transaction (ITI-41) request message as profiled in [IHE ITI TF-2b]

The following table shows how the createPartition SFM is mapped onto the ITI-41 transaction:

createECR	ITI-41		Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook	

ecrRef	XDS Folder Attribute: patientID XDS Folder Attribute: codeList	The codeList shall contain all purpose codes as assigned to the existing ECR the new partition is to be linked with
partitionInfo	XDS Folder Attribute: title XDS Folder Attribute: uniqueID	Further elements of the partitionInfo structure MAY be set by the ECR provider.
initialDoc	XDS Document	At least a single document shall be provided when a new partition is initialized.

Following this, implementations SHALL consider the following constraints:

- All provided documents SHALL be associated with a newly created XDS folder. Folder metadata SHALL be used as specified in the EFA XDS Folder Metadata Binding.
- The request shall provide one or more documents to the newly created folder.
- All document metadata SHALL be provided as specified in the EFA XDS Document Metadata Binding.
- The requestor (EFA Client) SHOULD embrace the provided documents as a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- The EFA provider SHOULD ignore the submission set grouping and MUST ignore all associations between documents and submission sets.
- The EFA provider MUST NOT process any metadata assigned to the submission set, it MUST solely rely on the document metadata and contents.
- The EFA provider MUST NOT register documents that are only provided through associations.

The Resource Manager SFM allows for initializing empty partitions while XDS requires at least a single document to be provided whenever a new folder is created.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.02}

The XDS Document Repository provider SHALL respond to an ProvideAndRegisterDocument request message with the ProvideAndRegisterDocument response message containing a success indicator.

The provider of the XDS Document Repository provider MUST verify that the requesting service user has sufficient rights to setup a new partition at this ECR Provider ant to link this partiton with an existing ECR.

In processing of this request the ECR Provider SHALL

- assess the access control policy of the ECR with the "create partition" operation
- setup a folder as specified in the request message
- store the provided documents within the XDR Document Repository
- forward the metadata of the received documents to the XDS Document Registry for registration

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the XDS Document Repository MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.03}

If the EFA Document Registry Service provider is able to decode the received message and to properly initialize the new partition it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.04}

If the XDS Document Repository is able to decode the received message but the processing of the request failed, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

If the partiton could not be created or if none of the provided documents was processed succesfully, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If the partition was successfully initialized and at least one document was processed successfully, the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”. A failure location MUST be provided if the error does not apply to all provided documents. It MUST NOT be given if the error applies to all provided documents.

The severity of each registry error message MUST be set to ”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for EFA:

Condition and Severity	Location	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
An ECR of the given purpose does not exist for the patient (ERROR)	-	Policy Violation	4109	The request MUST NOT be processed by the service provider.
The ECR provider only accepts medical documents if they are digitally signed by an HP. (ERROR)	OID of the consentInfo document	No Signature	4704	If possible, the EFA Client SHOULD re-issue the request with the data signed by an HP.
The requestor has not sufficient permission to perform the requested operation (ERROR)	-	No Consent	4701	The request MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.
For data of the given kind the EFA provider only accepts PDF coded documents (ERROR)	OID of the document	PDF required	4107	The provided document MUST NOT be processed by the EFA provider. The EFA Client MUST re-transmit the document in PDF format.
A document of the provided kind does not comply with the EFA policy or the patient consent (ERROR)	OID of the document	No Consent	4701	The provided document MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.05}

Message Protection

See Message Protection topic in createECR section.

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.03.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS/XDR Binding: closeECR

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04}

The explicit shutdown of an ECR is performed by placing a consentInfo document that invalidates all previously given permissions into one of the ECR's partitions (folders). This may either be a newly created folder of an existing folder that is classified by the ECR purpose codes and as such implicitly represents the ECR that is to be closed.

This EFA binding introduces the following extensions and restrictions on the IHE XDR actor and transaction definitions in order to properly cover the EFA closeECR operation and to align with the EFA security framework:

- A new folder may be created. Purpose codes shall be provided for the newly created folder as codeList
- A consent information document that invalidates all previously given permissions shall be provided through BPPC. A scanned consent revocation document may be additionaly provided.
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.01}

The closeECR request message implements the IHE Provide And Register DocumentSet transaction (ITI-41) request message as profiled in [IHE ITI TF-2b]

The following table shows how the closeECR SFM is mapped onto the ITI-41 transaction:

closeECR	ITI-41	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
ecrRef	XDS Folder Attribute: patientID XDS Folder Attribute: codeList	The codeList shall contain all purpose codes as assigned to the ECR that is to be closed
consentInfo	XDS Document	
consentDoc (optional)	XDS Document	Scaned documents SHALL be provided acc. to the XDS SD Integration Profile.

Following this, implementations SHALL consider the following constraints:

- All provided documents SHALL be associated with a newly created XDS folder or with a folder that is already part of the ECR. Folder metadata SHALL be used as specified in the EFA XDS Folder Metadata Binding.
- The request carries one or more documents. One of these documents SHALL be a consent information document.
- All document metadata SHALL be provided as specified in the EFA XDS Document Metadata Binding.
- The requestor (EFA Client) SHOULD embrace the provided documents as a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- The EFA provider SHOULD ignore the submission set grouping and MUST ignore all associations between documents and submission sets.
- The EFA provider MUST NOT process any metadata assigned to the submission set, it MUST solely rely on the document metadata and contents.
- The EFA provider MUST NOT register documents that are only provided through associations.

The Resource Manager SFM allows for closing partitions without providing any arguments but the ECR identifer. This binding makes the consentInfo document mandatory because ITI-41 provides more comfortable means for closing an ECR as other transactions that may be considered instead.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.02}

The XDS Document Repository provider SHALL respond to an ProvideAndRegisterDocument request message with the ProvideAndRegisterDocument response message containing a success indicator.

The provider of the XDS Document Repository MUST verify that the requesting service user has sufficient rights to close an ECR at this ECR Provider. This includes that the service user is registered with the provider and familiar with using ECRs. Additionaly the ECR provider SHALL verify the completeness and consistency of the provided *consentInfo* document.

In processing this request the ECR Provider SHALL

- assess the access control policy of that ECR with the "modify consent" operation. If this access is denied an error status SHALL be returned.
- setup a folder as specified in the request message
- store the provided documents within the XDR Document Repository
- forward the metadata of the received documents to the XDS Document Registry for registration
- change the status of the ECR and all its partitions (folders) to "grace"
- Adapt all permissions to the new status of the ECR

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the EFA Resource Manager Service provider MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.03}

If the EFA Document Registry Service provider is able to decode the received message and to properly change the status of the ECR and its partitions it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

If the service provider wants to respond with further information on the processing of the transmitted data or with a non-critical warning it SHOULD include an additional <RegistryErrorList> element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”.

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
Request was received but not processed; e.g. because a manual intervention by the ECR provider is required to close an ECR	Processing deferred	2201	None

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.04}

If the XDS Document Repository is able to decode the received message but the processing of the request failed, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

The shutdown of an ECR is an All-or-Nothing operation. Therefore in any case of failure the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure".

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for EFA:

Condition and Severity	Location	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The ECR provider only accepts *consentInfo* documents if they are digitally signed by an HP. (ERROR)	OID of the consentInfo document	No Signature	4704	If possible, the EFA Client SHOULD re-issue the request with the data signed by an HP.
The requestor has not sufficient permission to perform the requested operation (ERROR)	-	No Consent	4701	The request MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.

An ECR of the given purpose does not exist for the patient (ERROR)	-	Policy Violation	4109	The request MUST NOT be processed by the service provider.

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.05}

Message Protection

See Message Protection topic in createECR section.

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.04.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS Binding: listPartitions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05}

ECR partitions are bound as XDS folders. Therefore listing partitions corresponds to listing accessible folders which

- are assigned to a given patient, and
- are ECR-classified, and
- are classified with the given purpose.

This EFA binding introduces the following extensions and restrictions on the IHE XDS actor and transaction definitions in order to properly cover the EFA listPartitions operation and to align with the EFA security framework:

- The query is restricted to folder metadata and does not return any data contained within that folders.
- Additional error messages are defined that cover specific failure conditions of the EFA use cases

- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.01}

The listPartitions request message implements the FindFolder flavor of the IHE Registry Stored Query transaction (ITI-18) request message as defined in [IHE ITI TF-2b#3.18.4.1.2.3.7.3].

The following table shows how the listPartitions SFM is mapped onto the ITI-18 transaction's query arguments:

listPartitions	ITI-18	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
patientID	$XDSFolderPatientId	The patient ID used must be resolvable by the ECR Provider.
purpose	$XDSFolderCodeList	The codeList MUST contain the ECR-Folder classification code (see EFA XDS Folder Metadata Binding for the respective code). The codeList MUST contain a purpose code, which restricts the query to the partitons of a specific ECR.

In addition the following constrains must be considered:

- The $XDSFolderLastUpdateTimeFrom and/or $XDSFolderLastUpdateTimeTo query arguments MAY be used. If given, they MUST be considered by the Document Registry.
- The $XDSFolderStatus query arguent SHALL be set to "Approved".

Example

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.01.01}

```
<query:AdhocQueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
   xsi:schemaLocation="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0 ../schemas/query.xsd"
   xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
   xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
   <query:ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
   <rim:AdhocQuery id="urn:uuid:958f3006-baad-4929-a4de-ff1114824431">
      <rim:Slot name="$XDSFolderPatientId">
         <rim:ValueList>
            <rim:Value>'90378912821^^^&amp;amp1.3.6.1.4.1.21367.2005.3.7&amp;ampISO'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSFolderStatus">
         <rim:ValueList>
            <rim:Value>'urn:oasis:names:tc:ebxml-regrep:StatusType:Approved'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
      <rim:Slot name="$XDSFolderCodeList">
         <rim:ValueList>
            <rim:Value>'ECR^^^IHE-D-Cookbook-FolderClassCode'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
   </rim:AdhocQuery>
</query:AdhocQueryRequest>
```

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.02}

The XDS Document Registry provider SHALL respond to a Registry Stored Query request message with the Registry Stored Query response message containing a success indicator and listing XDS metadata of all folders that match the given query. The provider of the XDS Document Registry provider MUST verify that the requesting service user has sufficient rights to access the discovered XDS folders.

In processing of this request the ECR Provider SHALL

- assess the access control policy of all folders assigned to the given patient
- discover all folders that match the query and the policy

- respond to the requestor with the metadata of the discovered folders. Metadata provided SHALL comply to the EFA XDS Folder Metadata Binding.

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the XDS Document Registry MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.03}

If the EFA Document Registry Service provider

- is able to decode and process the received message and
- at least one partition exists for the given patient that is accessible to the requestor

it responds with the registry metadata of the discovered partitions.

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.04}

If the XDS Document Registry is unable to successfuly process the query request it MUST respond with a ListResponse message that only contains a <AdhocQueryResponse/RegistryResponse> element.

If no matching folder is discovered or an error occured during the processing of the request, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If partitons of the patient are discovered but may be incomplete (e.g. due to a not-responding peer in an ECR P2P network), the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”.

The severity of each registry error message MUST be set to ”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for ECR:

Condition and Severity	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The ECR provider is unable to verify the identity and/or the authenticity of the requestor (ERROR)	Invalid Subject	4703	The request MUST NOT be processed by the service provider.
The patient is unknown to the ECR provider.	No Data	1102	-
No partitions are registered for the given patient.	No Data	1102	-
None of the patient's partitions is accessible to the requestor.	No Data	1102	-

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.05}

Message Protection

See Message Protection topic in createECR section.

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.05.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS/XDR Binding: registerConsent

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06}

The registration and enforcement of a new patient consent to an existing ECR is performed by placing a consentInfo document that expresses the new consent into one of the ECR's partitions (folders). This may either be a newly created folder of an existing folder that is classified by the ECR purpose codes and as such implicitly represents the ECR that is to be aligned to a new treatment setup.

This EFA binding introduces the following extensions and restrictions on the IHE XDR actor and transaction definitions in order to properly cover the EFA registerConsent operation and to align with the EFA security framework:

- A new folder may be created. Purpose codes shall be provided for the newly created folder as codeList
- A consent information document that expresses the new permissions shall be provided through BPPC. A scanned consent revocation document may be additionaly provided.
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.01}

The registerConsent request message implements the IHE Provide And Register DocumentSet transaction (ITI-41) request message as profiled in [IHE ITI TF-2b]

The following table shows how the registerConsent SFM is mapped onto the ITI-41 transaction:

registerConsent	ITI-41	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
ecrRef	XDS Folder Attribute: patientID XDS Folder Attribute: codeList	The codeList shall contain all purpose codes as assigned to the ECR that is to be aligned
consentInfo	XDS Document	
consentDoc	XDS Document	Scaned documents SHALL be provided acc. to the XDS SD Integration

(optional) Profile.

Following this, implementations SHALL consider the following constraints:

- All provided documents SHALL be associated with a newly created XDS folder or with a folder that is already part of the ECR. Folder metadata SHALL be used as specified in the EFA XDS Folder Metadata Binding.
- The request carries one or more documents. One of these documents SHALL be a consent information document.
- All document metadata SHALL be provided as specified in the EFA XDS Document Metadata Binding.
- The requestor (EFA Client) SHOULD embrace the provided documents as a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- The EFA provider SHOULD ignore the submission set grouping and MUST ignore all associations between documents and submission sets.
- The EFA provider MUST NOT process any metadata assigned to the submission set, it MUST solely rely on the document metadata and contents.
- The EFA provider MUST NOT register documents that are only provided through associations.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.02}

The XDS Document Repository provider SHALL respond to an ProvideAndRegisterDocument request message with the ProvideAndRegisterDocument response message containing a success indicator.

The provider of the XDS Document Repository MUST verify that the requesting service user has sufficient rights to register a consent document at this ECR Provider. This includes that the service user is registered with the provider and familiar with using ECRs. Additionaly the ECR provider SHALL verify the completeness and consistency of the provided *consentInfo* document.

In processing this request the ECR Provider SHALL

- assess the access control policy of that ECR with the "modify consent" operation. If this access is denied an error status SHALL be returned.
- setup a folder as specified in the request message
- store the provided documents within the XDR Document Repository
- forward the metadata of the received documents to the XDS Document Registry for registration

- adapt all permissions that are assigned to the ecrRef to the care team setting as described in the newly provided consent. All previously set permissions must be invalidated.
- if the validity date is changed by the consent: register the new validity with the access control system
- if the purpose is aligned by the new consent: change the eventList codes of all containers that are assigned to the eCR to the new purpose

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the EFA Resource Manager Service provider MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.03}

If the EFA Document Registry Service provider is able to decode the received message and to properly change the settings of the ECR and its partitions it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

If the service provider wants to respond with further information on the processing of the transmitted data or with a non-critical warning it SHOULD include an additional <RegistryErrorList> element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”.

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
Request was received but not processed; e.g. because a manual intervention by the ECR provider is required to change the security settings of an ECR	Processing deferred	2201	None

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.04}

If the XDS Document Repository is able to decode the received message but the processing of the request failed, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

The modification of an ECR's security settings is an All-or-Nothing operation. Therefore in any case of failure the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”.

The severity of each registry error message MUST be set to ”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for EFA:

Condition and Severity	Location	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The ECR provider only accepts *consentInfo* documents if they are digitally signed by an HP. (ERROR)	OID of the consentInfo document	No Signature	4704	If possible, the EFA Client SHOULD re-issue the request with the data signed by an HP.
The requestor has not sufficient permission to perform the requested operation (ERROR)	-	No Consent	4701	The request MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.
An ECR of the given purpose does not exist for the patient (ERROR)	-	Policy Violation	4109	The request MUST NOT be processed by the service provider.

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.05}

Message Protection

See Message Protection topic in createECR section.

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDesa.06.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

Referenzen und Querverweise

- EFA-2.0-Spezifikation
- Implementation Guide for CDA®, Release 2: Consent Directives, Release 1

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS Document Registry Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Document Registry XDS Binding

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.01}

Within EFA the actors and transactions of the IHE XDS integration profile are mapped onto EFA Document Registry actors and operations as follows:

Role	EFA Document Registry Service	IHE XDS
Actor	EFA Client	Document Consumer
Actor	EFA Document Registry	XDS Document Registry
Actor	EFA Document Repository	XDS Document Repository
Transaction	registerData	Register Document Set ITI-42
Transaction	listPartitionContent	Registry Stored Query ITI-18

EFA XDS Binding: registerData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02}

While medical data is received and stored by the XDS Document Repository it is the responsibility of the Document Registry to register that data in a way that it can be queried through search and browse operations.

Such registration of a document to an ECR provider's registry service is bound to the IHE *Register Document Set* transaction (ITI-42). This EFA binding introduces minor extensions and restrictions on the respective XDS actor and transaction definitions in order to properly cover the EFA use cases and to align with the EFA security framework:

- Documents must be associated with folders in order to reflect that each ECR data element must be placed within a partition which in turn is part of a case record that carries the permissions for accessing data
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02.01}

The RegisterDocument request message is issued by an ECR Document Repository actor for registering a medical document to an existing folder which is bound to an EFA instance. Each transmission carries metadata and associations for one or more documents. All referenced documents will be registered with the same folder within the same logical EFA.

The request message implements the IHE Register DocumentSet transaction (ITI-42) request message as profiled in [IHE ITI TF-2b] considering the following constraints:

- Each registered document SHALL be associated with a folder.
- The target folder SHALL be available in advance to this transaction. All documents SHALL be associated with the same folder (these restrictions ensure the proper implementation of the EFA Document Repository SFM which implies the existence of a partition and only allows for a single partitionID to be included with the request).
- The requestor (ECR Document Repository) SHOULD embrace the provided documents as a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- The EFA provider SHOULD ignore this grouping and MUST ignore all associations between documents and submission sets.
- The XDS Document Registy MUST NOT process any metadata assigned to the submission set, it MUST solely rely on the document metadata.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02.02}

The EFA Document Registry Service provider MUST verify that the requesting service is trustworthy in a way that the registry service can rely on the access control decision that has already been performed by the document repository in advance to this request. The EFA Document Registry Service SHALL respond to an RegisterDocumentSet request message with the RegisterDocumentSet response message containing a success indicator.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02.03}

If the EFA Document Registry Service provider is able to decode the received message and to properly register all documents it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02.04}

If the EFA Document Registry Service provider is able to decode the received message but the registration of one or more documents failed, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

If none of the documents was processed succesfully, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If at least one document was processed successfully, the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”. A failure location MUST be provided if the error does not apply to all documents. It MUST NOT be given if the error applies to all documents.

The severity of each registry error message MUST be set to ”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. For a list of valid error codes and message see Table 4.1-11 of [IHE ITI TF-3].

Security Audit Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.02.05}

The document registry actor SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS Binding: listPartitionContent

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03}

ECR partitions are implemented as XDS folders. Therefore listing the content of a partition corresponds to listing all document metadata objects that are associated to a given XDS folder.

This EFA binding introduces the following extensions and restrictions on the IHE XDS actor and transaction definitions in order to properly cover the EFA listPartitionContent operation and to align with the EFA security framework:

- The query is restricted to listing the content of a single folder
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.01}

The listData request message implements the GetFolderAndContents flavor of the IHE Registry Stored Query transaction (ITI-18) request message as defined in [IHE ITI TF-2b#3.18.4.1.2.3.7.3].

The following table shows how the listData SFM is mapped onto the ITI-18 transaction's query arguments:

listData	ITI-18	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
partitionID	$XDSFolderUniqueId	The requestor SHALL provide the unique folder ID as obtained when the partitions of an ECR were intially listed.
docMetadata	registryObjectList	document metadata SHALL comply to the ECR Document Metadata Binding. If returnType=ObjectRef is defined for the query then only the partition identifiers will be provided.

In addition the following constrains must be considered:

- Other query arguments than the $XDSFolderUniqueID SHALL NOT be used.

Example

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.01.01}

```
<query:AdhocQueryRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0 ../schemas/query.xsd"
   xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
   xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
   xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
   <query:ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
   <rim:AdhocQuery id="urn:uuid:b909a503-523d-4517-8acf-8e5834dfc4c7">
      <rim:Slot name="$XDSFolderUniqueId">
         <rim:ValueList>
            <rim:Value>'2871627126387^^^&amp;1.2.3.4.213.234.3.7&amp;ISO'</rim:Value>
         </rim:ValueList>
      </rim:Slot>
   </rim:AdhocQuery>
</query:AdhocQueryRequest>
```

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.02}

The XDS Document Registry provider SHALL respond to a Registry Stored Query request message with the Registry Stored Query response message containing a success indicator and listing XDS metadata of all documents that match the given query. The provider of the XDS Document Registry provider MUST verify that the requesting service user has sufficient rights to access the given XDS folders.

In processing of this request the ECR Provider SHALL

- assess the access control policy of the ecrRef object that is assigned with the given folder. If no such object is assigned to the folder, the XDS Document Registry MUST respond with a "policy violation" error.
- respond to the requestor with the metadata of the discovered documents. Metadata provided SHALL comply to the EFA XDS Document Metadata Binding.

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the XDS Document Registry MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.03}

If the EFA Document Registry Service provider is able to decode and process the received message it responds with the registry metadata of the discovered documents.

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.04}

If the XDS Document Registry is unable to successfuly process the query request it MUST respond with a ListResponse message that only contains a <AdhocQueryResponse/RegistryResponse> element.

If no matching document is discovered or an error occured during the processing of the request, the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure".

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for ECR:

Condition and Severity	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The ECR provider is unable to verify the identity and/or the authenticity of the requestor (ERROR)	Invalid Subject	4703	The request MUST NOT be processed by the service provider.
The partition is unknown to the ECR provider.	No Data	1102	The requestor should use a MPI service to discovery an identifier for the patient that is known to the ECR provider.
The requestor has insufficient permissions to access the given	No Consent	4701	-

partition.
The given partition is not classified as an ECR folder. Policy Violation 4109 -

Security Considerations

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.05}

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EDcui.03.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

Dieses Dokument gibt wieder:

*Implementierungsleitfaden **EFA XDS Document Repository Binding**.*

Die Teilmaterialien gehören der Kategorie cdaefa an.

Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

EFA Document Repository XDS Binding

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.01}

Within EFA the actors and transactions of the IHE XDS integration profile are mapped onto EFA Document Repository actors and operations as follows:

Role	EFA Document Repository Service	IHE XDS
Actor	EFA Client	Document Source (for provideData) Document Consumer (for retrieveData)
Actor	EFA Document Repository	XDS Document Repository
Transaction	provideData	Provide and Register Document Set ITI-41
Transaction	retrieveData	Retrieve Document Set ITI-43

EFA XDS Binding: provideData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02}

Providing a document to an ECR provider's repository service is bound to the IHE *Provide and Register Document Set* transaction (ITI-41). This EFA binding introduces minor extensions and restrictions on the respective XDS actor and transaction definitions in order to properly cover the EFA use cases and to align with the EFA security framework:

- Documents must be associated with an XDS Folders, i.e an ECR partition, which in turn is part of an ECR that carries the permissions for accessing data.
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02.01}

The ProvideAndRegisterDocument request message is issued by an EFA client at the point of care for providing and registering a medical document to an existing ECR partition. Each transmission carries one or more documents. All provided documents will be registered with the same XDS Folder within the same logical EFA. The request message implements the IHE Provide And Register DocumentSet transaction (ITI-41) request message as profiled in [IHE ITI TF-2b] considering the following constraints:

- Each provided document SHALL be associated with an XDS Folder.
- The target XDS Folder SHALL be available in advance to this transaction. All provided documents SHALL be associated with the same XDS Folder (these restrictions ensure the proper implementation of the EFA Document Repository SFM which implies the existence of a ECR partition and only allows for a single partitionID to be included with the request).
- The requestor (EFA Client) SHOULD provide documents embraced by a single IHE XDS submission set acc. to [IHE ITI TF-2a].
- All metadata of the submission set and all associations between documents and submission sets MUST NOT have EFA semantics. The EFA Provider MUST solely rely on the document metadata and contents.
- The EFA provider MUST NOT register documents that are only provided through metadata and/or associations.

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02.02}

The XDS Document Repository SHALL forward the received documents to the EFA Document Registry using the ECR profiled Register Documents transaction.

The EFA Document Registry MUST verify that the requesting service user has sufficient rights to submit the given kind of documents for the identified patient and into the identified XDS Folder.

After processing the request the XDS Document Repository actor SHALL respond to an ProvideAndRegisterDocument request message with the ProvideAndRegisterDocument response message containing a success indicator.

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the EFA Document Registry Service provider MUST respond with a fault message according to section xx.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02.03}

If the EFA Document Repository Service provider is able to decode the received message and to properly process/forward all transmitted documents it responds with an ebXML Registry Response with its status set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"

If the service provider wants to respond with further information on the processing of the transmitted data or with a non-critical warning it SHOULD include an additional <RegistryErrorList> element. The severity MUST be set to “urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”:

```
<rs:RegistryResponse
         status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
   <rs:RegistryErrorList>
     <rs:RegistryError
         severity=”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning”
         errorCode=”2201”
         codeContext=”Processing deferred”
         location="" />
   </rs:RegistryErrorList>
 </rs:RegistryResponse>
```

The following warning messages and codes are defined:

Condition and Severity	Message	Code	Action to be taken
Documents were received but not processed	Processing deferred	2201	None

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02.04}

If the EFA Document Repository failed with processing all of the documents or failed with forwarding all documents to the EFA Document Registry, it responds with an ebXML Registry Response that contains a respective status indicator (see below).The response MUST contain a RegistryErrorList element that indicates the failure condition.

If none of the documents was processed succesfully, the response status MUST be set to “urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure”. If at least one document was processed successfully, the response status MUST be set to “urn:ihe:iti:2007:ResponseStatusType:PartialSuccess”. A failure location MUST be provided if the error does not apply to all provided documents. It MUST NOT be given if the error applies to all provided documents.

The severity of each registry error message MUST be set to ”urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error”. Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for EFA:

Condition and Severity	Location	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	-	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The EFA Document Registry service provider only accepts data of the given kind if it is digitally signed by an HCP. (ERROR)	OID of the document that caused the error.	No Signature	4704	If possible, the EFA Client SHOULD re-issue the request with the data signed by an HP.
For data of the given kind the EFA provider only accepts PDF coded documents (ERROR)	OID of the document	PDF required	4107	The provided document MUST NOT be processed by the EFA provider. The EFA Client MUST re-transmit the document in PDF format.
A document of the provided kind does not comply with the EFA policy or the patient consent (ERROR)	OID of the document	Policy Violation	4109	The provided document MUST NOT be processed by the service provider. The HP MAY request the patient to extend the consent.

Security Considerations

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.02.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

EFA XDS Binding: retrieveData

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03}

This EFA binding introduces the following extensions and restrictions on the IHE XDS actor and transaction definitions in order to properly cover the EFA retrieveData operation and to align with the EFA security framework:

- Constraints on the retrieved documents due to the ECR usage conventions for XDS folders
- Additional error messages are defined that cover specific failure conditions of the EFA use cases
- The availability of data fields is aligned to EFA privacy requirements
- The application of security measures and the contents of the SOAP security header are specified normatively

Constraints on the Request Message

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03.01}

The retrieveData request message implements the IHE Retrieve Document Set transaction (ITI-43) request message.

The following table shows how the retrieveData SFM is mapped onto the ITI-43 transaction's query arguments:

retrieveData	ITI-43	Constraints
context	SAML Identity Assertion within the SOAP Security Header	see IHE Cookbook
documentID	DocumentResponse/repositoryUniqueId DocumentResponse/documentUniqueId	The requestor SHALL provide these unique IDs as obtained when the contents of an ECR partition were intially listed.
docData	DocumentResponse/document	-

In addition the following constrains must be considered:

- The data to be retrieved SHALL all be associated with the same XDS Folder. It SHALL be classified as an ECR partition.

Example

```
<RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
   <DocumentRequest>
      <RepositoryUniqueId>1.19.6.24.109.42.1.5</RepositoryUniqueId>
      <DocumentUniqueId>1.42.20101110141555.15</DocumentUniqueId>
   </DocumentRequest>
</RetrieveDocumentSetRequest>
```

Expected Actions

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03.02}

The XDS Document Repository SHALL respond to a Retrieve Document Set request message with the Retrieve Document Set response message containing a success indicator and listing all requested documents. The provider of the XDS Document Repository MUST verify that the requestor has sufficient rights to access the requested documents.

In processing of this request the ECR Provider SHALL

- assess the access control policy of the ecrRef object that is assigned with the XDS Folder that is associated to the requested documents. If a document is not associated with an XDS Folder or if no ecrRef object is assigned to the XDS Folder, the XDS Document Repository MUST respond with a "policy violation" error.
- respond to the requestor with the requested documents.

In case of an error that relates to the transmission of the request or the processing of the EFA security token, the XDS Document Registry MUST respond with the respective error status.

Response Message (Full Success Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03.03}

If the EFA Document Repository Service provider is able to decode and process the received message it responds with the discovered documents acc. to the specification of the ITI-43 response message.

Response Message (Failure or Partial Failure Scenario)

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03.04}

If the XDS Document Repository is unable to successfuly process the query request it MUST respond with a *RetrieveDocumentSetResponse* message that only contains a *RegistryResponse* element.

If no matching document is discovered or an error occured during the processing of the request, the response status MUST be set to "urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure". The failure semantics is all-or-nothing; as soon as one of the requested documents cannot be provided the XDS Document Repository responds with a full failure by providing none of the requested documents.

The severity of each registry error message MUST be set to "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error". Multiple registry error messages MAY be included within a single <rs:RegistryErrorList> element. Apart from the XDS-b error messages defined in Table 4.1-11 of [IHE ITI TF-3] the following error codes are defined for ECR:

Condition and Severity	Message	Code	Action to be taken
The EFA provider requests a higher authentication trust level than assigned to the HP (e.g. password-based login is not accepted for the requested operation). (ERROR)	Weak Authentication	4702	If possible, the HP SHOULD log in again with a stronger mechansims (e.g. smartcard) and re-issue the request with the respective identity assertion.
The ECR provider is unable to verify the identity and/or the authenticity of the requestor (ERROR)	Invalid Subject	4703	The request MUST NOT be processed by the service provider.
One or more document identifiers are unknown to the ECR provider.	No Data	1102	-
The requestor has insufficient permissions to access one or more of the requested documents.	No Consent	4701	-
Multiple XDS Folders are associated with the requested documents or at least one of the associated XDS Folders is not classified as an ECR partition.	Policy Violation	4109	-

Security Considerations

Audit Trail

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EXoce.03.05.02}

Service consumer and service provider actors SHALL write an audit trail according to the EFAv2 Audit Trail Binding.

Querverweise und Referenzen

- EFA-2.0-Spezifikation

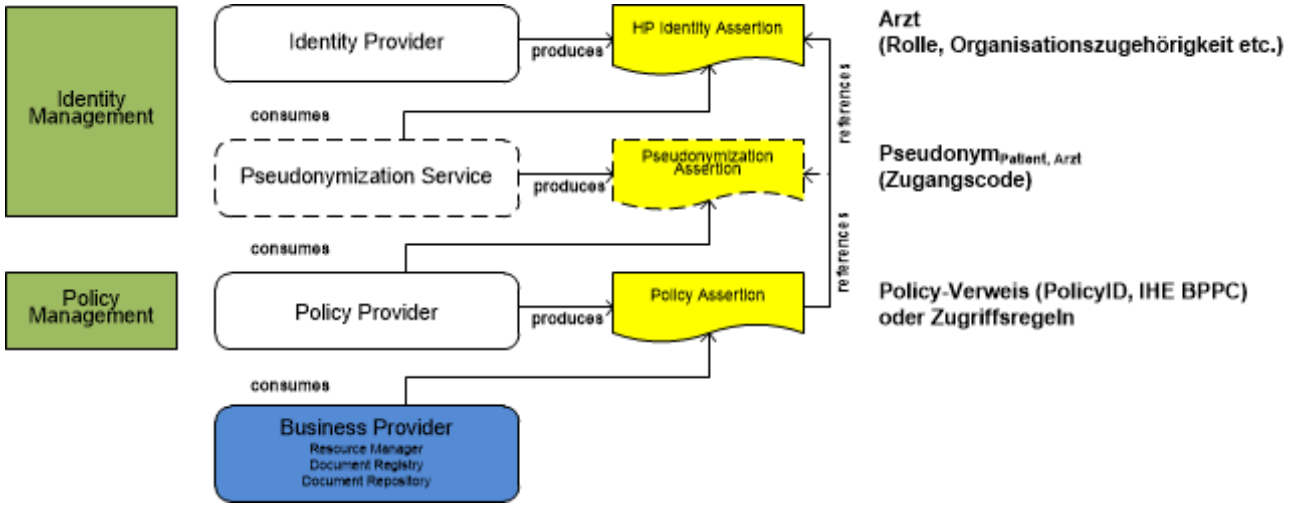
Anmerkung: Die Kürzel unter den einzelnen Überschriften dienen der Unterstützung des Kommentierungsverfahrens. Bitte geben Sie bei einem Kommentar oder einem Verbesserungsvorschlag zu dieser Spezifikation immer das Kürzel des Abschnitts an, auf den sich Ihr Kommentar bezieht. Alle Kommentare werden in der Lasche "Diskussion" zu der kommentierten Seite gesammelt und gegenkommentiert.
Hinweise zum Kommentierungsverfahren einschließlich aller Formulare und Kontaktadressen finden Sie auf der Seite "Kommentierung EFAv2.0".

Bindung von Policies an Schnittstellen

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EcssS.01}

Die Sicherheitsarchitektur der elektronischen Fallakte definiert für jeden Anwendungsdienst mittels WS-Policy und WS-SecurityPolicy welche Sicherheitsnachweise (Security Assertions, z. B. kodiert als Security Token) notwendig sind, um die Operationen aufrufen zu können. SAML Assertions [SAML2.0] kodieren die notwendigen Authentisierungs- und Autorisierungsinformationen, welche von speziellen Security Token Services ausgestellt werden. Hierbei kann ein Security Token Service zur Ausstellung eines geforderten Sicherheitsnachweises (Security Assertion) die Vorlage eines Security Token verlangen, dass in die Zuständigkeit eines anderen Security Token Service fällt. Auf diese Weise können Abhängigkeiten in Sicherheitsdiensten (z. B. Autorisierung erfordert Authentifizierung) auf sequentielle Ketten von Sicherheitsnachweisen

abgebildet werden. Die nachfolgende Abbildung stellt dies in der maximalen Komplexitätsstufe dar, in der neben dem Authentisierungsnachweis auch ein Admission Code und ein Autorisierungsnachweis Bestandteil der Nachweis-Kette sind.



In der Deklaration der zur Umsetzung der Schutzziele beizubringenden Sicherheitsobjekte können „klassische“ X.509 Token und Security Context Token mit SAML Token kombiniert werden. Die eFA-Sicherheitsarchitektur erlaubt es auch, mehrere SAML Token an einen Web Service zu versenden, d. h. iterativ ganze Ketten von aufeinander verweisenden Sicherheitsnachweisen aufzubauen. Hiermit können die Nachweise der Nutzung einzelner Sicherheitsdienste (Authentisierung, Pseudonymisierung, Autorisierung, etc.) als vom unterliegenden Security Framework zu bearbeitende Bestandteile des Aufrufs eines Anwendungsdienstes kodiert werden.

Durch diese Flexibilität kann eine EFA-Implementierung alle im IHE White Paper "Access Control" benannten Verfahren zum Austausch von Autorisierungsnachweisen (policy push, policy pull, policy cache) nutzen. Grundsätzlich gelten hierbei jedoch die folgenden Vorgaben:

- jeder providerseitige EFA-Dienst muss die Verfahren "policy pull" und "policy push" unterstützen.
- ein providerseitiger Dienst kann zusätzlich ein policy Cache Verfahren umsetzen.
- ein EFA-Client kann ein "policy push" unterstützen.

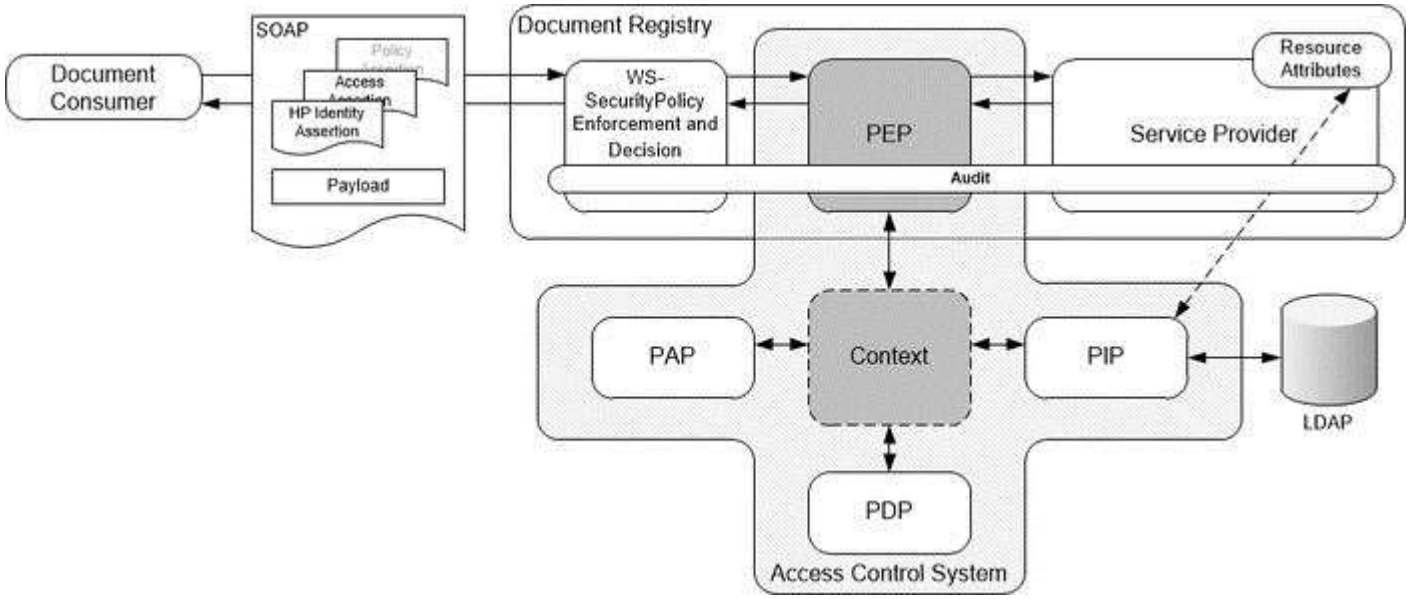
Die beschriebene Einbettung mehrerer SAML Assertions in das SOAP Security Header stellt auf der Implementierungsseite vielerlei Ansprüche: Zum einen muss die Semantik der Assertions selbst (strukturierte Elemente in Attributen) und zum anderen die korrekte Kombination einer Assertion-Kette überprüft werden können. Einem Aufrufenden muss zudem ein Besitznachweis für diese SAML Assertions abverlangt werden.

Um unterschiedliche Sicherheitsanforderungen für die verschiedenen Vertrauensbeziehungen zwischen Dienstnutzern und -anbietern deklarieren zu können, wird für jede Vertrauensbeziehung in der Schnittstellenspezifikation ein eigener Port definiert. So können z. B. sehr einfach unterschiedliche Policies für Zugriffe aus verschiedenen Sicherheitszonen heraus definiert werden (z. B. Zugriffe innerhalb eines Circle-of-Trust und in einen Circle-of-Trust hinein).

Bausteine des Access Control System

Bitte markieren Sie Kommentare zu diesem Abschnitt mit dem Code {EcssS.01.01}

Die nachfolgende Grafik stellt das Prinzip der Zugriffskontrolle abstrakt mit den XACML-Akteuren dar. Ein Zugriff auf den eigentlichen Dienst einer Document Registry wird serverseitig von einem PEP unterbrochen. Ein PEP implementiert einen Authorization Requestor, welcher eine Autorisierungsanfrage an einen PDP (Authorization Decision Provider) stellt. Der in der Abbildung gezeigte optionale Context Handler kann diese Anfrage in ein standardisiertes Protokoll (bspw. SAML)[1] überführen oder der Authorization Requestor kann direkt mit einem Authorization Decision Provider kommunizieren. Über einen PAP (Policy Repository) können die eigentlichen Autorisierungsrichtlinien kodiert als XACML Policies abgerufen werden. Der Transport einer Autorisierungsanfrage bzw. Policy-Abfrage kann über einen HTTP SOAP Request erfolgen.[2] Sind weitere Attribute für die Evaluierung einer Autorisierungsentscheidung notwendig (eine Policy bestimmt die notwendigen Attribute), so können diese über einen PIP bezogen werden.



IHE Cookbook

IHE White Paper on Access Control [3]

Referenzen

1. ↑ A. Anderson und H. Lockhart (2005), SAML 2.0 profile of XACML v2.0.
2. ↑ C. L. Joie (2007), SOAP Profile for XACML-SAML.
3. ↑ J. Caumanns et al. (2009), IHE White Paper on Access Control, S. 56f. [Online]. Available: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf

- EFA-2.0-Spezifikation

Anhang

HL7 SAIF

tbd

HL7 ECCF Framework

Die EFA-Spezifikation orientiert sich an der Spezifikationsmatrix des *Enterprise Consistency and Conformity Framework* (ECCF) als Teil des HL7 *Service-Aware Interoperability Framework* (SAIF).

	Enterprise Dimension *"Why"* ***Policy***	**Information Dimension** *"What"* ***Content***	**Computational Dimension** *"How"* ***Behavior***	**Engineering Dimension** *"Where"* ***Implementation***	**Technical Dimension** *"Where"* ***Deployment***
Conceptual Perspective					
Logical Perspective					
Implementable Perspective					

Die Spalten der Tabelle stellen bestimmte Eigenschaften des zu analysierenden und zu spezifizierenden Systems dar:

- Die *Enterprise Dimension* definiert den geschäftlichen Zusammenhang und befasst sich primär mit den EFA-Informationsobjekten und EFA-Geschäftsprozessen.
- Die *Information Dimension* befasst sich mit dem Informationsmodell der Fallakte sowie damit zusammenhängenden Restiktionen bei der Nutzung und Interpretation dieser Information.

- Die *Computational Dimension* fokussiert auf die fachlichen Funktionen der EFA mit den zugehörigen Akteuren, welche durch Transaktionen mit einem bestimmtem Verhalten und Interaktionen charakterisiert sind.

Die Zeilen der Tabelle geben verschiedene Abstraktionsgrade wieder und adressieren somit verschiedene Expertengruppen:

- Die *Conceptual Perspective* ist vollständig rechnerunabhängig und eher problem- als lösungsorientiert. Artefakte dieser Ebene skizzieren die Grundlagen und Kernkonzepte der EFA aus der Fachexpertensicht und definieren als solche das ganzheitliche konzeptionelle Modell der EFA.
- Artefakte in der *Logical Perspective* stellen nachvollziehbare Transformationen von Artefakten der konzeptuellen Ebene in Formate für Architekten/Analysten dar. Diese Perspektive repräsentiert die funktionale/logische Spezifikation der EFA und definiert somit den EFA-Lösungsraum mit seinen Klassen, Diensten und Operationen.
- Artefakte in der *Implementable Perspective* enthalten alle notwendigen, technischen Bindungen (z. B. Datentypen, Wertemengen, Schnittstellen-Spezifikationen etc.) mit denen Entwickler in die Lage versetzt werden, Bausteine der funktionalen/logischen Spezifikation mittels Standards-basierender technischer Komponenten umzusetzen zu können.

- zurück zur EFA-2.0-Spezifikation

IHE White Paper "Access Control"

Diese Seite gibt einen kurzen Überblick über die im IHE White Paper "Access Control" eingeführten Konzepte und Begrifflichkeiten, wie sie auch im IHE Cookbook und in der EFAv2-Spezifikation verwendet werden.

Access Control Subsysteme

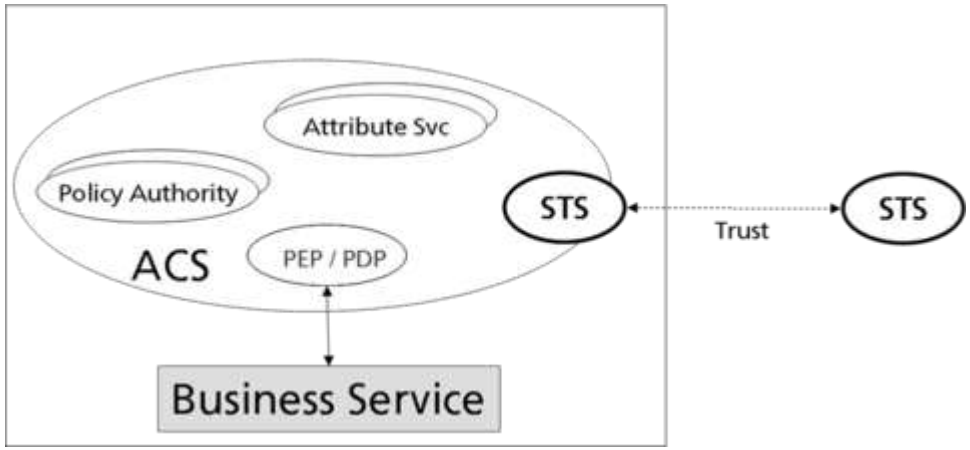
Prinzipien Service-Orientierter Architekturen wie z.B. die Entkopplung von Diensten und die deklarative Steuerung von Abläufen über Diensten lassen sich auch auf Sicherheitsinfrastrukturen und Sicherheitsdienste abbilden. Sicherheitsdienste zur Authentifizierung, Autorisierung, Nicht-Abstreitbarkeit, etc. können so voneinander entkoppelt als eigenständige, wiederverwendbare Subsysteme definiert und mit beliebigen Akteuren

gruppiert werden. Ein Access Control Subsystem (ACS) integriert dabei insbesondere die in einschlägigen Standards wie z.B. RFC2753 und XACML definierten logische Komponenten zur Verwaltung, Entscheidung und Durchsetzung von Zugriffsregeln (Policies):

- Policy Authorities (technisch: Policy Administration Point, PAP) für die Verwaltung und Bereitstellung von Policies
- Attribute Services (auch: Policy Information Point, PIP) für die Verwaltung und Bereitstellung von Attributen, die zur Laufzeit für die Auswertung von Policies benötigt werden
- Policy Decision Points (PDP) und Policy Enforcement Points (PEP) für die Auswertung und Durchsetzung von Policies

Um Policies, Policy Entscheidungen, für Policy-Auswertungen benötigte Attribute, etc. sicher zwischen an verschiedene Akteure gebundene ACS austauschen zu können, werden sog. Sicherheitstoken verwendet, die von dedizierten Security Token Services (STS) ausgestellt werden.

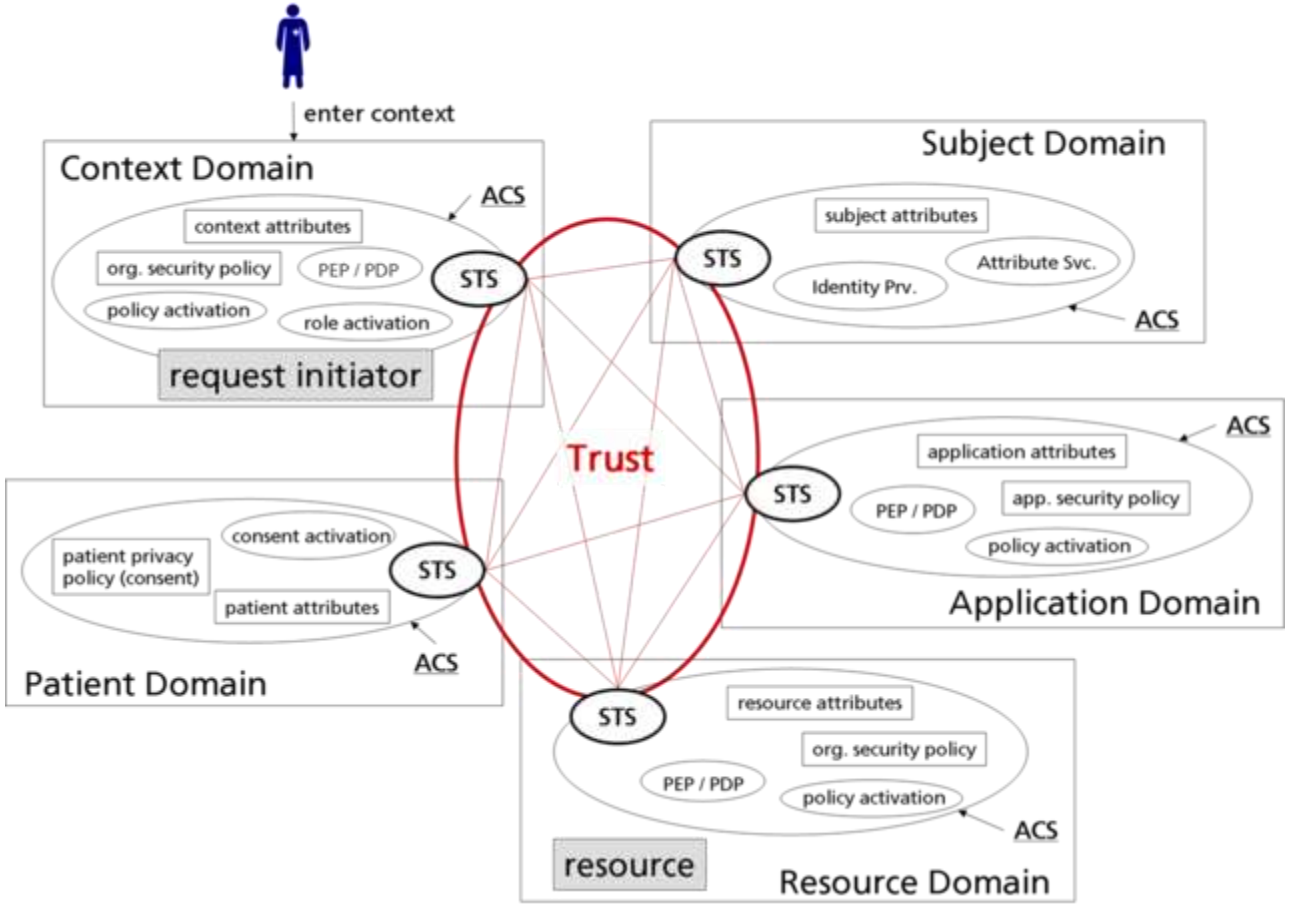
Die nachfolgende Abbildung stellt den generischen Aufbau eines Access Control Subsystems im Überblick dar.



5-Domänen-Modell

Das IHE White Paper "Access Control" beschreibt eine Methodik zur Analyse, zum Design und zur Bewertung von Access Control Lösungen für eHealth-Anwendungen. Kern dieser Methodik ist das sog. 5-Domänen-Modell, das die verschiedenen Aspekte einer jeden Access Control Lösung auf von konkreten Anwendungsdiensten und Deployments unabhängige logische Domänen abbildet. An jede dieser Domänen ist an ACS gebunden, das domänenspezifische Ausprägungen der oben skizzierten logischen ACS-Komponenten kapselt:

- Die **Context Domain** bildet den Ausführungskontext des Nutzers ab. Hier werden z.B. Kontext-Attribute (z.B. Zweck eines Datenabrufs) verwaltet und die für eine Anwendung im aktuellen Kontext aktivierte Nutzerrolle festgelegt.
- Die **Subject Domain** kapselt alle Funktionalitäten zur Identifizierung, Beschreibung und Authentifizierung eines Nutzers.
- Die **Resource Domain** bildet die durch die Access Control Lösung zu schützende Ressource (z.B. medizinische Daten) ab. Der Zugang zu dieser Ressource wird durch einen vorgelagerten PEP abgesichert.
- In der **Patient Domain** werden alle direkt mit dem Patienten verknüpften Policies - insb. auch Einwilligungen - verwaltet und bereitgestellt.
- Die **Application Domain** kapselt alle mit einer Anwendung verknüpften Policies und Nutzungskonventionen. Da diese Policies nur selten explizit sind, repräsentiert diese Domäne für die meisten Anwendungen lediglich eine Sammlung von organisatorischen Vorgaben, die sich z.B. im Sicherheits- und Datenschutzkonzept der Anwendung widerspiegeln.



Nutzung des 5-Domänen-Modells