Table of Contents

1 Vorwort 10
1.1 Stellung des Cookbooks 10
1.2 Danksagung 11
2 Grundlagen 12
2.1 Rechtliche Rahmenbedingungen 12
2.1.1 Vertraulichkeit patientenbezogener Information 12
2.1.2 Umgang mit personenbezogenen Daten 13
2.1.2.1 Bundesdatenschutzgesetz 13
2.1.2.2 Sozialgesetzbuch 14
2.1.2.3 Telemediengesetz und Datenschutz 14
2.1.3 Auftragsdatenverarbeitung - Funktionsübertragung 15
2.1.4 Einwilligung 17
2.1.5 Schutz der personenbezogenen Daten 18
2.1.6 Zusammenfassung: Anforderungen an die Umsetzung 18
2.2 IHE-Profile und weitere Standards 19
2.2.1 Cross-Enterprise Document Sharing (XDS.b) 20
2.2.1.1 Akteure 20
2.2.1.2 Transaktionen 23
2.2.1.2.1 Patient Identity Feed 23
2.2.1.2.2 (Provide and) Register Document Set-b 24
2.2.1.2.3 Registry Stored Query 25
2.2.1.2.4 Retrieve Document Set 25
2.2.2 Das XDS-I Profil 26
2.2.2.1 Akteure und Transaktionen 26
2.2.2.2 Einstellen von DICOM-Objekten 26
2.2.2.3 Herunterladen von DICOM-Objekten 27
2.2.3 IHE XDS Metadata Update 28
2.2.4 IHE Patient Identifier Cross-referencing (PIX) 28
2.2.5 Patient Demographics Query (PDQ) 29
2.2.6 Healthcare Provider Directory (HPD) 30
2.2.7 IHE Consistent Time (CT) 31
2.2.8 IHE Audit Trail and Node Authentication (ATNA) 32
2.2.9 Cross-Enterprise User Assertion (XUA) 32
2.2.10 IHE Basic Patient Privacy Consents (BPPC) 33
2.2.11 Extensible Access Control Markup Language (XACML) 34

2.2.12 Security Assertion Markup Language (SAML) ... 36
2.3 Typen einrichtungsübergreifender elektronischer Patientenakten ... 36
2.3.1 Einrichtungsübergreifende elektronische Patientenakte ... 37
2.3.2 Persönliche einrichtungsübergreifende elektronische Patientenakte ... 37
2.3.3 Fallbezogene einrichtungsübergreifende elektronische Patientenakte ... 37
3 Anwendungsszenarien ... 38
3.1 Mamma-Diagnostik ... 38
3.2 Kolorektales Karzinom ... 41
3.3 Akutversorgung Schwerverletzter (Polytrauma) ... 44
4 Lösungsarchitektur ... 47
4.1 Grundsatzentscheidungen ... 47
4.1.1 Flexible Umsetzungen ... 47
4.1.2 Transparente Ergänzungen vorhandener Profile und Empfehlungen ... 48
4.1.3 Unterstützung von feingranularen Zugriffsregelungen ... 48
4.1.4 Ausschließliche Verwendung von existierenden Standards ... 48
4.2 Umsetzung von Datenschutz und Datensicherheit ... 48
4.2.1 Zugangskontrolle ... 48
4.2.2 Zugriffskontrolle ... 48
4.2.3 Weitergabekontrolle ... 48
4.2.4 Eingabekontrolle ... 49
4.2.5 Auftragskontrolle ... 49
4.2.6 Trennungsgebot ... 49
4.3 Standardisierte Lösungsmodule ... 49
4.3.1 Patientenidentifikation ... 49
4.3.1.1 Master Patient Index ... 49
4.3.1.2 Patientenregister ... 50
4.3.1.3 Verteilte Erstellung ohne Abfragemöglichkeit ... 51
4.3.1.4 Zusammenfassung ... 52
4.3.2 Benutzerauthentifizierung und -identifikation ... 53
4.3.2.1 Charakterisierung der Lösung ... 54
4.3.2.2 Zuordnung zwischen der lokalen und der zentralen Benutzeridentität ... 55
4.3.2.3 Verwendung lokaler Benutzeridentitäten ... 56
4.3.2.4 Lokale Eingabe der zentralen Benutzeridentität ... 58
4.3.2.5 Dynamisches Mapping der Benutzeridentität ... 60
4.3.2.6 Statisches Mapping der Benutzeridentität ... 62
4.3.2.7 Zentrales Healthcare Provider Directory ... 63
4.3.2.8 Eigenschaften der Assertion ... 63
4.3.2.9 Zentrale Ausstellung der Assertion ... 64

4.3.2.10 Lokale Ausstellung der Assertion 66
4.3.2.11 Zusammenfassung 66
4.3.3 Verwalten von Berechtigungen 67
4.3.3.1 Verwaltung der Patientenzustimmung und Zugriffsregeln 67
4.3.3.2 Struktur des Patientenzustimmungsdokuments 67
4.3.3.3 Struktur der Zugriffsregeln 68
4.3.4 Überprüfen von Berechtigungen 69
4.3.4.1 Akteure und Transaktionen 69
4.3.4.2 Kombination mit zu existierenden Akteuren und Transaktionen 71
4.3.4.2.1 1. Autorisierung für ITI-18 XDS Registry Stored Query 72
4.3.4.2.2 2. Autorisierung für ITI-41 XDS Provide & Register Document Set-b und ITI-42 XDS Register Document Set-b 73
4.3.4.2.3 3. Autorisierung für ITI-43 XDS Retrieve Document Set 74
4.3.5 Folder Management 74
4.3.5.1 Strukturierung der Akte in der Benutzeroberfläche 75
4.3.5.2 Abbildung Administrativer Fallinformationen durch XDS Folder 75
4.3.5.3 Abbildung von Ordnern zur Zweckbindung durch XDS Folders 76
4.3.5.4 Abbildung von Patientenordnern 77
4.3.5.5 Abbildung von Notfallordnern 77
4.3.6 Akteninhalte 78
4.3.6.1 Verwendung von CDA 78
4.3.6.2 Dokument einstellen 78
4.3.6.3 Dokument abrufen 78
4.4 Besonderheiten der Aktentypen 78
4.4.1 Einrichtungsübergreifende elektronische Patientenakte (eEPA) 78
4.4.1.1 Integration in Primärsysteme 78
4.4.1.2 Funktionsfähigkeit mit und ohne Abfragemöglichkeit für Patienten IDs 78
4.4.1.3 Benutzerauthentifizierung an einer eEPA 79
4.4.1.4 Benutzeroberfläche der eEPA 79
4.4.1.5 Fähigkeit zur Einbindung in die Telematik-Infrastruktur 79
4.4.1.6 Use Cases 79
4.4.1.6.1 Akte Anlegen 79
4.4.1.6.2 Dokument einstellen 80
4.4.1.6.3 Dokument abrufen 80
4.4.1.6.4 Berechtigungen ändern 80
4.4.2 Persönliche einrichtungsübergreifende elektronische Patientenakte (PEPA) 80
4.4.2.1 Patientenidentifikation 80
4.4.2.2 Benutzeridentifikation und –authentifikation 80

4.4.2.3 Verwaltung und Prüfung von Berechtigungen 80
4.4.2.4 Architektur 80
4.4.2.4.1 Benutzeroberflächen / Portale 81
4.4.2.4.2 Strukturierung der Akteninhalte 81
4.4.2.4.3 Primärsystemintegration 81
4.4.2.4.4 Einbindung in die Telematikinfrastruktur 81
4.4.2.5 Use-Cases 82
4.4.2.5.1 Akte Anlegen 82
4.4.2.5.2 Aktivierung des Zugangs zum Patientenportal 82
4.4.2.5.3 Aufnahme, Einwilligung und initiale Anlage der Akte 82
4.4.2.5.4 Patienten suchen 82
4.4.2.5.5 Dokumente verwalten 83
4.4.2.5.6 Einstellen 83
4.4.2.5.7 Abrufen 83
4.4.2.5.8 Ändern/Löschen 83
4.4.2.5.9 Berechtigungen verwalten 83
4.4.3 Fallbezogene einrichtungsübergreifende elektronische Patientenakte (eFA) 84
5 Definitionen des deutschen Leitfadens 85
5.1 Terminologien für Metadaten 85
5.2 Checkliste für Implementierungen 86
6 Themen für Folgejahre 87
6.1 Cross-community Profiles 87
6.1.1 Cross-Community Access (XCA) 87
6.1.2 Cross-Community Patient Discovery (XCPD) 88
6.1.3 Cross-Community Fetch (XCF) 88
6.2 Deutsche Content Profiles 89
7 Anhang A - Konformität 90
7.1 Konformitätskriterien 90
7.2 Konformitätserklärung von Herstellern 91
7.3 Profilierungsmechanismen 92
7.4 Conformance Statements 93
7.5 Konformanzprüfung 93
8 Anhang B - Mitgeltende Literatur bzgl. Datenschutz und Datensicherheit 95
8.1 Gesetze / Richtlinien / Verordnungen 95
8.1.1 Europa 95
8.1.2 Deutschland 95
8.1.2.1 Bund 95
8.1.2.2 Katholische Kirche 96

8.1.2.3 Evangelische Kirche 96
8.1.2.4 Evangelisch-Lutherische Kirche 96
8.1.2.5 Evangelisch-reformierte Kirche 97
8.1.2.6 Baden-Württemberg 97
8.1.2.7 Bayern 97
8.1.2.8 Berlin 97
8.1.2.9 Brandenburg 97
8.1.2.10 Bremen 97
8.1.2.11 Hamburg 98
8.1.2.12 Hessen 98
8.1.2.13 Mecklenburg-Vorpommern 98
8.1.2.14 Niedersachsen 98
8.1.2.15 Nordrhein-Westfalen 98
8.1.2.16 Rheinland-Pfalz 98
8.1.2.17 Saarland 99
8.1.2.18 Sachsen 99
8.1.2.19 Sachsen-Anhalt 99
8.1.2.20 Schleswig-Holstein 99
8.1.2.21 Thüringen 99
8.1.3 Berufsgruppenspezifische Vorschriften 100
8.1.3.1 Baden-Württemberg 100
8.1.3.2 Bayern 100
8.1.3.3 Berlin 100
8.1.3.4 Brandenburg 100
8.1.3.5 Bremen 100
8.1.3.6 Hamburg 100
8.1.3.7 Hessen 101
8.1.3.8 Mecklenburg-Vorpommern 101
8.1.3.9 Niedersachsen 101
8.1.3.10 Nordrhein-Westfalen 101
8.1.3.11 Rheinland-Pfalz 101
8.1.3.12 Saarland 101
8.1.3.13 Sachsen 101
8.1.3.14 Sachsen-Anhalt 102
8.1.3.15 Schleswig-Holstein 102
8.1.3.16 Thüringen 102
8.2 Normen 102
8.2.1 Deutschland 102

8.2.2 Internationale Normen 103
8.3 Literaturangaben (Referenzen) 105

1 Vorwort

Das Interesse an Themen der einrichtungsübergreifenden Kommunikation, in Deutschland auch intersektorale Kommunikation oder integrierte Versorgung genannt, hat in den vergangenen Jahren massiv zugenommen. Die technischen Möglichkeiten der Gesundheits-IT (GIT) bilden hierbei oft eine tragende Säule, so dass sich unter dem Begriff eHealth ein weitgehend neues Feld innerhalb der Medizin-Informatik entwickelt hat, auch wenn die konzeptuellen und technischen Grundlagen hierfür bereits vor geraumer Zeit gelegt wurden.

Viele europäische Länder haben auf nationaler Ebene eHealth Projekte initiiert oder durchgeführt. Gleichzeitig haben aber auch viele Regionen in derartige Projekte investiert. Diese unterscheiden sich dabei aus technischer Sicht oft in zwei Hauptaspekten: den architektonischen Ansätzen und dem Maß der Verwendung internationaler GIT-Standards, wobei hinsichtlich des letzten Punktes die Grenzen zwischen der Verwendung internationaler Standards und eher nationaler Ansätze oft fließend sind.

Der GIT-Standard, der sich international am ehesten für den eHealth Bereich etabliert hat ist IHE. In Deutschland lag der Fokus bisher auf nationalen Spezifikationen, was unter anderem an besonderen Anforderungen hinsichtlich des Datenschutzes und der IT-Sicherheit gelegen haben mag. Andererseits werden sowohl aus Anwender- und Betreiber- als auch aus Herstellersicht nationale Spezifikationen und Umsetzungen stets kritisch beäugt, da sie erhebliche Risiken u.a. hinsichtlich ihrer Zukunftssicherheit und Wirtschaftlichkeit beinhaltet. So ist auch in mehreren eHealth Evaluations-Studien die mangelnde Standardisierung als ein Haupthemmfaktor (inhibiting factor) identifiziert worden, der entsprechend auch die jeweilige Marktentwicklung erheblich verzögert, wenn nicht gar unterbunden hat.

Das Hauptziel der Erarbeitung des hier vorliegenden Cookbooks war somit die „Nationalisierung" der internationalen IHE-Profile und damit der Anpassung eines internationalen Standards auf die spezifisch deutschen Gegebenheiten. Ein derartiges Vorgehen ist innerhalb von IHE vorgesehen, bricht also nicht mit dem internationalen Ansatz. Man spricht dann von "Lokalisierung" bzw. "local extensions" – oder sogar "national extensions" wenn diese über einen entsprechenden Prozess ausgearbeitet wurden.

Unter dem Begriff eHealth werden verschieden technische Verfahren zusammengefasst. Historisch gesehen haben sich die Telemedizin und in ihrem Gefolge die Home Care-Szenarien als erste platziert. Hauptmangel bei diesen Verfahren ist jedoch ihre Eindimensionalität, da sie oft nur einen Teilbereich bzw. einen zeitlichen Ausschnitt isoliert betrachten. Diese Defizite können durch einrichtungsübergreifende elektronische Akten kompensiert werden, die deshalb meistens auch als Grundpfeiler und Hauptelement einer weitergehenden Optimierung der Gesundheitsversorgung angesehen werden, wobei der Bildkommunikation oft eine besondere Bedeutung beikommt. Entsprechend wurde hier der inhaltliche Schwerpunkt für das Cookbook gesetzt und Umsetzungsempfehlungen für die drei in Deutschland gängigsten Architekturmodelle für einrichtungsübergreifende Akten ausgearbeitet.

Das Cookbook wurde, wie bei IHE üblich, gemeinschaftlich von Anwendern, Betreibern und Herstellen geschrieben. Von eminenter Bedeutung war es dabei eine möglichst breite Basis zu schaffen um die Akzeptanz zu gewährleisten. Gleichzeitig war allen Autoren klar, dass es sich um einen dynamischen Prozess und ein sich änderndes Dokument handeln würde. Aus beiden Gründen begrüßen wir alle Kommentare und die Mitarbeit von jeder Seite ausdrücklich! Bitte wenden Sie sich bei Interesse einfach an die Geschäftsstelle von IHE-Deutschland.

1.1 Stellung des Cookbooks

FO: kleine Grafik, wie sich das Cookbook in die Profilhierarchie einsortiert.

1.2 Danksagung

tbd: Danksagung an die verschiedenen Projekte:

- INFOPAT (Informationstechnologie für die patientenorientierte Gesundheitsversorgung in der Metropolregion Rhein-Neckar)
- EFA
- EBPG

2 Grundlagen

Im Folgenden werden rechtliche und technische Rahmenbedingungen im Zusammenhang mit dem einrichtungsübergreifenden Austausch von Bild- und Befunddaten in Deutschland aufgeführt, um daraus Anforderungen an die technischen Lösungen ableiten zu können.

2.1 Rechtliche Rahmenbedingungen

Grundsätzlich sind die folgenden rechtlichen Rahmenbedingungen relevant für die konforme Spezifikation des einrichtungsübergreifenden Datenaustauschs:

- der konkrete Behandlungsauftrag
- die konkrete Patienteneinwilligung
- deutsche Datenschutzgesetze in Umsetzung der aktuellen EU-Datenschutzrichtlinie
- Patientenrechte (z. B.: BMG-Eckpunkte)
- Strafrecht
- Haftungsrecht

Eine etwaige zukünftige EU-Verordnung (im Gegensatz zur derzeitigen EU-Direktive) zum Datenschutz würde übrigens direkt als nationale Gesetzgebung gelten, so dass heutige nationale Gesetzgebungen als Ergänzung zur kommenden Verordnung angesehen werden können. Allerdings ist nach derzeitigem Stand die Spezialgesetzgebung (z. B. Arbeitnehmerdatenschutz, Gesundheitsdatenschutz) weiterhin in nationaler gesetzgeberischer Verantwortung. Ob eine EU-Verordnung kommt, gilt heute noch als unsicher. Dementsprechend können hier natürlich auch keine Zeitangaben erfolgen. Es muss gesondert erwähnt werden, dass derzeit kein Konsens über die Angemessenheit technischer und organisatorischer Mittel zur Wahrung o.g. Rechtsgrundlagen besteht, sodass die konkrete elektronische Umsetzung des Datenaustauschs zwischen verschiedenen Einrichtungen in Deutschland nur auf einer vertraglich gesicherten Basis zwischen den Institutionen erfolgen kann, wie es beispielsweise auch bei der Teleradiologie nach Röntgenverordnung vorgeschrieben ist. Liegt eine Auftragsdatenverarbeitung vor, muss der Vertrag natürlich auch die entsprechenden bundesrechtlichen Anforderungen (§11 BDSG, §80 SGB X) wie auch ggf. vorhandene bundeslandspezifischen Anforderungen (z. B. NRW §11 DSG NRW) berücksichtigen.

2.1.1 Vertraulichkeit patientenbezogener Information

Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheidet, wer wann unter welchen Umständen auf welche seiner persönlichen Daten zugreifen darf. Dementsprechend ist der Zweck datenschutzrechtlicher Gesetze, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird" (BDSG §1 Abs. 1). Der Datenschutz hat eine besondere Bedeutung für den einrichtungsübergreifenden Austausch von Bild- und Befunddaten, da die Akzeptanz entsprechender Lösungen bei Ärzten und Patienten zu Recht nur dann gegeben ist, wenn Datenschutz und Datensicherheit umfänglich berücksichtigt sind und so die Vertraulichkeit zwischen Patient und Behandler gewährleistet ist. Aus diesem Grund ist Datenschutz ein besonderer Schwerpunkt im Cookbook. Für die Bundesbehörden und den privaten Bereich, z. B. für Krankenhäuser mit privater Trägerschaft oder niedergelassene Ärzte regelt das Bundesdatenschutzgesetz (BDSG) den Datenschutz auf Bundesebene. Daneben regeln die Datenschutzgesetze der Länder den Datenschutz in Landes- und Kommunalbehörden, weshalb diese für Krankenhäuser mit öffentlich-rechtlicher Trägerschaft gelten. In beiden Fällen wird jedoch nicht der Umgang mit den im Krankenhaus bei der Behandlung anfallenden Gesundheitsdaten geregelt. Daher gibt es noch länderspezifische Gesetze, welche genau dieses regeln. Diese Gesetze gelten in der Regel für die Verarbeitung personenbezogener Daten von Personen, welche

- in einem (zugelassenen) Krankenhaus im Sinne von §107 Abs. 1 und §108 SGB V oder

- in einer Vorsorge- und Rehabilitationseinrichtung gemäß §107 Abs. 2 und §111 SGB V

ambulant oder stationär untersucht oder behandelt werden. Kirchen und Religionsgemeinschaften wiederum haben das Recht für von Ihnen betriebene Einrichtungen eigene Gesetze zu erlassen, dementsprechend gelten für kirchliche Krankenhäuser ebenfalls eigene Gesetze, wie z.B. die Anordnung über den kirchlichen Datenschutz (KDO) für katholische Krankenhäuser und das Datenschutzgesetz der Evangelischen Kirche Deutschlands (DSG-EKD) für evangelische Krankenhäuser.

2.1.2 Umgang mit personenbezogenen Daten

Auf Grund der Vielfältigkeit der Gesetze kann an dieser Stelle nicht auf die Bundeslandspezifischen Anforderungen eingegangen werden, so dass die jeweilige Zulässigkeit im jeweiligen Projekt geprüft werden muss. Eine Übersicht der wichtigsten rechtlichen und normativen Anforderungen befindet sich im Anhang.

2.1.2.1 Bundesdatenschutzgesetz

Der Zweck des Bundesdatenschutzgesetzes ist es, gemäß §1 den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. § 3 Abs. 1 BDSG definiert personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). § 3 Abs. 3 BDSG definiert das Erheben als das Beschaffen von Daten über den Betroffenen. Das Verarbeiten ist gemäß § 3 Abs. 4 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten, wobei in diesem Zusammenhang das Speichern und Übermitteln von besonderer Bedeutung sind. Das Speichern umfasst das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Das Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

- die Daten an den Dritten weitergegeben werden oder
- der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.

Das Nutzen ist gemäß § 3 Abs. 5 BDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt. § 3 Abs. 9 BDSG definiert zusätzlich noch besondere Arten personenbezogener Daten als Angaben über die rassische und ethnische Herkunft, …, Gesundheit oder Sexualleben. Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Der Patienteneinwilligung kommt demnach eine besondere Bedeutung zu, weshalb diese in § 4 Abs. 1 BDSG konkretisiert wird. Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Letzteres bedeutet, dass der Patient im Fall des einrichtungsübergreifenden Austausches von Bild- und Befunddaten über die Übermittlung seiner personenbezogenen Daten von der behandelnden Einrichtung unterrichtet werden muss, da er nicht mit dieser Übermittlung rechnen muss. Gemäß § 28 Abs. 7 BDSG ist das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Allerdings gelten – abgesehen von den vom Bund betriebenen Krankenhäusern wie Bundeswehrkrankenhäusern – in nahezu allen Krankenhäusern die Spezialgesetzgebungen des Landes.

2.1.2.2 Sozialgesetzbuch

Entsprechend §35 Abs. 1 SGB I ist eine Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen der §§ 67a bis 78 des SGB X zulässig. Daher erfordert eine Zweckänderung der zum Zwecke der Patientenversorgung erhobenen Daten eine (schriftliche) Einwilligung des betroffenen Patienten. Entsprechend §67d ist eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt. Dies sind:

- § 68 Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr oder zur Durchsetzung öffentlich-rechtlicher Ansprüche.
- § 69 Übermittlung für die Erfüllung sozialer Aufgaben.
- § 70 Übermittlung für die Durchführung des Arbeitsschutzes.
- § 71 Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse.
- § 72 Übermittlung für den Schutz der inneren und äußeren Sicherheit.
- § 73 Übermittlung für die Durchführung eines Strafverfahrens.
- § 74 Übermittlung bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich.
- § 75 Übermittlung von Sozialdaten für die Forschung und Planung.
- § 76 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten.
- § 77 Übermittlung ins Ausland und an über- oder zwischenstaatliche Stellen.

Entsprechend §78 ist die Übermittlung von Sozialdaten, die einer in § 35 des Ersten Buches genannten Stelle von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Person zugänglich gemacht worden sind, nur unter den Voraussetzungen zulässig, unter denen diese Person selbst übermittlungsbefugt wäre. D.h., nur wenn die für den Datenschutz verantwortliche erhebende ärztliche Stelle eine Übermittlung durchführen darf, ist dies nach dem SGB erlaubt. D.h., auch eine Datenübermittlung von zum Zwecke der Patientenversorgung erhobenen Daten erfordert eine (schriftliche) Einwilligung des betroffenen Patienten, wenn keine Rechtsvorschrift die Übermittlung fordert.

2.1.2.3 Telemediengesetz und Datenschutz

Das Telemediengesetz gilt erst einmal prinzipiell für die Betreiber von Webseiten, d.h. bei einem Gesundheitsportal sind selbstverständlich die Anforderungen des TMG gültig. Dementsprechend gelten die Vorschriften:

- zur Bekämpfung von Spam, d.h. das Verbot einer Verschleierung und Verheimlichung von Absender und Inhalt bei Werbe-E-Mails ist zu beachten; Werbe-E-Mails können Mails an Patienten, Krankenhäuser und Arztpraxen sein, welche zur Nutzung des Portals auffordern

- zur Haftung von Dienstebetreibern für gesetzeswidrige Inhalte in Telemediendiensten
- zum Datenschutz beim Betrieb von Telemediendiensten und zur Herausgabe von Daten

natürlich auch für Portallösungen im Gesundheitswesen. Dementsprechend muss der Diensteanbieter entsprechend §13 TMG unter anderem gewährleisten, dass

- der Patient die Einwilligung jederzeit abrufen und mit Wirkung für die Zukunft widerrufen kann, wobei der Diensteanbieter dies dem Patienten vor der Einwilligung mitzuteilen hat
- die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können
- die Nutzung von Telemedien wie auch der evtl. erforderlichen Bezahlung anonym oder unter einem Pseudonym möglich ist (Zumutbarkeit und technische Möglichkeit vorausgesetzt) und muss den Nutzer der Telemedien hiervon unterrichten.

2.1.3 Auftragsdatenverarbeitung – Funktionsübertragung

Die Abgrenzung von Auftragsdatenverarbeitung zu Funktionsübertragung ist in der Praxis oft schwierig, die Konsequenzen aus der Entscheidung jedoch weitreichend: im Fall der Auftragsdatenverarbeitung handelt es sich nicht um eine Übermittlung, so dass der Auftraggeber für den Schutz der Daten verantwortlich bleibt und der Auftragnehmer geringeren gesetzlichen Anforderungen unterliegt. Im Fall der Funktionsübertragung handelt es sich um eine Übermittlung mit den daraus folgenden Lasten der Überprüfung, ob diese überhaupt zulässig ist und der Einholung der Einwilligung und/oder der Unterrichtung der jeweils betroffenen Person bzgl. der geplanten Datenverarbeitung. Die Auftragsdatenverarbeitung stellt also eine privilegierte Funktionsübertragung dar. Zudem ist eine Auftragsdatenverarbeitung nur innerhalb der EWG (Europäischen Wirtschaftsgemeinschaft) möglich, außerhalb fällt immer eine Datenübermittlung mit den entsprechenden Anforderungen an. Erkennungsmerkmale für Auftragsdatenverarbeitung können sein:

- fehlende Entscheidungsbefugnis des Auftragnehmers
- Weisungsgebundenheit des Auftragnehmers bezüglich dessen, was mit den Daten geschieht
- Umgang nur mit Daten, die der Auftraggeber zur Verfügung stellt; es sei denn, der Auftrag ist auch auf die Erhebung personenbezogener Daten gerichtet
- Ausschluss der Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers
- keine (vertragliche) Beziehung des Auftragnehmers zum Betroffenen
- Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

Dementsprechend können folgende Erkennungsmerkmale auf eine Funktionsübertragung hindeuten:

- Weisungsfreiheit des Dienstleisters bezüglich dessen, was mit den Daten geschieht
- Überlassung von Nutzungsrechten an den Daten
- eigenverantwortliche Sicherstellung von Zulässigkeit und Richtigkeit der Daten durch den Dienstleister, einschließlich des Sicherstellens der Rechte von Betroffenen (Benachrichtigungspflicht, Auskunftsanspruch)
- Handeln des Dienstleisters (gegenüber dem Betroffenen) im eigenen Namen
- Entscheidungsbefugnis des Dienstleisters in der Sache

Einen Sonderfall bildet die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen. Solche Tätigkeiten sind z.B.

- Installation, Wartung, Pflege und Prüfung von Netzwerken, Hardware (einschließlich Telekommunikationsanlagen) und Software u.a. (Betriebssysteme, Middleware, Anwendungen)
- Parametrisieren von Software
- Programmentwicklungen/-anpassungen/-umstellungen, Fehlersuche und Tests
- Durchführung von Migrationen im Produktivsystem

Sie können direkt vor Ort oder per Fernwartung durchgeführt werden. Die Tätigkeiten sind nicht auf den Umgang mit personenbezogenen Daten gerichtet, allerdings ist die Kenntnisnahme von personenbezogenen Daten nicht immer ausgeschlossen. Daher unterwirft der Bundesgesetzgeber im Bundesdatenschutzgesetz (BDSG) gänzlich und der Landesgesetzgeber (LDSG) weitgehend die Erbringung von Wartungs- und Pflegearbeiten den Regelungen zur Auftragsdatenverarbeitung, soweit bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten unvermeidlich ist und die Tätigkeit innerhalb des EWG durchgeführt wird. Einige Landesgesetze wie auch das SGB X gestatten nur die Auftragsdatenverarbeitung, so dass eine Funktionsübertragung nicht möglich ist. Analog zum BDSG wird in §80 SGB X ein schriftlicher Vertrag gefordert, welcher mindestens die folgenden Punkte beinhalten muss:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 78a zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz von Sozialdaten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

2.1.4 Einwilligung

Entsprechend dem allgemeinen Vertragsrecht ist eine verständliche und umfassende Information eine Grundvoraussetzung für die Wirksamkeit einer erlangten Einwilligungserklärung. Wäre diese Information nicht auf Anhieb für den Patienten als solche zu erkennen, so bestünde die Gefahr einer fehlerhaften Einschätzung dessen, was dem Patienten mit dem betreffenden Papier vermittelt werden soll. Daher gilt für eine Einwilligungserklärung der Grundsatz der „Laienverständlichkeit": nur ein informierter und aufgeklärter Patient kann eine wirksame Einverständniserklärung abgeben. Gemäß § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Entsprechend §4 Abs. 3 Satz 2 besteht die Verpflichtung, dem Aufzuklärenden auf die Freiwilligkeit bzgl. der Teilnahme hinzuweisen. Auf Verlangen muss dem Patienten auch die Folgen der Verweigerung einer Einwilligung mitgeteilt werden. Ist die Kenntnis dieser Folgen für den Patienten zwingender Bestandteil für eine informierte Einwilligung, sollte dem Patienten diese Information auf jedem Fall mitgeteilt werden. Ansonsten kann es sein, dass die Einwilligung auf Grund der fehlenden Aufklärung des Patienten nicht rechtskräftig ist. §4a Abs. 1 Satz 2 BDSG verlangt die Nennung des Zweckes der Datenerhebung, -verarbeitung oder -nutzung, wobei die Erklärung für den Patienten verständlich sein muss, zugleich auch inhaltlich und formal einwandfrei sein muss. Eine Zweckänderung muss dem Patienten mitgeteilt werden und - falls keine andere Rechtsvorschrift die Zweckänderung verlangt - darf nur mit ausdrücklicher Einwilligung des Patienten erfolgen. Entsprechend §4a Abs. 3 muss sich bei besonderen Arten von personenbezogenen Daten (dies sind u. a. auch Gesundheitsdaten) die Einwilligung ausdrücklich auf die Daten beziehen. Daher gehört eine Auflistung der Art der erhobenen Daten notwendigerweise zu einer wirksamen Einverständniserklärung dazu. Allerdings wäre eine vollständige Auflistung der einzelnen Daten (z.B. HB, Leukozyten, GOT, GPT, HZV, usw.) für den Patienten nicht überschaubar und in vielen Fällen auch unverständlich, so dass die jeweiligen Kategorien genannt werden müssen. Damit die Kategorien für den Patienten verständlich sind, können Beispiele hilfreich sein. Nach §4 Abs. 3 sind die Kategorien von Empfängern zu benennen, wenn Daten übermittelt werden. Auch wenn diese Vorschrift nur die Übermittlung an sich betrifft, muss hier das Urteil des Bundesverfassungsgerichtes entsprechend berücksichtigt werden: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß." D.h., mit dem Verzicht der Nennung der Nutzungsberechtigten würde das datenschutzrechtliche Grundziel der informationellen Selbstbestimmung verfehlt und die Einverständniserklärung nichtig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben. Ein Hinweis in einer Einverständniserklärung, welcher aufzeigt, dass der Patient Möglichkeiten zur Fragestellung hatte, verdeutlicht, dass der Patient vor Abgabe seiner Willenserklärung alle Möglichkeiten zur Information hatte. Selbstverständlich müssen eventuell erfolgte Zusatzabsprachen in der Einverständniserklärung schriftlich festgehalten werden. Eine Abstufung ermöglicht dem Patienten zu entscheiden, welcher Datenübermittlung und Datennutzung er zustimmt, z.B.:

- Qualitätssicherung
- Forschung
- Beidem
- Keine der genannten Möglichkeiten.

Da der Patient die ausdrückliche Wahl der Zustimmung oder des Widerspruchs hat, wird hier der informationellen Selbstbestimmung des Patienten genüge getan. Entsprechend §35 Abs. 2 BDSG sind personenbezogene Daten zu löschen, sobald „ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist". Bei einer unspezifischen Zeitangabe – insbesondere mit dem Vorbehalt auf die Nutzung weiterer Vorhaben (z.B. epidemiologischer Forschung) – muss dem Patienten unmissverständlich klar gemacht werden, das dies ggf. eine dauerhafte Speicherung seiner Daten zur Folge hat, ebenso dass er jederzeit widersprechen kann. Im Rahmen der Einwilligung ist es nicht möglich, die Rechte auf Auskunft, Berichtigung, Sperrung und Löschung der Daten auszuschließen oder zu beschränken (§ 6 Abs.1 BDSG).

2.1.5 Schutz der personenbezogenen Daten

Gemäß § 9 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die in § 9 BDSG referenzierte Anlage definiert, dass wenn personenbezogene Daten automatisiert verarbeitet oder genutzt werden, die innerbehördliche oder innerbetriebliche Organisation so zu gestalten ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

2.1.6 Zusammenfassung: Anforderungen an die Umsetzung

Wie oben erläutert, muss die elektronische Einwilligung des Patienten in die Datenverarbeitung

- mit Schutzmaßnahmen erfolgen
- neben gleichzeitig erfassten Erklärungen gesondert hervorgehoben werden
- den Grund für die Datenerhebung und -speicherung nennen
- die Folgen der Verweigerung nennen

- Die Daten selbst benennen bzw. bei eindeutiger Kenntnis durch den Patienten reichen auch die Kategorien der Daten aus
- die (Kategorien der) Empfänger nennen

Die Spezifikation des Cookbooks kann die ersten zwei Maßnahmen nach § 9 BDSG (Anlage) nicht bzw. nur unterstützend umsetzen:

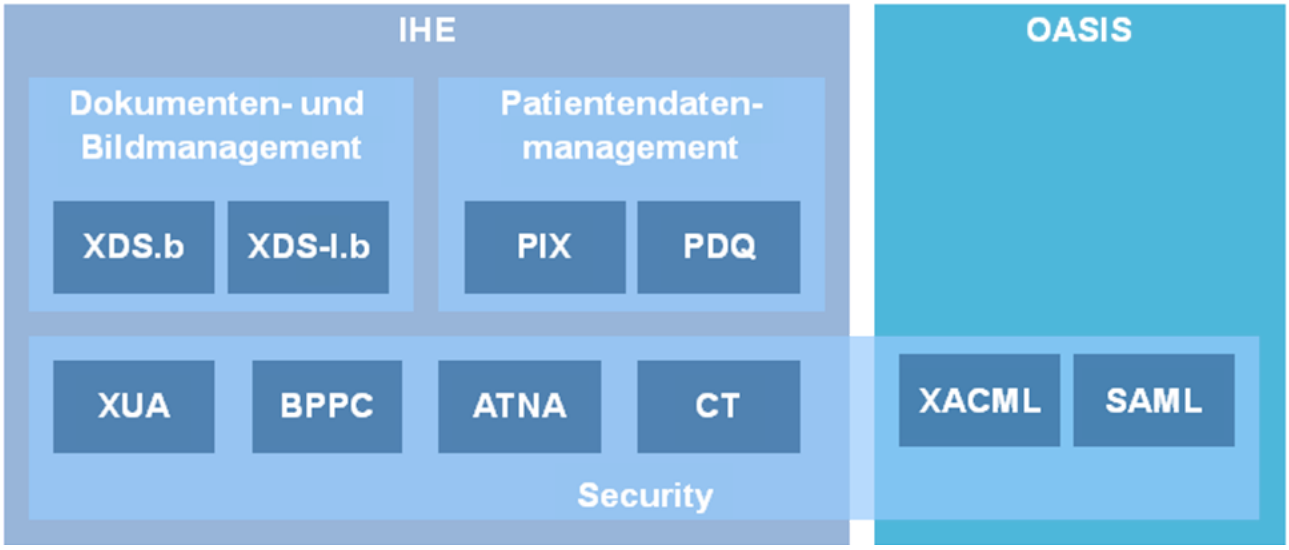
- Zutrittskontrolle, die wesentlich außerhalb Software stattfindet, und
- Verfügbarkeitskontrolle, die durch Maßnahmen des Softwarebetriebs sicherzustellen ist

wohingegen die folgenden Maßnahmen nach § 9 BDSG (Anlage) wesentliche Anforderungen an das Cookbook sind:

- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Trennung der Verarbeitung nach Zweck

2.2 IHE-Profile und weitere Standards

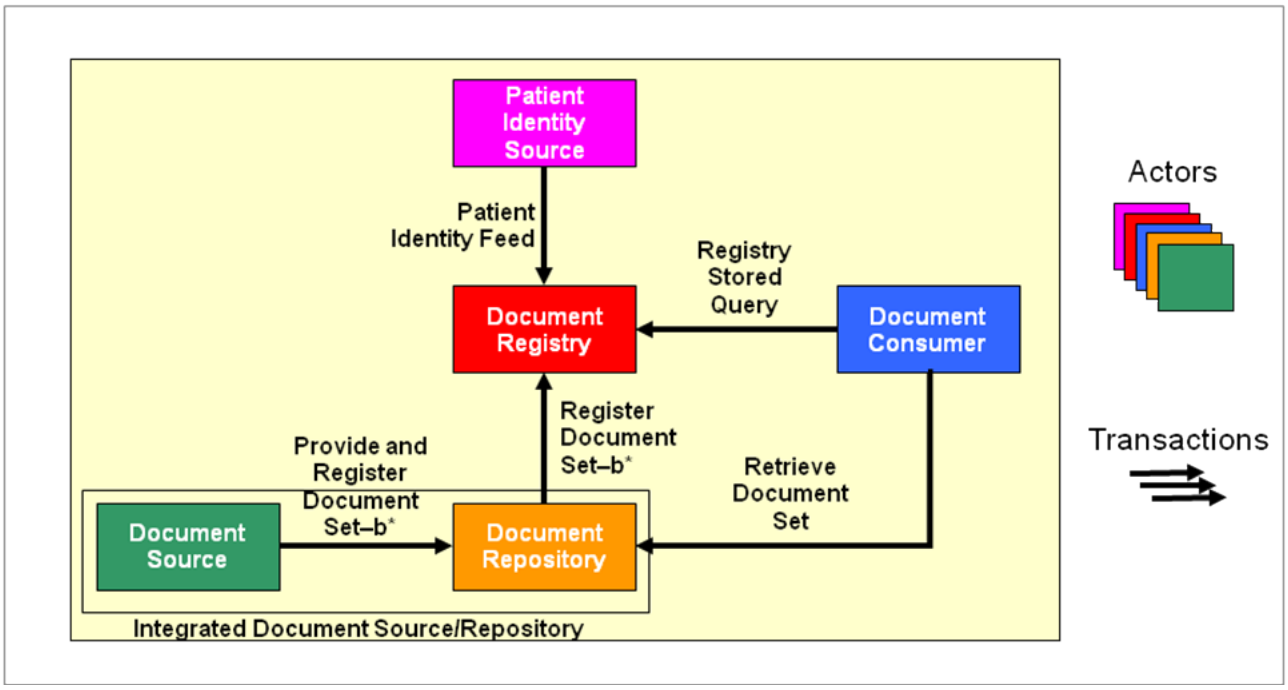
Im Folgenden werden aktuell verfügbare Standards und Profile aufgeführt, die für die einrichtungsübergreifende elektronische Kommunikation von Bildern und Befunden eine Rolle spielen. In der folgenden Abbildung sind diese zusammenfassend dargestellt. Ausgehend vom IHE-Profil XDS-I werden diejenigen relevanten IHE-Profile benannt und kurz erläutert, die den Ausgangspunkt für die technische Spezifikation bilden. Sofern diese als nicht ausreichend angesehen werden, wird auf zusätzliche internationale Standards eingegangen, um eine tragfähige Lösung zu erreichen. Die Spezifikationen werden an dieser Stelle nur kurz und kontextbezogen erläutert, um relevante Details darzustellen. Für weitergehende Informationen sei auf die Spezifikationen selbst verwiesen.



FO: Die hier aufgelisteten Profile sind aber nicht alle in allen Szenarien erforderlich. Ausserdem fehlen übergreifende wie XDS-SD, XDS-MS, XDW, etc.

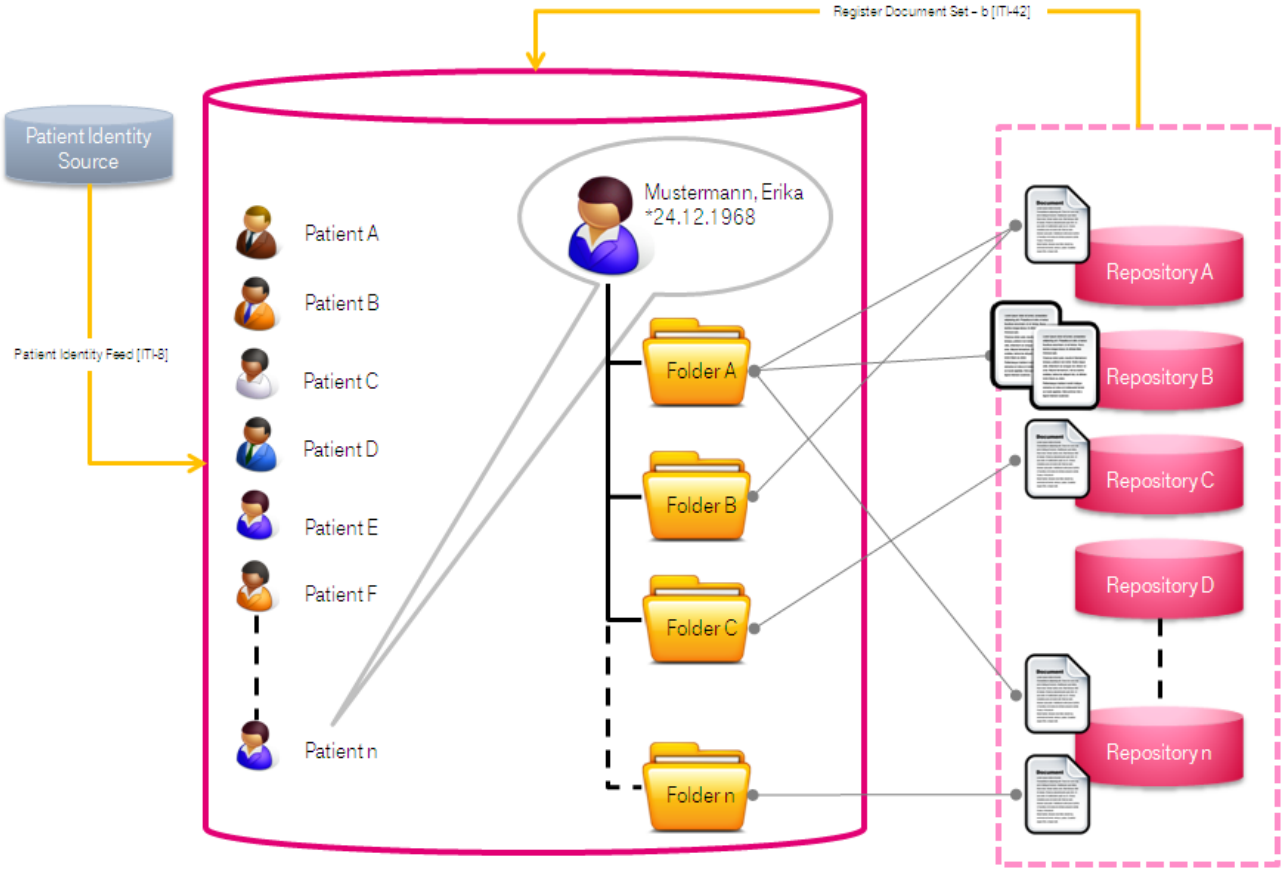
2.2.1 Cross-Enterprise Document Sharing (XDS.b)

Das Profil XDS.b (Cross-Enterprise Document Sharing) legt den Grundstein für jede XDS-Umgebung, indem es wie bei IHE-Profilen üblich sogenannte Akteure einführt, die über Transaktionen miteinander kommunizieren. Das eigentliche XDS-Profil eignet sich zum Austausch von Dokumenten beliebigen Typs (Bilder, Befunde, Videos, etc.). XDS entkoppelt den Dokumenteninhalt (z.B. unstrukturiertes PDF-Dokument) von den Metadaten (strukturierte und suchbare Objektmerkmale, „Indices", „Verschlagwortung"). Das Profil „XDS.b" löste 2009 das Vorgängerprofil mit der Bezeichnung „XDS.a" ab, wodurch sich die Bedeutung des Begriffs „XDS" verändert hat. Im Weiteren werden „XDS" und „XDS.b" als gleichbedeutend verwendet. Die folgende Abbildung zeigt die im XDS-Profil beteiligten Akteure und Transaktionen. Es werden, wie bei allen nachfolgenden Grafiken und Erläuterungen auch, die in IHE gebräuchlichen englischen Bezeichnungen verwendet.

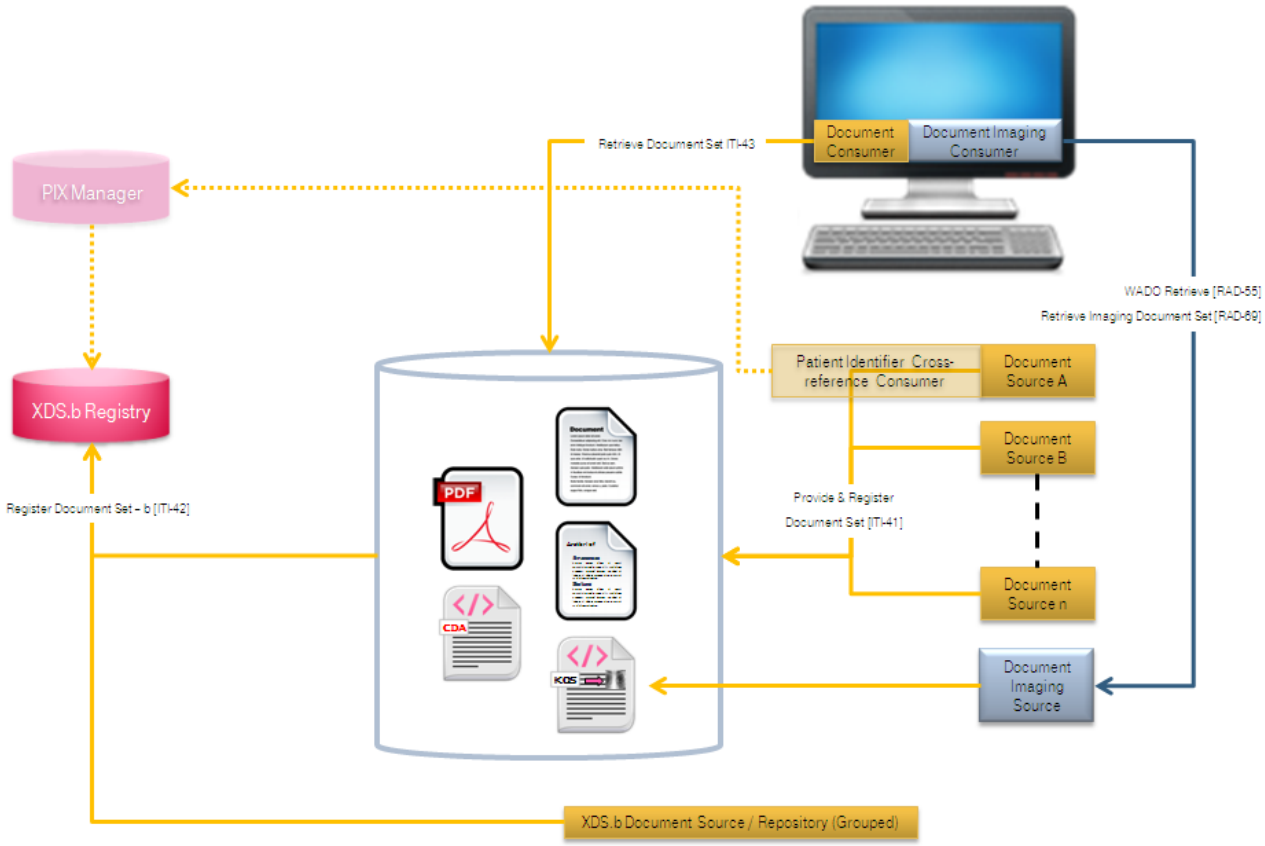


2.2.1.1 Akteure

Die Document Registry ist das Herzstück einer XDS-Umgebung. Sie verwaltet zentral die Verweise auf alle Dokumente, welche die angeschlossenen Partner untereinander teilen möchten. In jeder XDS-Umgebung existiert nur eine einzige Registry. Statt des Begriffs der XDS-Umgebung oder XDS-Installation wird von IHE stattdessen im Regelfall die Bezeichnung XDS Affinity Domain benutzt, um eine spezifische Registry und die daran angeschlossenen Akteure zu bezeichnen.



Desweiteren gibt es Document Repositories, welche die Dokumente selbst vorhalten. Wie die obige Abbildung bereits nahelegt, verweilen die Dokumente bei XDS also nicht in der Registry sondern in Document Repositories, von denen beliebig viele existieren können.



Die Registry verwaltet ausschließlich Meta-Daten, d. h. Informationen, welche Art von Dokumente zu welchen Patienten existieren und in welchem Document Repository diese gespeichert sind. Aus der Deployment-Sicht verbleiben die Repositories üblicherweise (jedoch nicht gezwungenermaßen) bei den jeweiligen Einrichtungen.

Akteure namens „Document Consumer" können Dokumente suchen und herunterladen. Dazu wendet sich ein Consumer zunächst mit einer Suchanfrage an die Registry, um die für ihn relevanten Dokumente ausfindig zu machen (z. B. Bilder zu einem bestimmten Patienten). Anschließend kann der Consumer die für ihn interessanten Dokumente vom entsprechenden Repository herunterladen.

Selbstverständlich existiert auch ein Akteur, der für das Einstellen von Dokumenten in ein Repository verantwortlich ist, die Document Source. Sie überträgt die Dokumente in ein (oder gar mehrere) Repositories und entscheidet somit darüber, welche Dokumente für die XDS-Partner zur Verfügung stehen, also „sichtbar" sind. Es können beliebig viele Document Sources in einer Affinity Domain integriert werden.

Ein System, welches Dokumente produziert und gleichzeitig lokal speichert, vereint in sich die Rollen „Document Source" und „Document Repository" – dies wird als „Integrated Source/Repository" bezeichnet. Der Hauptunterschied zum Actor Document Repository besteht darin, dass das Einstellen des Dokumenteninhalts in das Repository auf einem proprietären nicht-XDS-Weg erfolgen kann.

Die Registry als „Spinne im Netz" ist Ansprechpartner für alle Document Consumer, wenn es um das Auffinden von Dokumenten geht. Deshalb muss sie nicht nur Informationen über alle Dokumente besitzen, sondern auch über alle dazugehörigen Patienten Bescheid wissen, da jedes Dokument zu genau einem Patienten gehört.

Für das Anlegen eines Patienten in der Registry sind in XDS nicht die Repositories verantwortlich. Stattdessen wird diese Verantwortlichkeit an einen separaten Akteur ausgegliedert, die Patient Identity Source, welche als einziger Akteur Patienten in einer Affinity Domain anlegt oder ändert. Dieser Akteur vergibt für jeden Patienten eine eindeutige Patientenkennung , die sogenannte XAD-Pid (XDS Affinity Domain Patient Identification, auch häufig XAD-PID geschrieben).

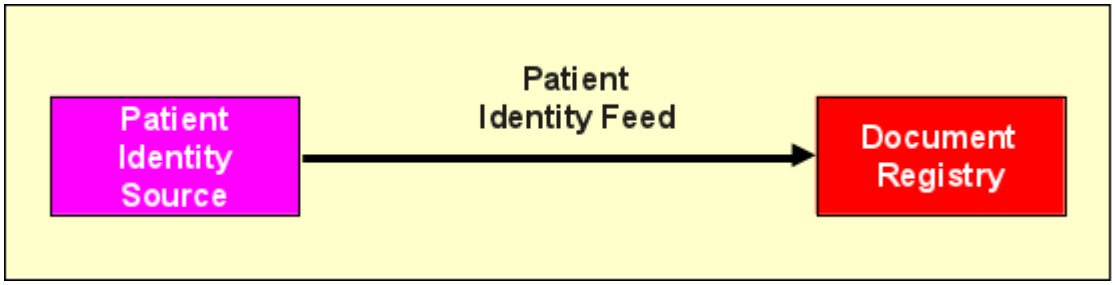
Insgesamt ergibt sich demnach folgendes Gesamtbild: Die Document Sources stellen Dokumente in die Document Repositories (häufig eine Source pro Repository) ein. Die Document Repositories informieren die Registries über neue Dokumente und teilen ihr u. a. mit, zu welchem Patienten diese gehören. Nur wenn die Patient Identity Source den jeweiligen Patienten vorher angelegt hat, wird die Registry einen Verweis auf das entsprechende Dokument übernehmen. Document Consumers können anschließend Dokumente in der Registry suchen und auf Wunsch vom jeweiligen Document Repository abrufen. Der nachfolgende Abschnitt geht nun näher auf die Nachrichten zwischen den einzelnen Akteuren ein.

2.2.1.2 Transaktionen

Die Transaktionen, über welche die Akteure Dokumente, Suchanfragen und ähnliches austauschen, lassen sich ebenfalls in obigen Abbildung ablesen. Dieser Abschnitt erläutert die den Inhalt der Nachrichten sowie die dabei benutzten Standards. Alle Transaktionen in IHE besitzen eine eindeutige Kennung, im Kontext von IT-Infrastructure und Radiologie fängt diese Kennung mit dem Präfix „ITI-" bzw. „RAD-„ an.

2.2.1.2.1 Patient Identity Feed

Wie im vorigen Abschnitt angedeutet, muss zunächst jeder Patient der Registry initial bekannt gemacht werden. Dies geschieht über die Transaktion (Nachricht) „Patient Identity Feed".



Die Nachricht verwendet den HL7 (Health Level 7) Standard, wobei sowohl eine Variante auf Basis von HL7 Version 2 (HL7v2) als auch unter Verwendung von HL7 Version 3 (HL7v3) zur Verfügung steht, von denen mindestens eine von Patient Identity Source und Registry unterstützt werden muss. Hier ist bei der Planung einer Affinity Domain sicherzustellen, dass beide Systeme dieselbe Variante oder sogar beide implementieren. Für Patient Identity Feed lauten die Transaktionskennungen ITI-8 (HL7v2) und ITI-44 (HL7v3). Bei ITI-8 handelt es sich technisch gesehen um verschiedene HL7-Nachrichten, die für verschiedene Zwecke eingesetzt werden:

Nachricht	HL7-Definition	IHE - Nutzung
ADT^A01	Einweisung eines Patienten	Anlegen einer Akte
ADT^A04	Ambulante Einweisung eines Patienten	dto.
ADT^A05	Ankündigung einer Patienteneinweisung	dto.
ADT^A08	Aktualisierung von Patienteninformationen	Ändern der Patientendaten
ADT^A40	Zusammenführen („Merge") von verschiedenen Patienten	Zusammenlegen von Akten

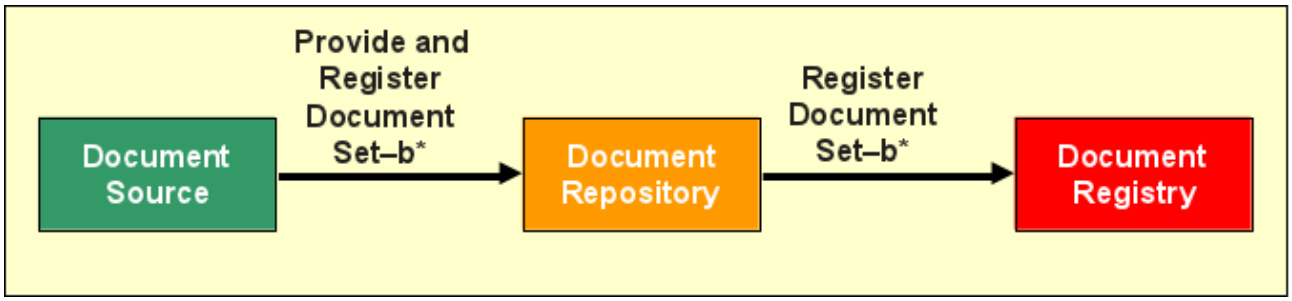
A01, A04 und A05 dienen aus Sicht der Registry ausschließlich dem Anlegen eines Patienten. Für die Registry ist dabei vor allem die zentrale Patientenkennung der Affinity Domain wichtig, die anschließend von Document Repositories und Document Sources bei der Kommunikation mit der Registry genutzt werden. Für Audit-Zwecke speichert die Registry zusätzlich auch einige demographische Patientendaten. An dieser Stelle kommt die Frage auf, wie Repositories und Sources überhaupt die XAD-Pid herausbekommen, denn eine Document Source kennt üblicherweise nur den Namen des Patienten oder möglicherweise seine lokale Krankenhauskennung. Mögliche Lösungen bieten das PIX- sowie das PDQ-Profil, die in nachfolgenden Abschnitten beschrieben werden. In der Praxis implementiert i.d.R. ein Master Patient Index die Patient Identity Source des Affinity Domain und gleichzeitig die Akteure PIX Manager und PDQ Supplier und verlinkt die lokalen Krankenhauskennungen mit der zentralen Master Patient ID. Die A40-Nachricht hat die Funktion, zwei Patienten (d. h. zwei unterschiedliche Master Patient IDs in der Registry) zusammenzuführen. Diese Aktion kann notwendig werden, wenn versehentlich für einen Patienten zwei Master Patient IDs angelegt wurden. Diese Situation kann mit dem Zusammenführen („Merge") der Kennungen auf Veranlassung der Patient Identity Source behoben werden. Die ADT^A08-Nachricht dient zur Aktualisierung von Patientendaten.

Wenn HL7v3 genutzt wird (ITI-44), können alle oben genannten Aktionen über die folgenden Nachricht durchgeführt werden:

Nachricht	Zweck
PRPA_IN201301UV02	Neuanlage von Patienteninformationen
PRPA_IN201302UV02	Aktualisierung von Patienteninformationen
PRPA_IN201304UV02	Zusammenführen von verschiedenen Patienten

2.2.1.2.2 (Provide and) Register Document Set-b

Das Einstellen von Dokumenten in XDS geschieht zweistufig: Zunächst wird ein Dokument von der Document Source über die Transaktion „Provide and Register Document Set-b" (ITI-41) an das gewünschte (üblicherweise institutionseigene) Document Repository zur Speicherung übergeben, zusammen mit einigen weiteren (Meta)Informationen wie etwa der Zuordnung zur zentralen Patientenkennung und dem Typ des Dokuments. Anschließend leitet das Repository mittels ITI-42 („Register Document Set-b") die Meta-Informationen (nicht das Dokument!) an die Registry weiter, angereichert um einige wenige weitere Datenfelder. Bei Erfolg ist das übermittelte Dokument nun für alle XDS Document Consumer in der Affinity Domain verfügbar.



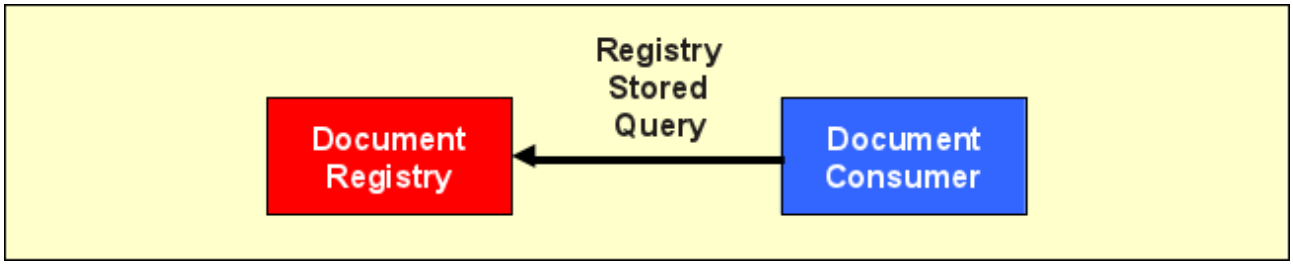
Genau genommen lässt sich über beide Transaktionen nicht nur jeweils ein einzelnes Dokument übertragen. Wie ihre Bezeichnungen bereits andeuten, wird immer ein sogenanntes „Document Set" übertragen, in dem beliebig viele Dokumente (zu einem einzelnen Patienten) transportiert werden können. Neben einfachen Dokumenten definiert XDS zwei Konzepte, um Dokumente logisch zu gruppieren:

- Submission Set enthält alle Dokumente aus einer Transaktion, d. h. alle Dokumente, die zusammen „hochgeladen" wurden.
- Folder ist ein generischer „Container" für Dokumente. Über die genaue Anwendungsweise entscheidet die Affinity-Domain. Das Verschachteln von Folders lässt XDS nicht zu, dagegen ist die Zugehörigkeit eines Documents zu mehreren Folders möglich (ähnlich zu symbolischen Links in Unix-Filesysteme).

Dokumente, Folders und Submission Sets werden untereinander durch Beziehungsobjekte (Associations) verknüpft. ITI-41 und ITI-42 enthalten jeweils genau einen Submission Set. Die Verwaltung von Ordnern und Dokumentenstatus ist für Document Sources gemäß IHE Vorgabe optional, für Registries verpflichtend – die Repositories leiten die entsprechenden Datenfelder nur „blind" weiter. ITI-41 und ITI-42 verwenden Web Service Nachrichten, die wiederum auf dem SOAP-Standard aufsetzen. Die Nachrichteninhalte werden in XML (eXtensible Markup Language) kodiert. Zur möglichst effizienten Übertragung von etwaig eingebetteten Binärdaten (woraus die meisten Dokumente bestehen) kommt in ITI-41 MTOM/XOP (Message Transmission Optimization Mechanism und XML-binary Optimized Packaging) zum Einsatz. Dies ist für ITI-42 nicht notwendig, da hier nur Meta-Informationen, nicht die eigentlichen Dokumente in der Nachricht enthalten sind. Große Teile von XDS (Architektur und Meta-Informationen) und seinen Transaktionen basieren auf einem Standard namens ebXML (Electronic Business XML), der nicht gezielt für das Gesundheitswesen entwickelt wurde.

2.2.1.2.3 Registry Stored Query

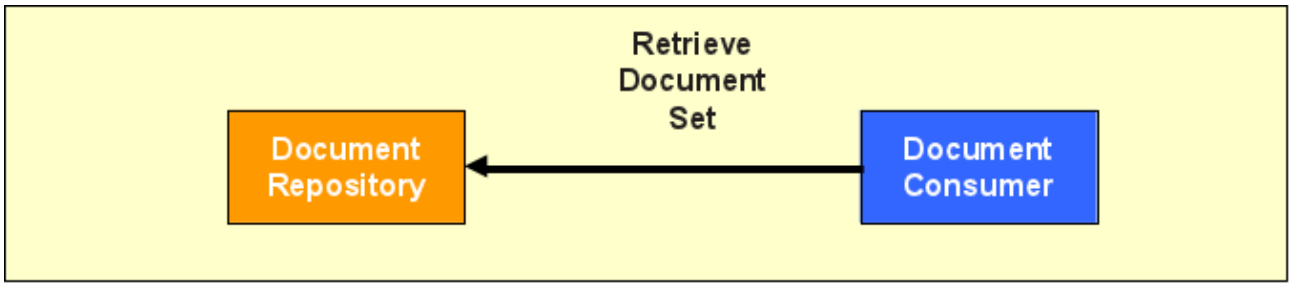
Die Transaktion „Registry Stored Query" (ITI-18) dient der Suche nach Dokumenten in der Registry. Die Dokumente in einer XDS Affinity Domain sind üblicherweise über mehrere Document Repositories verteilt. Um als Document Consumer ein Dokument finden zu können, wendet sich dieser nicht etwa mit einer Anfrage an jedes einzelne Repository, sondern an die zentrale Document Registry. Dies ist eine Design-Entscheidung, die für XDS (bzw. ebXML) getroffen wurde und verbindlich für XDS-konforme Systeme ist.



Die Ausdrucksmöglichkeiten der Abfragen sind in XDS.b (gegenüber der Vorgängerversion) eingeschränkt. Es werden insgesamt 13 „vorgefertigte" Query-Arten definiert, die einzelne Anwendungsfälle einer Suche abdecken (deshalb „Stored Query"). So lassen sich Dokumente über ihre Patientenkennung, Datum, Ordner oder Submission Set finden. Bei komplizierteren Auswahlkriterien muss ein Document Consumer ggf. Ergebnisse von mehreren Abfragen miteinander kombinieren. Das Ergebnis der Abfrage enthält Verweise auf Document Repositories, mit Hilfe deren der Dokumentinhalt heruntergeladen werden kann. Optional kann das Abfrageergebnis auch sämtliche Metadaten der zurückgegebenen XDS-Objekte (Dokumente, Folders, Submission Sets) enthalten. Als Standards kommen wiederum u. a. Web Services, SOAP, MTOM/XOP und ebXML zum Einsatz.

2.2.1.2.4 Retrieve Document Set

Nachdem ein Document Consumer eine Menge von Dokumenten über die Registry lokalisiert hat, kann er diese vom jeweiligen Repository mittels der Transaktion „Retrieve Document Set" (ITI-43) herunterladen.



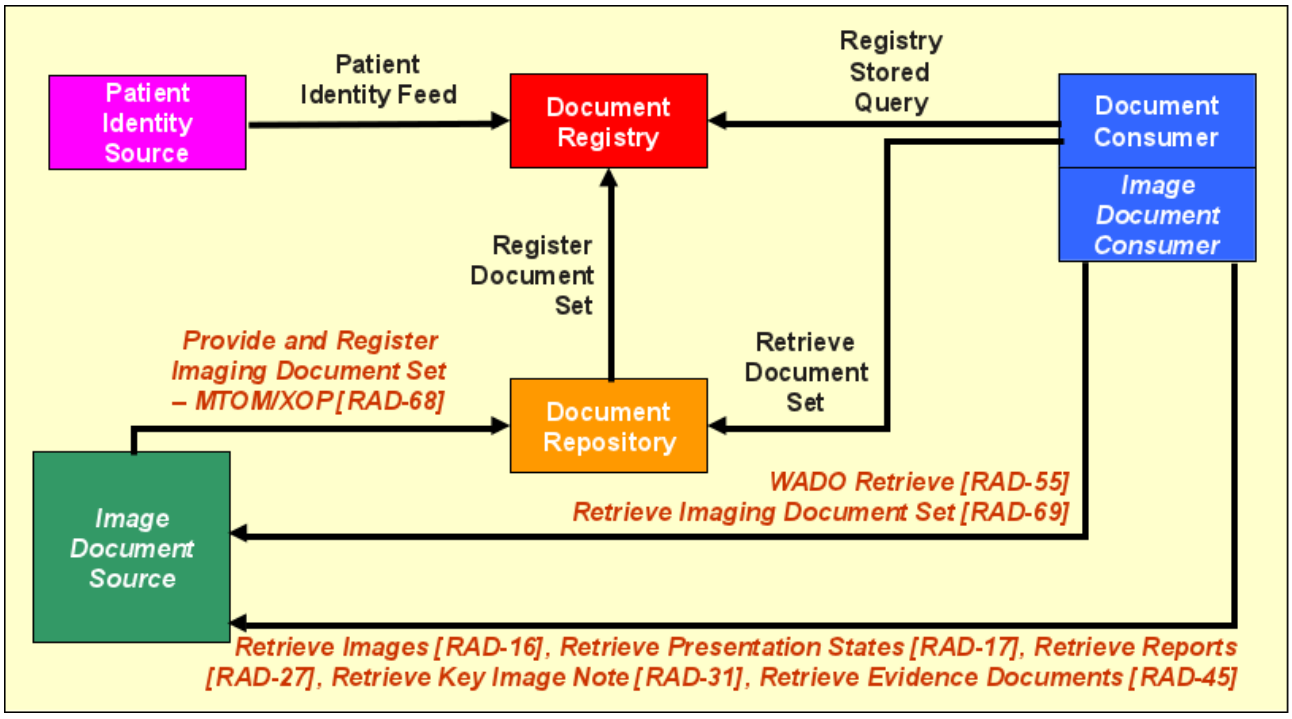
Dabei wird in erster Linie die Dokumentenkennung zur Identifikation des Dokuments angefragt. Anfrage und Antwort benutzen wiederum die bereits bekannten Web Service Standards und ebXML.

2.2.2 Das XDS-I Profil

Das XDS-Profil ist „content agnostic" – es lassen sich alle möglichen Dokumentenformate austauschen, seien es PDF-Dateien oder (theoretisch) sogar proprietäre Formate wie Microsoft Word-Dokumente. Nun ist es jedoch sinnvoll, je nach Dokumenttyp zusätzliche Regeln (sog. Content Profiles) oder sogar zusätzliche Akteure und Transaktionen festzulegen. Genau dieser Weg wurde auch beschritten, um XDS für den Austausch medizinischer Dokumente im DICOM-Format (DICOM-Objekte wie Bilder) zu erweitern. Dieser Abschnitt beschreibt das von IHE dazu bereitgestellte Profil XDS-I (XDS for Imaging). Seit einiger Zeit besteht eine geringfügig weiter entwickelte Variante von XDS-I mit dem Namen XDS-I.b. Alle folgenden Erläuterungen beziehen sich auf diese noch nicht offiziell verabschiedete, jedoch zum Testen bereits freigegebene Spezifikation (Status: „For Trial Implementation").

2.2.2.1 Akteure und Transaktionen

XDS-I beschreibt keinen Ersatz für XDS, sondern definiert eine Erweiterung von XDS zur Verwaltung von DICOM-Objekten. Für den überwiegenden Teil der XDS-Akteure und Transaktionen ändert sich nichts. Die nachfolgende Abbildung zeigt die geänderten Transaktionen in orangefarbener Kursivbeschriftung. Eine XDS-I-spezifische Variante des Akteurs „Document Source" trägt die Bezeichnung „Image Document Source". Dieser Akteur hat zum einen spezielle Anforderungen an das Veröffentlichen der Dokumente zu erfüllen (Transaktion RAD-68), zum anderen einen Teil der Bilddaten selbst für den Abruf zur Verfügung zu stellen (RAD-55, RAD-69, RAD-16, RAD-17, RAD-31, RAD-45). Um die Bilddaten vom „Image Document Source" abzurufen, wird der Akteur „Image Document Consumer" benötigt, der mit dem XDS Document Consumer gruppiert ist.



2.2.2.2 Einstellen von DICOM-Objekten

Bilder (und andere DICOM-Objekte) belegen viel Speicherplatz. Zudem sind bei weitem nicht alle Bilder zum Austausch mit anderen Institutionen interessant. Vielmehr wird häufig nur ein Bruchteil verwendet, wie z. B. die befundrelevanten Bilder. Da der Consumer (bzw. dessen Benutzer) unter Umständen nicht im Vorfeld entscheiden kann, welche Bilder denn relevant sind, sollte möglichst eine Vorauswahl getroffen werden, damit nicht alle Bilder für eine XDS-Übertragung bereitgehalten oder gar übermitteln werden müssen. Aus diesen Überlegungen heraus wurde für XDS-I die Entscheidung getroffen, alle Bilder bei der Quelle zu belassen (d. h. üblicherweise im DICOM-Bildarchiv der Einrichtung) und nur eine Auswahl von Bildern überhaupt in der XDS Affinity Domain zu veröffentlichen.

Statt also Bilder an das Document Repository zu übertragen, wird von der Imaging Document Source ein sogenanntes Key Object Selection (KOS) Dokument erstellt und mit der Transaktion „Provide and Register Document Set – MTOM/XOP" (RAD-68) an das Repository zum Speichern versendet. Dieses spezielle DICOM-Dokument enthält nur Verweise auf die bei der Source bereitstehenden, relevanten DICOM-Bilder. Das Document Repository speichert ein solches DICOM-Objekt wie jedes andere Dokument und leitet die Meta-Informationen (in erster Linie Patienten- und Dokumentenkennung) an die Registry weiter.

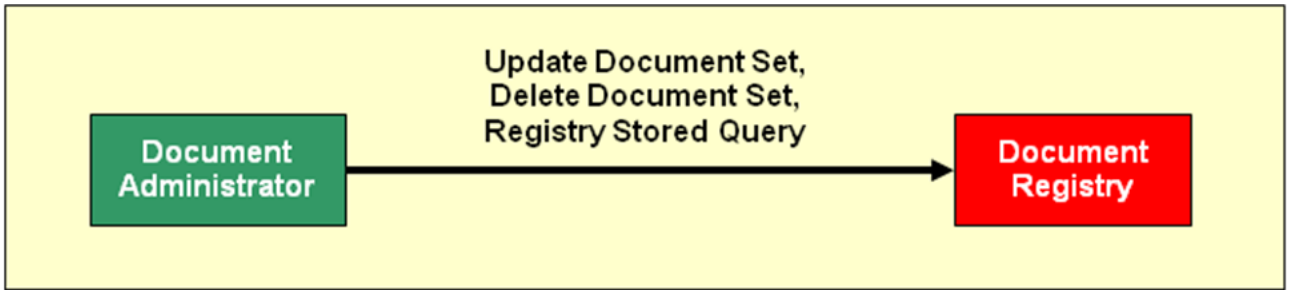
Die Imaging Document Source speichert also im Gegensatz zur Document Source im normalen XDS-Profil gezwungenermaßen alle Dokumente (hier: DICOM-Bilder) selbst und teilt zunächst über die Registry mit den XDS-Partnern ausschließlich ein DICOM KOS-Dokument, das eine Auswahl von Bildern (genauer: Referenzen auf diese) zusammenstellt. Im Vergleich zum XDS-Profil benötigt also die (Image) Document Source in XDS-I besondere (DICOM-)Fähigkeiten zum Einstellen von Bildern. Registry und Repositories verlangen dagegen keine speziellen Anpassungen, müssen aber ggf. konfiguriert werden, um DICOM als Dokumententyp zu akzeptieren.

2.2.2.3 Herunterladen von DICOM-Objekten

Möchte ein Consumer DICOM-Bilder zu einem Patienten einsehen, muss er sich wie gehabt an die Registry wenden. Diese verwaltet allerdings in XDS-I nun nicht mehr Verweise auf die eigentlichen Bilder, sondern Verweise auf KOS-Dokumente in den Repositories, welche wiederum auf die Bilder verweisen. Ein XDS-I Image Document Consumer muss also gegenüber dem XDS Consumer einen Schritt mehr ausführen, um an die relevanten Informationen (Bilder) zu gelangen. Nach der Lokalisierung der entsprechenden KOS-Dokumente kann er diese mit der bereits bekannten XDS-Transaktion Retrieve Document Set herunterladen. Anschließend muss er das DICOM-Dokument parsen können, um die enthaltenen Bildverweise zu extrahieren. Entscheidet er sich, alle oder eine Auswahl der dabei entdeckten Bilder mittels der beiliegenden Kennung herunterzuladen, stehen ihm unterschiedliche Transaktionen zur Verfügung. Dabei erfolgt der Download direkt von der Imaging Document Source. Eine Möglichkeit besteht darin, eine Variante der üblichen Retrieve Document Set Transaktion auszuführen, die geringfügig für DICOM-Dokumente angepasst wurde und als Retrieve Imaging Document Set [RAD-69] zur Verfügung steht. Diese Transaktion sollte einfach zu implementieren sein, wenn ein XDS Document Consumer bereits die entsprechende XDS-Transaktion beherrscht. Alternativ lassen sich Transaktionen nutzen, die dem DICOM-Standard entlehnt wurden. Dabei gibt es zwei Varianten, die beide durch XDS-I unterstützt werden. Zum einen gibt es in DICOM seit vielen Jahren die Möglichkeit, DICOM-Objekte über das Web-Protokoll HTTP (HyperText Transfer Protocol) zu transferieren. Der entsprechende Teil des DICOM-Standards heißt WADO („Web Access to DICOM Persistent Objects") und wird in XDS-I durch die Transaktion „WADO Retrieve" (RAD-55) abgedeckt. Die zweite DICOM-konforme Variante besteht darin, das DICOM-spezifische Netzwerk-protokoll in Form der dort üblichen Retrieve- und Storage-Dienste zu nutzen. XDS-I sieht dabei für verschiedene Arten von DICOM-Objekten unterschiedliche Transaktionen vor, jeweils eine für Bilder (RAD-16), sogenannte Presentation States (RAD-27), Befunde (RAD-27), Key Image Notes (RAD-31) und weitere Objekttypen (RAD-45). Genau genommen werden DICOM-Retrieve Dienste im Study Root Modell (optional: Patient Root) in der Variante C-MOVE benutzt. Es bestehen zudem Vorgaben, welche Bildtypen (CT, MR, usw.) mindestens unterstützt werden müssen. Unterstützte Bildtypen müssen durch einen Imaging Document Consumer auch angezeigt werden können. In der Regel sind diese DICOM-konformen Transaktionsvarianten einfacher für bestehende DICOM-Systeme zu implementieren, die für XDS-I entsprechend erweitert werden sollen.

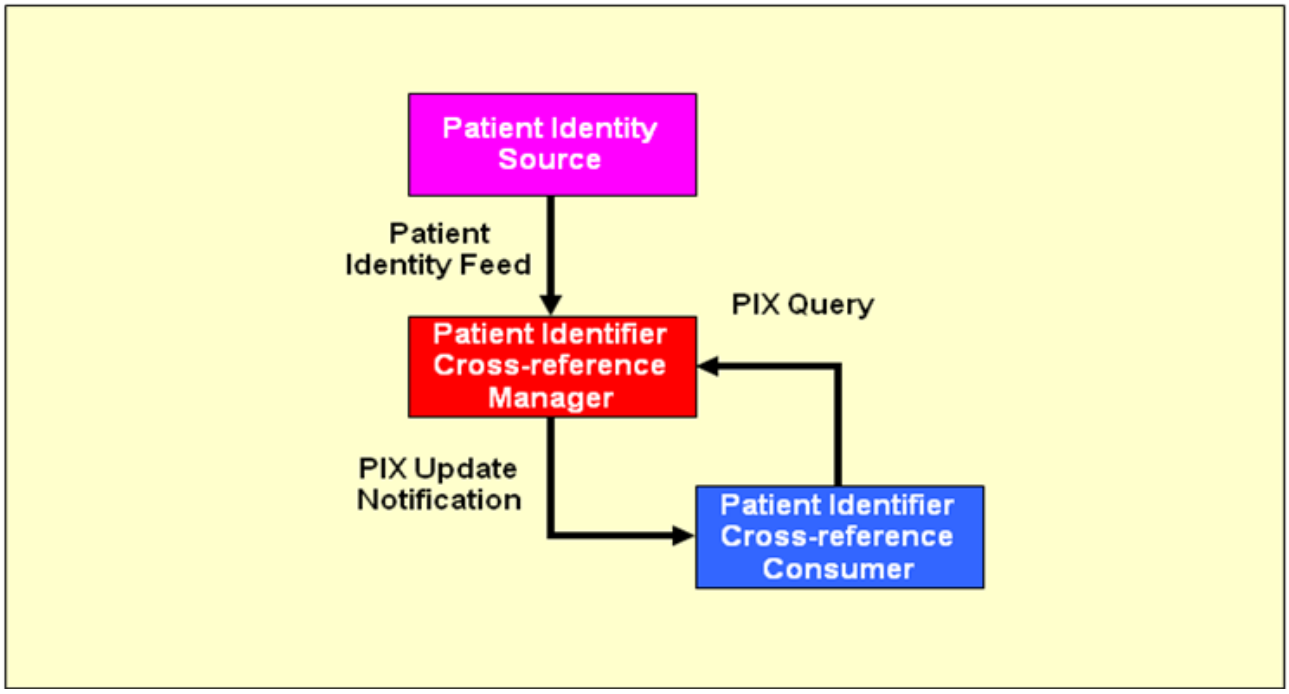
2.2.3 IHE XDS Metadata Update

Das IHE Profil XDS Metadata Update ist eine Ergänzung zum XDS.b Profil, welches das Verändern und Löschen von Metadaten in der Document Registry ermöglicht. Die zusätzlichen Transaktionen für das Verändern bzw. Löschen von Metadaten werden direkt von einem zusätzlichen Akteur, dem Document Administrator, initiiert und unmittelbar an die Document Registry gesendet. Die Transaktion Update Document Set \[ITI-57\] ermöglich die Veränderung der Metadaten von Dokumenten, Foldern oder Assoziationen sowie die Änderung des Verfügbarkeitsstatus dieser Objekte. Durch diese Transaktion kann auch die zentrale Patienten ID eines Dokuments oder Folders geändert werden, wodurch Dokumente und Folder auch anderen Patienten zugeordnet werden können. Mit der Transaktion Delete Document Set \[ITI-62\] können die Metadaten beliebiger Objekte gelöscht werden. Die Löschung ist nicht nur eine Statusänderung von Metadaten, sondern das permanente Entfernen, das nicht rückgängig gemacht werden kann.



2.2.4 IHE Patient Identifier Cross-referencing (PIX)

Das IHE-Profil Patient Identifier Cross-referencing (PIX) ermöglicht die Verknüpfung von Patientenkennungen in einem Netzwerk von Einrichtungen, die für einen Patienten jeweils eigene Kennungen vergeben. Dafür werden dem sogenannten Patient Identifier Cross-reference Manager (PIX Manager) demographische Patientendaten und IDs übergeben. Der PIX Manager verlinkt dann die Einträge für gleiche Patienten aus unterschiedlichen Einrichtungen. Ein System, welches als Patient Identifier Cross-reference Consumer agiert, kann sich die Verknüpfungen entweder beim PIX Manager mit Hilfe einer bekannten ID aktiv anfragen oder (optional) sich darüber informieren lassen. Das PIX-Profil stellt damit eine Grundlage für den einrichtungsübergreifenden Dokumenten- und Bildaustausch auf Basis von XDS.b und XDS-I.b dar, da über dieses Profil die Daten aus unterschiedlichen Einrichtungen mit unterschiedlichen IDs für einen Patienten zusammengeführt werden können.



In der Praxis fungiert der PIX Manager in der Regel als Master Patient Index und stellt eine in der XDS Affinity Domain eindeutige Master Patient ID, die sogenannte XAD-Pid zu Verfügung. Durch diese Verbindung von PIX Manager und XDS.b Patient Identity Source wird die Zuordnung lokal verwendeter Patientenkennungen zur einrichtungsübergreifend eindeutigen Master Patient ID möglich. Diese Master Patient ID kann in weiterer Folge zu Suche und Abruf von Dokumenten und radiologischen Bildern, sowie zur domänenweiten Protokollierung verwendet werden (siehe auch XDS.b).

Der PIX Manager erlaubt somit die Verwendung einer lokalen, in einer Einrichtung verwendeten Patienten-ID sowohl

1. zum Abruf der Master Patient ID, als auch
2. zum Abruf, der in den anderen Einrichtungen verwendeten lokalen Patienten-IDs

Jeder Patient wird im PIX Manager als eine Patientenidentität gespeichert, die demographische Daten des Patienten, die Master Patient ID, sowie dessen lokale IDs enthält. Der PIX Manager verknüpft mehrere lokale Patienten IDs, die von unterschiedlichen Einrichtungen zu einer Patientenidentität gemeldet wurden miteinander und bildet somit zusammen mit der Master Patient ID eine Linkgruppe. Die Bildung der Linkgruppe (die Erkennung, dass es sich bei den gemeldeten lokalen Patientenidentitäten um denselben physischen Patienten handelt) erfolgt anhand der demographischen Daten wie z.B. Vorname, Nachname, Versicherungsnummer, Geburtsdatum und Geschlecht.

Die vom PIX-Manager erzeugte XAD-PID kann in den Szenarien verwendet werden, wenn die beteiligten Einrichtungen Zugriff auf denselben PIX-Manager haben.

Die IHE bietet 2 Versionen des PIX Profiles an, die sich auf die Schnittstellen beziehen. PIX ohne Versionszusatz bezeichnet HL7v2 Schnittstellen, PIXv3 bezeichnet HL7v3 Schnittstellen. Für die Transaktion Patient Identity Feed lauten die Transaktionskennungen ITI-8 (HL7v2) und ITI-44 (HL7v3). Für die PIX Query lauten die Transaktionskennungen ITI-9 (HL7v2) und ITI-45 (HL7v3). Für die Auswahl des entsprechenden Profils (HL7v2 oder HL7v3) im Rahmen der Umsetzung sollten folgende Aspekte berücksichtigt werden. Für die einrichtungsinterne Kommunikation (Patient Identity Source – Document Source / Document Consumer) können die heute von vielen Systemen unterstützten HL7v2-Schnittstellen eingesetzt werden. Für die einrichtungsübergreifende Kommunikation (Patient Identity Source / Document Source / Document Consumer – PIX Manager) sollten die auf Webservices basierenden HL7v3 Schnittstellen eingesetzt werden, was folgende Vorteile bringt:

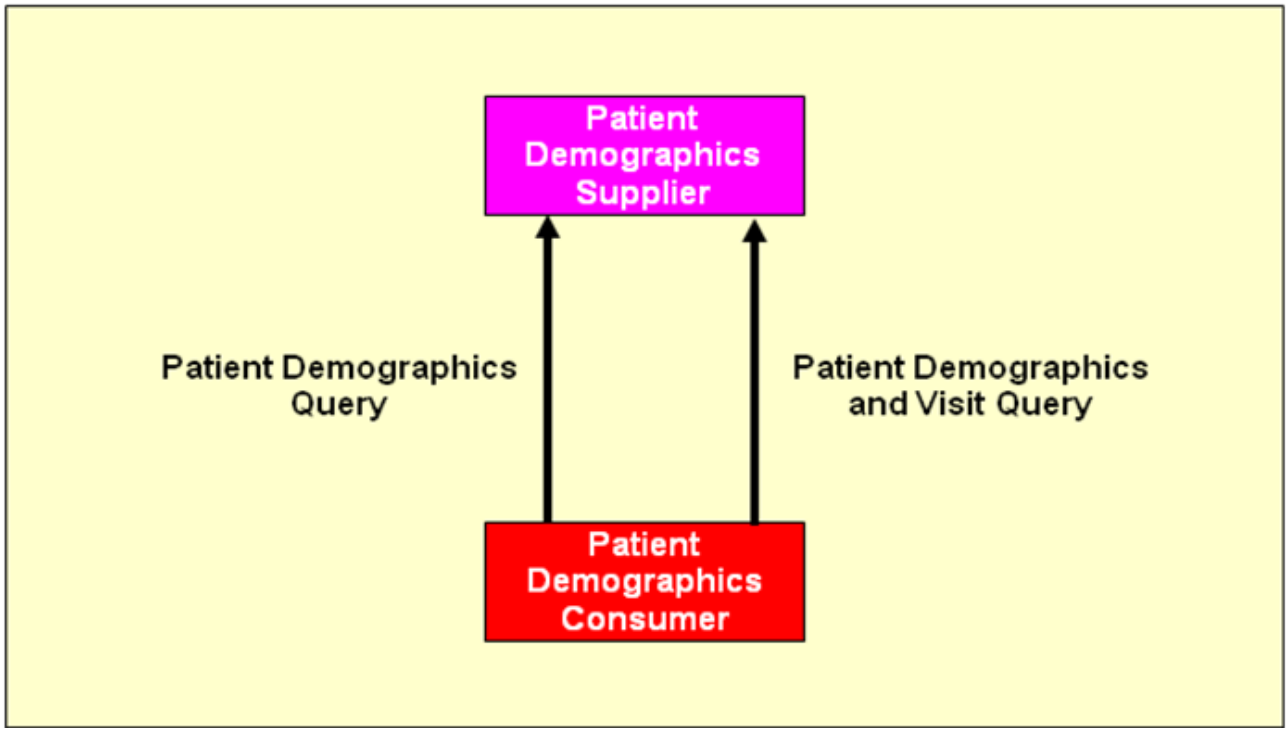
- Netzwerk und Firewall: Webservices verwenden Standard HTTP(s) Ports und keine TCP Socket Verbindungen wie bei HL7v2
- Die Verschlüsselung über HTTP(s) ist einfacher umzusetzen als für HL7v2 Nachrichten (wird von gängigen Applicationservern unterstützt).
- Security Token für das Berechtigungssystem können im Soap Header der Webservice Nachricht integriert werden. Für HL7v2 stehen diese Möglichkeiten nicht zur Verfügung.

2.2.5 Patient Demographics Query (PDQ)

Das IHE-Profil Patient Demographics Query (PDQ) ermöglicht die Abfrage von Patienten und deren demographischen Informationen und Kennungen. Die Abfrage durch den Patient Demographics Consumer erfolgt nicht wie bei PIX auf Basis von IDs, sondern auf Basis von demographischen Daten wie z.B. Vorname, Nachname oder Geburtsdatum.

Der Patient Demographics Supplier ist in der Praxis oft mit dem PIX Manager verknüpft und sie verwenden den gleichen Datenbestand. Der PDQ Supplier ermöglicht über unterschiedliche Suchalgorithmen exakte Suche, Wildcard Suche, sowie phonetische Suche. Als Ergebnis werden im Gegensatz zum PIX Trefferlisten zurückgegeben. Um ein sogenanntes „Patientensurfing" (Wildcardsuche nach Suchkriterien, die auf eine Vielzahl oder auf alle gespeicherten Patienten zutreffen) zu vermeiden, sollte die maximale Trefferanzahl eingeschränkt werden. Übersteigt das erwartete Ergebnis dieses Limit, erfolgt eine Fehlermeldung mit dem entsprechenden Hinweis die Suchkriterien einzuschränken.

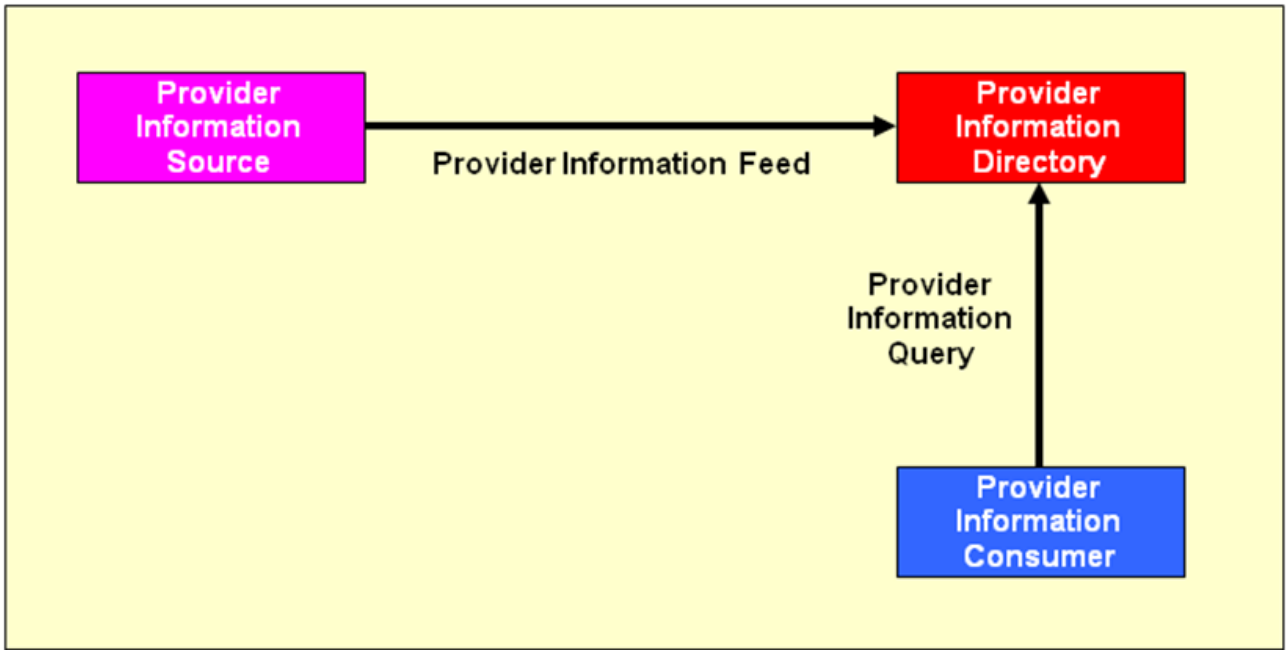
Die IHE bietet 2 Versionen des PDQ Profiles an, die sich auf die Schnittstellen beziehen. PDQ ohne Versionszusatz bezeichnet HL7v2 Schnittstellen \[ITI-21\], PDQv3 bezeichnet HL7v3 Schnittstellen \[ITI-47\]. Für den Einsatz der HL7v2 oder HL7v3 Transaktien gilt die gleiche Argumentation wie für das PIX Profil.



2.2.6 Healthcare Provider Directory (HPD)

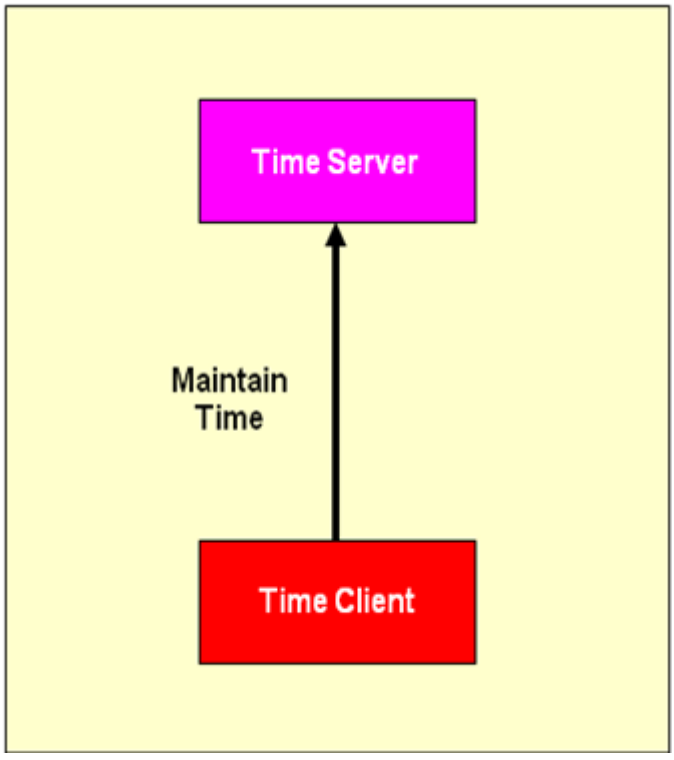
Das IHE-Profil Healthcare Provider Directory (HPD) ermöglicht die Verwaltung und Abfrage eines Verzeichnisses mit Informationen zu Leistungserbringern im Gesundheitswesen, die im Weiteren kurz als Provider bezeichnet werden. Dabei wird im Profil zwischen Organisationen (z.B. Krankenhäuser, Arztpraxen etc.) und den Personen (Ärzte, Krankenschwestern, etc.) selbst unterschieden. Typische Informationen eines Providers sind Name, Adresse und Fachbereich aber auch Informationen zur elektronischen Kommunikation wie IDs, Emailadressen oder Zertifikate können gespeichert und zur Verfügung gestellt werden. Die Providerinformationen können durch die Provider Information Source oder auch durch einen direkten Zugang zum Provider Information Directory zur Verfügung gestellt werden. Die Transaktion Provider Information Feed ermöglicht es Providerinformationen hinzuzufügen, zu ändern oder zu löschen. Die Abfrage der Informationen erfolgt über die Transaktion Provider Information Query \[ITI-58\] durch den Provider Information Consumer (siehe nachfolgende Abbildung).

Im Provider Information Directory können auch strukturelle Beziehungen der Provider zueinander abgebildet werden. Unter einer Wurzelorganisation wie z.B. einem Integrierten Versorgungsnetz können verschiedene weitere Organisationen wie z.B. Krankenhäuser oder Arztpraxen angeordnet sein. Die Krankenhäuser selbst können wiederum z.B. aus Fachabteilungen bestehen. Zu jeder der Organisationen können die im Versorgungsnetz handelnden Personen wie z.B. Ärzte mit ihren Informationen gespeichert werden, so dass flexibel auch komplexe Organisationsstrukturen abgebildet werden können.



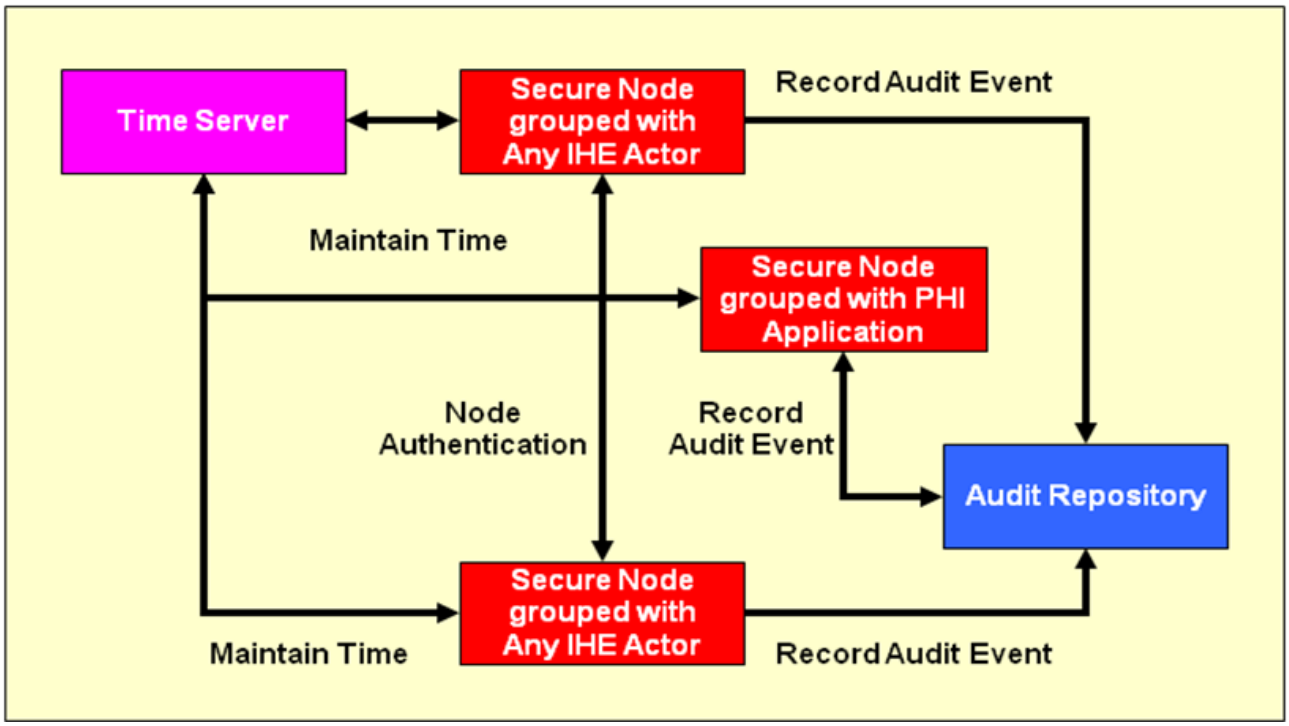
2.2.7 IHE Consistent Time (CT)

Das IHE-Profil Consistent Time (CT) dient der Synchronisierung der Systemzeit zwischen den kommunizierenden Systemen, um Probleme zu verhindern, die inkonsistente Zeitangaben bei der Kommunikation verursachen können. CT bildet damit die Voraussetzung für praktisch jedes andere IHE Profil. Es definiert die Verwendung des Network Time Protocol (NTP), welches in RFC 1305 definiert ist.



2.2.8 IHE Audit Trail and Node Authentication (ATNA)

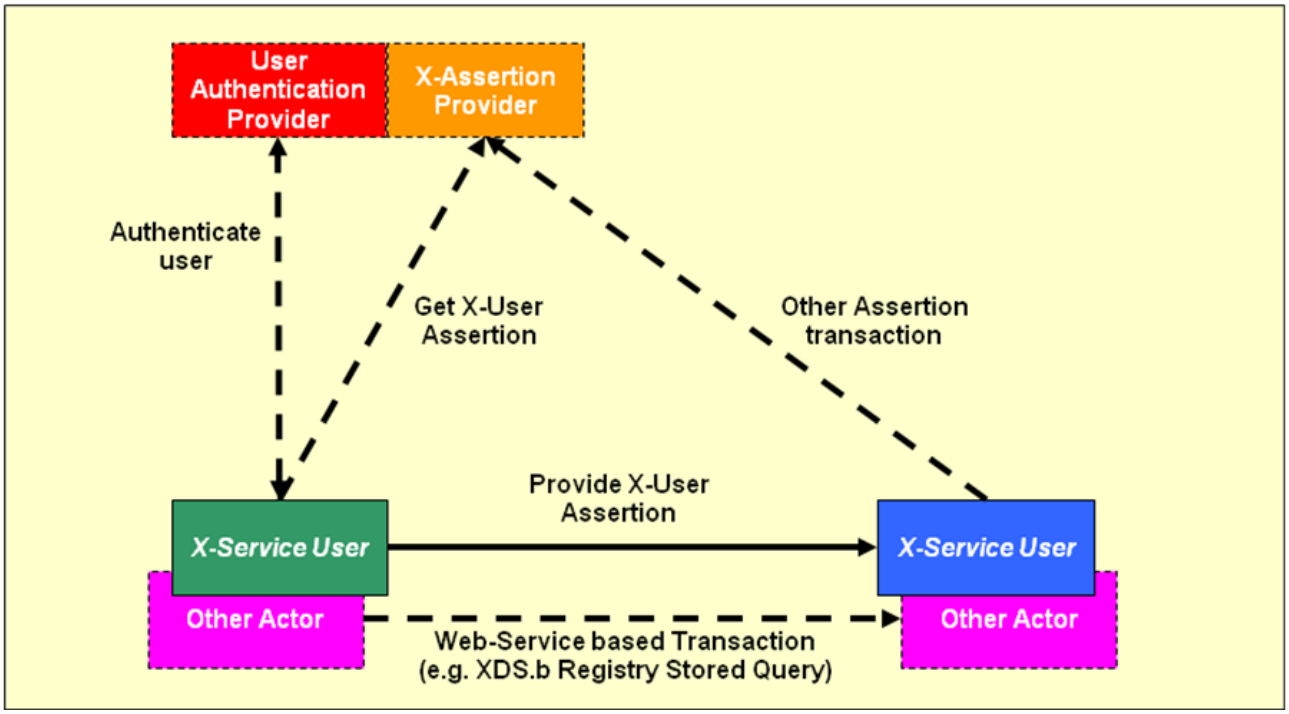
Das IHE-Profil Audit Trail and Node Authentication (ATNA) definiert die grundlegenden Sicherheitsanforderungen an die in einem Netzwerk kommunizierenden Systeme und wird von XDS.b als Sicherheitsinfrastruktur vorausgesetzt. Im Zusammenhang mit der Auditierung von Zugriffen auf Patientendaten werden die zu protokollierenden Ereignisse, das Format der Audit-Informationen sowie die Kommunikation mit einem zentralen Audit Repository zu Speicherung aller Audit-Informationen in einem Netzwerk definiert. Darüber hinaus spezifiziert ATNA die bidirektionale, zertifikatsbasierte Authentifizierung der kommunizierenden Systeme und ermöglicht die Transportverschlüsselung. Gemäß ATNA obliegt die Authentifizierung der Benutzer den Systemen selbst und für die systemübergreifende Authentifizierung von Benutzern wird auf andere IHE-Profile verwiesen. Nähere Informationen zu ATNA finden sich im IHE Technical Framework des Bereiches IT-Infrastruktur.



2.2.9 Cross-Enterprise User Assertion (XUA)

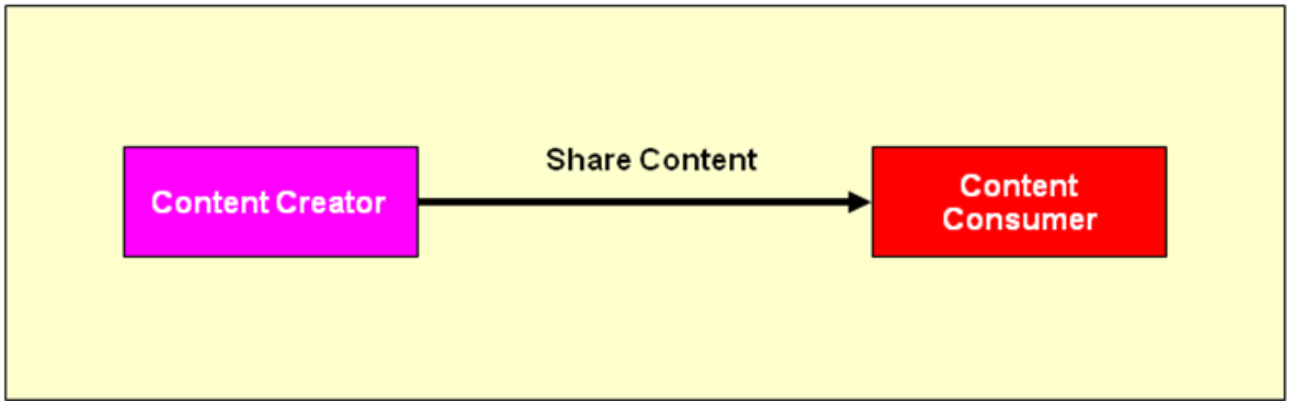
Das IHE-Profil Cross-Enterprise User Assertion (XUA) gibt die Möglichkeit, Informationen über authentifizierte Benutzer (Personen, Systeme, Anwendungen) über Einrichtungsgrenzen hinweg sicher zu kommunizieren. Dadurch können sich Benutzer innerhalb einer Einrichtung gegenüber ihrem Anwendungssystem oder einer zentralen Benutzerverwaltung authentifizieren und diese Informationen können im Rahmen der einrichtungsübergreifenden Kommunikation mit versendet werden, um im anderen System Berechtigungen oder Protokollierungen vornehmen zu können. Das XUA Profil basiert auf Webservice Security Standards und bildet ein Profil für SAML 2.0 Identity Assertions. Da über XUA neben der Identität eines Benutzers zwar auch weitere Attribute übertragen werden können, diese aber nicht festgelegt sind, wurde ergänzend das IHE Profil XUA++ spezifiziert. In XUA++ ist festgelegt, wie folgende zusätzliche Attribute übertragen werden können:

- Organisation,
- Rolle,
- Einwilligung,
- Patienten-ID,
- Verwendungszweck.



2.2.10 IHE Basic Patient Privacy Consents (BPPC)

Das IHE Profil Basic Patient Privacy Consents (BPPC) ermöglicht es, die Zustimmung des Patienten zum Austausch seiner personenbezogenen Daten (demographische Daten, medizinische Daten, Kontaktdaten, Versicherungsdaten etc.) in einem Netzwerk kooperierender Einrichtungen festzuhalten. BPPC setzt voraus, dass in einem Netzwerk mehrere vordefinierte Datenschutzrichtlinien (Privacy Policies) für den Zugriff auf Patienteninformationen existieren können und der Patient die Möglichkeit hat, aus diesen Richtlinien die zutreffenden auszuwählen und damit die Zugriffsmöglichkeiten auf seine Daten zu definieren. Die Einwilligungserklärung des Patienten (Basic Patient Privacy Acknowledgement Document) ist ein CDA-Dokument, welches die ID der gewählten Datenschutzrichtlinie und ggf. eine textuelle Beschreibung der Einwilligung enthält. Für Einwilligungserklärungen mit patientenspezifischen, strukturierten und kodierten Zugriffsregeln verweist BPPC auf andere Standards wie von HL7 oder OASIS und zukünftige IHE-Profile. Gemäß BPPC werden Datenschutzrichtlinien, welchen der Patient zugestimmt hat, von der entsprechenden Source bzw. vom Consumer der personenbezogenen Daten durchgesetzt, d.h. im Fall von XDS.b von der Document Source bzw. vom Document Consumer, die mit den Akteuren des BPPC Profils Content Creator bzw. Content Consumer zugeordnet sind (siehe nachfolgende Abbildung).



Für das Management von Einwilligungserklärungen selbst (d.h. Erstellen, Speichern, Ändern Abrufen etc.) kann wiederum eine XDS.b Infrastruktur eingesetzt werden. BPPC definiert das CDA-Dokument, dass die eigentliche Einwilligungserklärung darstellt, sowie die Abbildung auf XDS-Metadaten. Die Einwilligungserklärung kann über die IHE Transportprofile übertragen werden, die die XDS-Metadaten unterstützen (XDS, XDR, XDM, XCA), oder über ein beliebiges anderes Transportsprotokoll. BPPC geht von einer beschränkten Anzahl abzubildender Richtlinien aus. Die Einwilligungserklärung ist dem Patienten (und somit genau einer longitudinalen Patientenakte) zugeordnet, ohne weitere Strukturierungsebenen in der Dokumentensammlung eines Patienten zu berücksichtigen. Somit gilt die referenzierte Richtlinie (d.h. die Privacy Policy) für alle Dokumente ohne die Möglichkeit unterschiedliche Richtlinien für die vom Hausarzt eingestellten Dokumente und die vom Gynäkologen eingestellten Dokumente festzulegen. Eine so differenzierte, feingranulare Steuerung der Zugriffsrechte wäre nur durch eine exponentiell wachsende Anzahl an allumfassenden Privacy Policies möglich, in dem jede dieser Richtlinien die Zugriffsrechte jeden Teilnehmers auf die unterschiedlichen Dokumente ausdefiniert. Da BPPC aber keine Festlegungen trifft, wie Privacy Policies elektronisch und strukturiert (d.h. maschinenlesbar) definiert und transportiert werden können und da in BPPC alle Document Consumer und Sources für die Durchsetzung der Regeln verantwortlich sind, kann BPPC praktisch nicht mit einer großen Anzahl an Privacy Policies genutzt werden. Aufgrund dieser Einschränkungen ist BPPC grundsätzlich nur für eine grobgranulare Zugriffsteuerung geeignet.

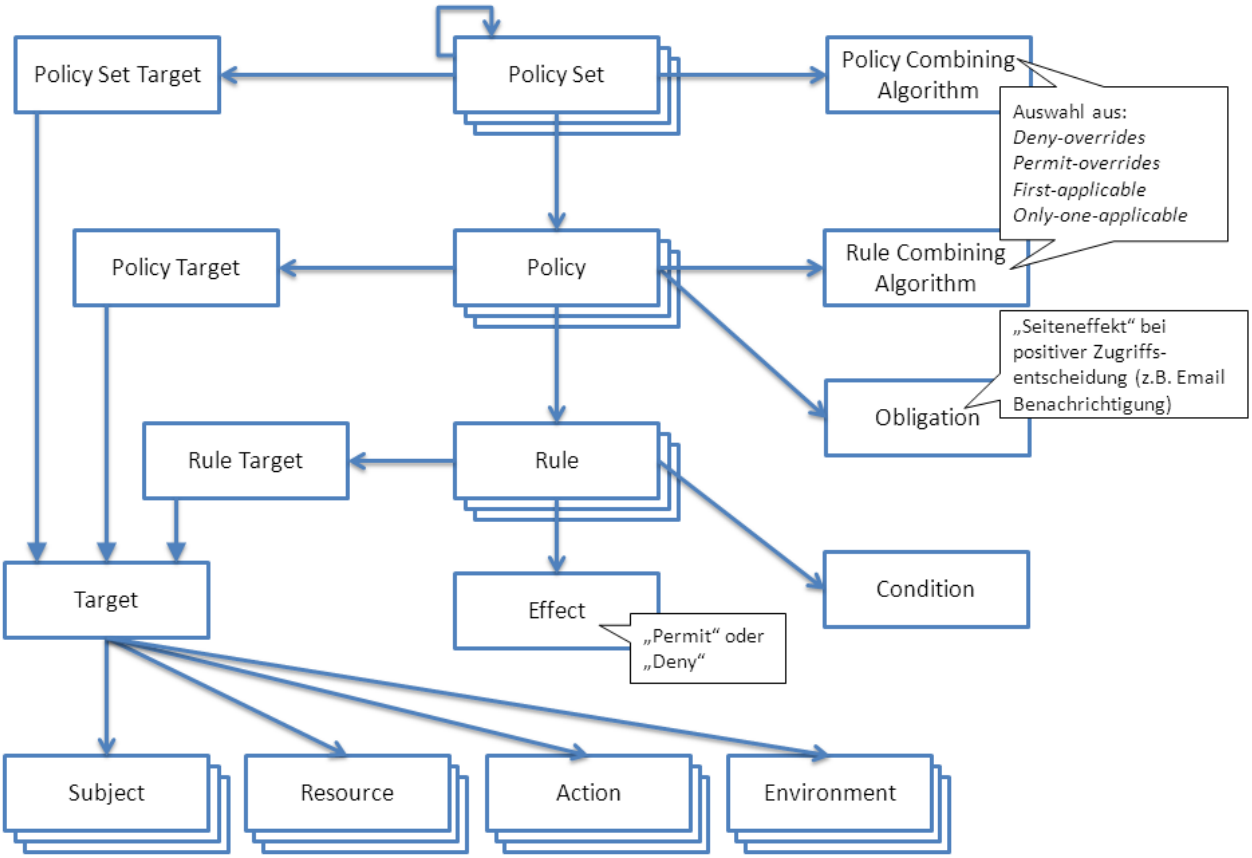
2.2.11 Extensible Access Control Markup Language (XACML)

Die Extensible Access Control Markup Language (XACML) ist ein XML-basierter OASIS Standard. Die letzte verabschiedete Version ist XACML 2.0. Dieser Standard bietet einerseits eine Sprache, mit der Policies, Authorisierungsanfragen und -antworten definiert werden können und andererseits ein (nicht-normatives) Kommunikationsmodell in dem verschiedene Akteure und Transaktionen vorgegeben werden. XACML spezifiziert außerdem, wie Policies interpretiert werden müssen, um eine Autorisierungsanfrage, beispielsweise einen Dokumentenzugriff, zu erlauben oder zu verbieten.

Ähnlich wie IHE Integrationsprofile legt XACML eine Reihe von abstrakten Akteuren fest, die in einem oder mehreren konkreten Systemen umgesetzt werden können. Die zwischen den Akteuren durchgeführten Transaktionen können prinzipiell über Bindings in verschiedene Kommunikationsprotokolle umgesetzt werden, praktisch ist aber ausschliesslich das Binding auf OASIS SAML standardisiert und verbreitet.

XACML sieht folgende Akteure vor: Der Policy Administration Point (PAP) ist für die Verwaltung der Policies zuständig. Dieser Akteur wird häufig mit einem Policy Repository kombiniert, das als persistenter Speicher für Policies zu verstehen ist. Der Policy Decicion Point (PDP) übernimmt die Evaluation von Anfragen, die Prüfung der Anfrage gegen die vorhandenen Policies und entscheidet über die Autorisierung. Der Policy Enforcement Point (PEP) ist schließlich für die Durchsetzung der Entscheidung des PDP verantwortlich. Es können ausserdem weitere Akteure wie ein Policy Information Point (PIP) und ein Context Handler zur Beschaffung weiterer Inputs für die Autorisierungsentscheidung eingesetzt werden, dies ist aber nicht in allen Situationen sinnvoll.

Die wichtigsten Strukturen in der Policy-Definitionssprache sind Policy Set, Policy und Rules. Ein Policy-Set besteht aus einer oder mehreren Policies, kann aber auch weitere Policy Sets referenzieren. Eine Policy besteht aus einer oder mehreren Regeln (Rules).



Sowohl Policy Sets, Policies als auch Rules beziehen sich auf genau ein Target. Anhand des Targets wird entschieden, ob dieses Objekt relevant für eine bestimmte Anfrage ist und somit genauer evaluiert werden muss. Targets haben Attribute aus folgenden vier Kategorien: Subject ("wer greift zu?"), Resource ("worauf wird zugegriffen?"), Action ("wie wird darauf zugegriffen?") und Environment ("unter welchen Umständen wird zugegriffen?"). Zum Beispiel kann eine Policy als Target definieren "Die folgenden Regeln gelten wenn Ärzte (Subject) auf die longitudinale Akte von Patient X (Resource) lesend (Action) im April 2012 (Environment) zugreifen". Das Target wird mit den Attributen der Anfrage abgeglichen. In diesem Beispiel würde bei einem Target Match die unterhalb dieser Policy definierten Rules als relevant angesehen werden und somit tiefergehend evaluiert werden.

Die einzelnen Regeln haben ausser einer eigenen Target Definition auch noch einen Effect und ggf. Conditions. Conditions sind Statements über Attribute die bei der Evaluation entweder "true" oder "false" (oder auch "indeterminate") zurückgeben. Der Effect beschreibt welche Entscheidung, d.h. "permit" (erlaubt) oder "deny" (verboten), aus dieser Regel resultiert wenn das Target zutrifft und die Condition "true" ergibt. Da bei einer Autorisierungsentscheidung mehrere Rules ein relevantes Target haben können, gibt es die sogenannten "Rule Combining Algorithms" die dafür zuständig sind, die häufig unterschiedlichen Resultate der zutreffenden Regeln zu einem Gesamtergebnis für die Policy zu kombinieren. Ebenso gibt es pro Policy Set einen "Policy Combining Algorithm", der die Ergebnisse der einzelnen Policies zu einem Gesamtergebnis für das Policy Set kombiniert. Folgende Algorithmen stehen für die Kombination von Policy Ergebnissen sowie die Kombination von Regel Ergebnissen zur Verfügung: Permit-override ("solange mindestens einer 'erlaubt' sagt, ist das Gesamtergebnis 'erlaubt'"), Deny-override ("solange mindestens einer 'verboten' sagt, ist das Gesamtergebnis 'verboten'"), First-applicable ("das erste richtige Ergebnis zählt als Gesamtergebnis"), Only-one-applicable ("wenn genau eine Regel/Policy zutraf ist ihr Ergebnis das Gesamtergebnis, ansonsten gibt es kein Gesamtergebnis").

Obligations sind die Actions, die der PEP in Verbindung mit dem Enforcement einer Autorisierungsentscheidung ausführen muss. Dies kann beispielsweise die Protokollierung der Transaktion sein. Nach der Evaluation einer Policy werden Obligations an den PEP gesendet. Er ist verpflichtet, diese Actions zusammen mit dem Enforcement auszuführen. Es gibt in XACML 2.0 keine Standard Obligations, d.h. die Definition von durchzuführenden Aktionen und die dafür notwendigen Daten müssen zwischen dem Policy Autor und dem PEP abgestimmt sein.

2.2.12 Security Assertion Markup Language (SAML)

Die Security Assertion Markup Language (SAML) ist wie XACML ein XML-basierter OASIS Standard und liegt mittlerweile in Version 2 vor. Sie bietet Mechanismen, wie Authenfizierungs- und Autorisierungsentscheidungen transportiert und ausgetauscht werden können. Im Gegensatz dazu liefert XACML die Werkzeuge eine solche Entscheidung herbeizuführen.

Die SAML-Spezifikation besteht aus insgesamt vier Teilen von denen vor allem die folgenden beiden für den Architekturteil des Cookbooks von Bedeutung sind: Assertions and Protocol beschreibt die Syntax und die Semantik von XML-basierten Assertions (Zusicherungen) sowie der Request- und der Response-Protokolle. Bindings and Profiles beinhaltet das Mapping dieser Protokolle auf Transportprotokolle wie z.B. SOAP über HTTP oder SOAP über FTP.

Assertions beinalten Informationen über die Authentifizierung eines Subjektes, seine Attribute und die Autorisierunsentscheidung, ob das Subjekt bestimmte Ressourcen zugreifen darf. Demnach gibt es drei Typen von Assertions: Authentication, Attribute und Authorization decision. Das SAML Request- und Resonse-Protokoll definiert ein Standardnachrichtenformat, um die Assertions zutransportieren (vgl. \[[2-]\]).

Ein Mapping der XACML und SAML Authorization Request Query und Response sind im SAML 2.0 Profile of XACML beschrieben. Es werden dort sechs Anfragetypen definiert:

- XACMLPolicyQuery: SAML Request to a PAP for Policies
- XACMLPolicyStatement: SAML Statement containing policies
- XACMLAttribute Query: SAML Request to Attribute Authority for user attributes
- XACMLAttribute Statement: SAML Statement containing one or more attributes
- XACMLAuthzDecisionQuery: SAML Request from PEP to PDP for Authorization Decision
- XACMLAuthzDecisionStatement: SAML Statement containing one or more Authorization Decisions

2.3 Typen einrichtungsübergreifender elektronischer Patientenakten

Im Gesundheitswesen haben sich drei elektronische Aktentypen herausgebildet, die die Unterstützung der einrichtungs- und sektorübergreifenden Kommunikation zum Ziel haben. Das Urkonzept für solche Akten stellt die sogenannte einrichtungsübergreifende, elektronische Patientenakte (eEPA) dar. Darauf aufbauend haben sich zwei Spezialisierungen gebildet: Die persönliche, einrichtungsübergreifende, elektronische Patientenakte (PEPA) und die fallbezogene, einrichtungsübergreifende, elektronische Patientenakte (EFA). Alle im Kapitel Use-Cases skizzierten Anwendungsfälle können mithilfe von Architekturen für die drei genannten Aktentypen abgebildet werden. Nachfolgend werden zunächst die drei Aktentypen definiert:

2.3.1 Einrichtungsübergreifende elektronische Patientenakte

Die einrichtungsübergreifende elektronische Patientenakte (engl. Electronic Health Record) führt Untermengen von elektronischen Dokumentensammlungen elektronischer Patientenakten (EPA) verschiedener Einrichtungen zu einer einrichtungsübergreifenden, longitudinalen Patientenakte zusammen. Eine eEPA dient dem Austausch der medizinischen Dokumentation des an der Behandlung beteiligten Personals verschiedener Einrichtungen. Sie ist eine arztgeführte Akte. Der Patient erteilt in der Regel für die beteiligten Einrichtungen jeweils eine Einwilligung zur Nutzung der Akte.

2.3.2 Persönliche einrichtungsübergreifende elektronische Patientenakte

Eine Persönliche, Einrichtungsübergreifende, Elektronische Patientenakte (PEPA) oder engl. Personal Electronic Healthrecord (PEHR) ist eine longitudinale Sammlung von medizinischen Inhalten, die entweder vom Patienten selbst oder über standardisierte Schnittstellen aus den Primärsystemen von Gesundheitsdiensteanbietern in die Akte übermittelt werden. Dabei spielt die Wahrung der informationellen Selbstbestimmung der Patienten/Bürger eine entscheidende Rolle. Sie wird dadurch gewahrt, dass zum einen die Steuerung der Berechtigungen alleine durch den Patienten oder einem von ihm Bevollmächtigten erfolgt. Zum anderen können Gesundheitsdiensteanbieter die eingestellten Informationen nur über ein dafür vorgesehenes Ärzteportal einsehen, ohne die Inhalte über einen standardisierten Rückkanal in ihre Primärsysteme zu übernehmen. Zum einen hat der Patient/Bürger so stets die volle Kontrolle, wer auf welche Gesundheitsinformationen Zugriff hat und hatte. Zum anderen ist so gewährleistet, dass das Recht auf Vergessen, also die Löschung aller Daten in seiner Akte möglich ist.

2.3.3 Fallbezogene einrichtungsübergreifende elektronische Patientenakte

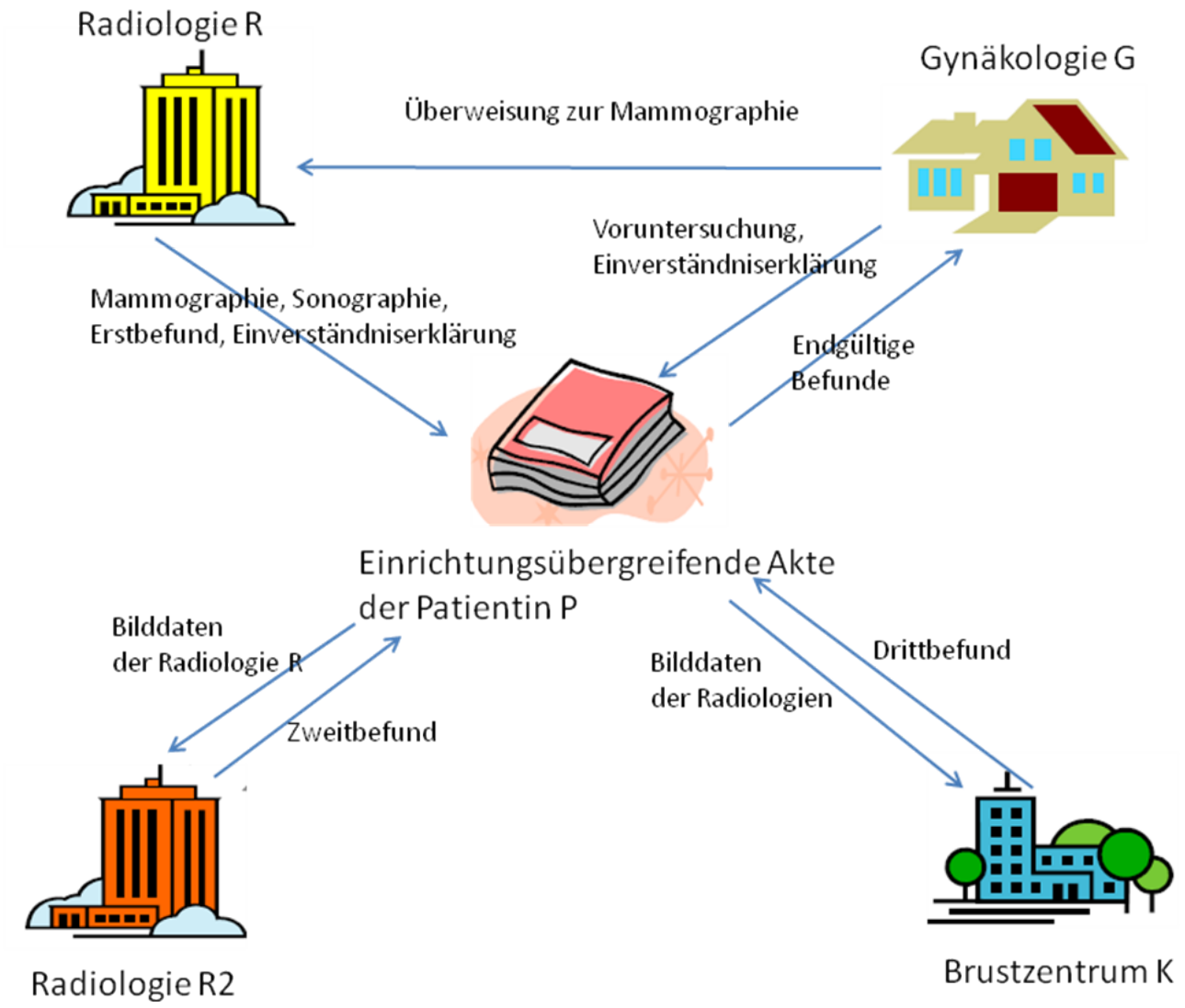
Die fallbezogene, einrichtungsübergreifende, elektronische Patientenakte (EFA) ist eine auf einen medizinischen Fall beschränkte Sonderform einer einrichtungsübergreifenden, elektronischen Patientenakte. Sie beschränkt sich auf die einrichtungsübergreifende Zusammenführung von Dokumenten eines Patienten zu einem bestimmten Zweck. Die Zweckgebundenheit ist in der Regel eine bestimmte Diagnose bzw. ein konkreter Behandlungsfall. (Aber auch ein Behandlungsvertrag fällt darunter.) Die hier beschriebene Akte ist eine arztgeführte Akte. Die Beteiligung des Patienten beruht auf einer einmaligen Einwilligung des Patienten für die behandelnden Ärzte und Einrichtungen. Bei der beschriebenen Variante werden fachliche Rahmenbedingungen und Konzepte verwendet, die sich auch so zu großen Teilen in den Definitionen des eFA-Vereins (einen Zusammenschluss von unterschiedlichen Partnern aus dem Gesundheitswesen) und der Industrie wiederfinden, allerdings bezieht sich dies nicht auf technische Konzepte und Umsetzungen.

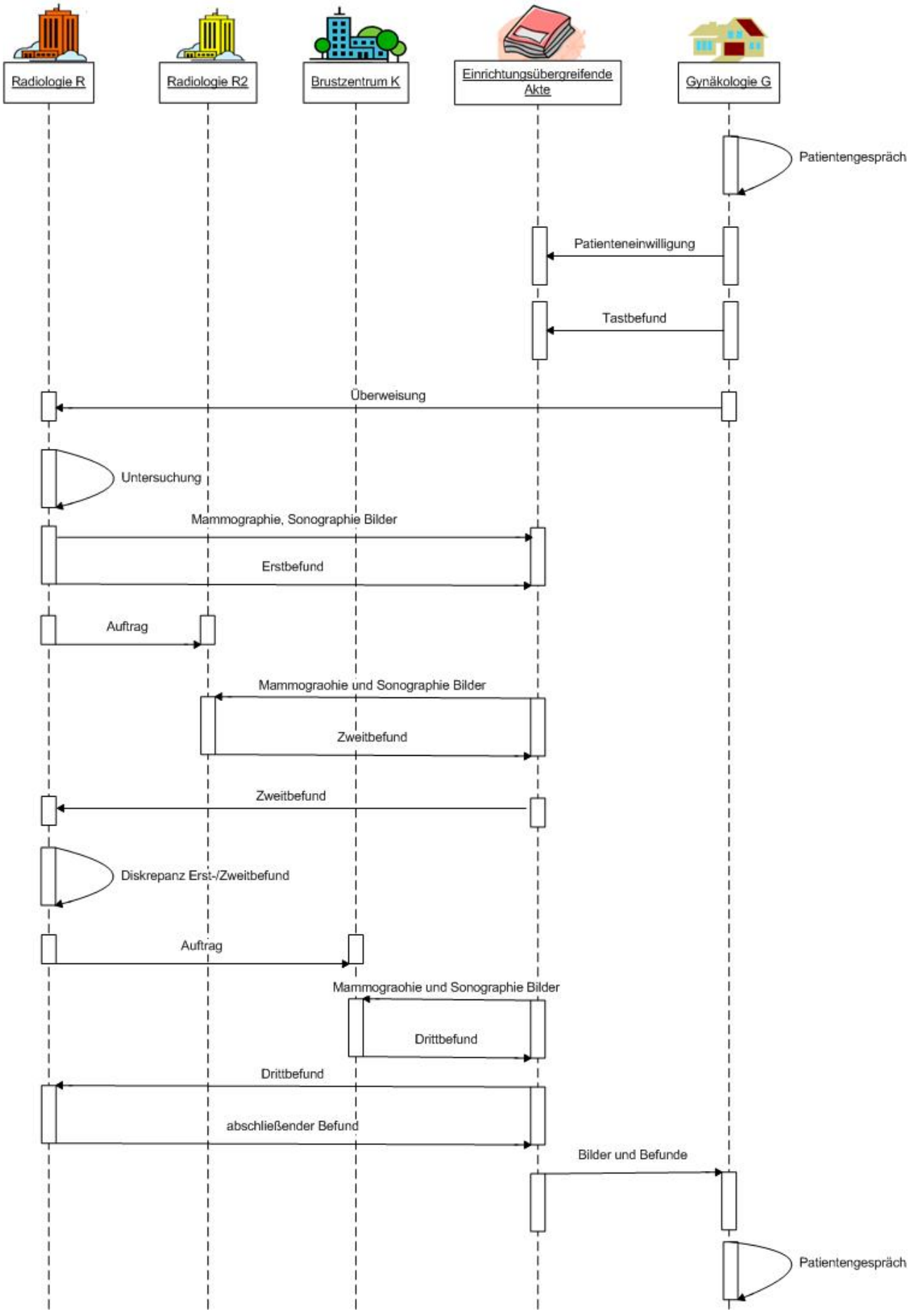
3 Anwendungsszenarien

Dieses Kapitel beschreibt exemplarisch 3 Anwendungsszenarien, die einen einrichtungsübergreifenden Austausch von medizinischen Dokumenten zwischen verschiedenen Akteuren im Gesundheitswesen erfordern. Durch diese Anwendungsszenarien werden auch die Anforderungen bzgl. des Arbeitsablaufs und der notwendigen Berechtigungen beschrieben und bilden damit die Basis der erarbeiteten Lösungsansätze in den folgenden Kapiteln.

3.1 Mamma-Diagnostik

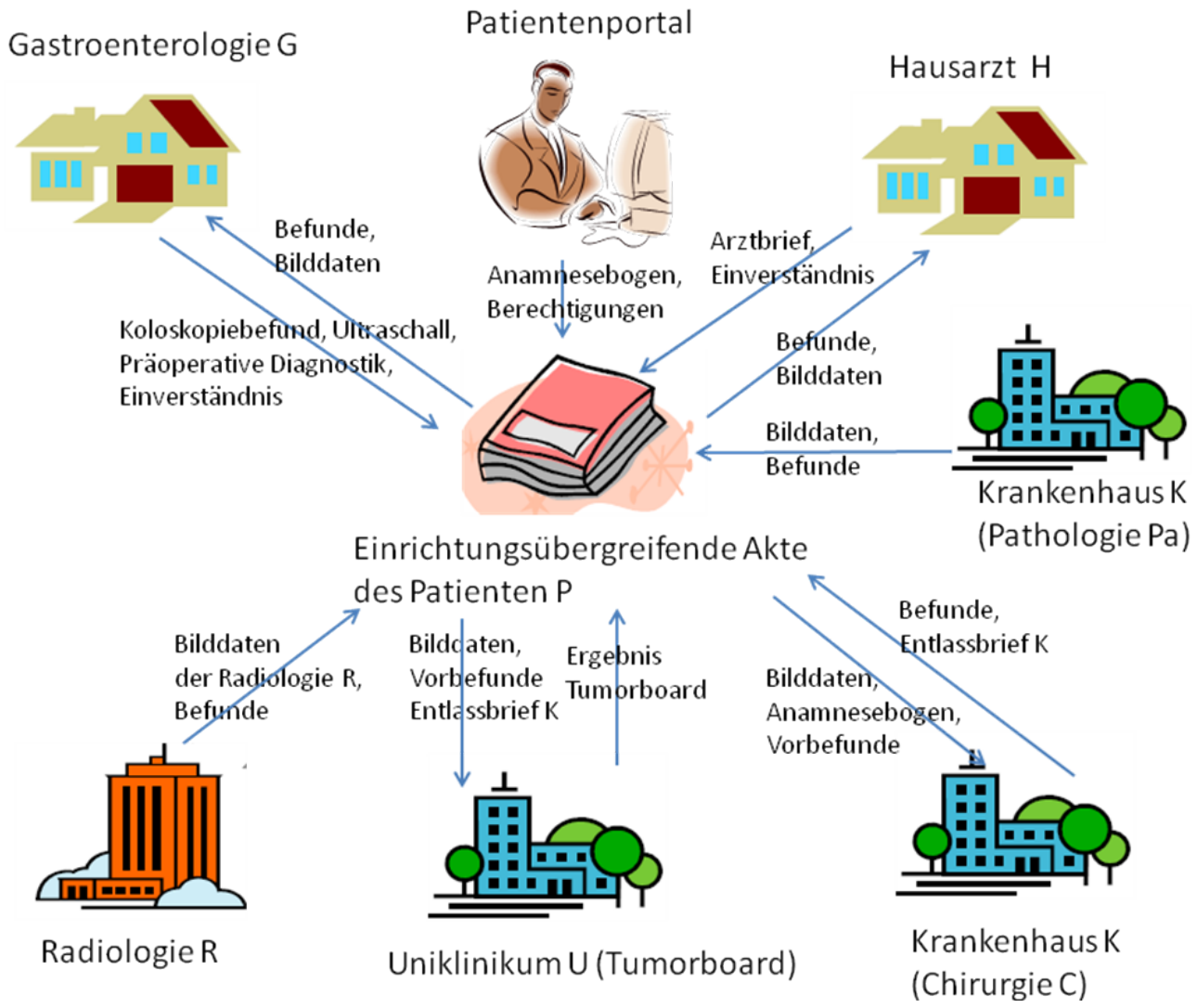
Im Radiologieverbund „Grüne Heide" sind verschiedene Organisationen zusammengeschlossen, die im Rahmen von Verträgen zur Integrierten Versorgung (IV-Verträge) Patienten aus der Region gemeinsam behandeln. Im vorliegenden Fall begleiten wir die Behandlung von Patientin P (42 Jahre). Frau P ertastet bei der morgendlichen Toilette eine leichte Veränderung ihrer linken Brust und vereinbart noch am selben Tage einen Termin bei ihrer Gynäkologin, Frau Dr. G. Frau Dr. G verfügt über kein Mammographiegerät und entscheidet nach eingehender Untersuchung die weitere diagnostische Abklärung durch einen dem Radiologieverbund angeschlossenen niedergelassenen Radiologen, Herrn Dr. R. Frau P gibt Frau Dr. G ihr Einverständnis für die digitale Weitergabe der bisherigen Untersuchungsdaten an die Radiologie R. Daraufhin legt Frau Dr. G für Frau P eine einrichtungsübergreifende elektronische Akte an und stellt über diese dem Radiologen R die Daten von Frau P zur Verfügung. Herr Dr. R führt eine digitale Mammographie zusammen mit einer Ultraschalluntersuchung durch und stellt in der linken Brust von Frau P Veränderungen fest. Da Herr Dr. R an einem Projekt seiner KV zur qualitätsgesicherten Mamma-Diagnostik teilnimmt, wird nach Einverständniserklärung von Frau P zur Projektteilnahme eine unabhängige Zweitbefundung durch eine andere Radiologie R2 des Verbundes durchgeführt. Die Radiologie R2 hat dabei zwar Zugriff auf die Bilddaten der Radiologie R, aber nicht auf den Befund. Der Zweitbefund bestätigt den Befund von Dr. R nicht, worauf eine Drittbefundung notwendig wird, die das Brustzentrum des örtlichen Krankenhauses K durchführt. Herr Dr. R teilt dies Frau P mit, die ihre Einverständniserklärung für eine weitere Befundung auf das Brustzentrum K ausdehnt. Im Brustzentrum werden die Bilddaten von Frau P nochmals begutachtet, wobei sich der Anfangsverdacht auf krankhafte Veränderungen ausschließen lässt. Das Brustzentrum empfiehlt eine Wiederholung der Untersuchung in einem halben Jahr. Frau P besucht erneut ihre Gynäkologin, welche ihr die Ergebnisse erläutert. Da Frau P weder die Radiologie R2 noch das Brustzentrum K kennt und will, dass ausschließlich ihr bekannte Personen, denen sie vertraut, Zugriff auf ihre Daten haben, schränkt sie für die Radiologie R2 und das Brustzentrum K die entsprechenden Zugriffsrechte ein. Bei der Wiedervorstellung der Patientin und der erneuten Mammographie in der Radiologie R nach einem halben Jahr werden keinerlei Veränderungen zur Erstuntersuchung festgestellt und Frau P kann in den normalen Prozess der Vorsorgeuntersuchungen zurückgeführt werden. Einige Jahre später zieht Frau P um und kann daher das Angebot der einrichtungsübergreifenden Akte des Radiologieverbundes "Grüne Heide" nicht mehr nutzen. Aus diesem Grunde löscht sie ihre von Frau Dr. G angelegte Akte.

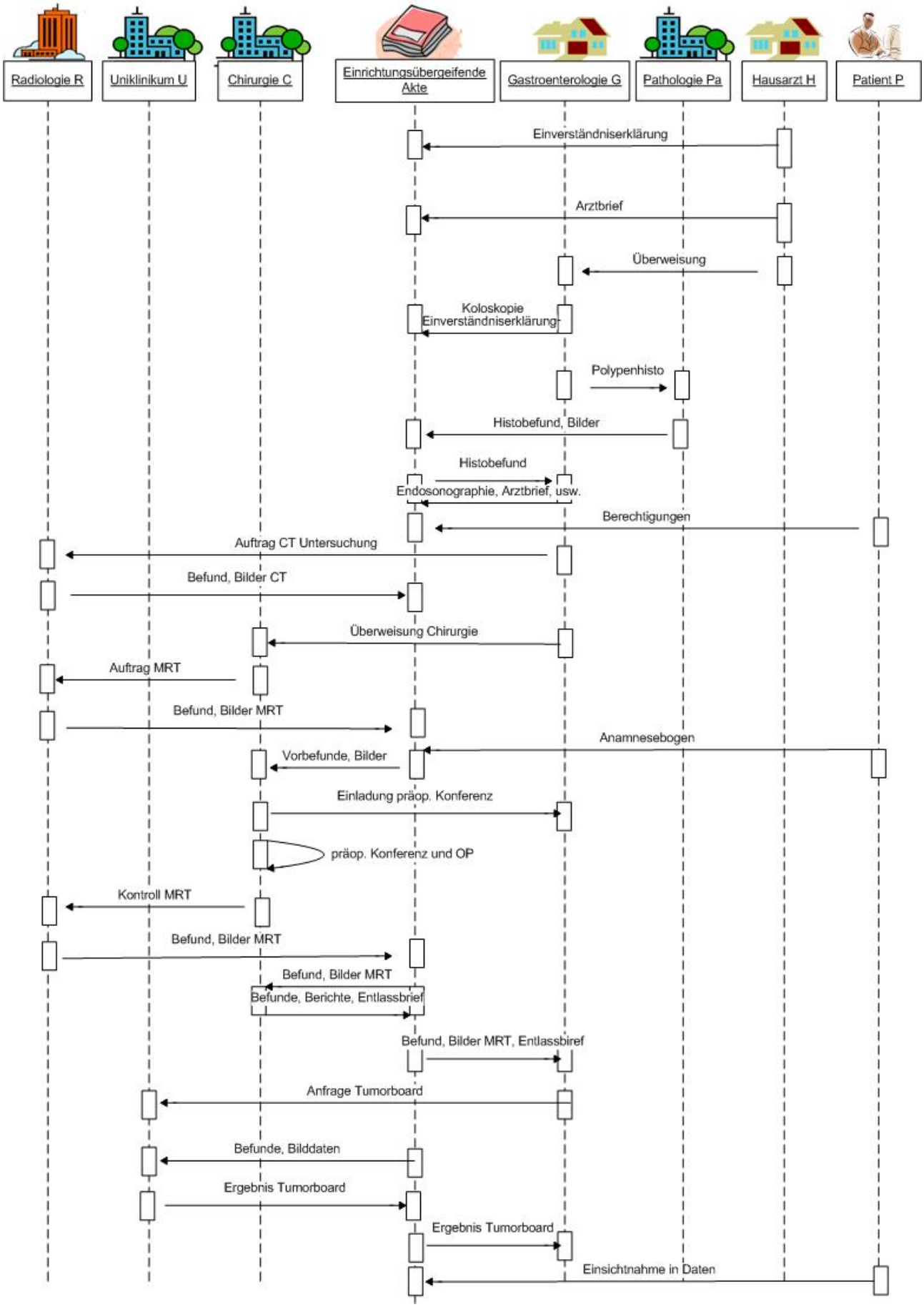

Radiologie R
Gynäkologie G
Überweisung zur Mammographie
Voruntersuchung,
Einverständniserklärung
Mammographie, Sonographie,
Erstbefund, Einverständniserklärung
Endgültige
Befunde
Einrichtungsübergreifende Akte
der Patientin P
Bilddaten
der Radiologie R
Zweitbefund
Bilddaten
der Radiologien
Drittbefund
Radiologie R2
Brustzentrum K


Radiologie R
Radiologie R2
Brustzentrum K
Einrichtungsübergreifende Akte
Gynäkologie G
Patientengespräch
Patienteneinwilligung
Tastbefund
Überweisung
Untersuchung
Mammographie, Sonographie Bilder
Erstbefund
Auftrag
Mammograohie und Sonographie Bilder
Zweitbefund
Zweitbefund
Diskrepanz Erst-/Zweitbefund
Auftrag
Mammograohie und Sonographie Bilder
Drittbefund
Drittbefund
abschließender Befund
Bilder und Befunde
Patientengespräch

3.2 Kolorektales Karzinom

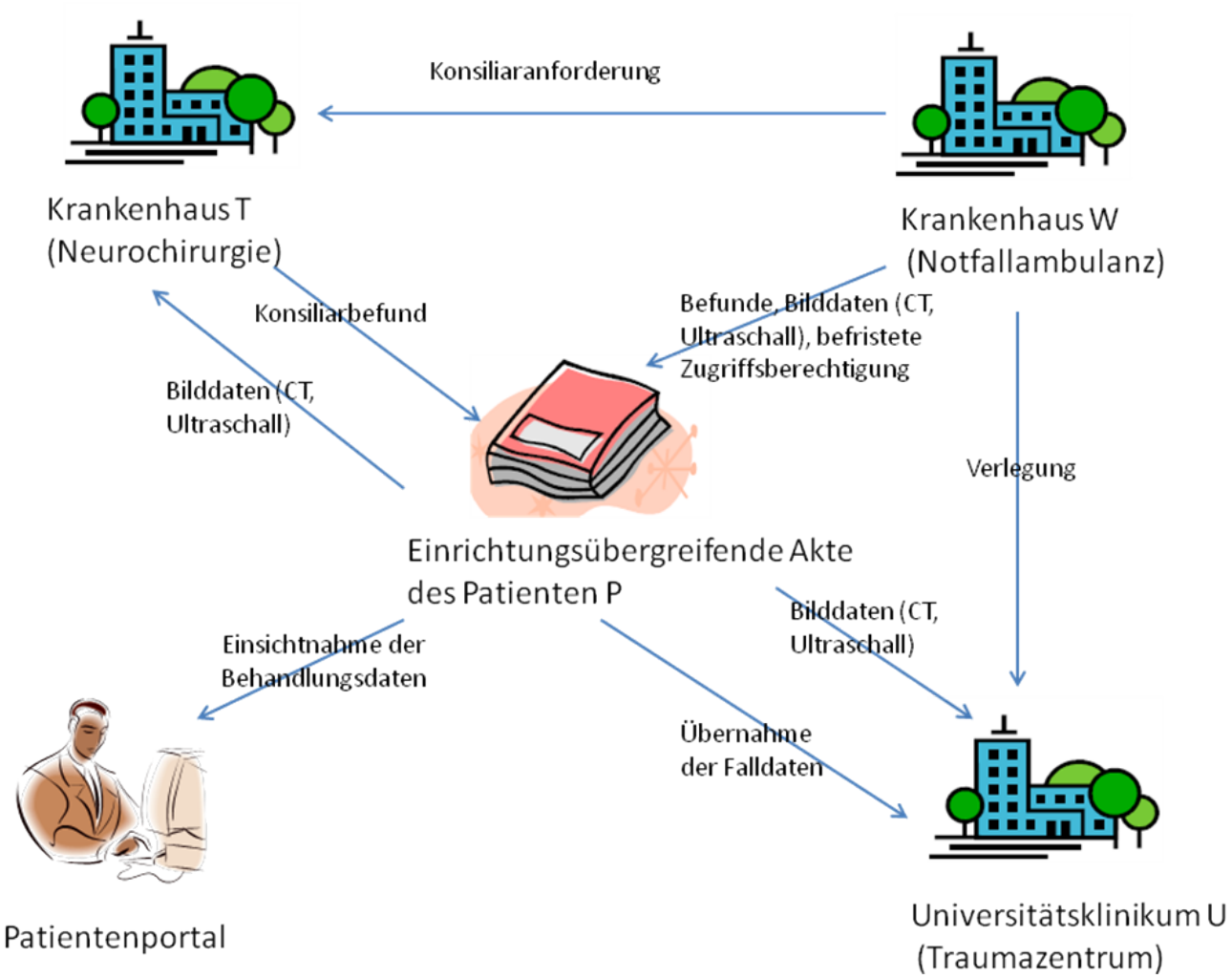
Im Gesundheitsnetz „Zukunft" sind verschiedene Organisationen zusammengeschlossen, die im Rahmen von Verträgen zur Integrierten Versorgung (IV-Verträge) Patienten aus der Region gemeinsam behandeln. Im vorliegenden Fall begleiten wir die Behandlung von Patient P (52 Jahre). Der Hausarzt von Herrn P, Herr Dr. H, stellt im Rahmen der regelmäßigen Darmkrebsvorsorge okkultes Blut im Stuhl von Herrn P fest. Er überweist daher Herrn P zur weiteren Abklärung an den Gastroenterologen, Herrn Dr. G. Nach erfolgter Aufklärung erklärt sich Herr P damit einverstanden, dass Herr Dr. H ihm eine einrichtungsübergreifende Akte anlegt und über diese die bisherigen Untersuchungsdaten Herrn Dr. G zur Verfügung stellt. Herr P erhält bei Herrn Dr. G am folgenden Tag einen Koloskopie-Termin. Im Rahmen der Koloskopie stellt Herr Dr. G Polypen im Darm von Herrn P fest und vergibt nach Entfernung der Polypen einen entsprechenden histologischen Auftrag an die externe Pathologie Pa des Krankenhauses K. Bereits am nächsten Tag kann Herr Dr. G auf den über die einrichtungsübergreifende Akte von der Pathologie Pa bereit gestellten histologischen Befund inklusive digitaler Bilder zugreifen. Zuvor hat Herr P sowohl Herrn Dr. G als auch die Pathologie Pa entsprechend für den Zugriff auf seine Akte berechtigt. Der Pathologiebefund ergibt eine bösartige Veränderung, die einen sofortigen chirurgischen Eingriff notwendig macht. Herr Dr. G führt weitere internistische Untersuchungen zur präoperativen Diagnostik durch (unter anderem auch eine Sonographie) und überweist Herrn P an die Chirurgie C des Krankenhauses K. Herr P gibt der Chirurgie C des Krankenhauses K die Einwilligung, auf die bisher gemachten Untersuchungsergebnisse zuzugreifen. Vor der Krankenhauseinweisung beauftragt Herr Dr. G bei der externen Radiologin R noch eine CT-Untersuchung zur Abklärung des Vorhandenseins von Metastasen. Außerdem wird Herr P vom Krankenhaus gebeten, als Vorbereitung zur OP einen Anamnesebogen vor dem persönlichen Gespräch auszufüllen. Der Anamnesebogen wird ihm über das Patientenportal des Gesundheitsnetzes „Zukunft" zur Verfügung gestellt, über das er auch seine bisherigen Behandlungsdaten einsehen kann. Herr P legt den ausgefüllten Anamnesebogen wiederum in dem Patientenportal ab, so dass er der Chirurgie C für die OP-Planung sofort zur Verfügung steht. Das Patientenportal bietet den Patienten Zugriff auf ihre in der einrichtungsübergreifenden Akte gespeicherten Daten. Die Patienten können unter anderem die Daten einsehen, Zugriffsberechtigungen auf die Daten vergeben oder, wie im Fall des Anamnesebogens, selbständig Daten eingeben. Der Anamnesebogen ist für die Chirurgie ausdrücklich als vom Patienten eingestelltes Dokument erkennbar, weil vom Patienten und von Leistungserbringern in die einrichtungsübergreifende Akte eingestellte Daten grundsätzlich unterschieden werden können. Zur Feststellung der genauen Tumorlokalisation beauftragt die Chirurgie C bei der Radiologie R noch eine MRT-Untersuchung. Für die prätherapeutische Fallvorstellung liegen nun dem Behandlungsteam K alle notwendigen Informationen aus Voruntersuchungen und Anamnese in der einrichtungsübergreifende Akte innerhalb kurzer Zeit vor. Herr P hat zuvor auch der Radiologie R entsprechende Berechtigungen auf seine Akte über das Patientenportal erteilt. Die Chirurgin lädt daraufhin den Gastroenterologen G ein, an der prätherapeutischen Fallvorstellung über eine Telefonkonferenz teilzunehmen. In der prätherapeutischen Fallvorstellung wird die Notwendigkeit der operativen Versorgung bestätigt. Nach dem chirurgischen Eingriff wird eine erneute MRT durchgeführt. Die Radiologin R stellt fest, dass der Tumor nicht vollständig entfernt werden konnte. Daher wird in der postoperativen Fallvorstellung die Weiterbehandlung am Universitätsklinikum U empfohlen. Die Befunde werden an den Gastroenterologen G geschickt, der zur Abklärung der weiteren Therapieoptionen nach Einverständniserklärung von Herrn P das Tumorboard des Universitätsklinikums U befragt. Die weitere Behandlung von Herrn P erfolgt am Universitätsklinikum U, das zuvor von Herrn P entsprechend berechtigt wurde, auf die Daten der bisher gemachten Untersuchungen zuzugreifen. Schließlich wird Herr P in den Nachsorge- und Rehaprozess überführt. Fünf Jahre später werden bei einer erneuten Vorsorgeuntersuchung wieder Polypen im Darm von Herrn P festgestellt. Eine weitere Therapie wird dadurch notwendig. Da Herr P mittlerweile umgezogen ist, wird diese vom Krankenhaus K2 durchgeführt, dem Herr P für die weitere Therapieplanung über das Patientenportal Zugriffsrechte auf die vor fünf Jahren erstellten Untersuchungs- und Behandlungsdaten erteilt. Den nicht mehr für seine Behandlung zuständigen Ärztinnen und Ärzten seines früheren Wohnortes dagegen hat er inzwischen die Zugriffsberechtigung auf seine Daten entzogen.

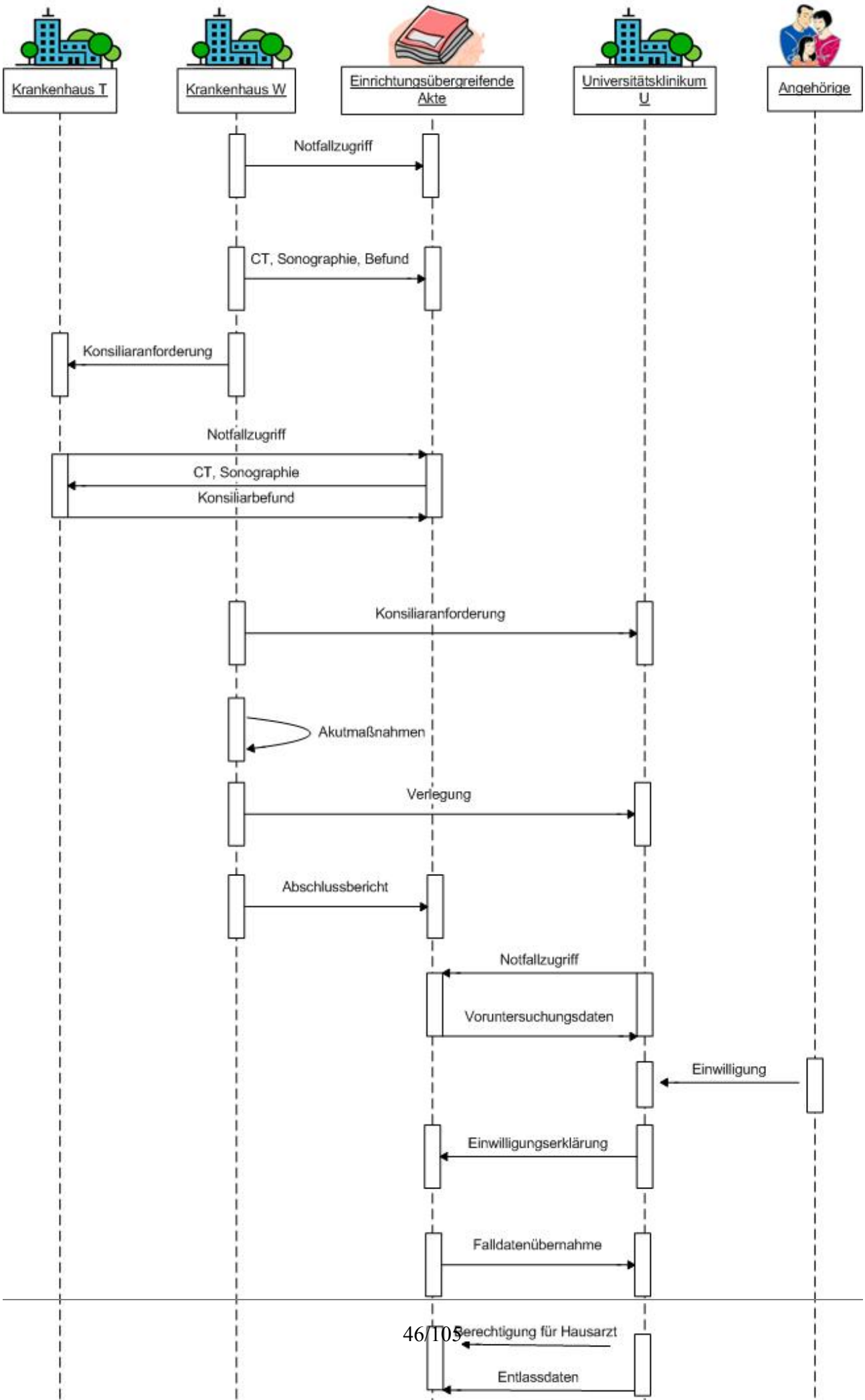

Gastroenterologie G
Patientenportal
Hausarzt H
Befunde,
Bilddaten
Anamnesebogen,
Berechtigungen
Arztbrief,
Einverständnis
Koloskopiebefund, Ultraschall,
Präoperative Diagnostik,
Einverständnis
Befunde,
Bilddaten
Bilddaten,
Befunde
Krankenhaus K
(Pathologie Pa)
Einrichtungsübergreifende Akte
des Patienten P
Bilddaten
der Radiologie R,
Befunde
Bilddaten,
Vorbefunde
Entlassbrief K
Ergebnis
Tumorboard
Befunde,
Entlassbrief K
Bilddaten,
Anamnesebogen,
Vorbefunde
Radiologie R
Uniklinikum U (Tumorboard)
Krankenhaus K
(Chirurgie C)


Radiologie R
Uniklinikum U
Chirurgie C
Einrichtungsübergeifende Akte
Gastroenterologie G
Pathologie Pa
Hausarzt H
Patient P
Einverständniserklärung
Arztbrief
Überweisung
Koloskopie Einverständniserklärung
Polypenhisto
Histobefund, Bilder
Histobefund
Endosonographie, Arztbrief, usw.
Berechtigungen
Auftrag CT Untersuchung
Befund, Bilder CT
Überweisung Chirurgie
Auftrag MRT
Befund, Bilder MRT
Anamnesebogen
Vorbefunde, Bilder
Einladung präop. Konferenz
präop. Konferenz und OP
Kontroll MRT
Befund, Bilder MRT
Befund, Bilder MRT
Befunde, Berichte, Entlassbrief
Befund, Bilder MRT, Entlassbiref
Anfrage Tumorboard
Befunde, Bilddaten
Ergebnis Tumorboard
Ergebnis Tumorboard
Einsichtnahme in Daten

3.3 Akutversorgung Schwerverletzter (Polytrauma)

Im Traumanetzwerk „Flaches Land" sind verschiedene Kliniken zusammengeschlossen, die entsprechend ihrer Ausstattung und Struktur unterschiedliche Aufgaben innerhalb des Netzwerkes übernehmen und bei der Versorgung polytraumatischer Patienten kooperieren. Im vorliegenden Fall begleiten wir die Behandlung von Patient P (23 Jahre). Herr P fährt am Abend mit dem PKW von der Arbeit nach Hause. Bei einem Ausweichmanöver kommt Herr P mit seinem Wagen von der Fahrbahn ab und das Fahrzeug überschlägt sich mehrfach. Nachdem der von Unfallzeugen alarmierte Rettungsdienst lebensrettende Sofortmaßnahmen durchgeführt und Patient P für den Transport vorbereitet hat, wird Herr P mit einem Helikopter in das nächstgelegene Krankenhaus W gebracht. Da Herr P bei seiner Notfallaufnahme im Krankenhaus W immer noch bewusstlos ist, wird er im Krankenhausinformationssystem des Krankenhauses W. als Notfallpatient angelegt. Nach Erstversorgung von Patient P im Krankenhaus W werden ein Schädel-CT und ein Ganzkörper-Trauma-CT erstellt, denen sich im Verlauf eine Kontroll -Sonographie des Brust- und Bauchraumes anschließt. Nach Beurteilung der Situation anhand der Bilder und Befunde zeigt sich, dass bei Patient P nach dem vorausgegangenen Unfall neben zahlreichen Prellungen und einer Beckenfraktur der dringende Verdacht auf ein schweres Schädel-Hirn-Trauma besteht. Da das Trauma-Team des Krankenhauses W bezüglich der Diagnose der Kopfverletzung unsicher ist und das Krankenhaus W zudem keine neurochirurgischen Kapazitäten aufweist, sieht der diensthabende Unfallarzt H die Notwendigkeit eines neurochirurgischen Konsils aus einer kooperierenden Einrichtung im Traumanetzwerk „Flaches Land". Hierfür wurden bereits bei der Erstellung der Trauma-Befunde alle traumarelevanten Bilder und Befunde des Patienten P in der einrichtungsübergreifende Akte, über die Patient P bereits aus vorhergehenden Erkrankungen verfügt, den anderen Partnerkliniken automatisiert über einen Notfallzugriff zur Verfügung gestellt. Aufgrund der Notfallsituation und der Bewusstlosigkeit von Patient P geht der behandelnde Arzt H des Krankenhauses W im Rahmen seiner Notkompetenz für die zweckgebundene Bereitstellung der Daten über einen Notfallzugriff von einer mutmaßlichen Einwilligung des Patienten P aus. Arzt H kontaktiert den diensthabenden Neurochirurgen J im Krankenhaus T des Verbundes und teilt diesem mit, wie die bereitgestellten Bilder und Befunde des Patienten P abgerufen werden können. Der Neurochirurg J ruft über den Notfallzugriff die für das Konsil benötigten Bilddaten aus der einrichtungsübergreifenden Akte des Patienten P ab und bestätigt nach der Befundung das Vorliegen eines Schädel-Hirn-Traumas. Auf Grund einer bereits vorhandenen intrakraniellen Blutung spricht er sich für die Verlegung des Patienten P in die Neurochirurgie des überregionalen Traumazentrums im Universitätsklinikum U aus. Um seine Beratung zu dokumentieren, legt Neurochirurg J die dem Konsil zugrunde liegenden Dokumente in der einrichtungsübergreifenden Akte des Patienten P ab. Arzt H informiert sofort das Universitätsklinikum U. Nachdem die Beckenfraktur für den Transport vor Ort stabilisiert wurde, wird Patient P mittels Helikopter in das Universitätsklinikum U transportiert. Hier wurde er bereits durch die Verfügbarkeit der entsprechenden Daten in der einrichtungsübergreifenden Akte als nicht vollständig datenqualifizierter Patient aufgenommen. Des Weiteren konnten hier durch die sofortige Verfügbarkeit der Voruntersuchungsdaten aus den anderen Einrichtungen bereits entsprechende Therapievorbereitungen getroffen werden. Im Universitätsklinikum U werden eine Trepanation sowie weitere Akutmaßnahmen durchgeführt, an die sich eine intensivmedizinische Behandlung von Patient P anschließt. In der einrichtungsübergreifenden Akte sind die Daten weiterhin ausschließlich für den Notfallzugriff über die Notfallpolicy verfügbar. Ein gerichtlicher Vormund verfügt an Stelle von Patient P über die Notwendigkeit der Weiterbehandlung und legitimiert damit den weiteren Notfallzugriff. Wenig später erteilt schließlich ein Angehöriger von Patient P dem Universitätsklinikum U die Erlaubnis für den normalen Zugriff auf die bereits in die einrichtungsübergreifende Akte eingestellten Daten und ermöglicht so eine Fortführung der Behandlung am Universitätsklinikum U über den regulären Aktenzugang. Die anderen Einrichtungen haben damit keinen Zugriff mehr auf die Daten von Herrn P. Die bereitgestellten Bilder und Befunde aus dem verlegenden Krankenhaus W können nun aus der einrichtungsübergreifenden Akte des Patienten P in die lokale Patientenakte des Universitätsklinikums U übernommen werden. Nach 20 Tagen kann Patient P die Intensivstation verlassen. Aufgrund der vorhandenen Schädelverletzungen wird Patient P vom Universitätsklinikum U zur neurologischen Früh-Rehabilitation in den Reha-Prozess überführt. Vor der Entlassung aus dem Krankenhaus erklärt sich Patient P damit einverstanden, dass der Entlassbericht und die bisher im Behandlungsprozess erstellten Daten seinem Hausarzt sowie der Reha-Klinik über die einrichtungsübergreifende Akte zur Verfügung gestellt werden. Zuhause schaut sich Patient P die Dokumentation der bisher durchgeführten Untersuchungen und Therapien über das Patientenportal des Traumanetzwerks „Flaches Land" an.


Konsiliaranforderung
Krankenhaus T
(Neurochirurgie)
Krankenhaus W
(Notfallambulanz)
Konsiliarbefund
Befunde, Bilddaten (CT,
Ultraschall), befristete
Zugriffsberechtigung
Bilddaten (CT,
Ultraschall)
Verlegung
Einrichtungsübergreifende Akte
des Patienten P
Einsichtnahme der
Behandlungsdaten
Bilddaten (CT,
Ultraschall)
Übernahme
der Falldaten
Patientenportal
Universitätsklinikum U
(Traumazentrum)


Krankenhaus T
Krankenhaus W
Einrichtungsübergreifende Akte
Universitätsklinikum U
Angehörige
Notfallzugriff
CT, Sonographie, Befund
Konsiliaranforderung
Notfallzugriff
CT, Sonographie
Konsiliarbefund
Konsiliaranforderung
Akutmaßnahmen
Verlegung
Abschlussbericht
Notfallzugriff
Voruntersuchungsdaten
Einwilligung
Einwilligungserklärung
Falldatenübernahme
Berechtigung für Hausarzt
Entlassdaten

4 Lösungsarchitektur

Das Kapitel Lösungsarchitektur stellt dar, wie unter Berücksichtigung der datenschutz- und sicherheitsrechtlichen Rahmenbedingungen (vgl. Kapitel 2.1) die im Kapitel 3 beschrieben Use-Cases mithilfe der im Kapitel 4.3 beschriebenen Lösungskomponenten als Bausteine technisch umgesetzt werden können. Dabei wird zunächst von einigen Grundsätzen ausgegangen, die zwingend von allen Architekturen berücksichtigt werden müssen. Die Umsetzung von Datenschutz und Datensicherheit wird erläutert. Für jede o.g. Aktenart wird die auf den Lösungskomponenten basierende Architektur beschrieben sowie die Umsetzung der den Anwendungsfällen zugrundeliegenden technischen Use-Cases mit ihren Datenflüssen und Transaktionen.

4.1 Grundsatzentscheidungen

Die nachfolgenden Grundsätze sind der Lösungsarchitektur zu Grunde gelegt:

- Primat des Bürgers: Die Datenhoheit und Steuerung der Zugriffsberechtigungen liegt uneingeschränkt bei ihm. Entweder indem erdiese selbst aktiv steuert oder diese Aufgabe an einen Stellvertreter delegiert.
- Sämtliche Zugriffsberechtigungen und ihre Änderungen sind durch alle an die Akte angebundenen Systeme, wie KIS, PVS, etc. ~~(in der jeweiligen Affinity Domain)~~ umzusetzen.

- Das Recht auf „Vergessen" (Löschung) ist hierbei ein wesentliches Grundprinzip und auf jeden Fall in allen Bereichen zu berücksichtigen.
- Die Steuerung der Zugriffsberechtigungen soll granular (abh. vom jeweiligen Aktensystem) möglich sein, um dem Patienten/Bürger eine dezidierte Möglichkeit zur Wahrung seiner informationellen Selbstbestimmung zu erlauben und die momentane Situation im realen Leben abzubilden.
- Als eine der untersten Ebenen bei der Granularität der Berechtigungssteuerung durch den Patienten/ Bürger wird das Dokument definiert. D.h. es gibt keine Berechtigungssteuerung innerhalb eines Dokumentes.
- Semantische Interoperabilität der Dokumenteninhalte und die Kommunikation zwischen verschiedenen Affinity Domains wird in späteren Versionen des Cookbooks angestrebt.

Um einen Leitfaden für die Implementierung von IHE XDS basierten Vernetzungslösungen in Deutschland zu definieren, muss die Lösungsarchitektur grundsätzlich den nachfolgenden Paradigmen folgen.

4.1.1 Flexible Umsetzungen

Die Einhaltung der notwendigen Sicherheitsarchitektur wie auch der Vorgaben zum Nachweis der informierten Einwilligung der Patientinnen und Patienten können in unterschiedlichen Anwendungsszenarien voneinander unterscheiden. Um diese Grundsätze dennoch einzuhalten wird die Architektur verschiedene Umsetzungen ermöglichen.

4.1.2 Transparente Ergänzungen vorhandener Profile und Empfehlungen

Die in der Architektur eingesetzten IHE Profile werden umfänglich, in ihrer vorliegenden Form zum Einsatz gebracht. Die notwendigen, nationalen Ergänzungen, Festlegungen und Empfehlungen sollen sich dabei auf Ausprägungen und inhaltliche Vorgaben für die definierten Informationsobjekte und deren Parameter beschränken. Dabei muss die o.g. Flexibilität erhalten bleiben, um projektspezifische Implementierungen nicht einzuschränken. Die Funktionalitäten der eingesetzten Akteure und Transaktionen sollen in ihrer ursprünglichen Form erhalten bleiben, um den Einsatz bereits vorhandener Lösungen zu ermöglichen.

4.1.3 Unterstützung von feingranularen Zugriffsregelungen

Gerade um eine möglichst breite Nutzung der hier vorgeschlagenen Architektur zu gewährleisten muss eine Reihe von Nutzer-Parametern (ID, Rolle, Organisation, Spezialität, etc.) nutzbar sein. Diese Parameter müssen dann auf den Ebenen Affinity Domain, Patient, Folder und Dokument anwendbar sein.

4.1.4 Ausschließliche Verwendung von existierenden Standards

Alle die IHE Profile ergänzenden Architekturelemente werden explizit auf existierende Standards (z.B. HL7, XACML, SAML) aufgesetzt. Es ist nicht Ziel dieses Dokumentes neue IT Standards zu definieren.

4.2 Umsetzung von Datenschutz und Datensicherheit

Für die erfolgreiche Nutzung der beschriebenen Lösungsarchitekturen sind neben den funktionalen Aspekten auch Vorgaben für die Umsetzung der in Abschnitt 2.1.5 beschriebenen Datenschutzanforderungen gemäß Anlage zu §9 BDSG zu berücksichtigen. Im Folgenden sind die Maßnahmen beschrieben, durch die die jeweiligen Datenschutzanforderungen erfüllt werden sollen.

4.2.1 Zugangskontrolle

Die Zugangskontrolle wird dadurch sichergestellt, dass sich alle Benutzer des Gesamtsystems bzw. seiner Komponenten (Personen, Systeme, Anwendungen) sicher authentifizieren müssen. Dies kann auf unterschiedliche Art und Weise geschehen, so dass Benutzernamen und sichere Passwörter, Zugangstoken oder Zertifikate zur Authentifizierung der Nutzer verwendet werden können. Zur sicheren Übermittlung von Informationen authentifizierter Benutzer wird das Profil XUA verwendet, welches in Abschnitt 2.2.9 beschrieben ist. Die bidirektionale, zertifikatsbasierte Authentifizierung bei der Kommunikation von Systemkomponenten sowie die Protokollierung von Nutzerdaten erfolgen auf Basis des ATNA Profils, welches in Abschnitt 2.2.8 beschrieben ist.

4.2.2 Zugriffskontrolle

Die Zugriffskontrolle wird dadurch sichergestellt, dass den authentifizierten Benutzern Rollen zugewiesen werden und diesen Rollen die jeweiligen Zugriffsrechte auf die unterschiedlichen Daten zugeordnet sind. Durch die Verwendung von feingranularen Policies auf Basis von XACML (siehe Abschnitt 2.2.11) können die beteiligten Einrichtungen und Patienten spezifische Zugriffsrechte für Organisationen, Rollen etc. definieren, die das Gesamtsystem bzw. die einzelnen Systemkomponenten bei jedem Datenzugriff (Speichern, Lesen, Ändern Löschen) prüfen und durchsetzen. Die Protokollierung von Datenzugriff erfolgt auf Basis des ATNA Profils, welches in Abschnitt 2.2.8 beschrieben ist.

4.2.3 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle ist durch die Verwendung der feingranularen Policies auf Basis von XACML (siehe Abschnitt 2.2.11) ersichtlich, wer wann welche Daten weitergeben kann und wer dann auf die Daten Zugriff hat. Die Protokollierung von Datenweitergaben erfolgt auf Basis des ATNA Profils, welches in Abschnitt 2.2.8 beschrieben ist. Bei Transport der Daten sind diese zu verschlüsseln und die kommunizierenden Systemkomponenten sind sicher zu authentifizieren, was ebenfalls im ATNA Profil beschrieben ist.

4.2.4 Eingabekontrolle

Die Eingabekontrolle erfolgt durch Verwendung des ATNA Profils, da alle Datenzugriffe im zentralen Audit Repository gespeichert und ausgewertet werden können.

4.2.5 Auftragskontrolle

Im Rahmen der Auftragskontrolle muss beachtet werden, dass administrative und medizinische Rollen und die entsprechenden Zugriffsberechtigungen strikt getrennt werden und nur auf Daten entsprechend den Weisungen des Auftraggebers zugegriffen werden kann. Die Auftragskontrolle umfasst ebenfalls die verschlüsselte Ablage der medizinischen Daten. Dies kann durch systembasierten Datenverschlüsselung erfolgen.

4.2.6 Trennungsgebot

Das Trennungsgebot wird dadurch umgesetzt, dass administrative Patientendaten, Dokumente und Bilder zu jeder Zeit unabhängig voneinander gespeichert, verändert, übermittelt, gesperrt oder gelöscht werden können. Diese Forderung kann durch die Verwendung spezifischer Transaktionen und Möglichkeiten der Profile PIX, XDS.b, XDS-I.b und XDS Metadata Update sowie XACML durchgesetzt werden.

4.3 Standardisierte Lösungsmodule

Hier folgenden die Beschreibungen der standardisierten Lösungsmodule, die von allen Aktentypen verwendet werden.

4.3.1 Patientenidentifikation

Für das Thema Patientenidentifikation werden üblicherweise 3 unterschiedliche Lösungsansätze diskutiert. Alle 3 Lösungsansätze führen zur Erzeugung einer XAD-Pid und damit zum "Anlegen einer Patientenakten".

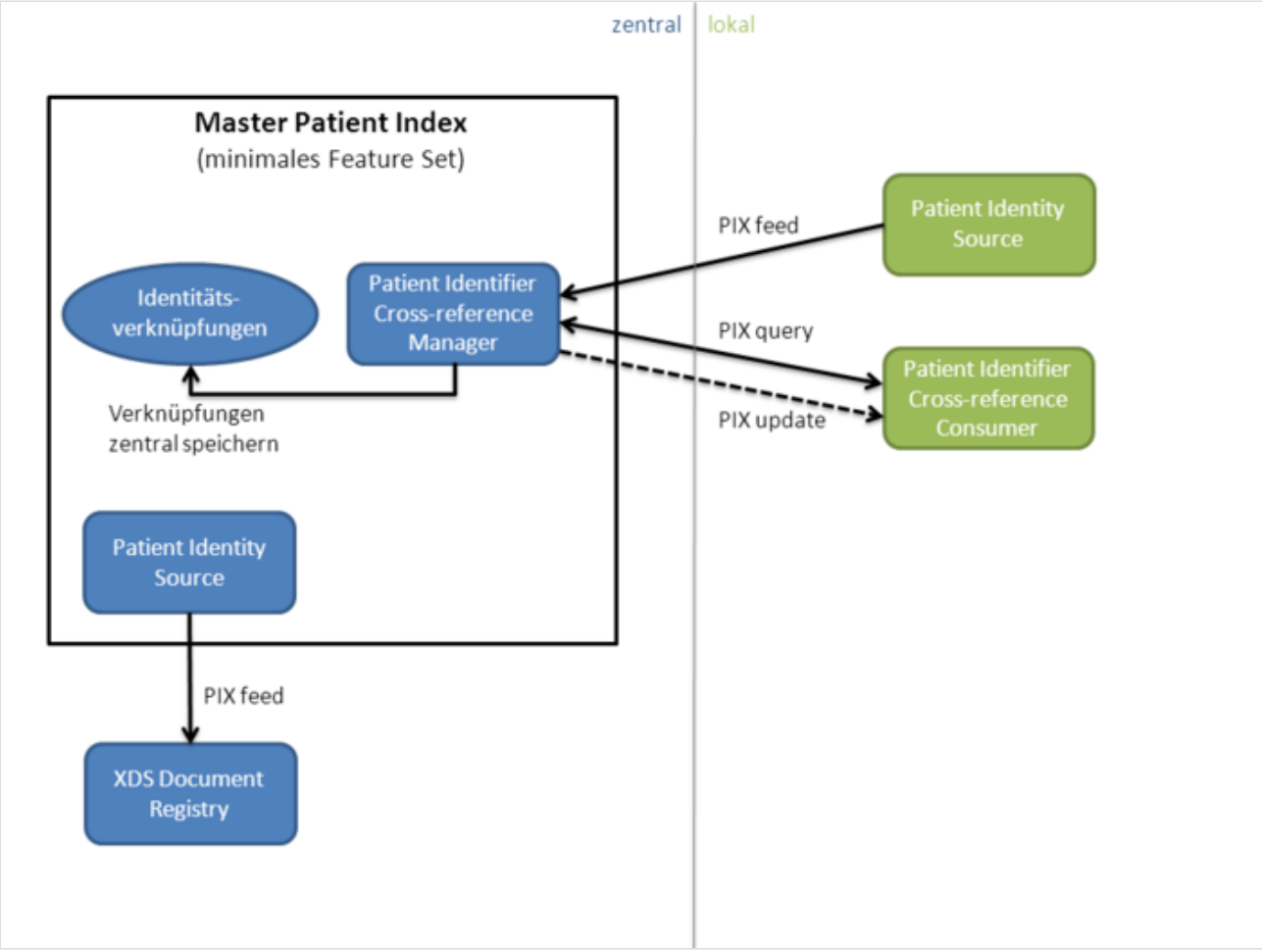
1. Master Patient Index
2. Patientenregister
3. Verteilte Erstellung ohne Abfragemöglichkeit

Im folgenden wird erläutert wie die Lösungsansätze im Detail umgesetzt werden können.

4.3.1.1 Master Patient Index

Ein Master Patient Index (MPI) speichert Verknüpfungen zwischen lokalen Patientenidentitäten. Üblicherweise stellt ein MPI ausserdem für jeden eindeutig identifizierten Patienten eine eindeutige ID (Master Patient ID) und einen kanonischen Datensatz zur Verfügung, der die neusten und genausten Stammdaten des Patienten sammelt. Der MPI hat üblicherweise die Aufgabe Verknüpfungen zwischen Patienten automatisch zu erstellen oder einem Benutzer in einer sogenannten Clearingstelle Verknüpfungsvorschläge zu unterbereiten.

Minimal erlaubt ein IHE konformer MPI die Anlieferung von lokalen Patientenidentitäten per Patient Identity Feed (PIX Feed) und die Abfrage der Master Patient ID oder der in den anderen Einrichtungen verwendeten lokalen Patienten-IDs per PIX Query. Um einem Datenaustausch per IHE XDS zu ermöglichen, muss der MPI natürlich auch seine Mater Patient IDs komplett oder in Teilen mit der XDS Document Registry per Patient Identity Feed (hier als Patient Identity Source) synchronisieren.



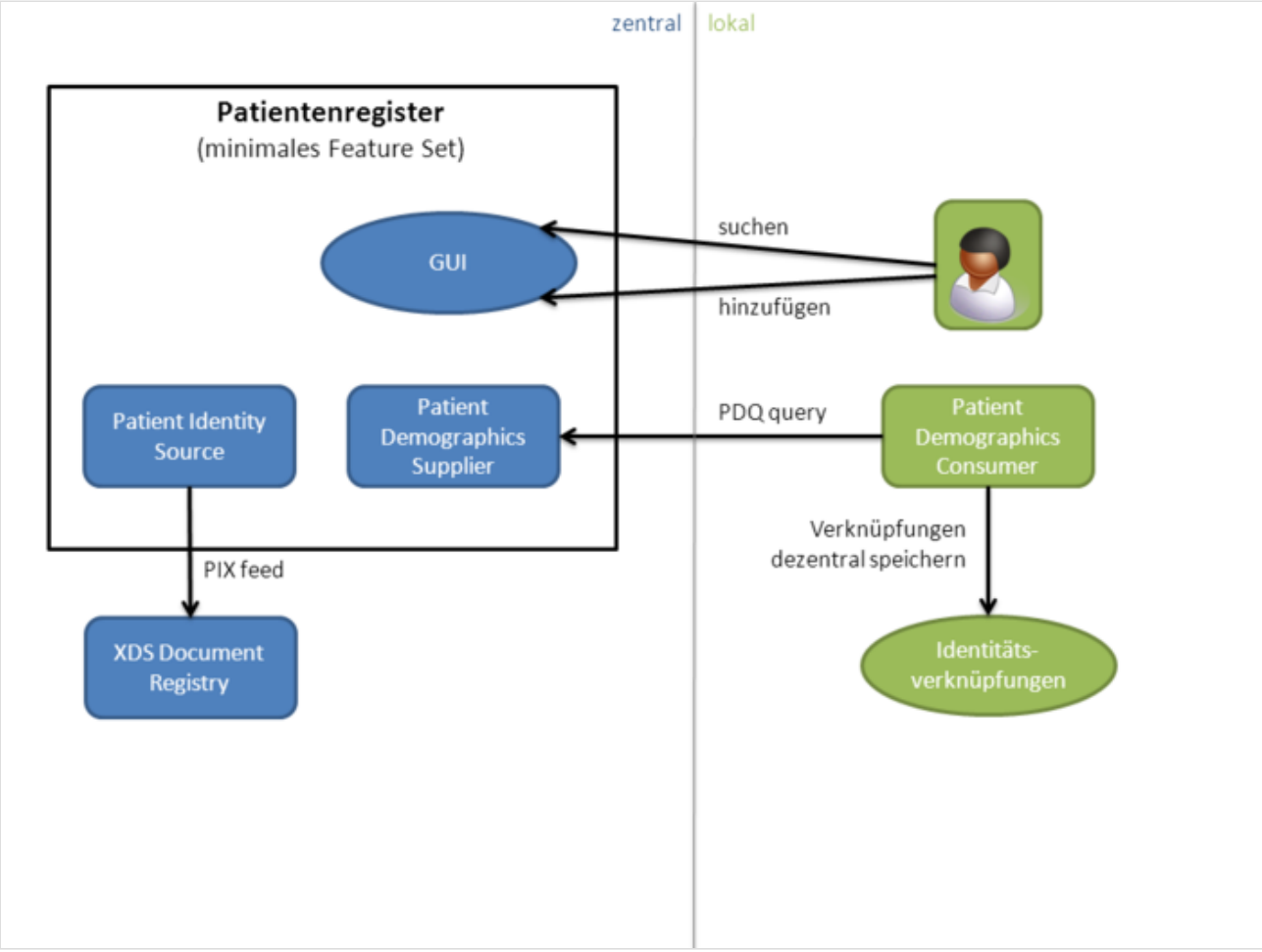
Optional kann ein MPI auch eine Suche per PDQ anbieten, wobei üblicherweise der kanonische Datensatz, die Master Patient ID und die lokalen IDs zurückgegeben wird. Eine Suche per GUI wird häufig auch angeboten. Da oft nicht alle anzubindenden Systeme ihre Patientenidentitäten übertragen können oder wollen, gibt es ausser den vom MPI geführten Verknüpfungen häufig auch noch patientenführende Systeme die ihre eigenen Patienteneinträge um die Master Patient ID erweitern. Dadurch ergeben sich Szenarien in denen der MPI nur einen Teil der Verknüpfungen zwischen Patientenidentitäten speichert und verwaltet. Die lokal geführten Verknüpfungen sind natürlich nicht durch die Ähnlichkeitsalgorithmen des MPI geprüft und können nicht zentral verwaltet werden.

Die Übertragung der Patientenidentität über ein Medium — wie z.B. ein Papierausdruck oder eine Smartcard — kann auch bei einem MPI genutzt werden.

4.3.1.2 Patientenregister

Ein Patientenregister verwaltet zentrale Patientenidentitäten. Im Gegensatz zu einem MPI speichert ein solches Register üblicherweise nicht die Verknüpfungen zwischen den lokalen Identitäten. Das Patientenregister lässt sich über PDQ oder eine GUI abfragen und überlässt es den anfragenden Systemen die Verknüpfung zu ihrer lokalen Patienten-ID abzuspeichern. Um einem Datenaustausch per IHE XDS zu ermöglichen, muss das Patientenregister natürlich auch seine Einträge bzw. die IDs komplett oder in Teilen mit der XDS Document Registry per Patient Identity Feed (als Patient Identity Source) synchronisieren.

Die Daten des Patientenregisters werden üblicherweise über eine GUI gepflegt, wobei gerade zum initialen Befüllen auch ein Batch Import aus einer autoritativen Quelle in Frage kommt.



Optional kann auch der PIX Query Mechanismus genutzt werden um zentrale Patientenidentitäten abzufragen. Da im Patientenregister aber keine Verknüpfungen zu lokalen Patienten-IDs gespeichert werden, kann eine solche Abfrage aber nur über eine alternative ID des Patienten — wie z.B. die Nummer der Krankenversicherten-Karte — durchgeführt werden.

Die Übertragung der Patientenidentität über ein Medium — wie z.B. ein Papierausdruck oder eine Smartcard — kann auch bei einem MPI genutzt werden.

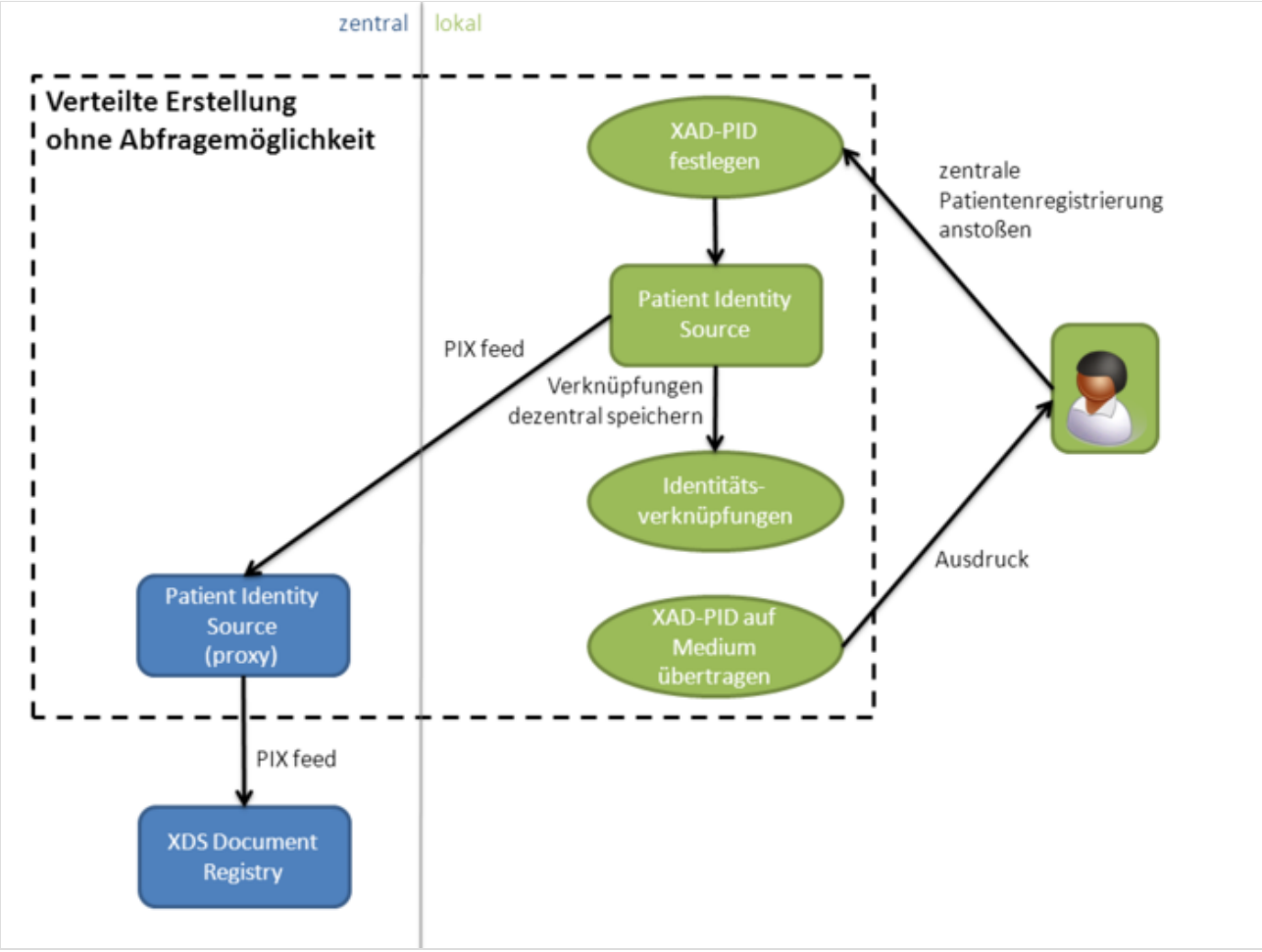
4.3.1.3 Verteilte Erstellung ohne Abfragemöglichkeit

Die verteilte Erstellung von Patientendatensätzen ohne Online-Abfragemöglichkeit ist ein bisher kaum erprobter Ansatz, der aber durchaus in Harmonie mit einigen IHE ITI Profilen genutzt werden kann. In diesem Ansatz wird ein Algorithmus eingesetzt, der sicherstellt, dass nicht miteinander verbundene Systeme unabhängig voneinander Patienten-IDs erstellen können, ohne dass es zu Überschneidungen kommt. Dies ermöglicht es den patientenführenden Systemen eigenständig eine zentrale ID für Austauschzwecke zu definieren (d.h. eine XAD-PID).

Eine XDS Document Registry erwartet eine einzige Quelle für alle Patient Identity Feed Nachrichten. Alle zusammengeschlossenen Systeme die XAD-PIDs erstellen müssen daher die gleiche OID als Namespace Identifier verwenden. Ausserdem muss ein Proxy die Nachrichten sammeln und an die Document Registry weiterleiten. Dadurch wird sichergestellt, dass die Document Registry nur einen Kommunikationspartner sieht und sich dieser standard-konform verhält.

Alternativ zu dieser Vorgehensweise kann jedes System seine eigene Affinity Domain im Zusammenspiel mit einer Registry spielen. Über Cross-Affinity-Gateways lassen sich dann die anderen Registries befragen.

Da es prinzipbedingt keine Online-Abfragemöglichkeit gibt, muss die Patientenidentität bei diesem Ansatz über ein Offline Medium übertragen werden. Zur Zeit bietet sich hier ein Papierausdruck an, der dem Patienten mitgegeben wird oder an den Patienten oder einen Arzt verschickt wird. Alternativ könnten in Zukunft auch Smartcards oder die eGK als Transport Medium genutzt werden. Aber auch das IHE-Profil XDM bietet sich hier an.



Solange die Eindeutigkeit sichergestellt ist und die Patienten-ID als eine OID ausgedrückt werden kann, bleibt die Wahl des Algorithmus dem Hersteller der Austauschplattform überlassen. Die Algorithmen reichen in der Komplexität von einfachen Präfixen, die den Namensraum statisch aufteilen, bis zu den gebräuchlichen UUIDs nach RFC 4122.

4.3.1.4 Zusammenfassung

Die folgende Tabelle vergleicht welche Features bei welchem Ansatz sinnvoll genutzt werden können. Pro Feature wird gelistet ob es ein Kernaspekt ist, ohne den der Ansatz nutzlos ist ("notwendig"), ob es ein Feature ist das mit dem Ansatz sinnvoll verbunden werden kann ohne notwendig zu sein ("optional") oder ob das Feature normalerweise nicht sinnvoll mit dem Ansatz kombinierbar ist ("-").

Übersicht der vorgestellten Lösungsansätze zur Patientenidentifikation

Feature	Master Patient Index	Patientenregister	Verteilte Erstellung
PIX Feed annehmen (ITI-8 oder ITI-44 als Patient Identifier Cross-reference Manager)	notwendig	-	-
PIX Query beantworten (ITI-9 oder ITI-45 als Patient Identifier Cross-reference Manager)	notwendig	optional	-
PIX Update senden (ITI-10 oder ITI-46 als Patient Identifier Cross-reference Manager)	optional	-	-
PDQ Patient Demographics Query (ITI-21 oder ITI-47 als Patient Demographics Supplier)	optional	notwendig	-
PIX Feed an die XDS Document Registry senden (ITI-8 oder ITI-44 als Patient Identifier Source)	notwendig	notwendig	notwendig
Suche nach zentraler Patientenidentität per GUI	optional	notwendig	-
Hinzufügen einer zentralen Patientenidentität per GUI	-	notwendig	-
Identitätsverknüpfungen können dezentral gespeichert werden	optional	notwendig	notwendig
Identitätsverknüpfungen können zentral gespeichert werden	notwendig	-	-
Übertragung der XAD-PID auf einem Medium	optional	optional	notwendig

4.3.2 Benutzerauthentifizierung und -identifikation

Einrichtungsübergreifenden Datenaustausch stellt besondere Ansprüche an Datenschutz (siehe Kapitel 4.2). Anforderungen bzgl. Nachvollziehbarkeit und Zugriffkontrolle sind grundsätzlich nur mit Hilfe eines personalisierten Zugriffs auf die zu schützenden Daten erfüllbar. Um die Zugriffsrechte zu definieren und zu prüfen, werden in der Regel weitere Eigenschaften der Nutzeridentitäten (z. B. Organisationszugehörigkeit) und des Kontexts (z. B. Verwendungsweck) herangezogen. Daraus ergeben sich die folgenden Rahmenanforderungen: - Mindestens eine Benutzerverwaltung mit unterscheidbaren Nutzeridentitäten (Benutzeridentifikation) ist etabliert. - Es kann sichergestellt werden, dass der der Benutzer und die angegebene Benutzeridentität übereinstimmen (Benutzerauthentifizierung). - Zusätzliche Merkmale der Benutzeridentität sind bekannt und abrufbar (Organisationsverzeichnis), ebenso Merkmale des Nutzungskontexts

Statement: Die Auswertung der Benutzeridentität beim Datenzugriff ist für die Nachvollziehbarkeit notwendig.

Statement: Um die Echtheit der Identitätsinformation zu gewährleisten, ist die Kommunikation über beidseitig abgesichertes TLS erforderlich, d. h. eine Authentifizierung über Client-Zertifikate.

Von einer Passwort-basierten Authentifizierung für Systeme wird abgeraten, da die Speicherung des Passworts im Klartext ein Sicherheitsrisiko darstellt und Best Practices des Passwort-Managements — wie kurze Gültigkeitsfristen für Passwörter, forcierte Änderungsaufforderungen beim Login, etc. — nicht sinnvoll eingesetzt werden können.

Statement: Am Datenaustausch dürfen nur Benutzer mitwirken, die mindestens einen Identitätsnachweis (z.B. Passwort, Zertifikat, Hardware Token, etc.) gegenüber einem vertrauenswürdigen System erbracht haben.

Eine 2-Faktor Authentifizierung ist generell zu empfehlen, aber keine zwingende Anforderung für ein solches System. In der Literatur zu Identity Management Systemen unterscheidet man üblicherweise Föderiertes Identitäts-Management von zentralem Identitäts-Management. Bei Vernetzungsprojekten im deutschen Gesundheitswesen muss aufgrund der Kombination aus heterogenen Systemlandschaften und hohen Sicherheitsanforderungen in den meisten Fällen ein gemischter Ansatz verwendet werden. Im Folgenden wird daher nicht weiter darauf eingegangen ob das resultierende Sicherheitssystem als zentral oder als föderiert interpretiert werden sollte.

Statement: Im Kontext des Cookbooks ist sowohl förderiertes als auch nicht föderiertes Identitätsmanagement relevant.

Die Benutzeridentitäten des jeweiligen angeschlossenen Systems werden im Folgenden als "lokale Benutzeridentitäten" bezeichnet. Es ist nicht zu erwarten, dass angeschlossene Systeme wie ein KIS oder ein PVS/AIS ihre eigene Benutzerverwaltung aufgeben und stattdessen auf eine gemeinsame, an das einrichtungsübergreifende Aktensystem angeschlossene Benutzerverwaltung aufsetzen. Daher wird es nötig sein für die einrichtungsübergreifende Kommunikation entweder ein Mapping von der lokalen Benutzeridentität auf die zentrale Benutzeridentität durchzuführen oder direkt lokale Benutzeridentitäten einzusetzen (siehe Abschnitt Verwendung lokaler Benutzeridentitäten).

Statement: Wird im Rahmen des Datenaustausches eine zentrale Benutzeridentität verwendet, so ist die Abbildung der lokalen Identitäten auf diese zentrale Identität umzusetzen.

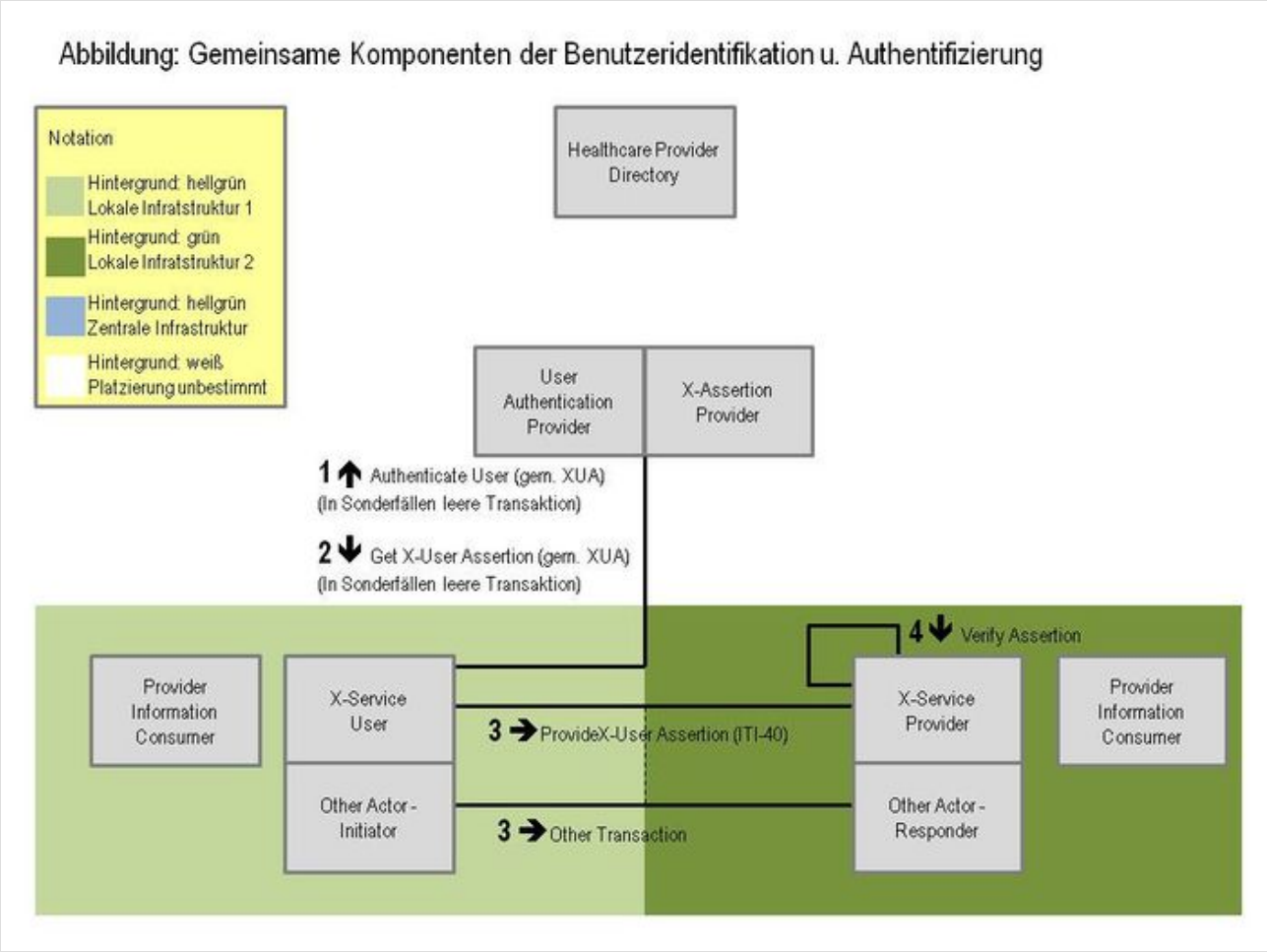
Statement: Wird im Rahmen des Datenaustauschs keine zentrale Benutzeridentität verwendet, so muss jedes angeschlossene System in der Lage sein, die Zugriffsrechte anhand der lokalen Identität aus einem anderen System zu ermitteln. Hierzu wird ein Organisationsverzeichnis herangezogen.

Außer der Entscheidung hinsichtlich des Mappings auf eine zentrale Benutzeridentität, muss auch geklärt werden, wer die Benutzeridentität über eine kryptografisch gesicherte Aussage (eine Assertion) bestätigt. Die Möglichkeiten der Realisierung werden im Weiteren beschrieben.

Statement: Zwei Fälle sind zu unterscheiden: Wenn die Echtheit der Benutzeridentifikation und weiterer Identitätsmerkmale vom Sender einer Transaktion gewährleistet wird, und wenn die Assertion von einer externen Instanz ausgestellt und signiert wurde.

4.3.2.1 Charakterisierung der Lösung

Die Kernaufgabe der Benutzeridentifikation und -authentifizierung ist es sicherzustellen, dass beim Empfänger zusammen mit einer Transaktion eine Aussage über die Person die die Transaktion initiiert hat ankommt. Diese Aussage (Assertion) muss vertrauenswürdig und unversehrt sein. Ebenfalls muss der Inhalt der Aussage dafür ausreichen, dass der Empfänger über die Zulässigkeit der Transaktion entscheiden kann. Die Assertion enthält die Information über den Benutzer, der die Transaktion angestoßen hat, über dessen Eigenschaften sowie über den Kontext der Transaktion. Die Erstellung und Überprüfung der Assertion wird durch die Akteure der Integrationsprofile XUA/XUA++ (siehe 2.2.9) umgesetzt: X-Service-User, X-Service-Provider, User Authentication Provider und X-Assertion Provider. Die Gruppierung eines User Authentication Provider und X-Assertion-Provider entspricht dem gängigen Verständnis eines Security Token Service (STS). Die vom jeweiligem Zugriffskontext unabhängigen Zusatzinformation für Benutzeridentitäten werden durch eine Healthcare Provider Directory (siehe 2.2.6) exponiert und von einem Provider Information Consumer abgefragt. Das Zusammenspiel der genannten Komponenten wird im Weiteren beschrieben.



4.3.2.2 Zuordnung zwischen der lokalen und der zentralen Benutzeridentität

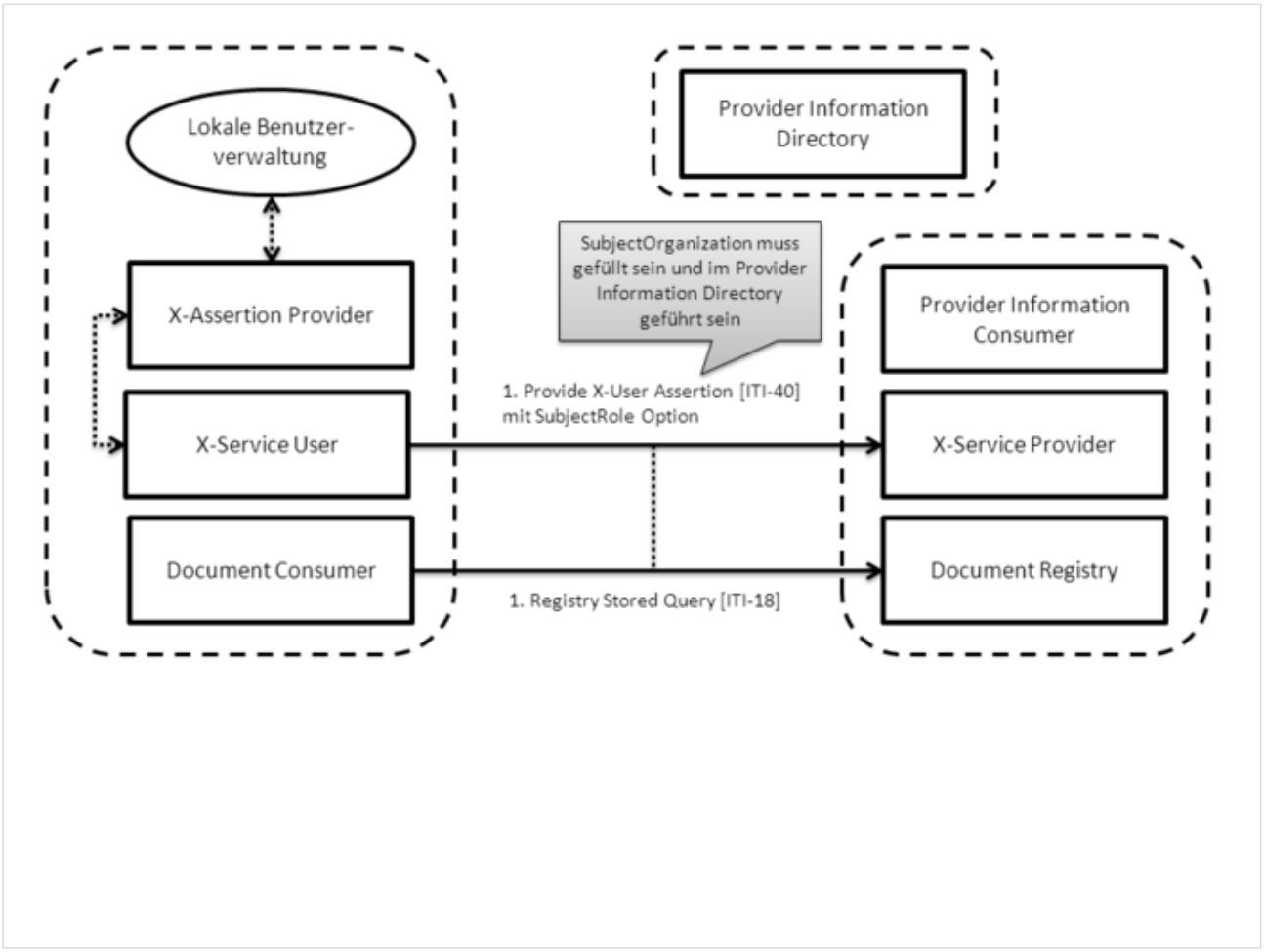
Bei der Handhabung der zentralen Benutzeridentität sind folgende Ansätze denkbar:

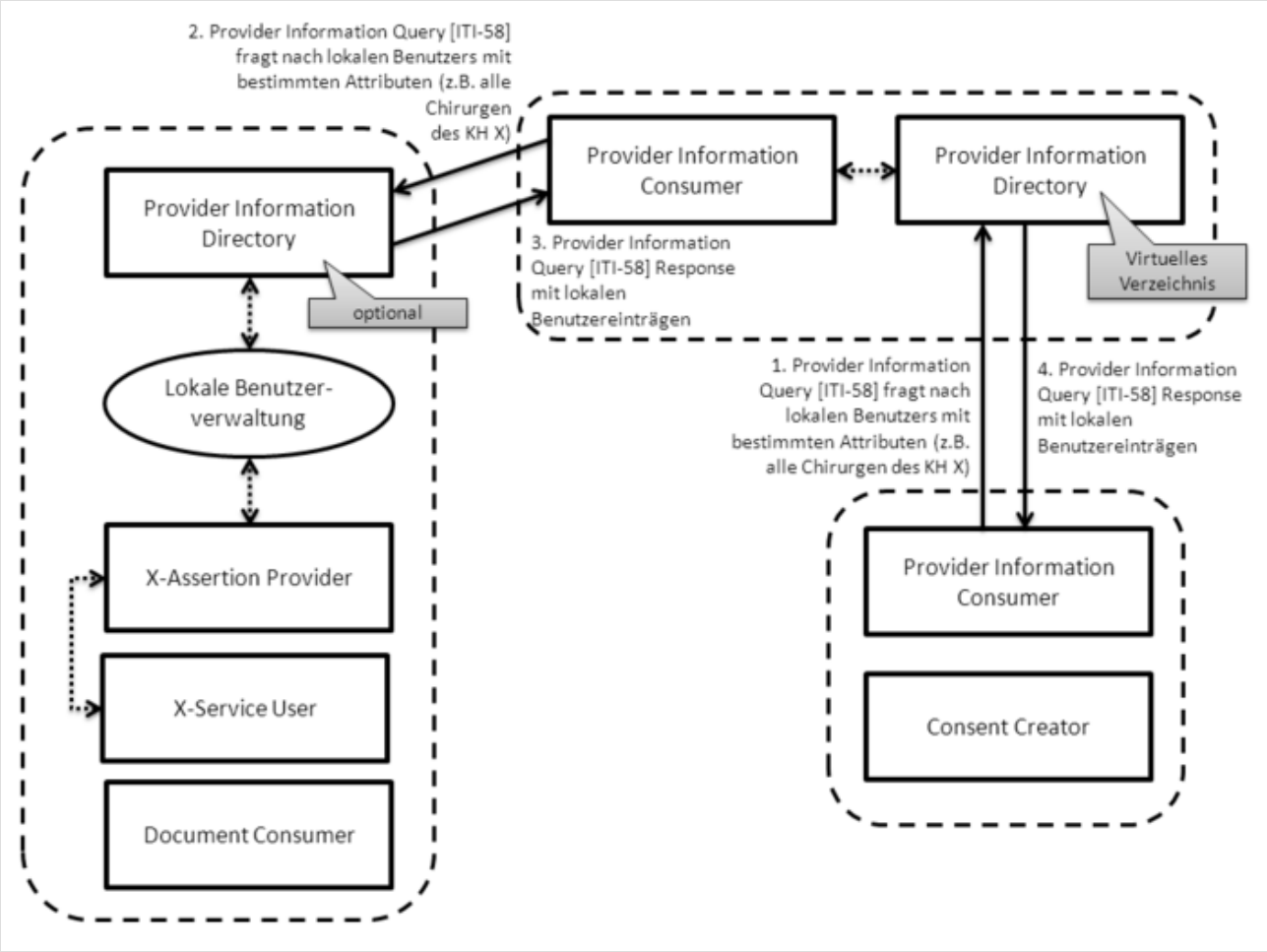
- zentrale Benutzeridentität wird nicht verwendet
- zentrale Benutzeridentität wird interaktiv eingegeben.
- das initiierende System unterhält ein Mapping zwischen lokalen und zentralen Benutzeridentitäten, entweder statisch oder dynamisch.

Die ersten beiden Fälle werden in Abschnitten Verwendung lokaler Benutzeridentitäten und Lokale Eingabe der zentralen Benutzeridentität diskutiert. Die dritte alternative wird in den beiden darauf folgenden Abschnitten Dynamisches Mapping der Benutzeridentität und Statisches Mapping der Benutzeridentität erläutert. Anschliessend werden die technischen Aspekte detailliert dargestellt.

4.3.2.3 Verwendung lokaler Benutzeridentitäten

Um lokale Benutzeridentitäten zu verwenden, sendet das anfragende System eine (SAML) Identity Assertion und mehrere Attribute Assertions, die den Benutzer und seine Attribute so detailliert beschreiben, dass das Berechtigungsmodul des zentralen Aktensystems eine sinnvolle Berechtigungsentscheidung treffen kann. Dadurch müssen für diese Benutzer keine zentralen Benutzeridentitäten gepflegt werden. Bei der ausschließlichen Verwendung lokaler Benutzeridentitäten kann auf eine zentrale Benutzerverwaltung verzichtet werden. Üblicher ist jedoch ein begrenzter Einsatz von lokalen Benutzeridentitäten aus Systemen die viele lokale Benutzer verwalten und deren Personal häufig wechselt, d.h. vor allem größere Krankenhäuser. Da die lokalen Benutzeridentitäten nicht in einem zentralen Healthcare Provider Directory (HPD) bekannt sind, können sie nicht ohne weiteres bei der Berechtigungsvergabe verwendet werden. Um trotzdem eine Vergabe von Berechtigung an Teilnehmer mit nur lokal gepflegten Benutzeridentitäten zu ermöglichen, sollten zumindest die Organisationsstrukturen von Einrichtungen, die lokale Benutzeridentitäten verwenden, zentral bekannt sein. Die Organisationen werden als Organizational Providers im HPD abgebildet, mitsamt ihren Beziehungen untereinander, aber ohne die zugehörigen Benutzer (d.h. ohne Individual Providers). Dabei ist es entscheidend, dass die Systeme, die lokale Benutzeridentitäten verwenden, in den Attribute Assertions die gleichen Organisationsidentifikatoren verwenden, die auch für die Berechtigungsvergabe verwendet werden.


Lokale Benutzer-verwaltung
X-Assertion Provider
X-Service User
Document Consumer
Provider Information Directory
SubjectOrganization muss gefüllt sein und im Provider Information Directory geführt sein
1. Provide X-User Assertion [ITI-40] mit SubjectRole Option
1. Registry Stored Query [ITI-18]
Provider Information Consumer
X-Service Provider
Document Registry

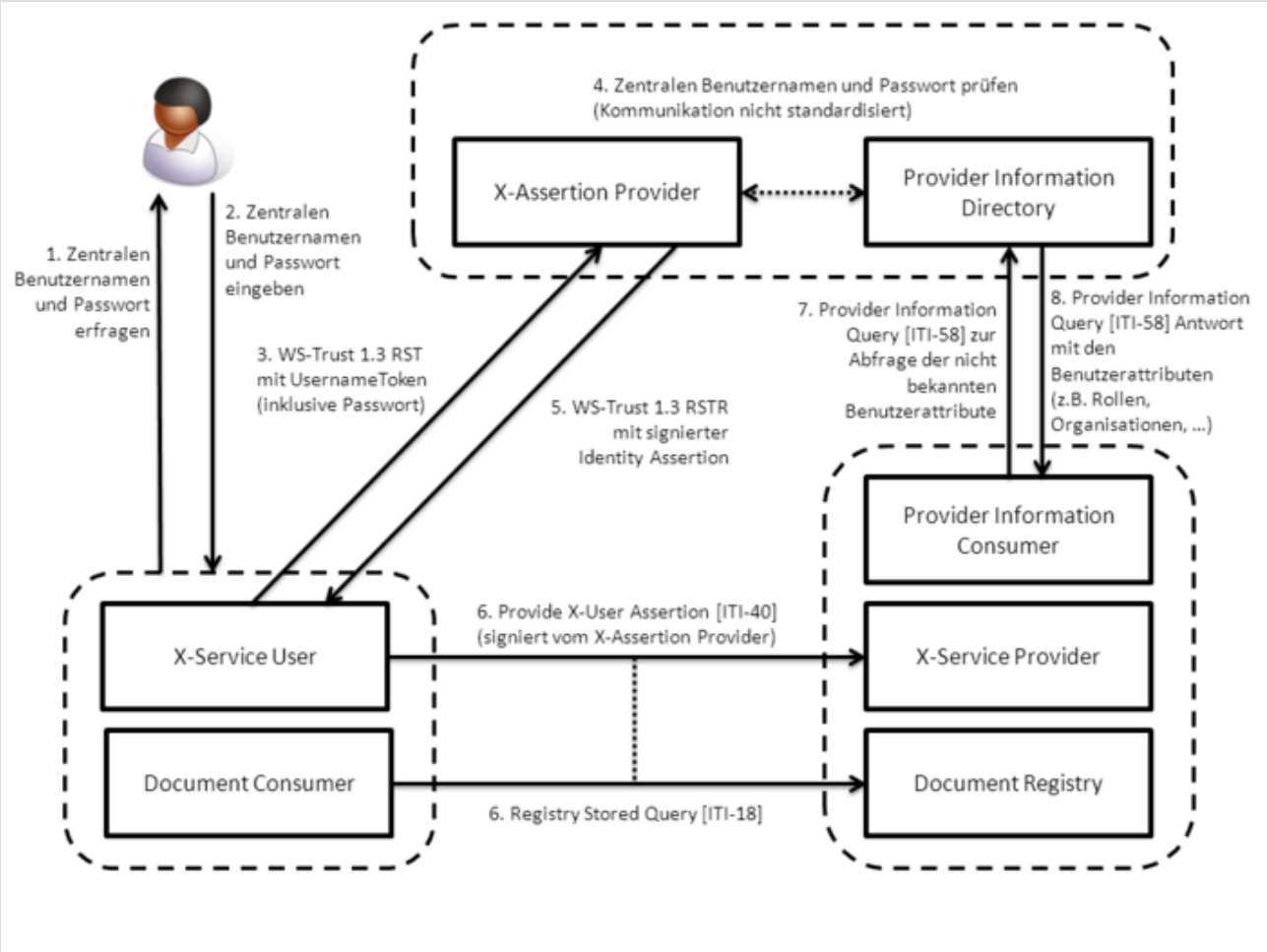


Die Organisationen sollten zumindest auf einer Granularitätsstufe zentral bekannt gemacht werden, die eine sinnvolle Berechtigungsvergabe ermöglicht. Zum Beispiel reicht eine einzelne Organisation "Universitätsklinikum X" nicht aus. Selbst eine Aufteilung auf Fachkliniken (z.B. "Universitätsklinikum X - Chirurgische Klinik") kann schon zu Grobgranular sein. Sinnvoll ist eine Abbildung der zu berechtigenden Organisationen im zentralen System die den Kreis der dadurch berechtigten Ärzte auf ca. 20 oder weniger beschränkt (z.B. "Universitätsklinikum X - Chirurgische Klinik - Gefässchirurgie"). Wenn eine Einrichtung, die lokale Benutzeridentitäten verwaltet, es anderen Teilnehmern ermöglichen will ihre lokal verwalteten Benutzer direkt zu berechtigen, muss sie zusätzlich eine HPD Provider Information Query Schnittstelle anbieten. Der zentrale HPD Server kann dann als virtuelles Verzeichnis auftreten und Anfragen nicht nur mit den eigenen Daten beantworten, sondern auch die Antworten aus den dezentralen Verzeichnissen aggregieren. Die Möglichkeit die lokalen Benutzeridentitäten zentral abzufragen, kann auch für andere Anwendungen sinnvoll genutzt werden, z.B. für Addressbuchfunktionen in einem Secure Messaging Dienst.

4.3.2.4 Lokale Eingabe der zentralen Benutzeridentität

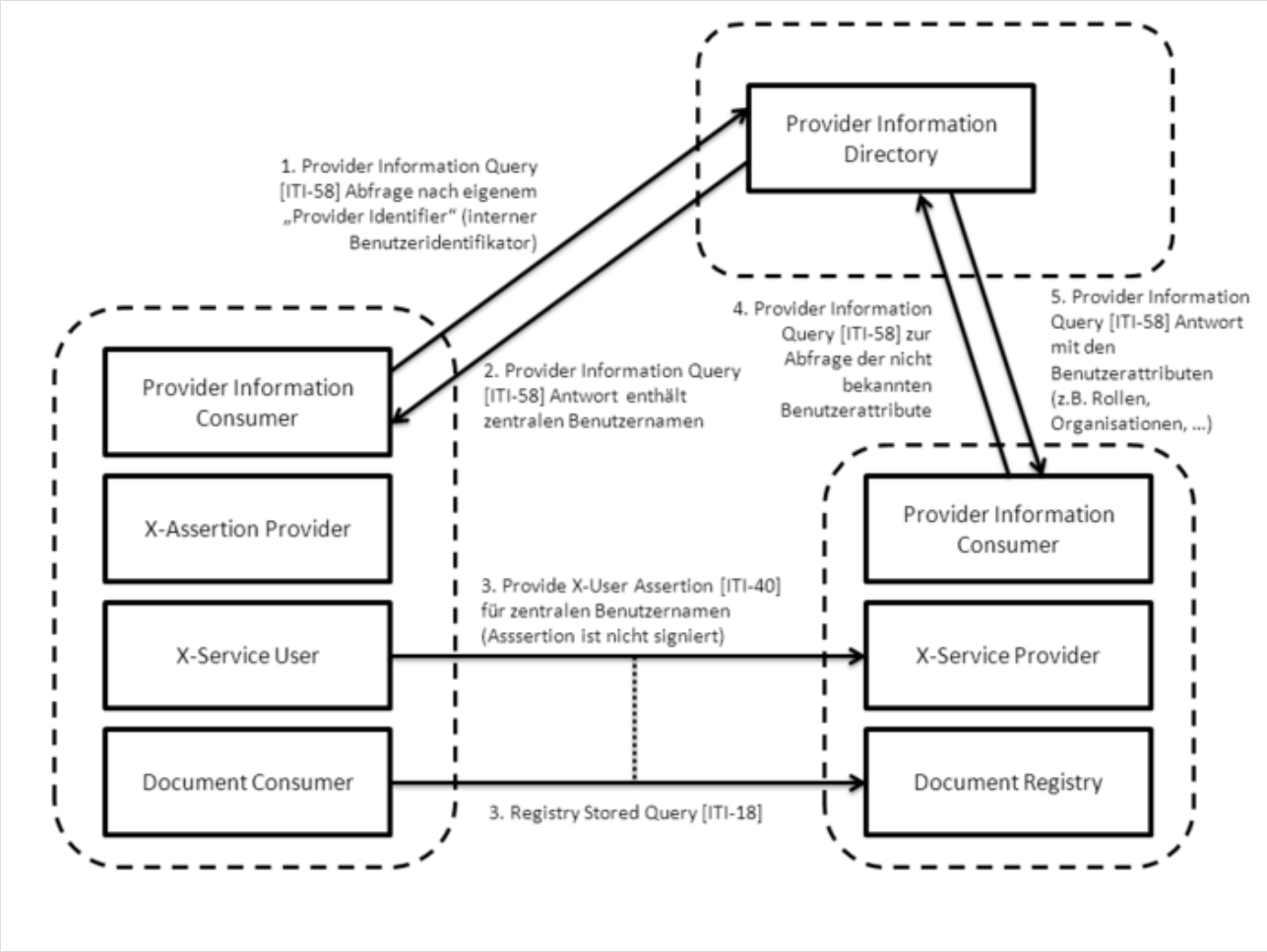
Dieser Ansatz setzt die Eingabe des zentralen Benutzernamens und des zugehörigen Passworts durch den Benutzer voraus. Die Aufgabe der Zuordnung einer zentralen Identität wird dadurch auf den Benutzer verlagert. Die Assertion mit der zentralen Benutzeridentität wird von einem zentralen Service geholt – der Ablauf deckt sich mit der technischen Lösung „Zentrale Ausstellung der Assertion“.

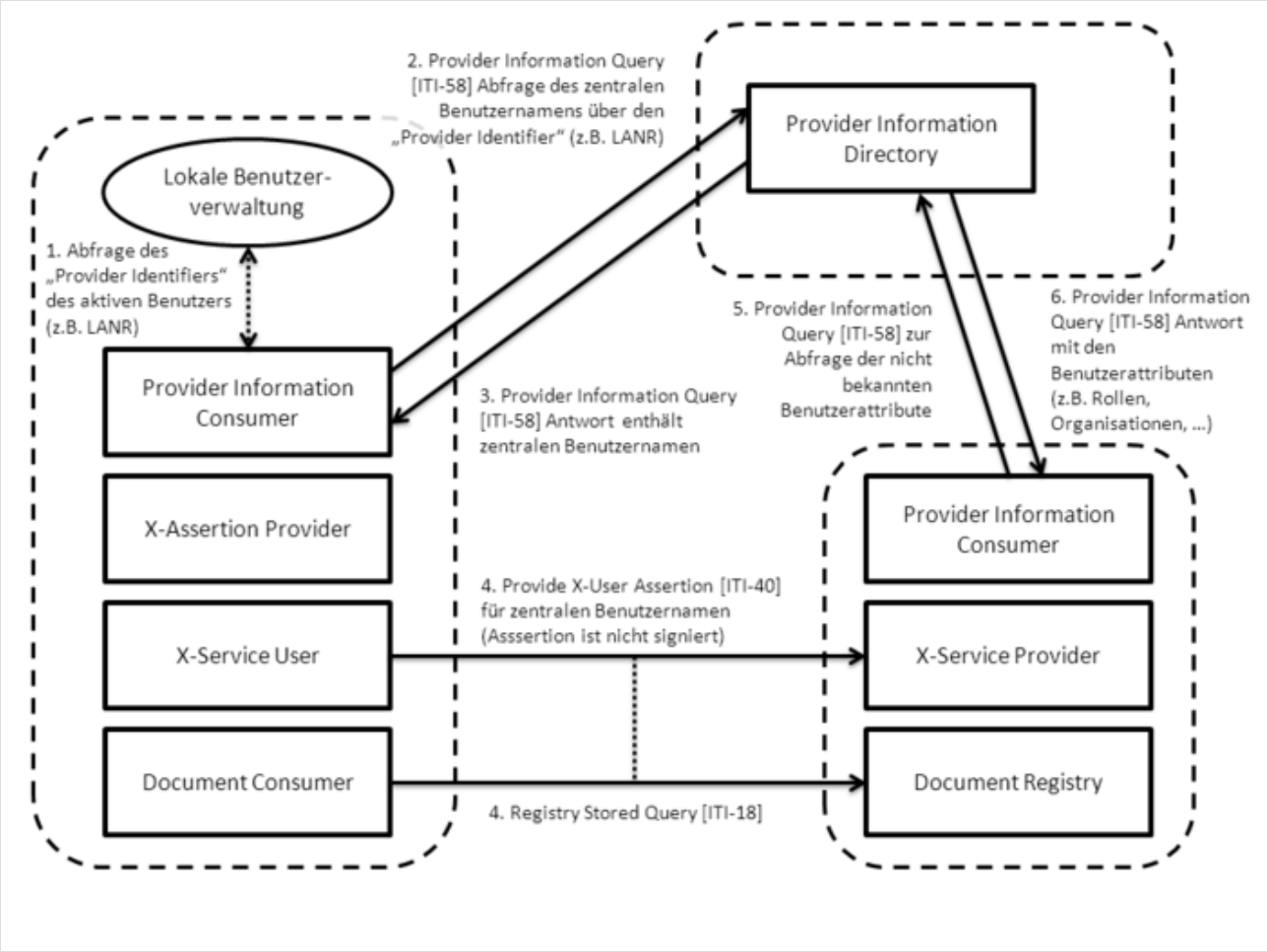
Im Gegensatz zu den anderen hier vorgestellten Methoden ist die Nutzung für den medizinischen Benutzer eher umständlich. Dies kann durch eine temporäre Speicherung des Passworts zwar gelindert werden, aus Sicherheitsgründen sollte aber keine permanente Speicherung des Passworts im anfragenden System durchgeführt werden. Ein sinnvoller Kompromiss wäre es, das Passwort im flüchtigen Speicher für die Dauer der Session zu halten, um bei zeitlich kurz aufeinanderfolgenden Abfragen und Additionen zur zentralen Akte das Passwort nicht mehrfach eingeben zu müssen. Ein Vorteil der manuellen Eingabe von zentralem Benutzernamen und Passwort gegenüber den anderen Ansätzen ist die Möglichkeit die Eingabe bei Installationen einzusetzen die — trotz anderslautender Datenschutz-Empfehlungen — einen lokalen Benutzeraccount für mehrere Benutzer verwenden (z.B. ein Login für alle Mitarbeiter einer Station eines Krankenhauses). Im Gegensatz zu einer Arztpraxis gibt es bei einem Stationslogin üblicherweise eine größere Anzahl an pflegerischen und ärztlichen Benutzern, die somit auch als unterschiedliche Benutzer in der zentralen Akte auftreten sollten. Während das lokale System keine Unterscheidung zwischen den unterschiedlichen Benutzern macht, kann die Kommunikation mit der zentralen Akte somit trotzdem einen spezifischen Benutzerkontext verwenden.



4.3.2.5 Dynamisches Mapping der Benutzeridentität

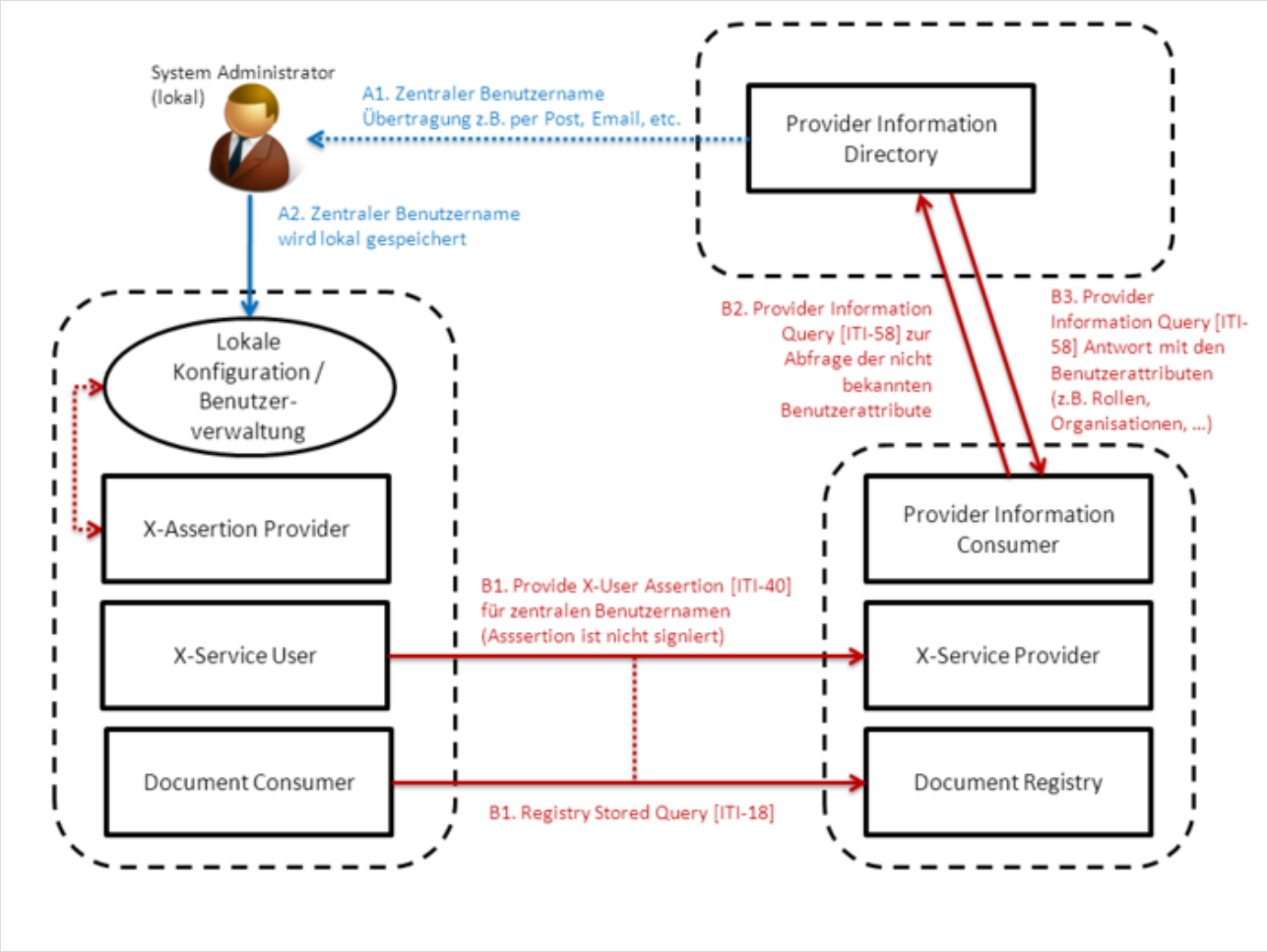
Die Ermittlung der zentralen Benutzeridentität (Schritt 0) besteht hier in der Abfrage an das HPD. Das lokale System erfragt über einen eigenen Identifier oder über einen unabhängig vergebenen Identifier den zentralen Benutzernamen des lokalen Benutzers und erstellt dadurch eine Verknüpfung zwischen der lokalen und der zentralen Benutzeridentität. Der zentrale Benutzername wird durch eine nicht signierte SAML Assertion im SOAP Header der Antwort übertragen. Um die Verknüpfung zwischen dem lokalen und dem zentralen Benutzeraccount herzustellen, muss ein im lokalem System gepflegter Identifikator auch im zentralen HPD vorhanden sein. Idealerweise werden dazu unabhängig vergebene Identifikatoren verwendet, d.h. Identifikatoren die landesweit (oder zumindest regional) eindeutig und öffentlich bekannt sind. Im kassenärtzlichen Bereich ist für Ärzte die LANR (Lebenslange Arztnummer (http://www.kbv.de/12296.html)) dafür geeignet. Im stationären Bereich gibt es für ärztliche Benutzer derzeit keinen equivalenten Identifikator. In einigen Fällen lässt sich ggf. die Mitgliedsnummer der jeweiligen Ärztekammer nutzen. Jedoch muss dies aus Sicherheitsgründen mit den Ärztekammern abgesprochen werden, da einige Ärztekammern die Mitgliedsnummer als Teil des Logins für einen Mitgliederbereich nutzen. In Zukunft lässt sich der Heilberufsausweis als Quelle einer eindeutigen Identifikation nutzen, da der Distinguished Name des Zertifikats eindeutig und nicht geheim sein sollte. Wenn kein von unabhängiger Stelle vergebener Identifikator verwendbar ist, kann ein System alternativ auch einen "lokalen" Provider Identifier zur zentralen Benutzeridentität hinzufügen. Ein solcher lokaler Identifier wäre z.B. die Benutzernummer im KIS. Aus Sicherheitsgründen sollte hier nicht der (lokale) Benutzername verwendet werden, der eine Anmeldung im lokalen System erlaubt (d.h. die Arztnummer im KIS eignet sich, der Benutzername des Arztes im KIS eignet sich nicht.) Ähnlich wie bei einem MPI würden die Quellsysteme ihre Benutzeridentitäten über die Feed Transaktion abliefern und das Healthcare Provider Directory würde voll- oder halbautomatisch Zuordnungen zu einer zentralen Benutzeridentität herstellen und den lokalen Provider Identifier zum zentralen HPD Eintrag hinzufügen. Ein solcher Mechanismus kann über die HPD Provider Information Feed [ITI-59] Transaktion angestoßen werden, wenn das Healthcare Provider Directory eine automatische "disambiguation" unterstützt. Da die für die Zuordnung verwendeten Provider Identifier im Healthcare Provider Directory gespeichert werden, sollte das lokale System den durch die ITI-58 Query ermittelten zentralen Benutzernamen nicht persistent im eigenen System ablegen. Die exklusive permanente Speicherung im HPD stellt sicher, dass Änderungen an der Zuordnung eines Provider Identifiers im HPD auch Auswirkungen im lokalen System haben und es somit nicht zu einem Auseinanderlaufen der beteiligten Systeme kommt. Um niedrige Antwortzeiten bei der Arbeit mit dem einrichtungsübergreifendem Aktensystem zu ermöglichen ist eine temporäre Zwischenspeicherung des zentralen Benutzernamens (d.h. ein Caching) aber durchaus angebracht und sinnvoll. Der Empfänger der per Provide X-User Assertion [ITI-40] übertragenen Benutzeridentität verwendet dann die Provider Information Query [ITI-58] aus IHE HPD um die nicht bekannten Benutzerattribute abzurufen. Der Ansatz ein automatisches Mapping der Benutzeridentität durchzuführen ist für mittelgroße Krankenhäuser sinnvoll. Kleinere Krankenhäuser mit wenigen Benutzern können effizienter mit einem manuellen Mapping arbeiten (siehe Abschnitt "Manuelles Mapping durch einen Administrator"), um die Integration möglichst einfach zu gestalten. Größere Krankenhäuser können einen umfangreichen Abgleich der Benutzeridentitäten vermeiden, in dem sie ihre lokalen Benutzeridentitäten verwenden und einen eigenen HPD Dienst anbieten (siehe Abschnitt "Verwendung lokaler Benutzeridentitäten").


Provider Information Directory
1. Provider Information Query [ITI-58] Abfrage nach eigenem „Provider Identifier" (interner Benutzeridentifikator)
2. Provider Information Query [ITI-58] Antwort enthält zentralen Benutzernamen
4. Provider Information Query [ITI-58] zur Abfrage der nicht bekannten Benutzerattribute
5. Provider Information Query [ITI-58] Antwort mit den Benutzerattributen (z.B. Rollen, Organisationen, ...)
Provider Information Consumer
X-Assertion Provider
X-Service User
Document Consumer
Provider Information Consumer
X-Service Provider
Document Registry
3. Provide X-User Assertion [ITI-40] für zentralen Benutzernamen (Asssertion ist nicht signiert)
3. Registry Stored Query [ITI-18]



4.3.2.6 Statisches Mapping der Benutzeridentität

In vielen Fällen ist die Minimallösung, die zentrale Identität des Benutzers durch einen Administrator im lokalen System fest zu konfigurieren, durchaus ausreichend (z.B. in einer Arztpraxis). Der Administrator erfährt die zu konfigurierenden Benutzernamen über einen beliebigen Mechanismus — z.B. per Post, Email, ein Webportal, ein HPD client. Der zentrale Benutzername wird im lokalen System permanent gespeichert. Anschliessend besteht die Ermittlung der zentralen Benutzeridentität nur darin, die ID vom lokalen Speicher abzurufen. Das lokale System fügt den Anfragen an das zentrale Aktensystem eine selbst-ausgestellte SAML Assertion hinzu, die den zentralen Benutzernamen beinhält. Wenn das anfragende System mehrere zentrale Benutzernamen gespeichert hat, muss es über den gerade aktiven Benutzer oder Mandanten den passenden zentralen Benutzernamen auswählen. Das zentrale Aktensystem benutzt den Benutzernamen aus der Assertion um die Benutzerattribute im zentralen Healthcare Provider Directory nachzuschlagen. Die vom lokalen System ausgestellte Assertion entspricht prinzipiell den Vorgaben des XUA Profils, mit den weiter unten beschriebenen Anpassungen für lokal ausgestellte Assertions. Der Ansatz eignet sich besonders für Arztpraxen und Einrichtungen mit wenigen Benutzern (z.B. kleinere Krankenhäuser, MVZs). In Arztpraxen (Individual- und Gemeinschaftspraxen) wäre eine Identifikation einzelner Benutzer (z.B. ArzthelferInnen) nicht praxisgerecht, da der Arzt dort üblicherweise Tätigkeiten an seine MitarbeiterInnen delegiert und diese im Berechtigungskontext des Arztes ausgeführt werden sollten. Entsprechend sollten Berechtigungen auch auf der Ebene der Arztpraxis gewährt werden, um die realen Zugriffsmöglichkeiten für alle Teilnehmer transparent sichtbar zu machen. Bei MVZs und Praxisgemeinschaften, die ihre Daten durch unterschiedliche Mandanten trennen, könnte eine zentrale Benutzeridentität pro Mandant verwendet werden. In einem kleinen Krankenhaus würde für jeden Benutzer, der einen Zugriff auf das zentrale Aktensystem benötigt, jeweils eine eigene zentrale Benutzeridentität geführt werden.



4.3.2.7 Zentrales Healthcare Provider Directory

Durch ein zentrales Benutzerverzeichnis sind alle zentralen Benutzeridentitäten und alle für die Zugriffskontrolle relevanten Organisationen über einen zentralen Dienst abrufbar. Ein solcher zentralisierter Dienst sollte in einem IHE-basierten System durch den Akteur Provider Information Directory des IHE HPD Profils (siehe 2.2.6) abgebildet werden. Ausser den im HPD Profil beschriebenen Funktionalitäten, ist es für einen Verzeichnisdienst in vielen Fällen sinnvoll auch einen WS-Trust Secure Token Service (STS) zu implementieren. Der STS kann über die Request Security Token Transaktion eine SAML Assertion bezüglich der Identität und Attribute eines Benutzers ausstellen (siehe Abschnitt "Eingabe des zentralen Benutzernamens und eines Passworts durch den Benutzer"). Eine besondere Variante des zentralen Benutzerverzeichnisses ist ein hierarchischer Verzeichnisbaum. Der zentrale Dienst ist dann nur ein virtuelles Verzeichnis, das die Anfragen an die untergeordneten Verzeichnisse weiterleitet und die Antworten bündelt und normalisiert. Ein hierarchisches System unterscheidet sich in der Pflege der Verzeichnisdaten (die dezentral durchgeführt wird), verhält sich für die Suche und die Authentifizierung aber effektiv wie ein einziges System (siehe Abschnitt "Verwendung lokaler Benutzeridentitäten").

4.3.2.8 Eigenschaften der Assertion

Das ITI TF Supplement "Cross-Enterprise User Assertion - Attribute Extension (XUA++)" beschreibt wie

- der Klarname des Benutzers (Subject ID),
- die Organisations-ID (Subject Organization ID),
- der Organisationsnamen (Subject Organization),
- die Home Community ID (homeCommunity ID),

- den Verwendungszweck (Purpose of Use),
- die Rolle (Subject-Role) und
- die gerade relevante Patienten-ID (Patient Identifier Attribute)

in einer SAML Assertion übertragen werden können. Jedes Attribut kann dabei laut XUA++ nur einen Wert annehmen, d.h. eine Übertragung von mehreren Rollen ist nicht möglich. Das empfangende zentrale Aktensystem kann viele dieser Informationen auch aus dem vorhandenem zentralen Benutzerverzeichnis (HPD) abfragen. Wenn ein lokales System eines dieser Attribute jedoch in der Assertion mitliefert, muss das Aktensystem ausschliesslich den AttributeValue aus der Assertion für Berechtigungsprüfung, Auditierung und alle anderen Zwecke verwenden. Eine Ausnahme stellen dem zentralen Aktensystem nicht bekannte oder verständliche Werte dar. Das heisst, wenn das anfragende System einen im zentralen Aktensystem geführten Rollencode mitgibt, gilt diese Rolle als einzige Rolle des Benutzers für diese Transaktion, auch wenn für den Benutzer noch andere Rollen im Benutzerverzeichnis geführt werden. Dadurch können z.B. auch Belegarzt-Konstellationen sinnvoll abgebildet werden: Ein Belegarzt ist im HPD zwei Organisationen zugeordnet (KH und eigene Arztpraxis), aber arbeitet entweder gerade mit dem KIS des KH oder mit seinem AIS. Da das KIS ggf. Kopien der Daten anfertigt und sie anderen Krankenhausärzten zur Verfügung stellt, ist es angebracht einen unterschiedlichen Sicherheitskontext für den Zugriff über das KIS zu etablieren.

Das in diesem Dokument beschriebene Sicherheitssystem hat folgende, über XUA hinausgehende Anforderung:

Statement: Um dem zentralen Aktensystem eine performante Sicherheitsüberprüfung zu ermöglichen, muss in allen Assertions (unabhängig davon wer sie ausstellt) die gerade relevante Patienten-ID als Attribut vorhanden sein. Dies ist notwendig, da nicht alle XDS Transaktionen die Patienten-ID beinhalten (z.B. Retrieve Document Set-b, FindFolders Registry Stored Query, etc.).

Statement: Eine weitere über XUA hinausgehende Festlegung ist, dass das zentrale Aktensystem folgende Verwendungszwecke (Purpose of Use) aus dem ISO 14265 Kodiersystem unterstützen muss:

- Code "1" ("Clinical care provision to an individual subject of care")
- Code "2" ("Emergency care provision to an individual subject of care")

Solange in der Assertion kein Verwendungszweck enthalten ist, muss das zentrale Aktensystem Code "1" annehmen.

Beim ersten Mapping Ansatz (siehe Abschnitt "Verwendung lokaler Benutzeridentitäten") sind die verwendeten Benutzeridentitäten nicht unbedingt in einem zentralen Verzeichnis vorhanden. Daher müssen bei diesem Ansatz ausser der Patienten-ID auch folgende Attribute in der Assertion vorhanden sein:

- der Klarname des Benutzers (Subject ID),
- die Organisations-ID (Subject Organization ID),
- der Organisationsnamen (Subject Organization) und
- die Rolle (Subject-Role).

Wenn dies für die durchzuführende Transaktion angebracht ist, können optional auch der Verwendungszweck und die Home Community ID als Teil der Assertion übertragen werden.

4.3.2.9 Zentrale Ausstellung der Assertion

Diese Architektur entspricht dem Integrationsprofil XUA. Neben den zusätzlichen Festlegungen für Assertion-Inhalte (siehe oben) werden im Weiteren zusätzliche Annahmen getroffen. Diese technische Lösung sollte nur dann eingesetzt werden, wenn der in Abschnitt 4.3.2.4 beschriebene Mapping Ansatz verwendet wird, da ansonsten die Assertion lokal ausgestellt wird.

Statement:Die Kommunikation zwischen den Actors X-Service User einerseits und dem X-Assertion-Provider andererseits entspricht den Vorgaben von WS-Trust 1.3, wie im Weiteren beschrieben.

Statement:Zur Authentifizierung des Actors X-Service User beim User Authentication Provider (gruppiert mit X-Assertion-Provider) wird das Passwort verwendet.

Das lokale System, nachdem es den zentralen Benutzernamen und das Passwort vom Benutzer eingeholt hat, stellt eine WS-Trust 1.3 konforme Request Security Token (RST) Anfrage an einen mit dem HPD gekoppelten X-Assertion Provider. Die Anfrage wird (wie jegliche hier beschriebene Kommunikation) über beidseitig authentifiziertes HTTPS abgesichert. Der Benutzername und das Passwort werden als UsernameToken (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf) mit Password (im Klartext) im OnBehalfOf Element der Request Security Token Anfrage übermittelt (http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html#_Toc162064988). Der X-Assertion Provider (hier ein WS-Trust STS) ist mit dem HPD gekoppelt und überprüft die Benutzername - Passwort Kombination. Wie diese Überprüfung kommuniziert wird, kann von der Implementierung festgelegt werden. Da das HPD Profil DSML zur Kommunikation verwendet wird, bietet sich eine Authentifizierung per DSML über den "BIND" Mechanismus oder den "whoami" Mechanismus an. Nach einer erfolgreichen Prüfung vom zentralen Benutzernamen und Passwort, stellt der WS-Trust STS eine Assertion aus und kommuniziert diese in einer WS-Trust Request Security Token Response. Die Assertion wird dabei vom STS signiert. Als SubjectConfirmationMethod wird "bearer" verwendet. Es muss in diesem Fall ausserdem "PasswordProtectedTransport" als Authorization Context Class verwendet werden (http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf). Die so erhaltene Identity Assertion, die vom X-Assertion Provider signiert wurde, fügt der X-Service Consumer in den durchzuführenden SOAP Aufruf im SOAP Header als WS-Security spezifizierte SAML Assertion ein, wie es in der IHE XUA Transaktion Provide X-User Assertion [ITI-40] beschrieben wird. Die Assertion kann optional auch noch durch eine Signatur des X-Service Consumers an die spezifische Nachricht gebunden werden. Dies ist nicht zwingend notwendig, da durch die HTTPS Verbindung ein Auslesen des Tokens (und somit die Verwendung in einem "Replay" Angriff) verhindert werden kann.

Der Benutzer gibt nur den Benutzernamen und das Passwort ein; die zugehörigen Attribute wie Rolle, Organisation, Fachrichtung, etc. sind nicht unbedingt im anfragendem System verfügbar, weil sie entweder dort anders geführt werden (z.B. in anderen Kodiersystemen oder kombiniert mit anderen Attributen) oder einfach nicht bekannt sind. Daher muss das zentrale Aktensystem die Attribute des Benutzers in einem zentralen Verzeichnis per HPD nachschlagen. Dazu verwendet das empfangende System (d.h. der X-Service Provider) einen Provider Information Consumer der über die Provider Information Query [ITI-58] die Attribute des über die Assertion identifizierten Benutzers abfragt. Da der X-Assertion-Provider in Form eines WS-Trust Secure Token Service (STS) in diesem Ansatz mit dem Actor HPD gruppiert ist, hat der STS die Möglichkeit AttributeStatements eigenständig hinzuzufügen. Dies gilt für die (auch) im HPD gepflegten Attribute Organization Name, Organization ID, Subject ID, Subject Role und homeCommunity ID. Da die Assertion vom STS ausgestellt und signiert wird, müssen die Attribute als Claims in der Request Security Token Nachricht vorliegen. Während das automatische *Hinzufügen* von Attributen, die nicht per Claim vom X-Service User angefragt wurden, durchaus sinnvoll ist, sollte das *Prüfen* von Claims vermieden werden. Das lokale System kann den gerade relevanten Sicherheitskontext normalerweise weitaus besser festlegen. Wenn zum Beispiel ein Benutzer nicht der Organisation KH 1 zugeordnet ist, er aber konsiliarisch hinzugezogen wird und seinen (zentralen) Benutzernamen und sein Passwort in der entsprechenden KIS-Maske eingibt, ist der Claim "Organization=KH1" korrekt, obwohl er vom zentralen HPD nicht verifiziert werden kann. Ein weiterer Aspekt ist, dass ein gewisses Vertrauen in das lokale System sowieso schon notwendig ist, da einige Claims überhaupt nicht automatisch zentral geprüft werden können (Patienten-ID, Verwendungszweck).

4.3.2.10 Lokale Ausstellung der Assertion

In diesem Ansatz ist der X-Assertion Provider mit dem X-Service User gruppiert. Dies kann sinnvoll in den unter Verwendung lokaler Benutzeridentitäten, Dynamisches Mapping der Benutzeridentität und Statisches Mapping der Benutzeridentität beschriebenen Mapping Ansätzen verwendet werden. Da hier das anfragende System die Assertion selbst ausstellt, kann es ohne weiteres beliebige Attribute Statements hinzufügen, die dem zentralen Aktensystem die oben beschriebenen Attribute des Benutzers mitteilen. Bei einer Gruppierung der Actors X-Service User und X-Assertion Provider ergeben sich gegenüber den aktuellen Vorgaben des XUA Profils zwei Vereinfachungen. Erstens ist als 'SubjectConfirmationMethod' "SenderVouches" zu verwenden. Dies signalisiert dem Empfänger, dass der Sender für die Identität des Benutzers "bürgt" und nicht ein Drittsystem (wie ein zentraler Verzeichnisdienst) die Verantwortung trägt. Zweitens muss die Assertion nicht signiert werden, da das gleiche System die Kommunikation über ihr SSL Zertifikat verschlüsselt und die zusätzliche Signatur der Assertion durch ein zweites Zertifikat desselben Systems keinen Sicherheitsgewinn bringt. IHE Deutschland wird sich für eine entsprechende Anpassung des IHE XUA Profils im Rahmen des Change Proposal Prozesses für Revision 10 des ITI Technical Frameworks einsetzen.

4.3.2.11 Zusammenfassung

Es wurden verschiedene Ansätze zur Benutzeridentifikation vorgestellt und technisch beschrieben. Jeder der Ansätze eignet sich für eine spezifische Anwenderzielgruppe:

Übersicht der vorgestellten Lösungsansätze zur Benutzeridentifikation.

Nummer	Mapping Ansatz	Zielgruppe	Bemerkungen
1	Verwendung lokaler Benutzeridentitäten	Große Krankenhäuser	Optional: lokales HPD als Teil eines zentralen virtuellen Verzeichnis
2	Eingabe des zentralen Benutzernamens und eines Passworts durch den Benutzer	Krankenhäuser mit Stations-Login	Assertions werden zentral ausgestellt und signiert
3	Automatisches Mapping über einen Identifier	Mittelgroße Krankenhäuser	Entweder über unabhängig vergebene Benutzer-IDs oder durch MPI-ähnliche Zuordnung lokaler Benutzer-IDs zum zentralen Account
4	Manuelles Mapping durch einen Administrator	Arztpraxen, Gemainschaftspraxen, Praxisgemeinschaften, MVZ, kleine Krankenhäuser	

Ein zentrales Healthcare Provider Directory (HPD) wird in allen Fällen gebraucht, aber bei Ansatz 1 ist es nur für die Organisationen (d.h. die Organizational Providers) verpflichtend. Die Benutzeridentität wird immer über eine SAML Assertion kommuniziert. Diese Assertion muss zumindest die Patienten-ID als AttributeStatement enthalten. Wenn die Assertion weitere Attribute beinhaltet, sind diese anstelle der im zentralen HPD vorhandenen Attribute zuverwenden. Nach der hier beschriebenen Übertragung der Benutzeridentität als SAML Assertion und einer ggf. notwendigen Abfrage der Benutzerattribute kennt das zentrale Aktensystem unabhängig vom gewählten Ansatz immer die folgende Information zur laufenden Transaktion: Namen des Benutzers (ID und Klartext), seine Rolle und Organisation, die relevante Patienten-ID sowie den Verwendungszweck.

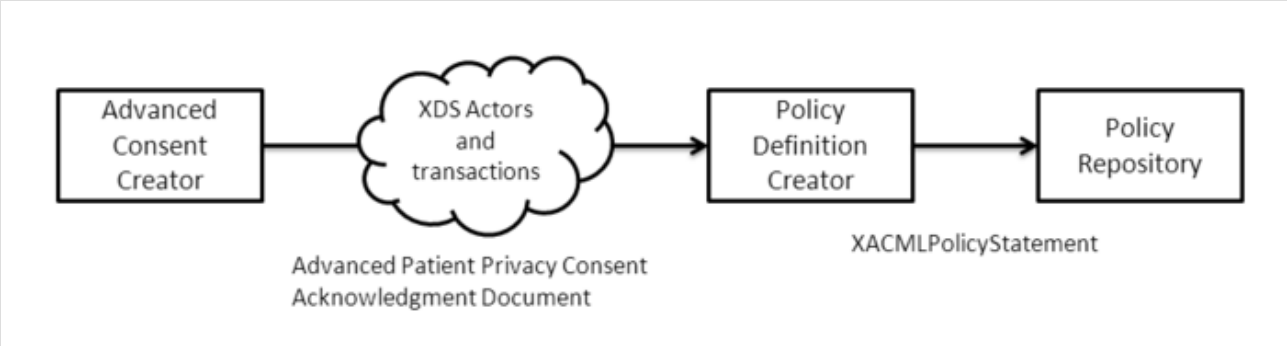
4.3.3 Verwalten von Berechtigungen

Der Patient steuert die Zugriffsrechte in der elektronischen Patientenakte über Patientenzustimmungsdokumente (hier synonym mit "Einwilligungserklärung", "Patient Consent" und "Privacy Policy Acknowledgment Document"). Das IHE BPPC Profil, wie in Abschnitt 2.2.10 erläutert, ermöglicht keine feingranulare Zugriffskontrolle. Eine solche feingranulare Kontrolle (z.B. Einschränkung auf berechtigte Organisationen) ist in deutschen Vernetzungsprojekten (unabhängig vom Aktentyp) jedoch notwendig (siehe Abschnitt 2.1). Daher wird in diesem Abschnitt ein alternativer Ansatz zur Zugriffskontrolle beschrieben. Dieser Ansatz basiert auf der in Abschnitt 2.2.11 vorgestellten eXtensible Access Control Markup Language (XACML). IHE Deutschland wird die hier vorgestellten Konzepte in zukünftigen Spezifikationen und Integrationsprofilen weiter formalisieren.

Während in diesem Abschnitt (4.3.3) die Erstellung, die zentrale Ablage und die Struktur von Patientenzustimmung und den Zugriffsregeln beschrieben wird, erläutert der Abschnitt 4.3.4 die Entscheidungsfindung für Zugriffsentscheidungen, deren Durchsetzung sowie die Anwendung auf die Cookbook-relevanten IHE Profile und Transaktionen.

Welche Steuerungsmöglichkeiten für seine Zugriffsrechte (d.h. für einen Fall, die ganze Akte, ein Dokument, etc.) der Patient hat, sowie die Form und der Zeitpunkt der Zustimmung werden spezifisch für jeden Aktentyp im Kapitel 4.4 beschrieben.

4.3.3.1 Verwaltung der Patientenzustimmung und Zugriffsregeln



Der Advanced Consent Creator erstellt ein elektronisches Patientenzustimmungsdokument als CDA-Dokument, gegebenenfalls mit eingebetteten XACML Regeln. Dieses Dokument wird über einen gruppierten Document Source Akteur an die XDS Infrastruktur übertragen. Ein Policy Definition Creator empfängt das Patientenzustimmungsdokument über einen gruppierten Document Consumer Akteur. Der Policy Definition Creator wandelt die Patientenzustimmung in ein detailliertes, direkt vom Authorisierungssystem nutzbares XACML PolicySet um und legt dieses, sowie die eingebetteten XACML Regeln, im Policy Repository ab. Der Advanced Consent Creator muss in vielen Fällen mit einem HPD Provider Information Consumer gruppiert werden, um die zu berechtigenden Organisationen oder Leistungserbringer eindeutig identifizieren zu können.

4.3.3.2 Struktur des Patientenzustimmungsdokuments

Es gibt zwei Möglichkeiten bei der Abbildung des Patientenzustimmungsdokuments:

1. als klassisches Basic Patient Privacy Consent Acknowledgment Document
2. als "bvitg-efa Patientenzustimmungs-CDA" mit optional eingebettetem XACML

Das klassische BPPC Acknowledgment Document wird unterstützt um Kompatibilität mit bestehenden BPPC-basierten Patientenzustimmungen zu ermöglichen. Während das gleiche CDA-Dokument wie bei BPPC verwendet wird, werden die Privacy Policies in Form von vorher hinterlegten XACML Policy Definitionen nach dem weiter unten detaillierten Standard abgebildet. Dadurch kann ein Zugriff auf Patientenakten ermöglicht werden, bei denen der Patient der Verwendung mittels eines BPPC Acknowledgment Documents zugestimmt hat. Die Durchsetzung der Zugriffsregeln wird dabei aber auf der in diesem Cookbook beschriebenen technologischen Basis umgesetzt.

Das bvitg-efa Patientenzustimmungs-CDA bietet die Möglichkeit Organisationen oder Benutzer zu benennen die vordefinierte Zugriffsrechte haben, ohne dafür XACML-Konstrukte verwenden zu müssen. Dies ist zum Beispiel bei zweckgebundenen Akten wie Fallakten hilfreich, da dort üblicherweise alle Mitbehandler über die gleichen Berechtigungen für den gleichen Zeitraum verfügen. Um auch Aktentypen mit komplexeren Berechtigungen umsetzen zu können, ermöglicht das CDA die Einbettung von XACML Regeln (wie weiter unten noch zu beschreiben). Die eingebetteten XACML Regeln erlauben feingranulare patientenspezifische und organisationsspezifische Zugriffsbeschränkungen.

4.3.3.3 Struktur der Zugriffsregeln

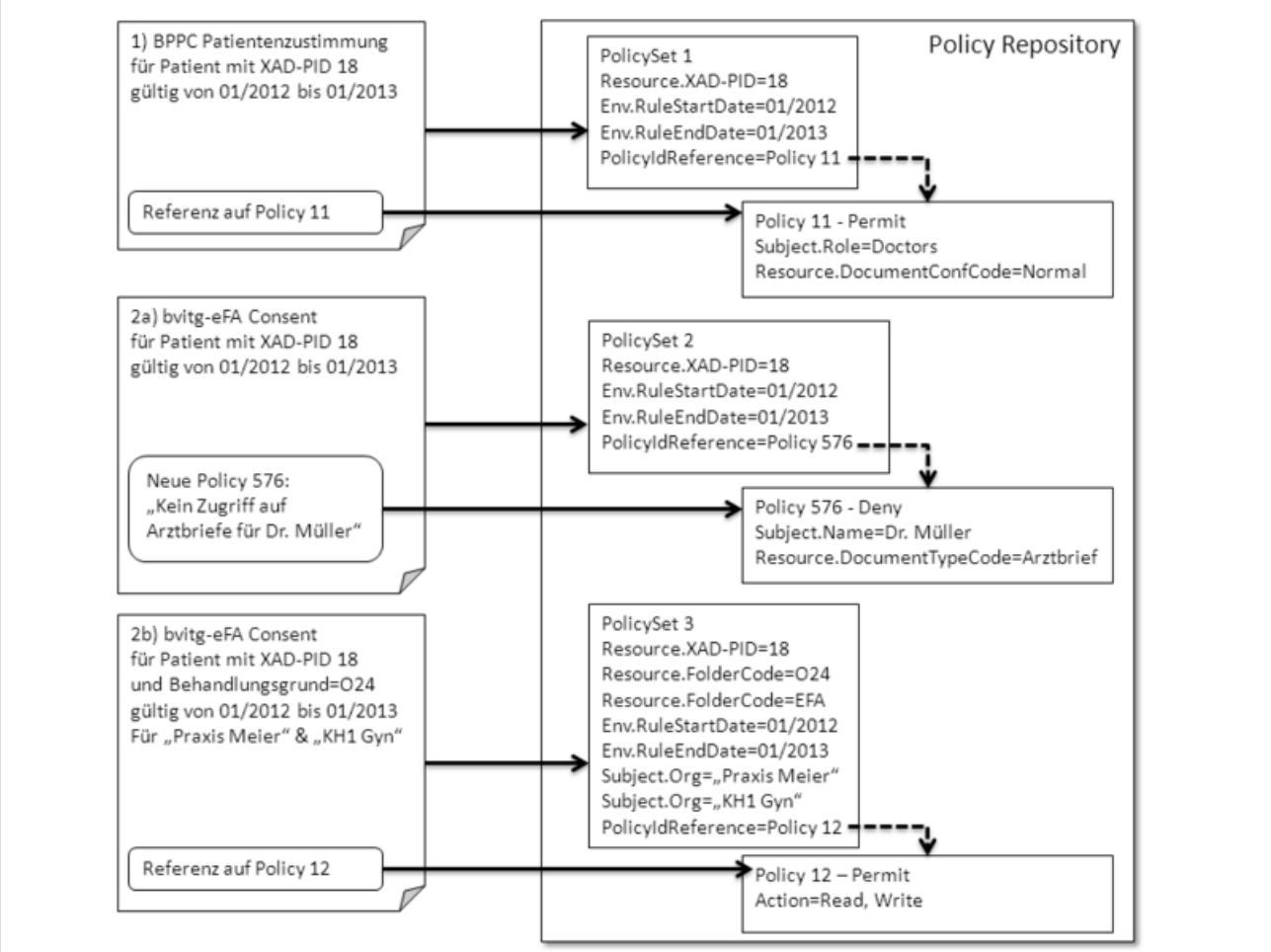
Das Abrufen und Prüfen des Patientenzustimmungsdokuments während der Entscheidungsfindung für eine Abfrage medizinischer Daten würde eine unnötig lange Verzögerung nach sich ziehen. Daher wird in diesem Abschnitt beschrieben wie die XACML Policy Definition Sprachkonstrukte genutzt werden können um sowohl die relevanten Teile der Patientenzustimmung als auch die eingebetteten oder referenzierten Zugriffsregeln abzubilden.

Die im vorherigen Abschnitt vorgestellten Varianten der Patientenzustimmungsdokumente können folgende für die Zugriffsentscheidung relevanten Informationen beinhalten:

Daten	1) BPPC	2) Advanced Consent / bvitg-eFA Consent
Patienten ID (XAD-PID)	ja	ja
Gültig von (Datum)	ja	ja
Gültig bis (Datum)	ja	ja
Behandlungsgrund	nein	ja
Autorisierte Organisationen	nein	ja
Referenz auf einen Regelsatz	ja	ja
Pat. spezifische Ausnahmeregeln	nein	ja

Die Daten "Patienten ID", "Gültig von/bis", "Behandlungsgrund", "Autorisierte Organisationen" werden als ein PolicySet in XACML abgebildet. Dieses PolicySet ist eine direkte Entsprechung der Patientenzustimmung und an deren Lifecycle gebunden. D.h. wenn das Patientenzustimmungsdokument als ungültig markiert wird (z.B. durch Änderung des XDSDocumentEntry.availabilityStatus auf "Deprecated"), muss auch das PolicySet invalidiert werden. Wenn die Patientenzustimmung eine oder mehrere patientenspezifische Ausnahmeregelungen beinhält, werden diese als eigenständige XACML Policy Elemente dem Policy Repository hinzugefügt und von dem Patientenzustimmungs-PolicySet referenziert. Dazu wird der XACML Mechanismus PolicyIdReference verwendet. Bei Referenzen auf einen vorhandenen (d.h. nicht in die Patientenzustimmung eingebetteten) Regelsatz, wird die PolicyIdReference zum Verweis auf die vorhandene Policy genutzt.

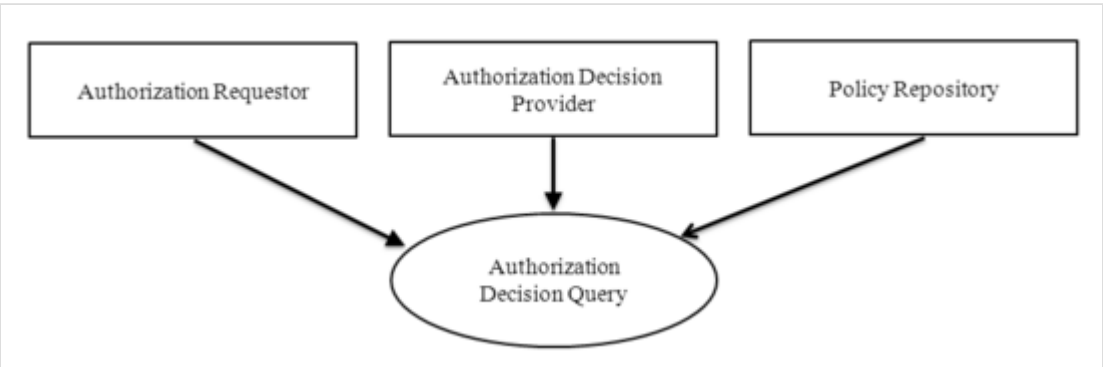
Beispiel zur Umsetzung der Patientenzustimmung auf XACML Konstrukte



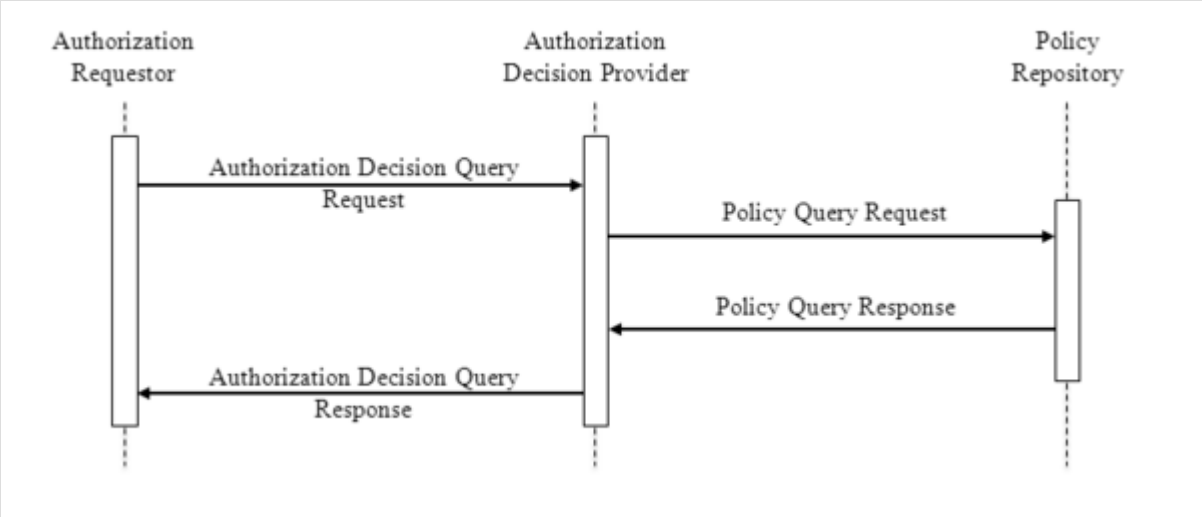
4.3.4 Überprüfen von Berechtigungen

4.3.4.1 Akteure und Transaktionen

In diesem Leitfaden werden folgende neue Akteure zur Feststellung und Durchsetzung der Zugriffsbeschränkungen eingesetzt:



Der neue Use Case "Authorization Decision Query" beschreibt die initiale Feststellung und Durchsetzung der Zugriffsbeschränkungen. Der Akteur Authorization Requestor ist für den Schutz einer bestimmten Ressource (z.B. eines Dokuments) verantwortlich. Ein Zugriff auf die Ressource wird nur gestattet, wenn eine Evaluierung der Zugriffsregeln durch den Akteur Authorization Decision Provider ergibt, dass ein Zugriff in dieser spezifischen Situation konform zu den Zugriffsregeln ist. Die Evaluation der Regeln durch den Authorization Decision Provider geschieht auf Anfrage des Authorization Requestor. Dafür greift der Authorization Decision Provider auf die Details der Anfrage und auf patienten-spezifische Zugriffsregeln (d.h. Policies) zu, die im Policy Repository abgelegt sind. Das Policy Repository gibt auf Anfrage einen Satz von Zugriffsregeln zurück und hat eine (weiter oben diskutierte) Schnittstelle zum Ablegen der Zugriffsregeln.



Die erste Transaktion ist die Anfrage des Authorization Requestor an den Authorization Decision Provider und wird als "Request Authorization Decisions" bezeichnet. Die Transaktion nutzt das SAML-binding für XACML, genauer die Methode "XACMLAuthzDecisionQuery", wobei der Authorization Requestor als XACML Policy Enforcement Point (PEP) agiert und der Authorization Decision Provider als XACML Policy Decision Point (PDP). Als Teil der Anfrage müssen die Benutzer-Identität und Attribute kommuniziert werden. Die Methoden zur Feststellung und Überprüfung der Attribute wird im Abschnitt "Benutzerauthentifizierung und -identifikation" weiter oben diskutiert. Ausserdem müssen die für die zu schützende IHE Transaktion notwendigen Informationen zur Ressource übermittelt werden (z.B. Patienten ID, Dokumenten IDs, etc.). Details zu den zu übermittelnden Informationen werden weiter unten transaktionspezifisch erläutert. Um mehrere Zugriffsentscheidungen auf einmal abfragen zu können (z.b. eine Entscheidung pro Dokument in einer ITI-18 Antwort) wird das "Multiple resource profile of XACML v2.0" eingesetzt.

Die zweite Transaktion, "Request Policies" wird vom Authorization Decision Provider ausgelöst und an das Policy Repository gerichtet. Technisch wird dies über die Methode "XACMLPolicyQuery" des SAML-bindings für XACML abgebildet, wobei der Authorization Decision Provider als PDP fungiert und das Policy Repository als Policy Administration Point (PAP). Um die Komplexität der Kommunikation und des Policy Repositories zu reduzieren, beschränkt sich die Anfrage hierbei auf die Identifikation des Patienten. Das Policy Repository liefert somit alle für diesen Patienten möglicherweise relevanten Policies zurück an den Authorization Decision Provider. Dieser muss die Anwendbarkeit und die Gültigkeit prüfen, d.h. ist der Regelsatz für die Zugriffsentscheidung zum jetzigen Zeitpunkt relevant oder gilt sie z.B. nicht mehr. Die Antwort wird in der dritten zu diskutierenden Transaktion, "Provide Policies", vom Policy Repository an den Authorization Decision Provider geliefert. Hierfür kommt die SAML/XACML Methode "XACMLPolicyStatement" zum Einsatz. Die Antwort beinhaltet alle Policies die der in der Anfrage erwähnten Patientennummer zugeordnet werden können und alle Policies die unabhängig vom spezifischen Patienten gültig sind (z.B. organisations- oder jurisdiktionsspezifische Zugriffsregelungen). Das Policy Repository muss ausser der Absicherung der Kommunikation durch beidseitige Zertifikate keine Sicherheitsüberprüfung durchführen und somit dem Authorization Decision Provider einen ungefilterten Zugriff auf die Policies des Patienten ermöglichen.

"Provide Authorization Decisions" ist die letzte Transaktion des Use Case "Authorization Decision Query". Sie stellt die Antwort des Authorization Decision Provider an den Authorization Requestor dar. Abgebildet wird dies durch die SAML/XACML Methode "XACMLAuthzDecisionStatement". Mittels dieser Methode gibt der Authorization Decision Provider (hier als PDP) dem Authorization Requestor (als PEP) eine Zugriffsentscheidung pro Ressource (z.B. pro Dokument für eine ITI-18 Registry Stored Query Antwort). Um mehrere Zugriffsentscheidungen auf einmal zurückliefern zu können (z.b. eine Entscheidung pro Dokument in einer ITI-18 Antwort) wird das "Multiple resource profile of XACML v2.0" eingesetzt. Diese vierte und letzte Transaktion folgt nicht direkt auf die dritte Transaktion "Provide Policies" sondern setzt vorraus, dass der Authorization Decision Provider die Informationen aus der ersten ("Request Authorization Decision") und die Policies aus der dritten Transaktion mit allen anderen relevanten Informationen (z.B. den Dokumentenmetadaten) kombiniert und eine Entscheidung pro Ressource fällt.

Wenn zwei oder mehr dieser Akteure im gleichen System implementiert werden, müssen die zwischen Ihnen notwendigen Transaktionen nicht über die definierten Schnittstellen umgesetzt werden, sondern können aus Effizienzgründen auch über andere, proprietäre Schnittstellen übertragen werden. So muss z.B. eine XDS Document Registry, die sowohl Authorization Requestor als auch Authorization Decision Provider ist, die Transaktionen "Authorization Decision Query Request" und "Authorization Decision Query Response" nicht wie dargestellt über die standardisierten, interoperablen Schnittstellen durchführen, sondern kann dafür interne Mechanismen nutzen, solange die resultierende Zugriffsentscheidung dadurch kein anderes Resultat hat.

4.3.4.2 Kombination mit zu existierenden Akteuren und Transaktionen

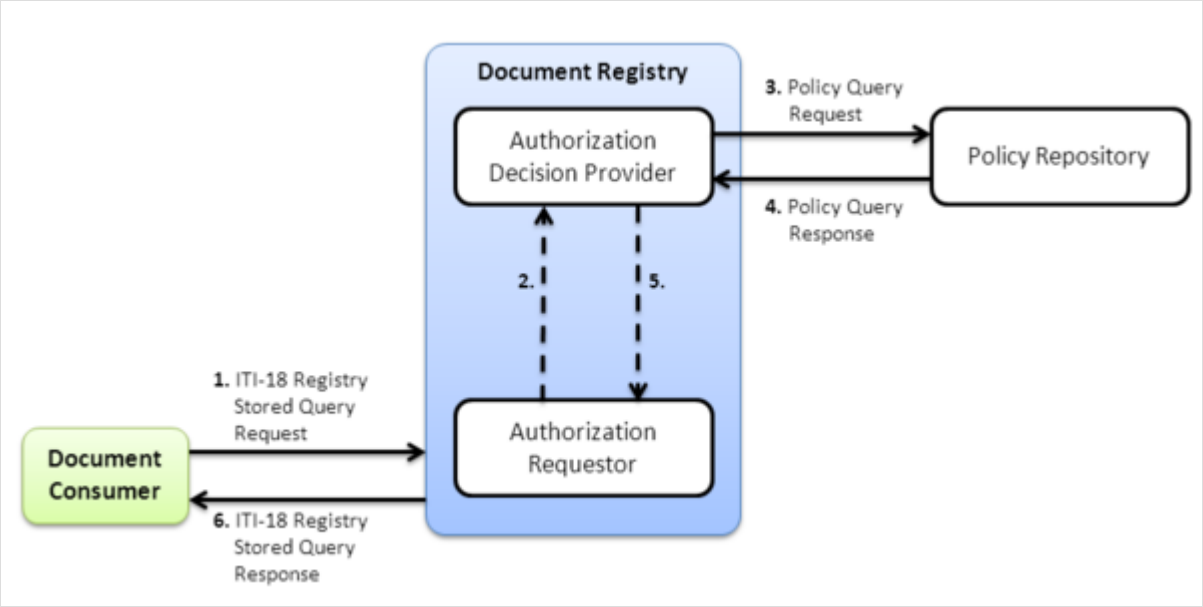
Aufgrund der sehr unterschiedlichen Semantiken der zu schützenden Transaktionen ist es nicht ausreichend den Ablauf der im vorigen Abschnitt vorgestellten Transaktionen unabhängig von XDS, PDQ, etc. zu diskutieren. Daher wird im folgenden darauf eingegangen wie man die Autorisierungs-Transaktionen und -Akteure mit den in diesem Leitfaden diskutierten grundlegenden IHE-ITI Transaktionen kombinieren sollte.

1. ITI-18 XDS Registry Stored Query
2. ITI-41 XDS Provide & Register Document Set-b und ITI-42 XDS Register Document Set-b
3. ITI-43 XDS Retrieve Document Set
4. *TODO* ITI-21 PDQ Query
5. *TODO* ITI-47 PDQv3 Query

TODO XDS-I Besonderheiten noch zu diskutieren.

In den folgenden Abschnitten wird dabei immer angenommen, dass die Patientenidentifikation über einen der unter 4.3.1 diskutierten Mechanismen zwischen den Akteuren ausgetauscht wurde und somit alle Kommunikationspartner die XAD-PID des Patienten kennen. Eine weitere Annahme ist, dass einer der unter 4.3.2 diskutierten Mechanismen zur Benutzerauthentifizierung verwendet wurde und das empfangende System somit zumindest den Namen des Benutzers (ID und Klartext), seine Rolle und Organisation, die relevante Patienten-ID sowie den Verwendungszweck kennt.

4.3.4.2.1 1. Autorisierung für ITI-18 XDS Registry Stored Query

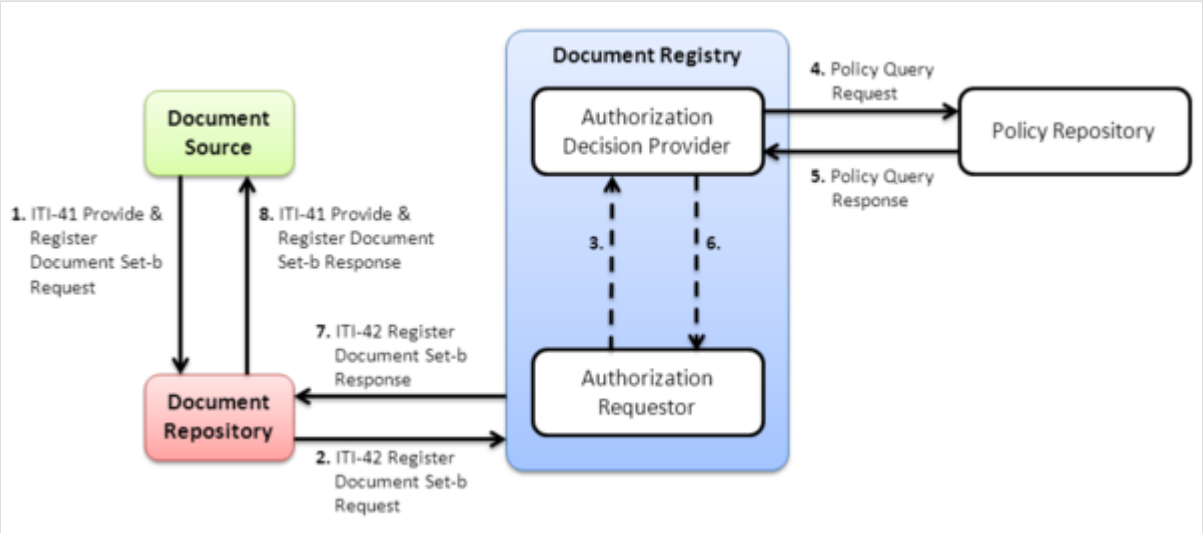


Der Document Consumer stellt eine gewöhnliche XDS-konforme ITI-18 Anfrage an die Document Registry. Die Document Registry ist nun dafür verantwortlich die Ergebnismenge so filtern, dass nur Einträge herausgegeben werden auf die der Benutzer berechtigt ist. Somit ist die Registry in der Rolle des Authorization Requestors. Der Authorization Decision Provider wird immer mit der Document Registry gruppiert, um einen möglichst direkten Zugriff auf die Dokumentenmetadaten und XDSFolders zu ermöglichen, die (kombiniert mit den Policies und den Benutzerattributen) ausschlaggebend für die Zugriffsentscheidung sind. Da sowohl der Authorization Requestor als auch der Authorization Decision Provider mit der Document Registry gruppiert sind, müssen die Transaktionen nicht über die standardisierten Schnittstellen umgesetzt werden, sondern dürfen über Document Registry-interne Mechanismen implementiert werden.

Risiko Patienten ID in Assertion (auslagern zur Assertion oder in ein Risikobetrachtungskapitel)

Die Abfrage der Policies durch den mit der Document Registry gruppierten Authorization Decision Provider wird anhand der in der 4.3.2.8 beschriebenen Attribute Assertion durchgeführt, die die XAD-PID des Patienten beinhält. Dies birgt natürlich das Risiko, dass es zu einer Differenz zwischen der Patienten ID in der Assertion und der Patienten ID in der Registry Stored Query kommt. Unbeabsichtige Konflikte treten wahrscheinlich am ehesten bei den Get* Queries auf (z.B. GetDocuments), da die Patienten ID hier nicht explizit als Query Parameter übermittelt wird, sondern sich aus der Patienten ID des abgefragten Objekts (also z.B. der XDSDocumentEntry.PatientID) ergibt. Diese Situation kann zum Beispiel eintreten wenn sich der Patientenbezug eines Dokuments wegen einer Zuordnungsänderung im MPI geändert hat, während der Document Consumer zugreift. Andererseits ist natürlich auch eine absichtliche Differenz zwischen der Patienten ID in der Assertion und der Patienten ID der Query denkbar, d.h. ein Document Consumer der versucht Zugriffsbeschränkungen zu umgehen. In den meisten Fällen wird dies in leeren Ergebnismengen resultieren, da die Policies des in der Assertion referenzierten Patienten den Zugriffskontext bestimmen und nicht auf die Dokumente der Query Response passen. Problematisch wäre ausschliesslich ein (in Deutschland rechtlich nicht umsetzbares) Opt-out Szenario, da hier durch eine falsche Patienten ID in der Assertion das laden von Deny Regeln verhindert werden könnte und keine patienten-spezifischen Permit Rechte notwendig sind.

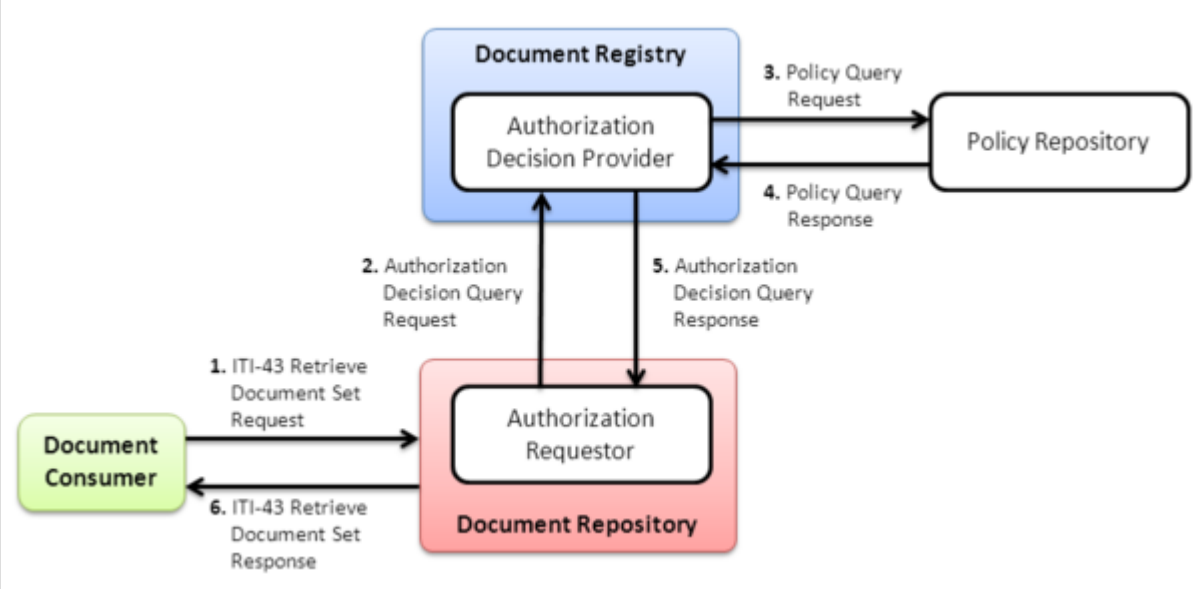
4.3.4.2.2 2. Autorisierung für ITI-41 XDS Provide & Register Document Set-b und ITI-42 XDS Register Document Set-b



Die Document Source stellt eine ITI-41 Provide and Register Document Set-b Anfrage unter Einsatz der in 4.3.2 beschriebenen Authentifizierungsmechanismen. Das Document Repository muss in dieser Situation keinerlei Prüfung durchführen, ob der Benutzer berechtigt ist das Dokument zur Patientenakte hinzuzufügen bzw. die gewünschten Änderungen an der Patientenakte durchzuführen. Dies ist möglich, da die Document Registry in der zwangsweise folgenden Transaktion ITI-42 Register Document Set involviert ist und eine Ablehnung der Dokumente zu einem Rollback (d.h. einer Löschung der Dokumente im Repository) führt. Die Registry ist in der "Register"-Transaktion ohnehin verpflichtet eine eigene Prüfung der Berechtigungen durchzuführen (Schritte 3. bis 6. im obigen Diagramm). Falls die Änderung an der Patientenakte aufgrund fehlender Rechte nicht durchgeführt werden kann, wird dies in Schritt 7. über die ITI-42 Response an das Document Repository gemeldet. Das Repository muss nun die Speicherung der Daten rückgängig machen und die Document Source über den Fehler informieren. Dies geschieht über die im heutigen Standard schon dafür vorgeschriebenen Rollback Mechanismen, die auch für Metadaten Fehler (z.B. falsche Codes, Ersetzung eines obsoleten Dokuments, etc.). verwendet werden. Um der Document Registry eine Prüfung zu ermöglichen, muss das Document Repository den Benutzerkontext der ITI-41 (Provide & Register) in die ITI-42 einbringen, d.h. die Identity Assertion und alle bekannten Attribute Assertions weiterreichen. Da die Document Source die Assertions die sie an das Document Repository sendet nicht signieren muss und da das Document Repository ggf. noch weitere Benutzerattribute in einem HPD Verzeichnis abgefragt hat, muss das Document Repository sich gegenüber der Registry als verantwortlich für die Assertions bezeichnen. Dies geschieht technisch über den SAML SubjectConfirmation Mechanismus "Sender-Vouches". Das Repository muss alle bekannten Informationen über den Benutzer an die Registry weiterleiten, d.h. alle von der Source gesendeten oder per HPD nachgeschlagenen Benutzerattribute, unabhängig davon ob das Repository diese selbst verwendet oder versteht.

4.3.4.2.3 3. Autorisierung für ITI-43 XDS Retrieve Document Set

Eine Abfrage der Dokumenteninhalte aus dem Document Repository wird unter Einsatz der in 4.3.2 beschriebenen Authentifizierungsmechanismen durch den Document Consumer veranlasst. Das Document Repository stellt daraufhin eine Authorization Decision Query Anfrage an den mit der Document Registry gruppierten Authorization Decision Provider. Die dafür verwendete Transaktion wird durch die Benutzeridentität und -attribute der ITI-43 Transaktion des Document Consumer begleitet. D.h. wie im vorherigen Abschnitt beschrieben wird der Benutzerkontext über SAML Assertions mit SubjectConfirmation Methode "Sender-Vouches" im SOAP Header der zweiten Transaktion (siehe Diagramm) übertragen. Eine empfohlene Optimierung für den üblichen Use Case "ITI-18 mit folgender ITI-43" ist der Einsatz eines "Authorization Decision Cache" im Authorization Decision Provider. Wenn ein Document Consumer zuerst die Metadaten für einige Dokumente eines Patienten abfragt und danach eines (oder mehrere) dieser Dokumente von einem Repository abruft, kann ein solcher Cache hilfreich sein. Er vermeidet, dass die Policy neu abgefragt wird und die Evaluierung der Policies, Dokumentenmetadaten und Benutzerattribute erneut erfolgt. Ein solcher Cache wird empfohlen, ist aber nicht zwingend notwendig. Wenn ein solcher Cache eingesetzt wird, muss sichergestellt sein, dass eine neue Autorisierungsentscheidung getroffen wird, sobald sich eines der Benutzerattribute von denen unterscheidet, die bei der usprünglichen Anfrage verwendet wurden. Ausserdem sollten Cache-Einträge gelöscht werden wenn sich die betrachteten Ressourcen (d.h. Dokumentenmetadaten) oder die (allgemeingültigen oder patientenspezifischen) Policies ändern. Um eine manuelles Invalidieren des Cache bei Änderungen an Ressourcen oder Policies zu vermeiden, kann auch eine begrenzte Gültigkeitsdauer für Cache-Einträge verwendet werden, die aber **eine Stunde** nicht überschreiten sollte.



4.3.5 Folder Management

Bei longitudinalen Akten stellt sich die Frage, wie die eingestellten Objekte - sprich Dokumente - verwaltet werden können. Die in IHE XDS vorhandenen Ordner (Folder) entsprechen Markierungen (oft auch als "Tags" bezeichnet), wobei einem Dokument auch mehrere solche Markierungen problemlos zugewiesen werden können. Dies entspricht dem bei Blogs häufig verwendetem System, bei dem ein Artikel mit einem oder mehreren Tags versehen werden. Dies erlaubt es, die Blog Einträge in mehrere, sich überschneide Teilmengen aufzuteilen, die unterschiedliche Themengebiete darstellen. Im Gegensatz zu Tags bei Blog Software werden die Folder in XDS jedoch nicht durch eine frei wählbare Zeichenkette festgelegt, sondern durch einen oder mehrere Codes.

Ein Dokument kann in XDS also mehreren Ordnern zugeordnet werden, die wiederum durch mehrere Codes gekennzeichnet sein können!

Die Ordner (Folder) in XDS entsprechen somit nicht dem Ordnerprinzip, mit dem die verbreiteten Betriebssysteme (Windows, UNIX, Linux) Dokumente organisieren. Dort werden die Dokumente in hierarchischen Strukturen entsprechenden Ankerpunkten zugeordnet. Diese Strukturen werden dabei über Pfadangaben realisiert, die durch voneinander getrennten Zeichenketten organisiert werden. Somit übernehmen diese zusammengesetzten Zeichenketten die Ablagelogik. (z.B. "C \ Windows \ System" oder "usr \ local"). Ein Dokument kann in diesen Systemen typischerweise nur einem Ordner zugeordnet werden. (Manche Betriebssysteme ermöglichen auch eine Mehrfachzuordnung, dies ist dann aber relativ aufwendig und führt zu anderen Nebeneffekten.) Die Ordner in XDS sind per se ersteinmal nicht hierarchisch, da sich keine Beziehungen zwischen Ordnern (wie Ordner A1 ist ein Unterordner von Ordner A) abbilden lassen.

XDS Folder unterscheiden sich wesentlich von Ordnern in Betriebssystemen!

4.3.5.1 Strukturierung der Akte in der Benutzeroberfläche

Viele heute am Markt befindlichen Systeme strukturieren medizinische Akten durch verschachtelte Ordner bzw. Baumstrukturen.So kann der Benutzer z.B. zuerst den administrativen Fall auswählen, dort dann die Befunde auswählen und auf der nächsten Unterebene dann die Laborbefunde zur Anzeige auswählen. Um eine solche Navigation zu ermöglichen, muss ein XDS-basiertes System keine Ordner-Hierarchie aufbauen. Stattdessen könnte eine Implementierung Ordner verwenden um die administrativen Fälle abzubilden, den XDSDocumentEntry.classCode um zwischen Befunden, Arztbriefen etc. zu unterscheiden und den XDSDocumentEntry.typeCode (oder den XDSDocumentEntry.practiceSettingCode) verwenden um Laborbefunde von radiologischen Befunden zu unterscheiden. Die hierarchische Darstellung an der Oberfläche muss nicht mühsam durch die einstellenden Systeme über XDSFolder angelegt werden, sondern ergibt sich aus den Metadaten der Dokumente.

Eine hierarchische Darstellung der Akte in der Benutzeroberfläche kann ohne hierarchische Ordner umgesetzt werden.

Die Einsatzzwecke von Ordnern in XDS sind vielfältig und werden durch das IHE Cookbook nicht weiter eingeschränkt. Stattdessen werden in diesem Abshnitt Hilfestellungen gegeben, um gebräuchliche Strukturierungskonstrukte (z.B. Administrative Fälle) mithilfe von XDS Foldern auf eine interoperable Art und Weise abzubilden. Über die hier vorgestellten Konstrukte hinaus, können Anwendungsprojekte und andere Profilierungsinitiativen somit noch weitere Anwendungsgebiete für Folder definieren. Um redundante Kennzeichnungen, die zu Widersprüchen führen können, zu vermeiden, wird empfohlen keine Ordner anzulegen, die die im XDSDocumentEntry vorhandenen Metadaten (unter der Berücksichtigung der empfohlenen und vorgeschriebenen Wertebereiche) duplizieren. Z.b. ist eine Grobklassifizierung von Dokumenten durch den classCode schon gegeben, daher muss kein XDSFolder für "Befunde" angelegt werden. Ebenso sind die Fachrichtungen durch den practiceSettingCode abgebildet, daher kann der code für Labormedizin verwendet werden, anstatt einen Ordner für Labordaten anzulegen. Die Nutzung der XDSDocumentEntry Metadaten ist prinzipiell zu bevorzugen, da sich diese in XDS Anfragen weitaus flexibler einsetzen lassen.

4.3.5.2 Abbildung Administrativer Fallinformationen durch XDS Folder

Ein administrativer Fall sollte in XDS immer zumindest durch die folgenden Codes im Feld XDSFolder.codeList gekennzeichnet werden:

- Ein Eintrag in der codeList um den Typ des administrativen Falls spezifischer einzugrenzen
  - code value (nodeRepresentation) = "VISIT"; display name = "Besuch bei niedergelassenem Arzt"; codingScheme *TBD*

    - code value (nodeRepresentation) = "OUTPAT"; display name = "Ambulanter Klinikaufenthalt (outpatient)"; codingScheme *TBD*
    - code value (nodeRepresentation) = "INPAT"; display name = "Stationärer Klinikaufenthalt (inpatient)"; codingScheme *TBD*
    - code value (nodeRepresentation) = "REHA"; display name = "Rehabilitation (rehabilitation)"; codingScheme *TBD*
- Ein Eintrag in der codeList um je nach spezifischer administrativer Fallart weitere Informationen zu transportieren
    - Bei administrativer Fallart "VISIT"
        - code value (nodeRepresentation) = Quartal (z.B. "Q2/2012"); display name = textuelle Beschreibung des Quartals (z.B. "Besuch in Q2/2012"); codingScheme *TBD*
    - Bei administrativer Fallart "OUTPAT", "INPAT" oder "REHA"
        - code value (nodeRepresentation) = Fallnummer (z.B. "72839181"); display name = textuelle Beschreibung des adm. Falls (z.B. "stationärer Aufenthalt mit Fallnummer 72839181"); codingScheme = OID-des Namespace (z.B. "2.16.840.1.113883.3.37.4.1.1")

Ein durch diese codes gekennzeichnete Folder beinhält Dokumente die mit einem spezifischen administrativen Fall assoziiert sind. Ein solcher Folder kann durch weitere codes auch als zweckgebunden gekennzeichnet werden (s.u.). Ein solcher Folder sollte nicht durch weitere codes als Patientenordner oder Notfallordner gekennzeichnet werden. Um Dokumente aus einem administrativen Fallordner als notfallrelevant zu kennzeichnen, sollten díe relevanten Dokumente mit einem unabhängigen Notfallordner assoziiert werden.

4.3.5.3 Abbildung von Ordnern zur Zweckbindung durch XDS Folders

Ein Ordner zur Zweckbindung sollte in XDS immer zumindest durch die folgenden Codes im Feld XDSFolder.codeList gekennzeichnet werden:

- Ein Eintrag in der codeList um den Typ der Zweckbindung spezifischer einzugrenzen
    - code value (nodeRepresentation) = "DIAG"; display name = "medizinischer Fall auf Diagnose Basis"; codingScheme *TBD*
    - code value (nodeRepresentation) = "DMP"; display name = "Disease Management Programm"; codingScheme *TBD*
    - code value (nodeRepresentation) = "IVA"; display name = "Integrierte Versorgung (IVa-Vertrag)"; codingScheme *TBD*
    - code value (nodeRepresentation) = "IVB"; display name = "Integrierte Versorgung (IVb-Vertrag)"; codingScheme *TBD*
- Ein Eintrag in der codeList um je nach spezifischer Zweckbindung weitere Informationen zu transportieren
    - Bei Zweckbindung "DIAG"
        - code value (nodeRepresentation) = ICD-10 Diagnose, ggf. mit eingeschränkter Granularität (z.B. "S52"); display name = textuelle Beschreibung des ICD Codes (z.B. "Fraktur des Unterarmes"); codingScheme = OID des Verwendeten ICD Katalogs (z.B. "1.2.276.0.76.5.413" für ICD-10 GM 2013)

- Bei Zweckbindung "DMP", "IVA" oder "IVB"
  - code value (nodeRepresentation) = Code aus KBV Tabelle S_VDX_VERTRAGSART (z.B. "30" für DMP Diabetes mellitus Typ 2); display name = textuelle Beschreibung aus KBV Tabelle S_VDX_VERTRAGSART (z.B. "DMP Diabetes mellitus Typ 2"); codingScheme = "1.2.276.0.76.5.257" (OID der KBV Tabelle S_VDX_VERTRAGSART)

Ein durch diese codes gekennzeichnete Folder beinhält Dokumente die einer Zweckbindung unterliegen. Ein solcher Folder kann durch weitere codes auch mit administrativen Fallinformationen angereichert werden (s.o.). Ein solcher Folder sollte nicht durch weitere codes als Patientenordner oder Notfallordner gekennzeichnet werden. Um Dokumente aus einem zweckgebundenen Ordner als notfallrelevant zu kennzeichnen, sollten díe relevanten Dokumente mit einem unabhängigen Notfallordner assoziiert werden.

4.3.5.4 Abbildung von Patientenordnern

Ein Patientenordner sollte in XDS immer zumindest durch die folgenden Codes im Feld XDSFolder.codeList gekennzeichnet werden:

- Ein Eintrag in der codeList um den Odner als Patientenordner zu kennzeichnen
  - code value (nodeRepresentation) = "PATI"; display name = "Durch Patient hinzugefügter Ordner"; codingScheme *TBD*

Ein durch diese codes gekennzeichnete Folder beinhält Dokumente die der Patient selbst hinzugefügt hat. Die im Titel und Kommentarfeld hinterlegten Informationen und die in der codeList verwendeten Code die über die hier spezifizierten hinausgehen sind unter der Kontrolle des Patienten und sollten daher von Leistungserbringern entsprechend interpretiert werden. Es wird empfohlen alle vom Patienten hinzugefügte Dokumente mit Patientenordnern zu assoziieren. Da die Dokumente aber durchaus auch für andere Folder relevant sein können (z.B. für die Behandlung im Rahmen eines IG-Vertrags oder im Rahmen einer Fallakte) und somit ggf. in anderen Foldern auftauchen können, ohne dass der Patientenordner für den Benutzer sichtbar wird, müssen alle vom Patienten beigefügten Dokumente zusätzlich durch einen XDSDocumentEntry.eventCode gekennzeichnet werden. Dies ist unabhängig davon, ob die Daten durch den Patienten erstellt wurden (z.B. Schmerztagebuch) oder nur von diesem elektronisch verfügbar gemacht wurden (z.B. Hochladen eines eingescannten OP-Bericht). Als eventCode wird dabei folgender Code eingesetzt:

- code value (nodeRepresentation) = "PAT_PROVIDED"; display name = "Vom Patienten zur Verfügung gestelltes Dokument"; codingScheme *TBD*

Ein Patientenordner sollte nicht durch weitere codes als administrativer Fallordner, zweckgebundener Ordner oder Notfallordner gekennzeichnet werden. Um Dokumente aus einem Patientenordner als notfallrelevant zu kennzeichnen, sollten díe relevanten Dokumente mit einem unabhängigen Notfallordner assoziiert werden.

4.3.5.5 Abbildung von Notfallordnern

Ein Norfallordner sollte in XDS immer zumindest durch die folgenden Codes im Feld XDSFolder.codeList gekennzeichnet werden:

- Ein Eintrag in der codeList um den Odner als Notfallordner zu kennzeichnen
  - code value (nodeRepresentation) = "EMERG"; display name = "Notfall-relevante Dokumente"; codingScheme *TBD*

4.3.6 Akteninhalte

4.3.6.1 Verwendung von CDA

4.3.6.2 Dokument einstellen

4.3.6.3 Dokument abrufen

4.4 Besonderheiten der Aktentypen

Wie werden die verschiedenen Aktentypen mit den Lösungsmodulen realisiert?

4.4.1 Einrichtungsübergreifende elektronische Patientenakte (eEPA)

Die eEPA wird im Kernbereich von medizinischen Fachkräften (Health Professionals) geführt und verantwortet, welche sich dem entsprechenden Netzwerk zum Dokumentenaustausch angeschlossen haben. Der Patient kann einen Health-Professional als Aktenmoderator benennen, um ihm damit weiterführende Verwaltungsrechte zu übertragen. Der Patient kann im Kernbereich einzustellende Inhalte nicht beeinflussen, ändern oder löschen. Damit ist sichergestellt, dass die Inhalte der eEPA eine Qualität besitzen, auf welcher medizinisches Handeln auch forensisch abgesichert sinnvoll aufbauen kann. Der Patient muss entscheiden, ob er eine eEPA überhaupt führen will (sogenanntes "Opt-In").

Die eEPA ermöglicht die Vergabe differenzierter Zugriffsrechte. Soweit ein Behandlungsverhältnis vorliegt, kann der Aktenzugriff vom Patienten vor Behandlungsbeginn optional über Kriterien eingeschränkt werden. Gewählte Kriterien sind:

- Gesundheitsdienstleister
- Dokumententyp
- Medizinisches Fachgebiet der Dokumente und
- Zeitraum.

Zusätzlich wird geprüft, ob seitens des Patienten Dokumente für den Zugriff gesperrt sind. Gesperrte Dokumente sind grundsätzlich nicht sichtbar. Die jeweils gewährten Zugriffsrechte werden protokolliert.

4.4.1.1 Integration in Primärsysteme

Die Daten und Dokumente der eEPA sind aus technischen und forensischen Gründen redundante Informationen der institutionellen Akten in den Primärsystemen (u.a. Krankenhaus- und Arztpraxen-systeme). Inhalte der eEPA können automatisiert in die Primärsysteme heruntergeladen und aus den Primärsystemen hochgeladen werden. Darin unterscheidet sich die eEPA wesentlich von einer durch einen ärztlichen Stellvertreter geführten PEPA.

4.4.1.2 Funktionsfähigkeit mit und ohne Abfragemöglichkeit für Patienten IDs

Die eEPA-Spezifikation lässt die Patientenidentifikation sowohl über die in Abschnitt 4.3 diskutierten Schnittstellen zu, wie auch den in 4.3.1.3 vorgestellten Ansatz ohne Abfragemöglichkeit. Wenn keine Abfragemöglichkeit besteht, muss die Patienten ID über ein anderes Verfahren übertragen werden, zum Beispiel über einen Ausdruck mit der Patienten ID im Klartext und/oder als Barcode, per USB-Stick, per eGK, per Secure Email, etc. So kann z.B. der Patient die Patienten ID über einen Ausdruck (oft auch "Ticket" oder "Offline-Token" genannt) an seinen Arzt oder die Aufnahmekraft im Krankenhaus übergeben. Dieser kann dann eine Patientenzustimmung für den so identifizierten Patienten hochladen und darüber den Behandlungszusammenhang abbilden und die Berechtigungen erweitern.

4.4.1.3 Benutzerauthentifizierung an einer eEPA

Die eEPA kann mit allen in Abschnitt 4.3.2 vorgestellten Authentifizierungsmethoden genutzt werden. Dabei sollte beachtet werden, dass für die Autorisierung von einzelnen Benutzern diese über ein zentrales Benutzerverzeichnis verfügbar sein müssen (siehe 4.3.2.7). Andernfalls kann das System, das das elektronische Patientenzustimmungsdokument erstellen muss, nicht die eindeutige Identifikation des Benutzers in den Zugriffsregeln sicherstellen. Eine Autorisierung von Einrichtungen ist aber immer ohne Einschränkungen möglich.

4.4.1.4 Benutzeroberfläche der eEPA

Grundsätzlich benötigt die eEPA keine eigene Benutzeroberfläche. Der Datenaustausch erfolgt über Primärsysteme, welche Dokumente bzw. Daten der eEPA abrufen und im Primärsystem nutzen und Dokumente bzw. Daten aus Primärsystemen in die eEPA laden.

Die ausschließliche Analyse der eEPA-Inhalte über Primärsysteme besitzt Grenzen, wenn der Patient autonom Zugriff auf „seine“ eEPA bekommen soll. Zum Beispiel ist es für den lesenden Zugriff des Patienten oft nicht praktikabel den Hausarzt aufzusuchen. Für den Zugriff auf eigene Daten oder das Einstellen von eigenen Daten kann eine Art Patientenportal bereitgestellt werden. Im Übrigen verlangt die „gesetzliche Akte“ nach § 291a SGB V, das der Patient selber ein Zugriffsrecht auf die Akte besitzt.

Schließlich ist eine eigene eEPA-Benutzeroberfläche als Interimsszenario für den Arzt sinnvoll, sofern das Primärsystem noch keine Kommunikation mit der eEPA unterstützt. Auch für technische Administrationsfunktionen der eEPA kann ein Frontend notwendig sein.

4.4.1.5 Fähigkeit zur Einbindung in die Telematik-Infrastruktur

Die Einbindung der eEPA in die Telematik-Infrastruktur kann mit zwei Zielrichtungen erfolgen. Als sogenannte „Mehrwertanwendung“ (keine explizite gesetzliche Spezifikation) oder als gesetzliche Akte nach § 291a Abs. 3 SGB V.

Für die Einbindung als Mehrwertanwendung wird derzeit von der DKG im Auftrag der gematik ein Zertifizierungsverfahren entwickelt. Vor dessen Abschluss sind keine validen Empfehlungen zur Einbindung möglich. Für die gesetzliche Akte ist eine Spezifikation der Vorgaben des § 291a SGB seitens des Gesetzgebers bzw. der gematik noch nicht erfolgt. Grundsätzlich wird davon ausgegangen, das aufgrund der flexiblen eEPA Architektur – insbesondere bei Umsetzung autonomer Zugriffsmöglichkeiten des Patienten und dem Angebot des Hinzufügens von Daten durch den Patienten über ein Portal – die eEPA das Potential als gesetzliche Akte besitzt. Für Aktensystemhersteller bedeutet die erfolgreiche Qualifizierung für die gesetzliche Akte ein wertvolles Produktmerkmal.

Spezifikation bzgl. Betrieb und (Langzeit-) Archivierung einer eEPA Der Langzeitbetrieb eines Aktensystems sollte grundsätzlich so ausgelegt sein, dass z.B. der Wechsel des Aktenanbieters unterstützt werden kann. Soweit Daten der eEPA an ein (elektronisches) Archivsystem übergeben werden, ist sicherzustellen, dass die Daten innerhalb gesetzlicher Fristen wieder lesbar gemacht werden können.

4.4.1.6 Use Cases

4.4.1.6.1 Akte Anlegen

- Identifikation erzeugen
- Identity Feed ausführen
- Ticket ausstellen
- notwendige Ordner anlegen
- Patientenzustimmung ablegen (legt gleichzeitig die Berechtigungen fest)

4.4.1.6.2 Dokument einstellen

- Voraussetzung: Ticket ist eingelesen bzw. Patienten-ID bekannt
- Dokument einstellen

4.4.1.6.3 Dokument abrufen

- Voraussetzung: Ticket ist eingelesen bzw. Patienten-ID bekannt
- Registry befragen
- Dokument abrufen

4.4.1.6.4 Berechtigungen ändern

- neues Patientenzustimmungs-Dokument erstellen
- Patientenzustimmungs-Dokument einstellen

4.4.2 Persönliche einrichtungsübergreifende elektronische Patientenakte (PEPA)

In diesem Kapitel werden die Besonderheiten der PEPA hinsichtlich der Verwendung der Standardisierten Lösungskomponenten, der Architektur sowie der darauf aufbauenden technischen Use-Cases beschrieben.

4.4.2.1 Patientenidentifikation

Für die Patientenidentifikation ist für die PEPA zwingend ein Master Patient Index (MPI) erforderlich. Dieser wird entsprechend den Ausführungen zum MPI im Kapitel „Standardisierte Lösungskomponenten“ verwendet.

4.4.2.2 Benutzeridentifikation und –authentifikation

Die Benutzeridentifikation und –authentifikation erfolgt für die PEPA im Rahmen der entsprechenden Ausführungen im Kapitel „Standardisierte Lösungskomponenten“. Es werden zwei der drei beschriebenen Möglichkeiten unterstützt, die beide ein zentrales HPD voraussetzen: Lokale Eingabe der zentralen Benutzeridentität und dynamisches Mapping der Benutzeridentität.

4.4.2.3 Verwaltung und Prüfung von Berechtigungen

Die Verwaltung und Prüfung von Berechtigungen erfolgt entsprechend den Ausführungen im Kapitel „Standardisierte Lösungskomponenten“. Für die PEPA ist die Verwendung der elektronischen Patientenzustimmung mit eingebettetem XACML (siehe 4.3.3.2) zwingend erforderlich. Die Erstellung der Einwilligung liegt primär in der Hand des Patienten. Deshalb ist im Portal der Aktor Advanced Consent Creator zu implementieren. Da ein Patient jedoch die Verwaltung auch an einen von ihm bestimmten Stellvertreter (z.B. Hausarzt oder den behandelnden Arzt) delegieren kann, muss auch das Professional-Portal diesen Aktor implementieren. Optional kann er auch von Primärsystemen implementiert werden.

4.4.2.4 Architektur

Für den Aufbau einer Affinity Domain basierend auf einer PEPA sind folgende Komponenten erforderlich:

Zentrale Komponenten der PEPA sind:

- Für den MPI: PIX Patient Identfier Cross-reference Manager
- Health Provider Directory (HPD)
- XDS(I).b Registry und Repository
- ATNA-Repository
- Time Server

- Authorization Decision Provider
- Policy Repository
- Authorization Requestor (PEP)
- Advanced Consent Creator
- Professional-Portal (Document Consumer, Document Source)
- Patienten-Portal (Document Consumer, Document Source)

Dezentrale Komponenten in den Primärsystemen sind:

- Patient Identity Source
- Document Sources
- Authorization Requestor (PEP)
- XDS(I).b Repository (optional)
- Advanced Consent Creator (optional)

4.4.2.4.1 Benutzeroberflächen / Portale

Für den Abruf von Inhalten und Dokumenten sind im PEPA-Ansatz allein die Portale verantwortlich. Eine direkte Übernahme von PEPA-Inhalten in die Primärsysteme mittels dort implementierten Document Consumern ist solange nicht vorgesehen, bis es eine adäquate Möglichkeit gibt, das „Recht auf Löschen“, sofern es nicht mit anderen Gesetzten in Widerspruch steht, umsetzen zu können.

4.4.2.4.2 Strukturierung der Akteninhalte

Mittels dem im Kapitel „Standardisierte Lösungskomponenten“ beschriebenen Konzept der XDS-Folder, können Inhalte der PEPA strukturiert werden. Dies sind insbesondere folgende Bereiche:

- Administrative Fälle und Besuche
- Bewegungen

Eine Auswahl des Codierungssystems für die Dokumentenklassen (z.B. LOINC) und weiteren, für die Affinity Domain nötigen Bezeichner muss noch erfolgen.

4.4.2.4.3 Primärsystemintegration

Damit Primärsysteme an die PEPA angeschlossen werden können, müssen sie die o.g. dezentralen Komponenten implementieren. Damit sich die Benutzer nicht unnötiger Weise auch am Portal authentifzieren müssen und den aktuellen Patienten erneut suchen müssen, wird eine kontext-basierte Integration des Professional-Portals in die Primärsysteme empfohlen.

4.4.2.4.4 Einbindung in die Telematikinfrastruktur

Sobald die Telematikinfrastruktur (TI) vorhanden ist, wird es möglich sein, eine PEPA als Mehrwertanwendung zu betreiben. In diesem Fall können die Mechanismen der TI, wie beispielsweise zur Identifikation und Authentifikation für Patienten und Benutzer, verwendet werden.

4.4.2.5 Use-Cases

4.4.2.5.1 Akte Anlegen

Aktivierung des Zugangs zum Patientenportal

Damit der Patient/Bürger auf die Inhalte seiner PEPA zugreifen kann und dort auch die Berechtigungen steuern kann, braucht er einen separaten Zugang. Dieser wird über ein Portal realisiert, das vergleichbar mit einem Onlinebanking-Portal oder einem Webmailkonto, durch eine Benutzername-Passwort-Kombination mit einer zusätzlichen TAN gesichert ist. Initialer Zugang: Authentifizierung über ein Email-Konto. In Zukunft denkbar: Zertifikat des ePersonalausweises oder der eGK, de-mail Konto (vlg. Auch BSI). Klickt der Patient auf den durch die initiale Anlage seiner Akte erzeugten Link, aktiviert er die Akte, die mit seinem Index-Patienten des PIX-Managers verknüpft ist. Dazu werden weitere, bei der Aufnahme noch nicht abgefragte Angaben erhoben: Auswahl des TAN-Verfahrens (TAN-Generierung per SMS, Telefon). Hinterlegung einer Handynummer, Sicherheitsfragen bei vergessenem Passwort, Nennung von Bevollmächtigten Personen.

Aufnahme, Einwilligung und initiale Anlage der Akte

Entsprechend dem Grundsatz, dass jeder Zugriff, jede Übermittlung und Anlage von med. Dokumenten vom Patienten autorisiert sein muss (vgl. Kapitel Datenschutz), beschreibt dieser Usecase wie eine initiale PEPA für einen Patienten bei der Aufnahme in einer Gesundheitseinrichtung angelegt wird. Dabei wird auch der Fall betrachtet, dass der Patient bereits über eine PEPA verfügt, die aufnehmende Einrichtung jedoch noch nicht berechtigt ist. Alle Workflows berücksichtigen, dass Aufnahmekräften und medizinischem Personal keine signifikanten Mehraufwände entstehen. Das Anlegen einer Akte kann zu jedem Zeitpunkt im Behandlungsprozess geschehen. Hier wird der typische Fall während der Aufnahme betrachtet. Vorbedingungen: Die den Patienten aufnehmende Einrichtung und ihr medizinisches Personal sind im zentralen Provider Information Directory (HPD) mit ihren lokalen Identifiern registriert. Das Einwilligungsmodul des Primärsystems hat den Provider Information Consumer des Profils Health Provider Directory implementiert und im Modul stehen so alle der Affinity Domain zugehörigen Gesundheitsdiensteanbieter für die Einwilligung zur Verfügung.

TODO Detaillierten Ablauf beschreiben

4.4.2.5.2 Patienten suchen

Für die Suche nach Patienten in der zentralen PEPA gibt es zwei Mechanismen. Wird der Patient bereits in einem Primärsystem gesucht und hat dort einen lokalen Identifier und wird anschließend über eine Kontextintegration das Ärzteportal der PEPA aufgerufen, so kann mithilfe der lokalen ID per PIX-Query der globale Identifier (d.h. die XAD-PID) ermittelt werden. Alle weiteren Transaktionen können mit ihm erfolgen (siehe 4.3.1). In der zweiten Variante ist ein Benutzer direkt auf dem Ärzteportal der PEPA angemeldet und nutzt die vorhandene Suche anhand von Attributen wie Name, Vorname und Geburtsdatum. In diesem Fall ist kein lokaler Patientenidentifier verfügbar. Deshalb erfolgt die Suche über die Transaktion Patient Demographics Query zwischen den beiden Aktoren Patient Demographie Consumer und Patient Demographic Supplier (siehe 4.3.1). Gibt es zu den vorhandenen Parametern mehrere Treffer, so ist eine Nutzerinteraktion erforderlich, um den richtigen Patienten zu wählen.

TODO Security Aspekte beschreiben

4.4.2.5.3 Dokumente verwalten

Einstellen

In diesem Usecase wird dargestellt, wie ein Primärsystem einer Gesundheitseinrichtung oder ein Patientenportal Dokumente in die PEPA einstellen kann. Der Fall Dokumente über ein Ärzteportal einzustellen weicht insofern davon ab, dass die globale Patienten-ID des PIX-Managers nicht über eine PIX-Query Transaktion erfragt werden kann, da im Ärzteportal keine lokale Patienten-ID als Anfrageparameter existiert. Daher muss z.B. Über die Parameter Vorname, Nachname und Geburtsdatum über die Transaktion PD-Query, die globale ID erfragt werden (vgl. Auch Usecase Patientensuche), wodurch sowohl auf Client als auch auf Server Seite ein separater Aktor erforderlich ist (Patient Dempgraphics Consumer und Supplier).

Vorbedingung: Der Patient, zu dem Dokumente übermittelt werden sollen, hat bereits eine PEPA. Die Einrichtung und ihr medizinisches Personal sind im zentralen Provider Information Directory mit ihren lokalen Identifiern registriert.

TODO Detaillierten Ablauf beschreiben

Abrufen

In diesem Usecase wird beschrieben, wie Dokumente aus der PEPA eingesehen werden können. Dabei werden die spezifizierten Lösungskomponenten verwendet. Zwei Möglichkeiten existieren. Bei der direkten Verwendung der Portaloberfläche muss sich der Gesundheitsdiensteanbieter zunächst mit seinem Account am Portal anmelden und über die Suchfunktion den gewünschten Patienten auswählen. Ist das Portal per Kontextintegration in das Primärsystem eingebunden, muss der Gesundheitsdienstleister im Primärsystem den Patienten suchen und von dort im Kontext in das Portal "abspringen". Näheres zu den Such-Typen im Usecase Patientensuche.

Vorbedingung: Der Patient, zu dem Dokumente eingesehen werden sollen, hat bereits eine PEPA. Die Einrichtung und ihr medizinisches Personal sind im zentralen Provider Information Directory mit ihren lokalen Identifiern registriert. Egal welche der oben beschriebenen Möglichkeiten verwendet wurde, die globale Patienten-ID der Affinity Domain (MPI-ID) ist bereits bekannt.

A) Standardablauf **TODO Detaillierten Ablauf beschreiben**

B) Notfall **TODO Detaillierten Ablauf beschreiben**

Ändern/Löschen

Zum updaten einer neuen Dokumentenversion steht die Transaktion [ITI41] Provide & Register Document Set-b mit eintsprechender Replacement Option zur Verfügung. Sollen lediglich Meta-Informationen geändert werden (Dokument umhängen, Fallrevision), wird das Profil XDS-Meta-Data-Update verwendet. Der Akteur Document Administrator stellt dazu die Transaktion [ITI57] Update Document Set bereit. Das Löschen von Inhalten erfolgt lediglich Meta-Daten-basiert in der Registry. Hierzu wird die Transaktion [ITI62] Delete Document Set des selben Aktors verwendet.

4.4.2.5.4 Berechtigungen verwalten

In diesem Usecase wird beschreiben, welche Lösungskomponenten involviert sind und wie sie zusammen arbeiten, wenn der Patient seine Einwilligung durch Hinzufügen oder Entziehen von Berechtigungen ändert. Vorbedingungen: Der Patient hat bereits eine eigene PEPA und einen autorisierten Zugang. Das Einwilligungsmodul des Patientenportals hat den Provider Information Consumer des Profils Health Provider Directory implementiert und im Modul stehen so alle der Affinity Domain zugehörigen Gesundheitsdiensteanbieter für die Einwilligung zur Verfügung.

TODO Detaillierten Ablauf beschreiben

4.4.3 Fallbezogene einrichtungsübergreifende elektronische Patientenakte (eFA)

Siehe die (sich zur Zeit ebenfalls in einer Kommentierungsphase befindliche) cdaefa:EFA Spezifikation v2.0

5 Definitionen des deutschen Leitfadens

5.1 Terminologien für Metadaten

TODO Definition der konkreten Terminologien

Das Festlegen von Terminologien für die kodierten Metadaten Felder ist auf der einen Seite nötig um Interoperabilität zu vereinfachen, andererseits schränkt es die Möglichkeiten von Implementierungsprojekten stark ein. Daher muss für jedes Feld seperat entschieden werden ob eine Festlegung auf konkrete Werte (d.h. value sets) angebracht ist, eine Festlegung auf einen spezifischen Katalog (code system) oder nur eine Empfehlung von möglichen value sets oder code systems.

- XDSDocumentEntry.**authorRole**: Empfehlung eines value sets geplant, z.B. aus SNOMED CT
  - *Vorsicht: Kein coded value, sondern Freitext; keine Angabe des codingScheme möglich; keine Validierungsanforderung in XDS*
- XDSDocumentEntry.**authorSpeciality**: Festlegung auf ein value set geplant, entsprechend dem practiceSettingCode
  - *Vorsicht: Kein coded value, sondern Freitext; keine Angabe des codingScheme möglich; keine Validierungsanforderung in XDS*
- XDSDocumentEntry.**classCode**: Festlegung auf ein value set geplant (ca. 5-10 Werte, z.B. Untersuchungsbefund, Diagnostische Rohdaten, Arztbrief, Bilddaten, Pflegedokumentation, Administratives Dokument, Patientendokument)
- XDSDocumentEntry.**confidentialityCode**: Festlegung auf ein value set geplant (z.B. 2.16.840.1.113883.5.25; HL7 Confidentiality Codes; 3 Werte - Normal, Eingeschränkt, Stark Eingeschränkt)
- XDSDocumentEntry.**eventCodeList**: Zur freien Verwendung, bis auf wenige vorgegebene Werte (z.B. IHE BPPC policy ID)
- XDSDocumentEntry.**formatCode**: Empfehlung eines value sets geplant
- XDSDocumentEntry.**healthcareFacilityTypeCode**: Festlegung eines value sets geplant (ca. 5-10 Werte, z.B. Arztpraxis, Hausärztliche Versorgung, Krankenhaus, Labor, MVZ, Pflegeeinrichtung, Poliklinik, Reha-Einrichtung)
- XDSDocumentEntry.**languageCode**: Festlegung eines value sets geplant (z.B. 1.0.639.1; ISO639-1 Language Codes)
- XDSDocumentEntry.**practiceSettingCode**: Festlegung eines value sets geplant (z.B. 1.2.276.0.76.5.114, S_BAR2_WBO Tabelle der KBV)
- XDSDocumentEntry.**typeCode**: Empfehlung eines value sets geplant (z.B. Auswahl von sinnvollen LOINC oder SNOMED Codes)
- XDSFolder.**codeList**: Zur freien Verwendung, bis auf wenige vorgegebene Werte (für administrative Fälle, Zweckbindung, etc.; siehe Folder Management)
- XDSSubmissionSet.**authorRole**: siehe XDSDocumentEntry.authorRole
- XDSSubmissionSet.**authorSpeciality**: siehe XDSDocumentEntry.authorSpeciality
- XDSSubmissionSet.**contentTypeCode**: Festlegung eines value sets geplant

verwendete Terminologie	Referenz
Dokumenttypen	vgl. Wikiseite
..	..

5.2 Checkliste für Implementierungen

6 Themen für Folgejahre

6.1 Cross-community Profiles

Das IHE Cookbook beschreibt den Aufbau unterschiedlicher Ausprägungen von "Affinity Domains", um eine möglichst breite Nutzung dieser Spezifikation zu gewährleisten.

Hierdurch können Anforderungen einheitlich erfüllt werden, die aus regionalen oder fachspezifischen Aufgabenstellungen resultieren.

Unabhängig davon für welche dieser Varianten sich einzelne Netzwerke in Deutschland entscheiden entsteht mit der steigenden Anzahl dieser Netzwerke die Notwendigkeit, diese wiederum miteinander zu verbinden.

Viele Patienten werden künftig von medizinischen Leistungserbringern aus mehreren Netzwerken (sprich "Affinity Domains") behandelt werden und auch dann müssen Technologien und Funktionalitäten bereit stehen, um die Daten auch über die Grenzen einzelner Netzwerke austauschen zu können.

Nicht zuletzt erfordern die vermehrt auftretenden Behandlungsketten, in denen medizinische Partner aus europäischen Nachbarländern eingebunden werden auch deren Einbindung in den digitalen Datenaustausch. In einem großen europäischen Projekt [1] (http://www.epsos.eu/) wurden hierzu bereits erfolgreiche Vorarbeiten geleistet, welche auch für den Austausch zwischen verschiedenen Netzwerken in Deutschland genutzt werden können.

Im vorgenannten europäischen Projekt epSOS aber beispielsweise auch in den Grundlagen der nationalen österreichischen Vernetzungsstrategie "Elektronische Gesundheitsakte (ELGA)" werden dabei immer wieder die nachfolgenden Profile der IHE zum Thema "Cross-Community" eingesetzt:

6.1.1 Cross-Community Access (XCA)

In diesem Profil wird grundsätzlich beschrieben, wie unterschiedliche Netzwerke über "Gateways" miteinander vernetzt werden können.

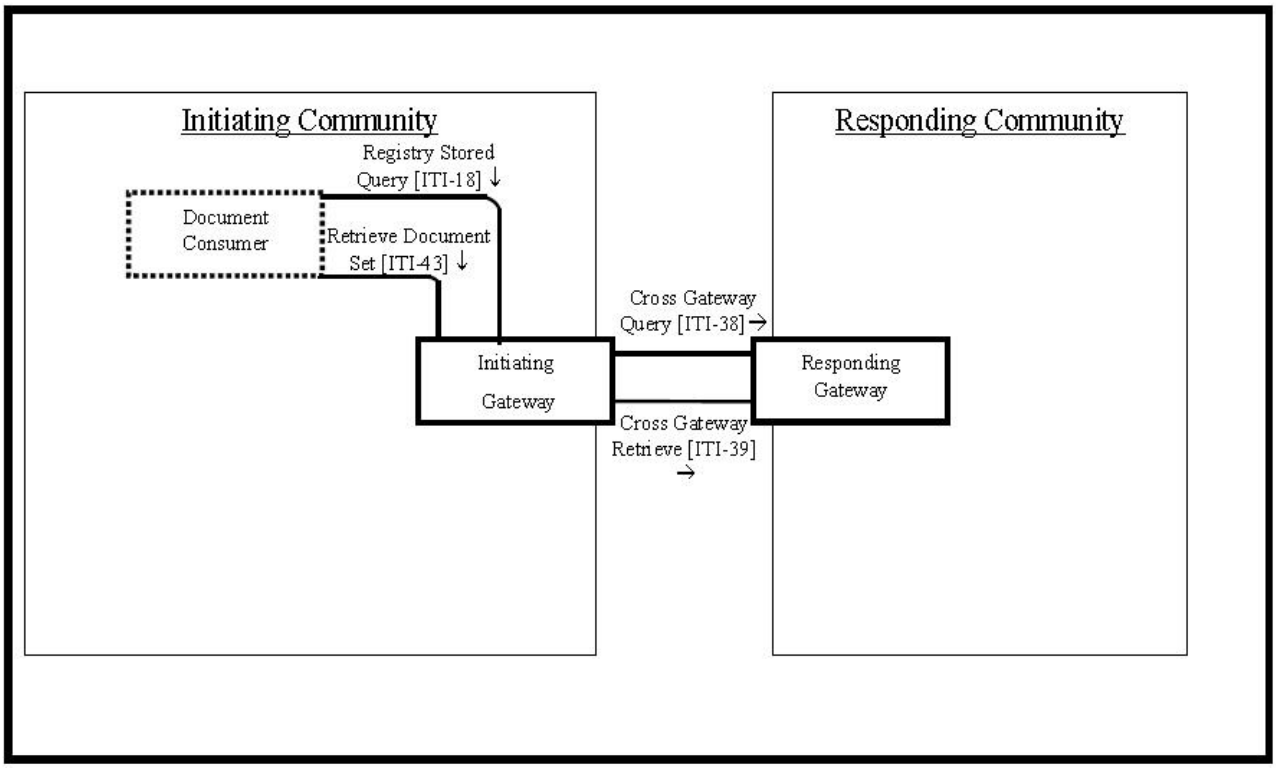


Diagramm der Akteure im XCA Profil.

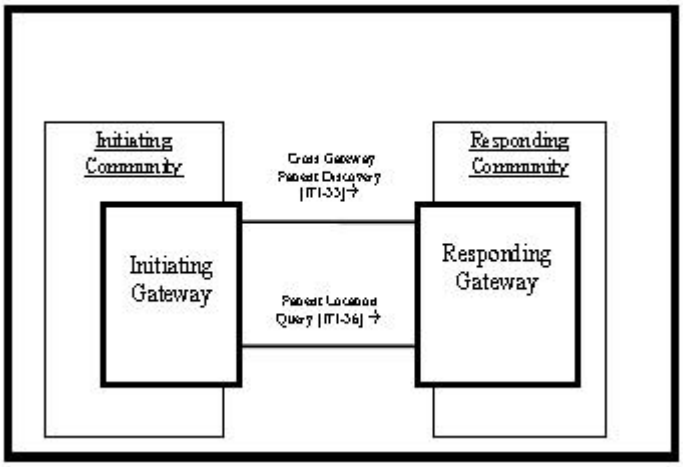
Dabei geht das Profil davon aus, dass eine Vertrauensstellung zwischen den kommunizierenden Domänen (also medizinischen Netzwerken) gibt und das die jeweiligen Regeln (Policies) für den rollenbasierten Zugriff auf die Dokumente abgeglichen sind.

Welche Ausprägung von den in diesem Cookbook beschriebenen "Affinity Domains" das jeweilige Netzwerk betreibt wird durch das XCA Profil nicht vorgegeben. Die Gateways der Netzwerke müssen lediglich in der Lage sein die Anfragen eines entfernten Gateways beantworten zu können.

6.1.2 Cross-Community Patient Discovery (XCPD)

Bevor ein Zugriff auf ein Dokument einer entfernten "Affinity Domain" erfolgen kann (wie oben unter XCA beschrieben) muss die anfragende Domäne wissen, wie der Patient in der angebundenen Domäne identifiziert ist.

Hierzu können die verschiedensten Mechanismen, wie Online- oder Offline-Token, Barcodes, Chipkarten, etc. genutzt werden. Um einen medien-freien Mechanismus zu realisieren, bei dem die Identifikation des Patienten bei der entfernten Domäne erfragt werden kann, zu implementieren, hat die IHE das Profil "Cross-Community Patient Discovery (XCPD)" spezifiziert.



Hierbei sendet das anfragende (initiating) Gateway eine Nachricht, in der einige demografischen Daten aus der eigenen Domäne enthalten sind. Mit diesen Daten kann dann das antwortende (responding) Gateway den Identifikationsanbieter seiner eigenen Domäne fragen und dessen Antwort an die anfragende Domäne zurück übermitteln.

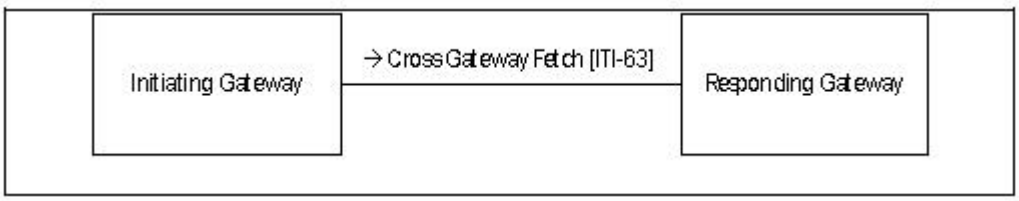
Anschließend können die Dokumentenabrufe (XCA, XCF) mit der korrekten Identifikation ausgeführt werden.

6.1.3 Cross-Community Fetch (XCF)

Nachdem in einigen Projekten, in denen eine domänenübergreifende Kommunikation mit den Profilen XCA und XCPD realisiert worden waren, stellte die Beteiligten fest, dass insbesondere beim Zugriff auf mehrere Dokumente eines Patienten ein Vielzahl von Transaktionen ausgeführt werden müssen, die die Performance der Gateways stark beanspruchen.

Dabei hat sich die ITI Domäne der IHE, in 2011 dazu entschlossen einen weiteren "Cross-Affinity Domain" Mechanismus zu beschreiben, mit dem insbesondere diesen Situationen Rechnung getragen werden kann.

Das Profil "Cross-Community Fetch (XCF)" ermöglicht den schnellen "Retrieve" von mehreren Dokumenten in einer Transaktion und schlägt darüber hinaus auch einen Caching Mechanismus vor.



6.2 Deutsche Content Profiles

"On top of XDS" werden weitergehende Spezifikationen benötigt, die Festlegungen zu den Inhalten treffen. Im Rahmen von IHE und dem deutschen Interoperabilitätsforums sind dazu bereits Dokumente erarbeitet worden:

- XDS-SD
- XDS-MS
- VhitG Arztbrief 1.5
- Arztbrief 2013
- Patientenzustimmung
- ePflegebericht
- ...

7 Anhang A – Konformität

Ein wichtiger Punkt in der Erstellung von Schnittstellensoftware ist die Erarbeitung und Einhaltung von Vorgaben zum Datenaustausch. Dies wird nachfolgend eingehender dargestellt.

7.1 Konformitätskriterien

IHE hat einen Prozess etabliert, um Spezifikationen zu erstellen, die öffentlich, allgemein verfügbar und abgestimmt sind. Dies erfolgt in einem Zyklus, der sich jährlich wiederholt:

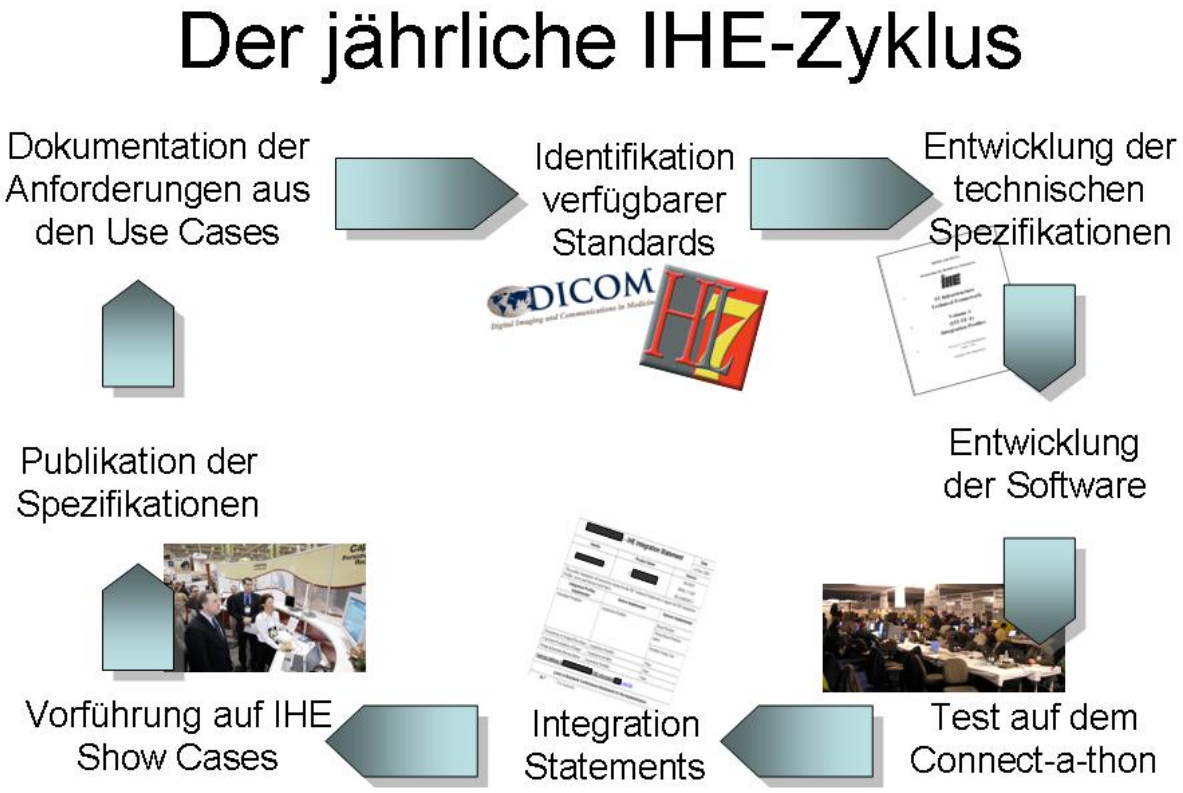


Abbildung 37: Der IHE-Zyklus

Es beginnt mit der Sammlung der Anforderungen seitens der Anwender, welches Szenarium zu realisieren ist und welcher dazugehörige Workflow etabliert werden soll. Das kann dann bspw. die Auftragskommunikation zur Radiologie unter Einbeziehung bildgebender Geräte und des Archives oder aber das Drucken von Barcode-Etiketten im Labor sein. Wenn der Workflow beschrieben ist, wird nach verfügbaren Standards gesucht, die zur Umsetzung eingesetzt werden können. Hierbei kommt dann häufig HL7, DICOM, ebXML oder auch NTP zum Einsatz. Diese Standards werden dann für die Nutzung innerhalb des Use Cases genauer spezifiziert. (Dieser Vorgang bezeichnet man als Profilierung und ist nachfolgend noch einmal näher erläutert.) Typischerweise entsteht dann eine Vorabspezifikation, die aus 2 Teilen besteht. Im ersten Teil ist der Workflow beschrieben, der dann als „Integration Profile" bezeichnet wird und die Interaktion zwischen verschiedenen Akteuren enthält. Beispiele dazu (wie XDS, ATNA oder CT) sind im Hauptteil dieses Cookbooks bereits aufgeführt. Im zweiten Teil sind dann die Transaktionsdetails auf Basis der verwendeten Standards genau dokumentiert, so dass ein Hersteller diese direkt implementieren kann.

Die dazu entstandene Software kann danach auf dem sog. Connect-a-thon getestet werden. Dieser Begriff ist ein Kunstwort, das sich aus „Connect" und „Marathon" zusammensetzt und im Prinzip eine einwöchige Veranstaltung bezeichnet, auf der sich viele Hersteller treffen, über eine LAN-Party direkt vernetzen und in einer geschützten Umgebung die neu entwickelte Software gegen- bzw. miteinander auf Einhaltung der Spezifikation und korrekten Umsetzung der Funktionalität testen können. Dies erfolgt unter Aufsicht sog. „Monitore" – das sind unabhängige Experten, die die umzusetzenden Spezifikationen im Detail kennen und entscheiden können, ob ein Hersteller die Spezifikation korrekt implementiert hat. Wenn das der Fall ist und der Hersteller in drei Tests mit unterschiedlichen Partnern dies demonstrieren kann, dann gilt die Vorgabe als erfüllt und der Hersteller bekommt dies als erfolgreiche Teilnahme bescheinigt.

Dies ist dann wiederum die Grundlage für die sog. Integration Statements als Konformitäts-erklärung (s.u.), die angibt, welche Akteure aus welchen Integrationsprofilen seine Software realisieren kann. Auf dieser Basis werden dann Showcases auf größeren Messen wie der HIMSS in den USA, der woHIT in Europa oder dem DRK in Deutschland durchgeführt. Gleichzeitig wird damit demonstriert, dass die neue Spezifikation geeignet ist, um den beschrie-benen Use Case zu realisieren. Diese wird dann als Technical Framework auf [www.ihe.net-http://www.ihe.net/] veröffentlicht.

7.2 Konformitätserklärung von Herstellern

Das IHE Integration Statement ist eine Konformitätserklärung eines Herstellers für seine Software:

IHE Integration Statement			
Vendor	**Product Name**	**Version**	**Date**
Super Vision Inc.	SuperVision	7.5.3	2011
This product implements all transactions required in the IHE Technical Framework to support the IHE Integration Profiles, Actors and Options listed below:			
Integration Profiles Implemented	**Actors Implemented**	**Options Implemented**	
Consistent Time (CT) http://ihe.univ-rennes1.fr/TF/actor.php?actor=TIME_CLIENT	(TIME_CLIENT) Time Client		
Patient Administration Management (PAM)	(PDS) Patient Demographics Consumer	Merge Option	
	(PES) Patient Encounter Consumer		
Patient Information Reconciliation (PIR)	(OP) Order Placer		
Scheduled Workflow (SWF)	(OP) Order Placer		
Internet address for vendor's IHE information: www.supervision.com/ihe			
Links to Standards Conformance Statements for the Implementation			
HL7	www.supervision.com/hl7		
DICOM	www.supervision.com/dicom		
Links to general information on IHE			
North America: www.ihe.net	Europe: www.ihe-europe.net	Japan: www.jira-net.or.jp/ihe-j	

Abbildung 38 IHE Integration Statement

Diese enthält neben Detailangaben zum Produkt auch eine Liste der umgesetzten Integrations-profile nebst den dazugehörigen Akteuren. Einige Integrationsprofile (wie bspw. PAM) erfordern noch eine weitere Präzisierung hinsichtlich geforderter Optionen innerhalb des Profils. So muss bei Patient Administration Management angegeben werden, ob die Software die „Merge" oder „Link"-Option realisiert hat, denn eines von beiden muss vorhanden sein. Auf dieser Basis kann dann leichter entschieden werden, ob zwei Softwarekomponenten unterschiedlicher Hersteller zueinander kompatibel sind oder nicht.

Anwender können bei ihrer Suche nach geeigneten Softwarekomponenten auf diese Kon-formitätserklärungen zurückgreifen, in dem in Ausschreibungen direkt danach gefragt wird.

7.3 Profilierungsmechanismen

Jeder Kommunikationsstandard besitzt eine mehr oder weniger große Anzahl an Nachrichten mit Feldern und ggf. Komponenten, die entweder verpflichtend („muss"), optional („kann") oder verboten sind. Damit sind dann eine Reihe von Wahlmöglichkeiten bei dem Einsatz dieser Standards geschaffen, die Konfliktpotential bergen.

Für den Einsatz in einem konkreten Szenarium muss der Grundlagenstandard eingeschränkt werden, d.h. einige der ursprünglich vorhandenen Wahlmöglichkeiten werden weiter präzisiert. So muss bei einem internationalen Standard bspw. angegeben werden, wie mit deutschen Besonderheiten (Namen oder Adressen) umzugehen ist:

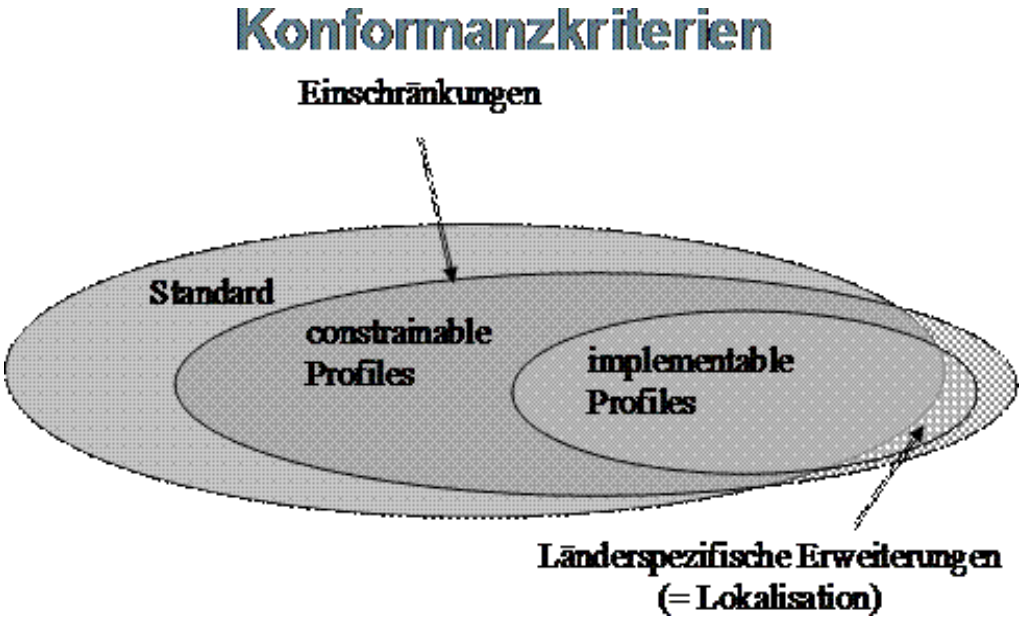


Abbildung 39 Konformanzkriterien

Dieser Prozess des Einschränkens kann iterativ geschehen, indem immer mehr Optionen weg-genommen werden, bis letztendlich keinerlei Wahlmöglichkeit mehr besteht. Man spricht hier von „constrainable profiles" (mit noch vorhandenen Optionen) und „implementable profiles" (keine Optionen mehr vorhanden).

Dabei kann es bei internationalen Standards mitunter auch passieren, dass Ergänzungen vor-genommen werden müssen, die dann quasi Erweiterungen außerhalb des Standards darstellen. Derartige Notwendigkeiten sollten dann aber Anlass sein, eine offizielle Erweiterung des Standards zu beantragen, um diesen Zustand zu beheben.

Natürlich sind bei der Festlegung von Einschränkungen Regeln einzuhalten, wie derartige Einschränkungen vorzunehmen sind, damit keine Widersprüche entstehen:

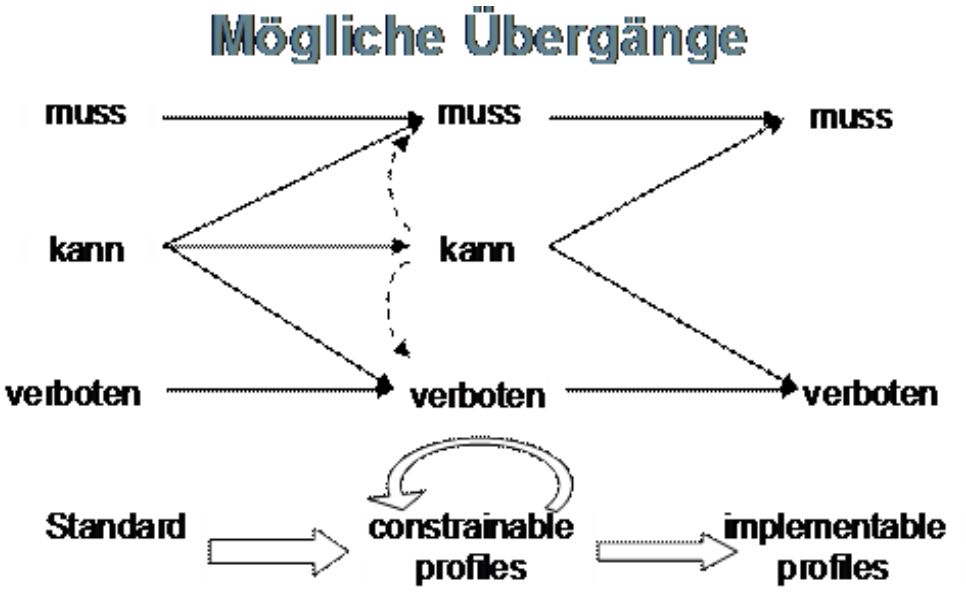


Abbildung 40 Konformanzübergänge

So müssen einmal verpflichtend gemachte Elemente („muss") immer verpflichtend bleiben. Das gleiche gilt für verbotene Elemente. Für optionale Elemente hingegen, kann entschieden werden, sie entweder verpflichtend zu machen oder sogar zu verbieten. So ist bspw. bei den deutschen Nachrichtenprofilen entschieden worden, aufgrund der deutschen Gesetzgebung die Information zu Rasse zu verbieten.

Spezifikationen ohne jegliche Optionen werden letztendlich nur von Herstellern herausgegeben. (Nationale) Vorgaben umfassen immer nur Teileinschränkungen auf den gesamten Standard und beinhalten somit immer noch Wahlmöglichkeiten, bei denen sich der Hersteller entscheiden muss, ob er dies umsetzt oder nicht.

Neben diesen grundsätzlichen Einschränkungsmechanismen gibt es noch eine Reihe weiterer Details, die es zu berücksichtigen gilt. Dazu gehören dann Kardinalitäten, Längenangaben, Vokabularienbindung mit Value Sets etc., was aber hier nicht weiter ausgeführt werden soll.

7.4 Conformance Statements

Umgekehrt sollte ein Hersteller nun für seine Schnittstelle präzise angeben können, welche Informationen berücksichtigt werden und welche nicht. Eine Aussage wie „optional" – was hier einem „weiß ich nicht" entspricht – sollte nicht vorkommen.

Eine derartige Detailspezifikation wird Conformance Statement genannt und in verschiedenen Detaillierungsgraden ausgeführt. Bei DICOM ist dies relativ oberflächlich, HL7 v2.8 geht hier bis ins kleinste Detail.

Je präziser eine derartige Dokumentation ist, desto leichter lässt sich die Kompatibilität der Software feststellen.

7.5 Konformanzprüfung

Die wahrscheinlich interessanteste Frage beim Einsatz von Schnittstellen zur Verbindung zweier Systeme ist wohl nach der Kompatibilität dieser beiden Systeme, d.h. können 2 Systeme problemlos untereinander Daten austauschen, wenn beide sich nach derselben Vorgabe richten oder nicht?

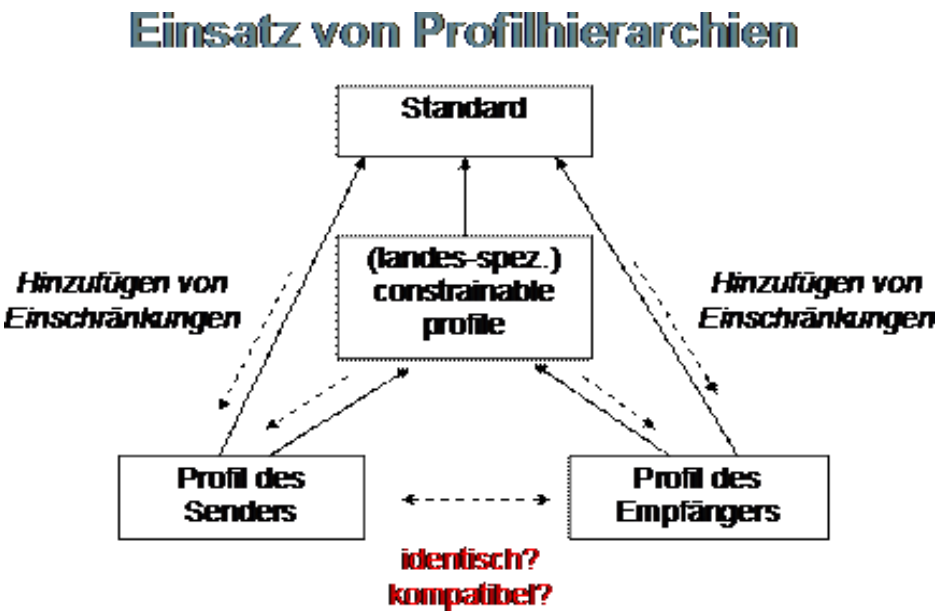


Abbildung 41 Profilhierarchien

Wie unter Berücksichtigung der o.g. Regeln wohl relativ leicht einzusehen ist, muss diese Frage leider mit „NEIN" beantwortet werden, weshalb die Dokumentation einer Schnittstelle einen sehr hohen Stellenwert in Bezug auf die Frage nach semantischer Interoperabilität einnimmt. Auf die damit verbundenen Möglichkeiten des Offline-Tests hinsichtllich Schnittstellen-kompatibilität von Softwarekomponenten soll an dieser Stelle allerdings nicht weiter eingegangen werden.

8 Anhang B – Mitgeltende Literatur bzgl. Datenschutz und Datensicherheit

8.1 Gesetze / Richtlinien / Verordnungen

8.1.1 Europa

- Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- 2001/497/EG: Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG
- Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates
- Verordnung Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation
- Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

8.1.2 Deutschland

8.1.2.1 Bund

- Grundgesetz
- Bundesdatenschutzgesetz [2] (http://www.gesetze-im-internet.de/bdsg_1990/)
- Strafgesetzbuch
- Krebsregistergesetz
- Erstes Buch Sozialgesetzbuch (Allgemeiner Teil)
- Fünftes Buch Sozialgesetzbuch (Gesetzliche Krankenversicherung)
- Siebtes Buch Sozialgesetzbuch (Gesetzliche Unfallversicherung)
- Neuntes Buch Sozialgesetzbuch (Rehabilitation und Teilhabe behinderter Menschen)
- Zehntes Buch Sozialgesetzbuch (Verwaltungsverfahren und Sozialdatenschutz)
- Elftes Buch Sozialgesetzbuch (Soziale Pflegeversicherung)
- Telekommunikationsgesetz
- Telemediengesetz
- Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation

- Gesetz gegen den unlauteren Wettbewerb

8.1.2.2 Katholische Kirche

- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Aachen
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Essen
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationkliniken in der Diözese Fulda
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Hildesheim
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Erzbistum Köln
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken in der Diözese Limburg
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Mainz
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Einrichtungen im Bistum Münster, nordrhein-westfälischer Teil
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern im Offizialatsbezirk Oldenburg
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Osnabrück
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Erzdiözese Hamburg
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern in der Diözese Speyer
- Ordnung zum Schutz von Patientendaten in katholischen Krankenhäusern und Rehabilitationskliniken im Bistum Trier

8.1.2.3 Evangelische Kirche

- Verordnung zum Schutz von Patientendaten in kirchlichen Krankenhäusern der evangelischen Kirche Bremen
- Datenschutzdurchführungsverordnung der evangelischen Lippischen Landeskirche
- Verordnung der Evangelischen Kirche der Pfalz zum Schutz von Patientendaten in kirchlichen Krankenhäusern
- Datenschutzdurchführungsverordnung der evangelischen Kirche von Westfalen

8.1.2.4 Evangelisch-Lutherische Kirche

- Datenschutzdurchführungsverordnung der evangelisch-lutherischen Landeskirche in Braunschweig
- Datenschutzdurchführungsverordnung der evangelisch-lutherischen Landeskirche Hannover
- Datenschutzdurchführungsverordnung der evangelisch-lutherischen Landeskirche Mecklenburgs
- Datenschutzdurchführungsverordnung der Nordelbischen evangelisch-lutherischen Landeskirche
- Datenschutzdurchführungsverordnung der evangelisch-lutherischen Landeskirche Oldenburg
- Datenschutzdurchführungsverordnung der evangelisch-lutherischen Landeskirche Schaumburg-Lippe
- Richtlinien zum Schutz von Patientendaten in kirchlichen Krankenhäusern, Alten- und Pflegeheimen der evangelisch-lutherischen Landeskirche Schaumburg-Lippe

8.1.2.5 Evangelisch-reformierte Kirche

- Datenschutzdurchführungsverordnung der evangelisch-reformierten Kirche

8.1.2.6 Baden-Württemberg

- Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz)[3] (http://www.baden-wuerttemberg.datenschutz.de/recht/ldsg/default.htm)
- Landeskrankenhausgesetz Baden-Württemberg [4] (http://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KHG+BW&psml=bsbawueprod.psml&max=true&aiz=true)
- Meldegesetz Baden-Württenberg
- Gesetz über die Krebsregistrierung in Baden-Württemberg
- Unterbringungsgesetz

8.1.2.7 Bayern

- Bayerisches Datenschutzgesetz
- Bayerisches Krankenhausgesetz
- Meldegesetz
- Gesetz über das bevölkerungsbezogene Krebsregister Bayern
- Unterbringungsgesetz

8.1.2.8 Berlin

- Berliner Datenschutzgesetz
- Krankenhaus-Verordnung
- Landeskrankenhausgesetz
- Meldegesetz
- Staatsvertrag über das gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt und der Freistaaten Sachsen und Thüringen
- Gesetz zur Einführung einer Meldepflicht für Krebserkrankungen
- Gesetz für psychisch Kranke

8.1.2.9 Brandenburg

- Brandenburgisches Datenschutzgesetz
- Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz
- Brandenburgisches Krankenhausentwicklungsgesetz
- Brandenburgisches Meldegesetz
- Krebsregistergesetz
- Gesetz zur Einführung einer Meldepflicht für Krebserkrankungen
- Brandenburgisches Psychisch-Kranken-Gesetz

8.1.2.10 Bremen

- Bremisches Datenschutzgesetz
- Bremisches Krankenhausdatenschutzgesetz
- Meldegesetz Bremen

- Gesetz über das Krebsregister der freien Hansestadt Bremen
- Gesetz über Hilfen und Schutzmaßnahmen ei psychischen Krankheiten

8.1.2.11 Hamburg

- Hamburgisches Datenschutzgesetz
- Hamburgisches Krankenhausgesetz
- Hamburgisches Meldegesetz
- Hamburgisches Krebsregistergesetz
- Hamburgisches Gesetz über Hilfen und Schutzmaßnahmen bei psychisch Kranken

8.1.2.12 Hessen

- Hessisches Datenschutzgesetz
- Hessisches Krankenhausgesetz
- Hessisches Meldegesetz
- Hessisches Krebsregistergesetz
- Gesetz über die Entziehung der Freiheit geisteskranker, geistesschwacher, rauschgift- oder alkoholsüchtiger Personen

8.1.2.13 Mecklenburg-Vorpommern

- Landesdatenschutzgesetz
- Landeskrankenhausgesetz
- Landesmeldegesetz
- Krebsregistergesetz
- Gesetz zur Ausführung des Krebsregistergesetzes
- Psychischkrankengesetz

8.1.2.14 Niedersachsen

- Niedersächsisches Datenschutzgesetz
- Niedersächsisches Meldegesetz
- Gesetz über das Epidemiologische Krebsregister Niedersachsen
- Niederländisches Gesetz über Hilfen und Schützmaßnahmen für psychisch Kranke

8.1.2.15 Nordrhein-Westfalen

- Datenschutzgesetz
- Gesundheitsdatenschutzgesetz NRW
- Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen
- Meldegesetz NRW
- Krebsregistergesetz NRW
- Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten

8.1.2.16 Rheinland-Pfalz

- Landesdatenschutzgesetz
- Landeskrankenhausgesetz Rheinland-Pfalz

- Meldegesetz Rheinland-Pfalz
- Landesgesetz zur Weiterführung des Krebsregisters
- Landesgesetz für psychisch kranke Personen

8.1.2.17 Saarland

- Saarländisches Datenschutzgesetz
- Saarländisches Krankenhausgesetz
- Meldegesetz Saarland
- Saarländisches Krebsregistergesetz
- Unterbringungsgesetz

8.1.2.18 Sachsen

- Sächsisches Datenschutzgesetz
- Sächsisches Krankenhausgesetz
- Sächsisches Meldegesetz
- Krebsregistergesetz
- Sächsisches Ausführungsgesetz zum Krebsregistergesetz
- Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten

8.1.2.19 Sachsen-Anhalt

- Gesetz zum Schutz personenbezogener Daten der Bürger
- Meldegesetz des Landes Sachsen-Anhalt
- Krebsregistergesetz
- Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen des Landes Sachsen-Anhalt

8.1.2.20 Schleswig-Holstein

- Landesdatenschutzgesetz
- Landesmeldegesetz Schleswig-Holstein
- Landeskrebsregistergesetz
- Psychisch-Kranken-Gesetz
- Datenschutzverordnung
- Landesverordnung über ein Datenschutzaudit

8.1.2.21 Thüringen

- Thüringer Datenschutzgesetz
- Thüringer Krankenhausgesetz
- Thüringer Meldegesetz
- Krebsregistergesetz
- Thüringer Gesetz zur Einführung der Meldepflicht an das Gemeinsame Krebsregister
- Thüringer Gesetz zur Hilfe und Unterbringung psychisch kranker Menschen

8.1.3 Berufsgruppenspezifische Vorschriften

8.1.3.1 Baden-Württemberg

- Berufsordnung Landesärztekammer Baden-Württemberg
- Berufsordnung für Zahnärzte der Landezahnsärztekammer Baden-Württemberg
- Berufsordnung der Landespsychotherapeutenkammer Baden-Württemberg
- Berufsordnung der Landesapothekerkammer Baden-Württemberg
- Berufsordnung des Landespflegerates Baden-Württemberg

8.1.3.2 Bayern

- Berufsordnung für die Ärzte Bayerns
- Berufsordnung für die Bayerischen Zahnärzte
- Berufsordnung für die Psychologischen Psychotherapeutinnen und Psychotherapeuten und für die Kinder- und Jugendlichenpsychotherapeutinnen - psychotherapeuten Bayerns

8.1.3.3 Berlin

- Berufsordnung der Ärztekammer Berlin
- Berufsordnung der Zahnärztekammer Berlin
- Berufsordnung der Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten im Land Berlin

8.1.3.4 Brandenburg

- Berufsordnung der Landesärztekammer Brandenburg
- Berufsordnung der Landeszahnärztekammer Brandenburg
- Berufsordnung der Ostdeutschen Psychotherapeutenkammer

8.1.3.5 Bremen

- Berufsordnung für Ärztinnen und Ärzte im Lande Bremen
- Berufsordnung der Zahnärztekammer Bremen
- Berufsordnung der Psychologischen Psychotherapeutinnen und Psychologischen Psychotherapeuten und der Linder- und Jugendlichenpsychotherapeutinnen und Kinder- und Jugendlichenpsychotherapeuten im Lande Bremen
- Berufsordnung für Gesundheits- und Krankenpflegerinnen, Gesundheits- und Krankenpfleger, Gesundheits- und Kinderkrankenpflegerinnen und Gesundheits- und Kinderkrankenpfleger im Lande Bremen

8.1.3.6 Hamburg

- Berufsordnung der Hamburger Ärzte und Ärztinnen
- Berufsordnung der Zahnärztekammer Hamburg
- Berufsordnung der Psychotherapeutenkammer Hamburg
- Berufsordnung für Gesundheits- und Krankenpflegerinnen, Gesundheits- und Krankenpfleger, Gesundheits- und Kinderkrankenpflegerinnen und Gesundheits- und Kinderkrankenpfleger sowie Altenpflegerinnen und Altenpfleger

8.1.3.7 Hessen

- Berufsordnung für Ärztinnen und Ärzte in Hessen
- Berufsordnung für hessische Zahnärztinnen und Zahnärzte
- Berufsordnung der Landeskammer für Psychologische Psychotherapeuten und -therapeutinnen und Kinder- und Jugendlichenpsychotherapeutinnen und -therapeuten Hessen

8.1.3.8 Mecklenburg-Vorpommern

- Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern
- Berufsordnung der Zahnärztekammer Mecklenburg-Vorpommern
- Berufsordnung der Ostdeutschen Psychotherapeutenkammer

8.1.3.9 Niedersachsen

- Berufsordnung der Ärztekammer Niedersachsen
- Berufsordnung der Zahnärztekammer Niedersachsen
- Berufsordnung der Psychotherapeutenkammer Niedersachsen
- Berufsordnung für Gesundheits- und Krankenpflegerinnen, Gesundheits- und Krankenpfleger, Gesundheits- und Kinderkrankenpflegerinnen und Gesundheits- und Kinderkrankenpfleger im Lande Niedersachsen (Entwurf)

8.1.3.10 Nordrhein-Westfalen

- Berufsordnung für die nordrheinischen Ärztinnen und Ärzte
- Berufsordnung der Ärztekammer Westfalen-Lippe
- Berufsordnung der Zahnärztekammer Nordrhein
- Berufsordnung der Zahnärztekammer Westfalen-Lippe
- Berufsordnung der Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen

8.1.3.11 Rheinland-Pfalz

- Berufsordnung für Ärztinnen und Ärzte in Rheinland-Pfalz
- Berufsordnung für Zahnärzte im Lande Rheinland-Pfalz
- Berufsordnung der Landespsychotherapeutenkammer Rheinland-Pfalz
- Berufsordnung des Dachverbandes der Pflegeorganisationen Rheinland-Pfalz e.V.

8.1.3.12 Saarland

- Berufsordnung für Ärztinnen und Ärzte des Saarlands
- Berufsordnung für die saarländischen Zahnärztinnen und Zahnärzte
- Berufsordnung der Psychotherapeutenkammer des Saarlandes
- Berufsordnung für Pflegekräfte im Saarland

8.1.3.13 Sachsen

- Berufsordnung der Sächsischen Landesärztekammer
- Berufsordnung für die Zahnärzte im Freistaat Sachsen
- Berufsordnung der Ostdeutschen Psychotherapeutenkammer

8.1.3.14 Sachsen-Anhalt

- Berufsordnung der Ärztekammer Sachsen-Anhalt
- Berufsordnung der Zahnärztekammer Sachsen-Anhalt
- Berufsordnung der Ostdeutschen Psychotherapeutenkammer

8.1.3.15 Schleswig-Holstein

- Berufsordnung der Ärztekammer Schleswig-Holstein
- Berufsordnung der Zahnärztekammer Schleswig-Holstein
- Berufsordnung der Psychotherapeutenkammer Schleswig-Holstein

8.1.3.16 Thüringen

- Berufsordnung der Landesärztekammer Thüringen
- Berufsordnung für Thüringer Zahnärzte
- Berufsordnung der Ostdeutschen Psychotherapeutenkammer

8.2 Normen

8.2.1 Deutschland

- DIN 31644: Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive(, Status: Norm-Entwurf)
- DIN 31645: Information und Dokumentation - Leitfaden zur Informationsübernahme in digitale Langzeitarchive(, Status: Norm)
- DIN 6789-6: Dokumentationssystematik - Teil 6: Verfälschungssicherheit digitaler technischer Dokumentation(1998-05, Status: Norm)
- DIN EN 12251: Sichere Nutzeridentifikation im Gesundheitswesen - Management und Sicherheit für die Authentifizierung durch Passwörter(2005-07, Status: Norm)
- DIN EN 13606-4: Kommunikation von Patientendaten in elektronischer Form - Teil 4(2007-06, Status: Norm)
- DIN EN 14169-1: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 1: Überblick(2011-05, Status: Norm-Entwurf)
- DIN EN 14169-2: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 2: Geräte mit Schlüsselerzeugung(2010-03, Status: Norm-Entwurf)
- DIN EN 14169-3: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 3: Einheiten mit Schlüsselimport(2010-08, Status: Norm-Entwurf)
- DIN EN 14169-4: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 4: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigem Kanal zur Zertifizierung von Generierungsanwendungen(2010-08, Status: Norm-Entwurf)
- DIN EN 14169-5: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 5: Erweiterung für Einheiten mit Schlüsselgenerierung und vertrauenswürdigem Kanal zur Signatur von Generierungsanwendungen(2010-08, Status: Norm-Entwurf)
- DIN EN 14169-6: Schutzprofile für Sichere Signaturerstellungseinheiten - Teil 6: Erweiterung für Einheiten mit Schlüsselimport und vertrauenswürdigem Kanal zur Signatur von Generierungsanwendungen(2010-08, Status: Norm-Entwurf)

- DIN EN 14484: Internationaler Austausch von unter die EU-Datenschutzrichtlinie fallenden persönlichen Gesundheitsdaten - Generelle Sicherheits-Statements(2004-03, Status: Norm)
- DIN EN 14485: Anleitung zur Verwendung von persönlichen Gesundheitsdaten in internationalen Anwendungen vor dem Hintergrund der EU-Datenschutzrichtlinie(2004-03, Status: Norm)
- DIN CEN/TS 15260: Klassifikation von Sicherheitsrisiken bei der Benutzung von Medizininformatikprodukten(2007-04, Status: Vornorm)
- DIN CEN/TS 15260: Medizinische Informatik - Klassifikation von Sicherheitsrisiken bei der Benutzung von Medizininformatikprodukten(2007-04, Status: Vornorm)
- DIN EN 15713: Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln(2009-08, Status: Norm)
- DIN ISO/IEC 27000: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie (2011-07, Status: Norm)
- DIN ISO/IEC 27001: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (2008-09, Status: Norm)
- DIN ISO/IEC 27002: Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management (2008-09, Status: Norm)
- DIN EN ISO 27789: Audit-Trails für elektronische Gesundheitsakten(2010-12, Status: Norm-Entwurf)
- DIN EN ISO 27799: Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002(2008-10, Status: Norm)
- DIN 66399-1: Büro- und Datentechnik - Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe(2011-09, Status: Norm-Entwurf)
- DIN 66399-2: Büro- und Datentechnik - Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern(2011-09, Status: Norm-Entwurf)
- DIN EN 80001-1: Anwendung des Risikomanagements für IT-Netzwerke mit Medizinprodukten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten(2009-10, Status: Norm-Entwurf)

8.2.2 Internationale Normen

- ISO/IEC 9798-1: Informationstechnik - IT Sicherheitsverfahren - Authentifikation von Instanzen - Teil 1: Allgemeines Modell (2010-07, Status: Norm)
- ISO/IEC 9798-2: Informationstechnik - IT-Sicherheitsverfahren - Authentifikation von Instanzen - Teil 2: Mechanismen auf Basis von Verschlüsselungsalgorithmen (2008-12, Status: Norm)
- ISO/IEC 9798-3: Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques (2009-09, Status: Norm)
- ISO/IEC 9798-4: Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function (2009-09, Status: Norm)
- ISO/IEC 9798-5: Informationstechnik - IT Sicherheitsverfahren - Authentifikation von Instanzen - Teil 5: Mechanismen auf Basis von zero-knowledge Techniken (2009-12, Status: Norm)
- ISO/IEC 9798-6: Informationstechnik - IT Sicherheitsverfahren - Authentifikation von Instanzen - Teil 6: Mechanismen auf Basis von manuellem Datentranfer (2009-12, Status: Norm)

- ISO/IEC 11586-1: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Konzepte, Modelle und Notation (1996-06, Status: Norm)
- ISO/IEC 11586-3: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Protokollspezifikationen für das Dienstelement für den Austausch von Sicherheitsinformationen (SESE) (1996-06, Status: Norm)
- ISO/IEC 11586-4: Informationstechnik - Kommunikation Offener Systeme - Allgemeine Sicherheitsmechanismen für die anwendungsorientierten OSI-Schichten: Spezifikationen der schützenden Übertragungssyntax (1996-06, Status: Norm)
- ISO/IEC 15408-1: Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (2009-12, Status: Norm)
- ISO/IEC 15408-2: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components (2008-08, Status: Norm)
- ISO/IEC 15408-3: Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (2008-08, Status: Norm)
- ISO/IEC 15816: Informationstechnik - IT-Sicherheitsverfahren - Sicherheitsobjekte für Zugriffskontrolle (2002-02, Status: Norm)
- ISO/IEC 18031: Information technology - Security techniques - Random bit generation (2011-08, Status: Norm-Entwurf)
- ISO/IEC 18033-1: IT-Sicherheitsverfahren - Verschlüsselungsalgorithmen - Teil 1: Allgemeines Modell; Änderung 1 (2011-03, Status: Norm)
- ISO/IEC 18033-2: Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers (2006-05, Status: Norm)
- ISO/IEC 18033-3: Informationstechnik - IT Sicherheitsverfahren - Verschlüsselungsalgorithmen - Teil 3: Blockziffern (2010-12, Status: Norm)
- ISO/IEC 18033-4: Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers (2011-09, Status: Norm-Entwurf)
- ISO/IEC 18043: Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (2006-06, Status: Norm)
- ISO/IEC 18045: Information technology - Security techniques - Methodology for IT security evaluation (2008-08, Status: Norm)
- ISO/IEC 19772: Information technology - Security techniques - Authenticated encryption (2009-02, Status: Norm)
- ISO/IEC 19792: Informationstechnik - IT-Sicherheitsverfahren - Sicherheitsevaluation der Biometrie (2009-08, Status: Norm)
- ISO 17090-1: Public-Key-Infrastruktur - Teil 1: Überblick über digitale Zertifizierungsdienste (2008-02, Status: Norm)
- ISO 17090-2: Public-Key-Infrastruktur - Teil 2: Zertifikatsprofile (2008-02, Status: Norm)
- ISO 17090-3: Public-Key-Infrastruktur - Teil 3: Policymanagement von Zertifizierungsinstanzen (2008-02, Status: Norm)

- ISO/DIS 22857: Leitlinien für den Datenschutz zur Ermöglichung grenzüberschreitender Kommunikation von persönlichen Gesundheitsinformationen (2011-06, Status: Norm-Entwurf)
- ISO/IEC 24761: Information technology - Security techniques - Authentication context for biometrics (2009-05, Status: Norm)
- ISO/IEC 24762: Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services (2008-02, Status: Norm)
- ISO/IEC 24767-1: Informationstechnik - Sicherheit von Heim-Netzwerken - Teil 1: Sicherheitsanforderungen (2008-09, Status: Norm)
- ISO/IEC 24745: Information technology - Security techniques - Biometric information protection (2011-06, Status: Norm)
- ISO/IEC 24767-2: Informationstechnik - Sicherheit von Heim-Netzwerken - Teil 2: Interne Sicherheitsdienste: Sicheres Kommunikationsprotokoll für Middleware (2009-01, Status: Norm)
- ISO/IEC 27003: Information technology - Security techniques - Information security management system implementation guidance (2010-02, Status: Norm)
- ISO/IEC 27004: Information technology - Security techniques - Information security management - Measurement (2009-12, Status: Norm)
- ISO/IEC 27005: Information technology - Security techniques - Information security risk management (2011-06, Status: Norm)
- ISO/IEC 27006: Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems (2011-04, Status: Norm-Entwurf)
- ISO/IEC 27007: Information technology - Security techniques - Guidelines for information security management systems auditing (2011-08, Status: Norm-Entwurf)
- ISO/IEC 27011: Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (2008-12, Status: Norm)
- ISO/IEC 27031: Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (2011-03, Status: Norm)
- ISO/IEC 27033-1: Information technology - Security techniques - Network security - Part 1: Overview and concepts (2009-12, Status: Norm)
- ISO/IEC 27033-3: Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues (2010-12, Status: Norm)
- ISO/IEC 27035: Information technology - Security techniques - Information security incident management (2011-09, Status: Norm)

8.3 Literaturangaben (Referenzen)