



## **Audit Trail**

Anforderung an die Erstellung von Audit Trails  
im Kontext der elektronischen Fallakte

**Editor: Olaf Rode, Jörg Caumanns, Sören Bittins**

Dokumenten-ID: Audit Trail  
Verantwortlich: Fraunhofer ISST  
Status: Release  
Version: 1.2.0.03  
Letztes Update: 29. Februar 2008  
Kategorie: Security and Privacy  
Non-Normative

## Copyright

Copyright 2008 © Fraunhofer-Institut für Software- and Systemtechnik (ISST), Asklepios Kliniken Verwaltungsgesellschaft mbH, Charité - Universitätsmedizin Berlin, Deutsche Krankenhausgesellschaft e.V., HELIOS Kliniken GmbH, Klinikum Dortmund gGmbH, Rhön-Klinikum AG, Sana e.med GmbH, Städtisches Klinikum München GmbH, Universitätsklinikum Aachen, Universitätsklinikum Tübingen and Vivantes GmbH Berlin. Alle Rechte vorbehalten.

Dieses Dokument und Übersetzungen, die davon angefertigt wurden, dürfen kopiert und weitergegeben werden und abgeleitete Werke, die es kommentieren, erklären, oder Hilfestellung bei der Implementierung leisten, dürfen vorbereitet, kopiert, veröffentlicht und verteilt werden, als Ganzes oder in Teilen, ohne dass hierbei Einschränkungen in irgendeiner Form bestehen; vorausgesetzt, dass die obige Urheberrechtserklärung und dieser Absatz in allen Kopien und abgeleiteten Werken enthalten sind. Dieses Dokument selbst darf nur mit schriftlichem Einverständnis der Urheber modifiziert werden. Die beschränkten Rechte, die durch obige Aussage gewährt werden, sind dauerhaft und werden von den oben genannten Urhebern, ihren Nachfolgeorganisationen und Rechtsnachfolgern nicht zurückgezogen werden. Dieses Dokument und die hierin enthaltene Information werden ohne Mängelgewähr zur Verfügung gestellt.

DAS FRAUNHOFER-INSTITUT FÜR SOFTWARE- AND SYSTEMTECHNIK (ISST), DIE ASKLEPIOS KLINIKEN VERWALTUNGSGESELLSCHAFT MBH, DIE CHARITÉ - UNIVERSITÄTSMEDIZIN BERLIN, DIE DEUTSCHE KRANKENHAUSGESELLSCHAFT E.V., DIE HELIOS KLINIKEN GMBH, DIE KLINIKUM DORTMUND GGMBH, DIE RHÖN-KLINIKUM AG, DIE SANA E.MED GMBH, DIE STÄDTISCHES KLINIKUM MÜNCHEN GMBH, DAS UNIVERSITÄTSKLINIKUM AACHEN, DAS UNIVERSITÄTSKLINIKUM TÜBINGEN UND DIE VIVANTES GMBH BERLIN UND DIE AN DER ERSTELLUNG DIESES DOKUMENTS BETEILIGTEN MITARBEITER DER GENANNTEN EINRICHTUNGEN SCHLIESSEN JEDE FORM DER HAFTUNG, OB GEÄUßERT ODER VERMUTET; AUS, DAFÜR DASS DIE VERWENDUNG DER INFORMATIONEN IN DIESEM DOKUMENT KEINE RECHTE VERLETZT; DASS SIE GEBRAUCHSTAUGLICH SIND ODER SICH FÜR EINEN SPEZIELLEN ZWECK EIGNEN.

Diese Spezifikation ist unter <http://www.fallakte.de> verfügbar.



## Änderungsübersicht

Version	Datum	Seite	Bemerkungen	Bearbeiter
0.1	20.08.07	Alle	Erste Version	JC, SB
0.5	02.10.07	Alle	Überarbeitung	OR
0.9	16.10.07	Alle	Ergänzung	OR
1.2	29.02.08	Alle	Anpassung an aktuellen Stand der Anwendungs- und Sicherheitsarchitektur	OR

## Statushistorie

Status	Datum	Bemerkungen	Bearbeiter
In Erstellung	20.08.07	Erste Version	JC, SB
Draft	02.10.07	Fertigstellung für Review	OR
PreFinal	29.02.08	PreFinal	OR
Final			

## Inhalt

<b>1</b>	<b>Einleitung</b>	<b>6</b>
1.1	Zielgruppe	6
1.2	Referenzierte Spezifikationen und Standards	7
1.3	Konventionen	7
<b>2</b>	<b>Grundlagen</b>	<b>8</b>
2.1	Erstellen von Zugriffsprotokollen	9
2.2	Archivierung von Zugriffsprotokollen	10
2.3	Schutz von Zugriffsprotokollen	11
2.4	Auswertung von Zugriffsprotokollen	12
2.4.1	Sicherheitsprüfung und -überprüfung	13
<b>3</b>	<b>EFA-spezifische Protokollierung</b>	<b>14</b>
3.1	Überblick	14
3.2	Event Identification	15
3.3	Active Participant Identification	16
3.4	Network Access Point Identification	17
3.5	Audit Source Identification	18
3.6	Participant Object Identification	18
<b>4</b>	<b>EFA-spezifische Audit-Nachrichten</b>	<b>20</b>
4.1	ECR Generic	21
4.1.1	Generic.AuditRecordingStarted / Generic.AuditRecordingStopped	21
4.2	ECR Identity Provider (IdtPrv)	22
4.2.1	IdtPrv.authenticate	22
4.3	ECR Admission Token Service (AdmTokSvc)	23
4.3.1	AdmTokSvc.requestAdmissionTokenCollection / AdmTokSvc.requestAdmissionTokenSelection	23
4.3.2	AdmTokSvc.requestAdmissionToken	25
4.4	ECR Access Token Service (AccTokSvc)	27
4.4.1	AccTokSvc.requestAccessToken	27
4.4.2	AccTokSvc.requestCreationToken	29
4.4.3	AccTokSvc.registerRecord	30
4.5	ECR Policy Token Service (PolTokSvc)	31
4.5.1	PolTokSvc.requestPolicyToken	31
4.5.2	PolTokSvc.resolveAccessToken	33
4.6	ECR Record Registry (RecReg)	34
4.6.1	RecReg.getRecordList	34
4.6.2	RecReg.setRecordMetadata / RecReg.getRecordMetadata /	



	RecReg.setRecordState / RecReg.getRecordState /	
	RecReg.getRecordStateHistory	36
4.6.3	RecReg.registerRecord	38
4.7	ECR Folder Registry (FldReg)	39
4.7.1	FldReg.getFolderList	39
4.7.2	FldReg.setFolderMetadata / FldReg.setFolderState	
	/FldReg.getFolderState /	
	FldReg.getFolderStateHistory /	
	FldReg.getFolderStateCollection /	
	FldReg.getFolderStateHistoryCollection	41
4.7.3	FldReg.resumeRecord / FldReg.suspendRecord	43
4.7.4	FldReg.createAndRegisterRecord	44
4.7.5	FldReg.registerFolder	45
4.8	ECR Document Registry (DocReg)	47
4.8.1	DocReg.createAndRegisterFolder	47
4.8.2	DocReg.getInformationObjectList / DocReg.	
	getInformationObjectListCollection	49
4.8.3	DocReg.suspendFolder / DocReg.resumeFolder	51
4.8.4	DocReg.setInformationObjectState /	
	DocReg.getInformationObjectState /	
	DocReg.getInformationObjectStateHistory /	
	DocReg.getInformationObjectStateCollection /	
	DocReg.getInformationObjectStateHistoryCollection	53
4.8.5	DocReg.registerInformationObject	55
4.9	ECR Document Repository (DocRep)	57
4.9.1	DocRep.createAndRegisterInformationObject	57
4.9.2	DocRep.getInformationObject /	
	DocRep.getInformationObjectCollection	59
4.9.3	DocRep.resumeInformationObject /	
	DocRep.suspendInformationObject	60
<b>5</b>	<b>Literatur</b>	<b>62</b>
<b>A</b>	<b>XML-Schema</b>	<b>64</b>
<b>B</b>	<b>Code System (Event ID)</b>	<b>72</b>
<b>C</b>	<b>Code System (Event Outcome Indicator)</b>	<b>74</b>
<b>D</b>	<b>Code System (Partition Object ID Type Code)</b>	<b>75</b>

## 1 Einleitung

Die Ereignisprotokollierung spielt für die Umsetzung der datenschutzrechtlichen Anforderungen eine entscheidende Rolle. [eFA\_DS-1.2] Insbesondere die Natur der durch die elektronische Fallakte verarbeiteten Daten stellt hohe Ansprüche an die zum Einsatz kommenden Protokollierungsverfahren. Nur mit angemessen und leistungsfähigen Lösungen kann den einzelnen Anforderungen entsprochen werden. Im Rahmen dieses Dokumentes werden insgesamt drei Schwerpunkte der Protokollierung betrachtet. Dazu gehören:

1. Definition allgemeiner Anforderungen hinsichtlich der Erstellung, Archivierung, dem Schutz und der Auswertung von Zugriffsprotokollen. (Kapitel 2)
2. Entwicklung eines generischen XML-Schemas für die Protokollierung von Zugriffen im Umfeld der elektronischen Fallakte auf Grundlage weit verbreiteter Industriestandards. (Kapitel 3)
3. Spezifizieren des Inhalts einzelner Audit Messages um den Besonderheiten der eFA-Anwendungs- und Sicherheitsarchitektur gerecht zu werden. (Kapitel 4)

Anmerkung: Die vorliegende Spezifikation trifft keine normativen Aussagen über die konkrete, providerspezifische Ausgestaltung und Umsetzung der Protokollierung. Die einzelnen Lösungen müssen jedoch sicherstellen, dass:

- die in Kapitel 2 beschriebenen allgemeinen Protokollierungsanforderungen umfassend adressiert werden und
- eine Überführung/Konvertierung der providerspezifischen Protokolle in die in Kapitel 3 und 4 beschriebene Struktur problemlos möglich ist.

### 1.1 Zielgruppe

Diese Spezifikation geht insbesondere auf die technischen und organisatorischen Anforderungen im Umfeld der Protokollierung ein. Sie richtet sich vorrangig an Unternehmen und Personen, die sich für die Implementierung der eFA-Architektur in konkrete Anwendungen und Produkte verantwortlich zeigen.



## 1.2 Referenzierte Spezifikationen und Standards

Dieses Dokument basiert auf einer Reihe international anerkannter Industriestandards. Dazu gehören:

- RFC3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications [RFC3881]
- IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication Profile (ATNA) [IHE-ITI-TF-1\_4.0]
- DICOM Supplement 95 [DICOM\_AT]
- XML-Schema [XML\_Schema-1.1]

Zusätzlich wird sich auf die folgenden Dokumente der eFA-Spezifikation bezogen:

- eFA-Sicherheitskonzept [*eFA\_SK-1.2*]
- eFA-Sicherheitsarchitektur [*eFA\_SA-1.2*]
- eFA-Anwendungsarchitektur [*eFA\_AA-1.2*]
- eFA-Datenschutzkonzept [*eFA\_DS-1.2*]

## 1.3 Konventionen

Die Wörter "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "MAY" sind entsprechend RFC2119 zu interpretieren.

## 2 Grundlagen

Medizinische Daten sind im besonderen Maße schützenswert. Deshalb ist es zwingend erforderlich, sämtliche Zugriffe auf eine elektronische Fallakte nachvollziehbar, überprüfbar, verständlich und rechtssicher zu protokollieren. Dabei sind, wie schon im Datenschutzkonzept der elektronischen Fallakte beschrieben, besondere rechtliche Regelungen zu beachten. [eFA\_DS-1.2]

Die auch für andere medizinische Anwendungen geltenden Grundanforderungen an das Trace- und Logmanagement sind hierbei:

- Protokollierung sämtlicher sachlicher und zeitlicher Systemzugriffe
- nachvollziehbare, personenbezogene und rechtssichere Informationen
- manipulationssichere, revisionssichere und zeitgerechte Speicherung
- redundante, angemessen ausfallsichere und lückenlose Datenerfassung
- revisionssichere und lückenlose (Langzeit-)Archivierung
- progressive und retrograde Prüfung
- verständliches, lesbares Datenformat

Protokolliert werden im Kontext der eFA folgende Ereignisse und Informationen:

- An- und Abmeldungen am System
- sämtliche Zugriffe auf elektronische Fallakten
- sämtliche Sicherheitspolicyverletzungen
- schwerwiegende Fehler, inklusive Übertragungsfehler
- Assertionketten, zur nachträglichen und eindeutigen Nutzeridentifizierung
- Start und Ende einer Protokolldatei

Der Zweck der Protokolle ist die:

- Durchführung von Sicherheitsprüfungen oder Audits
- Feststellung und Verfolgung von Datenschutzverstößen
- aus dem §18 Abs. 2 BDSG abgeleitete Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungssystemen
- Verfolgung strafrechtlich relevanter Tatbestände



Die Protokolldateien dürfen keinesfalls zur präventiven Benutzerüberwachung oder Arbeitszeitkontrolle verwendet werden.

Entfallen die in der Zweckbindung benannten Gründe zur Speicherung der Protokollsätze, so sind diese zeitnah nach dem beschriebenen Verfahren zu vernichten.

## 2.1 Erstellen von Zugriffsprotokollen

An die Erstellung, Archivierung, den Schutz und die Auswertung von Zugriffsprotokollen ergeben sich unabhängig von der konkreten Implementierung durch die einzelnen EFA-Serviceprovider eine Reihe von Anforderungen. Sofern nicht anders spezifiziert bilden die in Abschnitt 2.1 bis 2.4 definierten Vorgaben den Rahmen, innerhalb dessen sich Implementierungen „frei“ bewegen können.

Folgende Anforderungen werden an die Erstellung von Protokollen gestellt:

---

### Speicherstrategie

---

Die eFA-Dienste generieren die einzelnen Protokolleinträge und senden sie unverzüglich an den/die Logserver. Ist eine Übermittlung nicht möglich, werden die Nachrichten zwischengespeichert und zu einem späteren Zeitpunkt übertragen. Sobald die Protokolleinträge übermittelt wurden, müssen sie auf Seite des Anwendungsservers gelöscht werden. Zur Übertragung sollte analog zu IHE ATNA [IHE-ITI-TF-1\_4.0] Reliable Syslog im „cooked“ mode verwendet werden. (vgl. RFC3195).

---

### Protokollformat

---

An das Format der zu erstellenden Protokolldatei werden keine konkreten Anforderungen gestellt. Implementierungsspezifische Lösungen sind generell zulässig sofern gewährleistet werden kann, dass die einzelnen Einträge in menschenlesbarer Form kodiert sind. Der Export der Protokolldaten in die in Kapitel 4 und 5 spezifizierte Struktur muss in allen Lösungen möglich sein.

---

### Protokollsatzgröße

---

Die maximal zulässige Protokollsatzgröße kann einrichtungsspezifisch bestimmt werden. Der Logserver schreibt so lange Informationen in das Logfile, bis die festgelegte Maximalgröße der Datei oder ein vorab festgesetzter Zeitpunkt (z. B. tages- oder wochenweise Protokollierung) erreicht wurde. Dann wird die alte Logdatei ausgekoppelt und eine neue mit aufsteigender Versionsnummer erstellt und eingebunden. Neuere Protokollelemente werden von nun an in die neuere Logdatei geschrieben. Der Abschluss der alten Protokolldatei und der Beginn der neuen Datei sind durch ein gesondertes Element in den Dateien anzuzeigen (Start- und Terminatortoken). Abschnitt 4.1.1 trifft zur Gestaltung der entsprechenden Token weiterführende Aussagen.

---

### Verschlüsselung

---

Eine Verschlüsselung der Logfiles ist wünschenswert, aber nicht zwingend erforderlich, wenn die Vertraulichkeit der Protokolle mit adäquaten Schutzmaßnahmen (z. B. restriktive Zutritts-, Zugangs- und Zugriffsregelungen) sichergestellt werden kann. Wird sich für eine Verschlüsselung entschieden, so gelten die Festlegungen des eFA-Kryptokonzeptes. [eCR\_Crypt-1.1.9]

---

---

### **Integritätssicherung**

---

Ausgekoppelte Logdateien werden vom Logserver digital signiert und mit einem Zeitstempel versehen. Mittels eines geeigneten technischen Verfahrens wird dazu ein Hashwert der Logdatei gebildet und an einen TimeStamp-Server verschickt. Der TimeStamp-Server hängt an diesen Hashwert die aktuelle Uhrzeit an und signiert diesen mit seinem privaten Schlüssel. Der signierte Zeitstempel wird an den Logserver zurückgeschickt und mit der Logdatei zusammengeführt. Da an den Time-Stamp-Server lediglich ein Hashwert des Logfiles übermittelt wird, aus dem keinerlei schützenswerte Daten errechnet werden können, sind dabei keine datenschutzrechtlichen Bedenken abzuleiten.

In Phase 2 der eFA-Einführung können die Protokolldateien auch vom Protokollserver selbst mit einem Zeitstempel versehen werden. Im Regelbetrieb ist zwingend der in der Telematikinfrastruktur der gematik geplante TimeStamp-Service zu verwenden oder ein anderer, adäquat performanter und vertrauenswürdiger Dienst. Hinsichtlich der zu verwendenden Algorithmen und Schlüssellängen gelten die Bestimmungen des eFA-Kryptokonzeptes. [eCR\_Crypt-1.1.9]

---

### **Kompression**

---

Technische Verfahren zur Kompression der Protokollsätze sind generell zulässig, so lange diese zusätzlich Wiederherstellungsinformationen beinhalten und ein Dekomprimieren langfristig sichergestellt ist. Es dürfen generell nur offene Verfahren eingesetzt werden, bei denen die genaue Funktionsweise öffentlich bekannt und der Quellcode verfügbar ist.

---

## **2.2 Archivierung von Zugriffsprotokollen**

An die Archivierung der Zugriffsprotokolle werden unabhängig von der konkreten Implementierung durch die einzelnen eFA-Serviceprovider die folgenden Anforderungen gestellt:

---

### **Kurzzeitarchivierung**

---

Die ausgekoppelten, signierten und mit einem Zeitstempel versehene Logdateien müssen in ein Online-Archiv überführt werden, das die Daten für einen Zeitraum von mindestens drei Monaten nach Abschluss des zugrunde liegenden Abrechnungsfalles online vorhält. Nach Ablauf dieses Zeitraums können die Daten in ein Langzeitarchiv überführt werden.

---

---

#### Langzeitarchivierung

---

Die Protokollsätze sind geeignet langfristig zu speichern, um auch eventuelle frühere Verstöße gegen geltendes Recht entsprechend nachweisen zu können.<sup>1</sup>

Die Speichermedien des Archivs sind in doppelter Ausführung räumlich getrennt und ausreichend sicher vor Diebstahl zu lagern. Des Weiteren sind die Medien geeignet vor Unauffindbarkeit zu schützen. Außerdem ist in regelmäßigen Abständen die Lesbarkeit der Speichermedien zu überprüfen. Hierdurch sollen eventuelle Risiken in Bezug auf Vernichtung, Diebstahl und Unauffindbarkeit im erforderlichen Maße reduziert werden.

---

#### Aufbewahrungsfristen

---

Die Zugriffsprotokolle sind in der Regel 10 Jahre aufzubewahren, um der in §10 Abs. 3 MBO/Ärzte geregelten Dokumentationsfrist gerecht zu werden. Als maximale Aufbewahrungsfrist gilt des Weiteren die 30jährige Verjährungsfrist für Schadensersatzansprüche, die für die Verletzung von Leib, Leben und körperlicher Unversehrtheit gelten.

Die konkrete Aufbewahrungsfrist ist dabei institutionsspezifisch festzulegen und an die tatsächlichen Notwendigkeiten des Regelbetriebes anzupassen. Dabei ist es empfehlenswert, das institutionsinterne Risikomanagement mit einer geeigneten Festlegung der konkreten Speicherfristen zu betrauen.

---

## 2.3 Schutz von Zugriffsprotokollen

Die Zugriffsprotokolle beinhalten im überwiegenden Maße personenbezogene Daten. Deshalb sind diese vor unrechtmäßigen Zugriffen zu schützen und dürfen weiterhin nur einem möglichst kleinen Benutzerkreis zur Einsicht zur Verfügung stehen. Das Protokollsystem ist dabei so zu konzipieren, dass:

- keine Daten auf dem Weg in das Protokoll verändert oder gelöscht werden
- nachträglich keine Manipulation vorgenommen werden kann
- eine unrechtmäßige Einsicht in die Protokolle praktisch unmöglich ist
- zeitnah und lückenlos protokolliert wird
- die Protokolle manuell und automatisiert auswertbar sind
- die Protokollierung stets verfügbar ist und durch Redundanzen abgesichert

<sup>1</sup> Die Forderung nach Langzeit-Archivierung ist ohne die Verwendung von langzeit-gültigen IDs für Patienten, Benutzer und Objekte nach heutigem Stand nicht erfüllbar. Bisher verwendete Versichertenidentifikatoren und die nicht-zentral abgelegten DN-Einträge der X509-Zertifikate erfüllen diese Forderung noch nicht.

Die Protokollserver sollten demnach nach Möglichkeit als dedizierte Systeme konzipiert sein und über eine geeignete Schnittstelle Protokollelemente von anderen Systemen empfangen und abspeichern können. Dabei müssen sowohl Absender eines Protokollelements als auch die aktuelle Echtzeit dem Protokollsystem bekannt sein.

Eine Anmeldung auf den Protokollserver sollte dem Minimalprinzip folgen und lediglich so wenige lokale Administratoren wie möglich beinhalten. Netzwerkweite Anmeldungen sollten weitestgehend vermieden werden und für Personen mit datenschutzrechtlichen Kontrollaufgaben sollte im Regelfall kein eigener Zugang erstellt werden. Stattdessen ist es empfehlenswert, die betreffenden Protokolle durch einen Systemadministrator aus den Protokollarchiven zu extrahieren und dem Revisor in Kopie zur Verfügung zu stellen.

Die Verfügbarkeit der Protokollierungsdienste ist durch geeignete technische Verfahren, beispielsweise unter Zuhilfenahme eines heart-beat-Signals, stets zu überprüfen. Eventuelle Ausfälle müssen durch das EMS des Gesamtsystems zeitnah erkannt werden und es muss schnellstmöglich auf eventuelle Redundanzen zurückgegriffen werden. Die in der Ausfallzeit anfallenden Protokollelemente sind zwischenzuspeichern, beispielsweise durch einen Puffer im Ursprungssystem oder einen Konzentrador vor dem eigentlichen Protokollsystem, damit keine Protokollelemente verloren gehen.

Sämtliche Zugriffe auf die Zugriffsprotokolle, ausgenommen die Zugriffe des schreibenden Protokolldienstes, sind wiederum gesondert zu protokollieren.

## 2.4 Auswertung von Zugriffsprotokollen

In konkreten Verdachtsmomenten, regulären und regelmäßigen Sicherheitsaudits oder auf konkrete Aufforderung durch Personen mit besonderen datenschutzrechtlichen Kontrollaufgaben sind die Zugriffsprotokolle auszuwerten und auf eventuelle Rechts- oder Policyverstöße zu untersuchen.

Mit Ausnahme der Datenschutzkontrolle ist dabei generell das "Vier-Augen-Prinzip" anzuwenden, d. h. mehr als eine Person muss während der Prüfung/Auswertung der Protokolle anwesend sein. Die anwesenden Personen kontrollieren sich gegenseitig. Dies soll das Risiko eines eventuellen Mißbrauchs reduzieren und ist auf Grund der Tatsache notwendig, dass sich in Protokolldateien prinzipbedingt eine Vielzahl personenbezogener Daten ansammeln. Eine technische Umsetzung ist empfehlenswert jedoch nicht verpflichtend. Adäquate organisatorische Regelungen gelten als ausreichend.

Es sollte immer nur eine Kopie des Originalprotokollsatzes ausgewertet werden, um versehentliches Löschen oder ähnliche anderweitigen Manipulatio-



nen auszuschließen. Die Kopie ist nach Abschluss der Sichtung sofort und sicher zu zerstören.

Vor sämtlichen Sichtigungen ist die Integrität des gesamten Protokollsatzes durch Überprüfung der digitalen Signatur geeignet sicherzustellen.

#### 2.4.1 Sicherheitsprüfung und -überprüfung

Auch ohne konkrete Verdachtsmomente sollten die Zugriffsprotokolle in regelmäßigen Abständen sowohl automatisiert, als auch manuell auf eventuelle Verstöße gegen die Sicherheitspolicies untersucht werden.

Je nach zu untersuchender Datenmenge kann dabei stichprobenartig oder vollständig untersucht werden. Bei identifizierten Diskrepanzen sind sofort Gegenmaßnahmen zu ergreifen, der IT-Sicherheitsbeauftragte ist zu unterrichten und der betriebliche Datenschutzbeauftragte ist zu informieren.

Eventuelle relevante Anhaltspunkte für einen vermuteten Mißbrauch in den Protokollen sind rechtssicher zu extrahieren (beispielsweise durch Ausdruck) und zu markieren.

Eine automatisierte und regelmäßige Sicherheitsprüfung, die anhand spezieller, in der Sicherheitspolitik der betreffenden Institution festzulegender, Indikatoren die Protokolldateien auf eventuelle Verstöße gegen die IT-Sicherheit untersucht, ist der manuellen Methode vorzuziehen.

### 3 EFA-spezifische Protokollierung

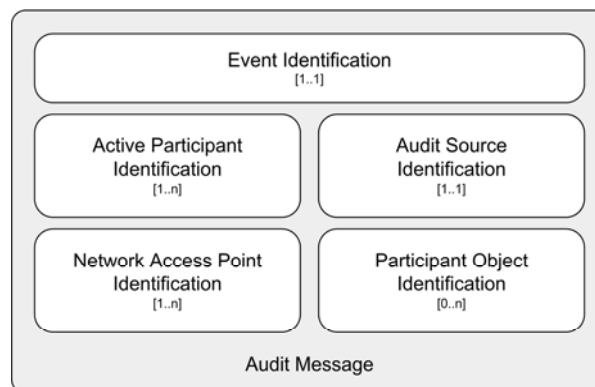
Um der Forderung nach einer verständlichen und lesbaren Protokollierung angemessen zu begegnen und die Kompatibilität der Zugriffsprotokolle über Organisationsgrenzen hinweg sicherzustellen, ist die Entwicklung eines einheitlichen und eFA-spezifischen Protokollierungsschemas notwendig. Das in den folgenden Kapiteln entwickelte Schema basiert dabei weitestgehend auf RFC3881 (Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications), IHE ATNA (Audit Trail and Node Authentication) sowie DICOM (Supplement 95 – Audit Trail Messages).

Die Umsetzung der Protokollierung auf Grundlage des entwickelten Schemas ist NICHT verpflichtend. Es muss ausschließlich sichergestellt werden, dass die umsetzungsspezifischen Protokollierungsdaten der einzelnen eFA-Provider in die dargestellte Struktur überführt werden können. Als verpflichtend gekennzeichnete Protokollelemente dürfen nicht verloren gehen.

Die beiden folgenden Kapitel definieren die genaue Struktur der einzelnen Audit Messages. Kapitel 3 gibt in diesem Zusammenhang einen Überblick über die einzelnen Elemente der Nachricht und die für sie jeweils zulässigen Wertebereiche. Kapitel 4 definiert weitere operationsspezifische Einschränkungen, die die Auditierbarkeit der Audit Logs vor dem Hintergrund der architekturbedingten Besonderheiten sicherstellen.

#### 3.1 Überblick

RFC3881 definiert insgesamt fünf Bereiche, die im Rahmen der Ereignisprotokollierung berücksichtigt werden:



**Event Identification** - Was wurde getan?

**Active Participant Identification** - Durch wen wurde es ausgelöst?

**Network Access Point Identification** - Von wo aus wurde es ausgelöst?

**Audit Source Identification** - Auf welches System wurde zugegriffen?

**Participant Object Identification** - Auf welche Objekte wurde zugegriffen?

Die folgenden Abschnitte geben einen genaueren Überblick über die einzelnen Bereiche und die entsprechenden Datendefinitionen im Umfeld der eFA-Protokollierung.

### 3.2 Event Identification

Wesentlicher Bestandteil des Protokolls sind die identifizierenden Merkmale des eingetretenen Ereignisses. Die folgende Übersicht definiert einzelne Elemente und ihre Verwendung im Umfeld der eFA-Protokollierung:

<b>Event ID</b>	<b>MUST</b>
Identifiziert das Ereignis anhand eines definierten Identifiers.	
Format/Wertebereich: Die EventID entspricht den aufgerufenen Web Service Operationen entsprechend dem in Anhang B dargestellten Codesystem.	
<b>Event Action Code</b>	<b>MUST</b>
Bezeichnet den Typ der während des Ereignisses durchgeführten Aktion.	
Format/Wertebereich: Gemäß RFC3881. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen entnommen werden.	
<b>Event Date/Time</b>	<b>MUST</b>
Definiert den genauen Eintrittszeitpunkt des Ereignisses.	
Format/Wertebereich: Gemäß RFC3881. Es ist sicherzustellen, dass die Systemzeit des protokollierenden Servers direkt oder indirekt mit der „gematik-time“ synchronisiert wird.	
<b>Event Outcome Indicator</b>	<b>MUST</b>
Beschreibt den Ausgang des Ereignisses.	
Format und Wertebereich des Event Outcome Indicators orientieren sich an dem in Anhang C dargestellten Codesystem.	
Anmerkungen: Waren nur einzelne Teile des Ereignisses erfolgreich, so ist für jeden Teil ein eigener Log-Eintrag zu generieren.	
<b>Event Type Code</b>	<b>MAY</b>
Identifiziert die Kategorie des Ereignisses.	
Format/Wertebereich: Gemäß RFC3881.	

### 3.3 Active Participant Identification

Um die Zuordenbarkeit eines Events zu einem „aktiv Mitwirkenden“ (Person, Dienst oder System) zu gewährleisten, müssen Informationen über diesen erhoben werden. Im Umfeld der eFA-Protokollierung sind die in RFC3881 vorgesehenen Felder wie folgt zu interpretieren:

---

**User ID** **MUST**

---

Eindeutiger Bezeichner für den das Ereignis auslösenden Nutzer.

Da die Architektur der elektronischen Fallakte das eindeutige Identifizieren der aktiv handelnden natürlichen Personen nur in einem Teil der Operationen ermöglicht, müssen abhängig vom Ereignis verschiedene Werte protokolliert werden.

Format/Wertebereich:

Operationen/Ereignisse Identity Provider:

- Subject des verwendeten X.509-Zertifikats
- Eindeutiger Nutzernamen aus der Guarantor Assertion

Operationen/Ereignisse Admission Token Service:

- Client-to-Service-Communication → Assertion ID der Identity Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Identity Assertion (als getrennte Active Participant Identifications)

Operationen/Ereignisse Access Token Service:

Operationen/Ereignisse Policy Token Service:

- Client-to-Service-Communication → Assertion ID der Access Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Access Assertion (als getrennte Active Participant Identifications)

Operationen/Ereignisse Record Registry:

- Client-to-Service-Communication → Assertion ID der Access oder Admission Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Admission oder Access Assertion (als getrennte Active Participant Identifications)

Operationen/Ereignisse Folder Registry:

- Client-to-Service-Communication → Assertion ID der Access Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Access Assertion (als getrennte Active Participant Identifications)

Operationen/Ereignisse Document Registry:

- Client-to-Service-Communication → Assertion ID der Access Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Access Assertion (als getrennte Active Participant Identifications)

Operationen/Ereignisse Document Repository:

- Client-to-Service-Communication → Assertion ID der Access Assertion
- Service-to-Service Communication → Subject des verwendeten Dienstzertifikats UND Assertion ID der Access Assertion (als getrennte Active Participant Identifications)

Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.

---



<b>Alternative User ID</b>	<b>MUST (MAY)</b>
Alternativer Bezeichner für den das Ereignis auslösenden Nutzer.	
Das Ausfüllen dieses Feldes ist im Rahmen der eFA- Protokollierung verpflichtend wenn eine Assertion ID als User ID verwendet wird.	
Format/Wertebereich: Gemäß RFC 3881. Wenn eine Assertion ID als User ID fungiert ist hier der Issuer der Assertion anzugeben. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>User Name</b>	<b>MUST NOT</b>
Name des Nutzers in „menschenslesbarer Form“.	
Dieses Feld besitzt im Rahmen der eFA- Protokollierung keine besondere Relevanz bzw. ist für einen Teil der Operationen nicht zulässig. Es darf daher nicht verwendet werden.	
<b>User Is Requestor</b>	<b>MAY</b>
Gibt an, ob der bezeichnete Nutzer Initiator des Ereignisses ist.	
Dieses Feld besitzt im Rahmen der eFA- Protokollierung keine besondere Relevanz. Die Verwendung ist optional.	
Format/Wertebereich: Gemäß RFC3881. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>Role ID Code</b>	<b>MAY</b>
Rolle(n) des Nutzers zum Zeitpunkt der Ausführung.	
Dieses Feld besitzt im Rahmen der eFA-Protokollierung keine besondere Relevanz bzw. kann der Wert aus den vorliegenden Assertions nicht ermittelt werden. Die Verwendung ist optional.	

### 3.4 Network Access Point Identification

Neben der Identifizierung des „aktiv Mitwirkenden“ sollte die Zuordenbarkeit des Ereignisses zu einem ereignisauslösenden IT-System gewährleistet sein. Die folgenden Felder sind in diesem Zusammenhang relevant:

<b>Network Access Point Type Code</b>	<b>MUST (MAY)</b>
Definiert den für die "Network Access Point ID" zu verwendenden Identifiertyp. (z. B. Typ: IP-Adresse, Typ: DNS-Name etc.)	
Die Notwendigkeit der Angabe des „Network Access Point Type Code“ ist abhängig von der jeweiligen Event ID. Die genaue Verwendung kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
Format/Wertebereich: Gemäß RFC3881.	

---

<b>Network Access Point ID</b>	<b>MUST (MAY)</b>
--------------------------------	-------------------

---

Eindeutiger Bezeichner des ereignisauslösenden Systems (System des Users).

Format/Wertebereich: Gemäß RFC3881 in Abhängigkeit vom „Network Acces Point Type Code“.

---

### 3.5 Audit Source Identification

Wesentlicher Bestandteil der Protokollierung ist das eindeutige Erfassen des ereignisverarbeitenden IT-Systems/Dienstes (Quelle des Ereignisses). Folgende Felder müssen berücksichtigt werden:

---

<b>Audit Enterprise Site ID</b>	<b>MAY (MUST)</b>
---------------------------------	-------------------

---

Identifiziert den logischen Standort des ereignisverarbeitenden Systems. (z. B. Name des Krankenhaus)

Die Nutzung des Feldes ist verbindlich, wenn innerhalb einer Klinik(kette) mehrere verarbeitende Systeme existieren und eine eindeutige Unterscheidung anhand der „Audit Source ID“ nicht möglich ist.

Format/Wertebereich: Ausgestaltung gemäß RFC3881.

---

<b>Audit Source ID</b>	<b>MUST</b>
------------------------	-------------

---

Identifiziert die Quelle des Ereignisses. (z.B. System-Name, Dienst-Name, SOAP-Endpoint-Adresse etc.)

Format/Wertebereich: Gemäß RFC3881.

---

<b>Audit Source Type Code</b>	<b>MAY</b>
-------------------------------	------------

---

Definiert den Typ des ereignisverarbeitenden Systems. (z. B. „Application server process tier in a multi-tier system“, „Security server, e.g., a domain controller, ...)

Format/Wertebereich: Gemäß RFC3881

---

### 3.6 Participant Object Identification

Die im folgenden beschriebenen Felder spezifizieren die vom Ereignis betroffenen Datenobjekte genauer und sind insbesondere unter der Voraussetzung relevant, dass das Ereignis mit den oben beschrieben Feldern nicht eindeutig und ausreichend dokumentiert werden kann.

---

<b>Participant Object Type Code</b>	<b>MUST</b>
-------------------------------------	-------------

---

Definiert den Typ des betroffenen (Daten)-Objects

Format/Wertebereich: Gemäß RFC3881. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.

---

<b>Participant Object Type Code Role</b>	<b>MUST</b>
Definiert	
Format/Wertebereich: Gemäß RFC3881. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>Participant Object Data Life Cycle</b>	<b>MAY</b>
Bestimmt den Zustand des betroffenen Objektes in Bezug auf seinen Life Cycle.	
Format/Wertebereich: Gemäß RFC3881.	
<b>Participant Object ID Type Code</b>	<b>MUST</b>
Definiert den Typ des unter „Participant Object ID“ referenzierten Objektes.	
Format/Wertebereich: Der „Participant Object ID Type Code“ greift auf das in Anhang D dargestellte Codesystem zurück. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>Participant Object Sensitivity</b>	<b>MAY</b>
Beschreibt die Sensitivität des in „Participant Object ID“ referenzierten Objektes.	
Format/Wertebereich: Nicht definiert. Kann bei Bedarf von den einzelnen Institutionen vorgegeben werden.	
<b>Participant Object ID</b>	<b>MUST</b>
Identifiziert das vom Ereignis betroffene (Daten)-Objekt.	
Format/Wertebereich: Abhängig von „Participant Object ID Type Code“. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>Participant Object Name</b>	<b>MAY</b>
Nähere Beschreibung für das unter „Participant Object ID“ referenzierte Objekt.	
Format/Wertebereich: Gemäß RFC3881.	
<b>Participant Object Query</b>	<b>MAY (MUST)</b>
Zusatzinformationen um das Ereignis in Bezug auf das referenzierte Datenobjekt genauer einordnen zu können (z. B. Abfrageparameter)	
Format/Wertebereich: Gemäß RFC3881. Die genaue Verwendung der Werte kann den individuellen Eventbeschreibungen (vgl. Kapitel 4) entnommen werden.	
<b>Participant Object Detail</b>	<b>MAY</b>
Implementierungsspezifische Zusatzinformationen über das unter „Participant Object ID“ referenzierte Objekt.	
Format/Wertebereich: Gemäß RFC3881.	

## 4 EFA-spezifische Audit-Nachrichten

Das in Anhang A dargestellte XML-Schema trifft grundlegende Aussagen über die Struktur der einzelnen Audit Messages. Ergänzend zu den strukturellen Vorgaben des vierten Kapitels werden in den folgenden Abschnitten weitere inhaltliche Festlegungen getroffen. Diese sollen garantieren, dass auf der einen Seite dem Grundsatz der Datensparsamkeit entsprochen wird und auf der Anderen die Möglichkeit besteht, trotz der architekturbedingten Besonderheiten (Pseudonymisierung, Assertionkettenm, P2P-Funktionalität etc.), Rückschlüsse auf natürliche Personen und deren Aktionen zu ziehen. Die Protokollierung der einzelnen eFA-Dienste erfolgt dabei unabhängig voneinander, d. h. jeder Dienst verfügt über ein eigenes Protokoll. Dabei ist es zulässig, die Protokollnachrichten der Dienste eines Peers an einen zentralen Loggingserver zu senden und durch diesen die dienstspezifische Trennung vornehmen zu lassen. Die Protokollierung von P2P-Aufrufen erfolgt ebenfalls dienst- und peerindividuell. Zentrale Auditsysteme sind nicht vorgesehen.

Dienstspezifischen Protokolle werden ausschließlich im Bedarfsfall (konkrete Verdachtsmomente auf datenschutzrechtliche Verstöße, Sicherheitsaudits, konkrete Aufforderung durch Personen mit besonderen datenschutzrechtlichen Kontrollaufgaben) zusammengeführt und ausgewertet. (vgl. Kapitel 2.4) Im Fall von verteilt liegenden Fallakten kann es erforderlich werden, die Protokolle verschiedener eFA-Provider zusammenzuführen.

Die Darstellung der zu protokollierenden Events und ihrer Besonderheiten (z.B. P2P-Aufruf) erfolgt in den folgenden Abschnitten dienstspezifisch. Ausnahme bildet Abschnitt 4.1, der Festlegungen zu Protokolleinträgen trifft, die über die einzelnen Dienstgrenzen hinweg gültig sind.

Die folgenden Abkürzungen kommen zur Anwendung:

<b>EV</b>	enumeration value (Abschließend definierter Aufzählungstyp)
<b>M</b>	mandatory (Verpflichtend anzugebendes Element)
<b>MC</b>	mandatory conditional (Unter genannter Bedingung verpflichtend anzugebendes Element)
<b>O</b>	optional (Optionales Element)

## 4.1 ECR Generic

### 4.1.1 Generic.AuditRecordingStarted / Generic.AuditRecordingStopped

Event [1..1]	<b>EventID</b>	(M)	EV (5610010, ECR, „Generic.AuditRecordingStarted“) (5610020, ECR, „Generic.AuditRecordingStopped“)
	<b>EventActionCode</b>	(M)	EV „E“ (Execute)
	<b>EventDateTime</b>	(M)	Siehe Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Siehe Kapitel 3
	<b>EventTypeCode</b>	(O)	Siehe Kapitel 3
Active Participant ID Dedicated Service [1..1]	<b>UserID</b>	(M)	Subject des durch den Application Service (Identity Provider, Admission Token Service etc.) genutzten Zertifikats
	<b>AlternateUserID</b>	(O)	Siehe Kapitel 3
	<b>UserName</b>	(O)	Siehe Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Siehe Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Siehe Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointID</b>	(M)	Siehe Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Siehe Kapitel 3
	<b>Audit Source ID</b>	(M)	Siehe Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Siehe Kapitel 3

## 4.2 ECR Identity Provider (IdtPrv)

### 4.2.1 IdtPrv.authenticate

Event [1..1]	<b>EventID</b>	(M)	EV (5610105, ECR, „IdtPrv.authenticate“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Siehe Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Siehe Kapitel 3
	<b>EventTypeCode</b>	(O)	Siehe Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	Subject des vom Zugreifenden für die Authentisierung genutzten Zertifikats
	<b>AlternateUserID</b>	(MC)	Wird eine Guarantor Assertion für die Authentisierung genutzt, so muss der Username für den „gebürgt“ wird verwendet werden. In allen anderen Fällen bleibt das Feld ungenutzt.
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Identity Assertion [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3
	<b>POIDTypeCode</b>	(M)	EV (5616010, ECR, „Identity Assertion“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Identity Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

## 4.3 ECR Admission Token Service (AdmTokSvc)

### 4.3.1 AdmTokSvc.requestAdmissionTokenCollection / AdmTokSvc.requestAdmissionTokenSelection

Event [1..1]	<b>EventID</b>	(M)	EV (5610205, ECR, „AdmTokSvc.requestAdmissionTokenCollection“) (5610210, ECR, “AdmTokSvc.requestAdmissionTokenSelection“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der für die Anfrage zugrunde liegenden Identity Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Identity Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Admission Assertions [0..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (56106030, ECR, „Admission Assertion“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Admission Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

Participant Object Patient [1..1]	<b>POTypeCode</b>	(M) EV 1 (person)
	<b>POTypeCodeRole</b>	(M) EV 1 (patient)
	<b>PODataLifeCycle</b>	(O) Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M) EV 2 (patient number)
	<b>POSensitivity</b>	(O) Vgl. Kapitel 3
	<b>POID</b>	(M) UID des Patienten (z. B. KVNR)
	<b>POName</b>	(O) Vgl. Kapitel 3
	<b>POQuery</b>	(O) Vgl. Kapitel 3
	<b>PODetail</b>	(O) Vgl. Kapitel 3

#### 4.3.2 AdmTokSvc.requestAdmissionToken

Event [1..1]	<b>EventID</b>	(M)	EV (5610215, ECR, „AdmTokSvc.requestAdmissionToken“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der für die Anfrage zugrunde liegenden Identity Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Identity Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	FALSE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID Service [1..1]	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointTypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
Participant Object Admission Assertion [0..1]	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616030, ECR, „Admission Assertion“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Admission Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
<b>POQuery</b>	(O)	Vgl. Kapitel 3	

Participant Object Patient [1..1]	<b>PODetail</b>	(O) Vgl. Kapitel 3
	<b>POTypeCode</b>	(M) EV 1 (person)
	<b>POTypeCodeRole</b>	(M) EV 1 (patient)
	<b>PODataLifeCycle</b>	(O) Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M) EV 2 (patient number)
	<b>POSensitivity</b>	(O) Vgl. Kapitel 3
	<b>POID</b>	(M) UID des Patienten (z. B. KVNR)
	<b>POName</b>	(O) Vgl. Kapitel 3
	<b>POQuery</b>	(O) Vgl. Kapitel 3
	<b>PODetail</b>	(O) Vgl. Kapitel 3

## 4.4 ECR Access Token Service (AccTokSvc)

### 4.4.1 AccTokSvc.requestAccessToken

Event [1..1]	<b>EventID</b>	(M)	EV (5610405, ECR, „ AccTokSvc.requestAccessToken“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Admission Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Admission Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object Access Assertions [0..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (56106040, ECR, „Access Assertion)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Access Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3
Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.4.2 AccTokSvc.requestCreationToken

Event [1..1]	<b>EventID</b>	(M)	EV (5610410, ECR, „ AccTokSvc.requestCreationToken“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Admission Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Admission Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Access ASsertion [0..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616040, ECR, „Access Assertion“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Access Assertion“
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.4.3 AccTokSvc.registerRecord

Event [1..1]	<b>EventID</b>	(M)	EV (5610415, ECR, „AccTokSvc.registerRecord“)
	<b>EventActionCode</b>	(M)	EV „U“ (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der der Anfrage zugrunde liegenden Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	FALSE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
Active Participant Dedicated Service [1..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertif
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

## 4.5 ECR Policy Token Service (PoITokSvc)

### 4.5.1 PoITokSvc.requestPolicyToken

Event [1..1]	<b>EventID</b>	(M)	EV (5610505, ECR, „PoITokSvc.requestPolicyToken“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der für die Anfrage zugrunde liegenden Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE (Push-Modell) FALSE (Pull-Modell)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object PolicyUID [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616090, ECR, „PolicyUID)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UID der Policy
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3
Participant Object Policy Assertions [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (56106050, ECR, „Policy Assertion)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Policy Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.5.2 PolTokSvc.resolveAccessToken

Event [1..1]	<b>EventID</b>	(M)	EV (5610510, ECR, „PolTokSvc.resolveAccessToken“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID Requestor [1..1]	<b>UserID</b>	(M)	
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Policy Assertions [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 13 (security resource)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (56106050, ECR, „Policy Assertion“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	UUID der ausgestellten Policy Assertion
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

## 4.6 ECR Record Registry (RecReg)

### 4.6.1 RecReg.getRecordList

Event [1..1]	<b>EventID</b>	(M)	EV (5610605, ECR, „RecReg.getRecordList“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant ID eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Identity Assertion → Dedicated Client ruft Operation auf UUID der vorgelegten Admission Assertion → Trusted Service ruft Operation auf
	<b>AlternateUserID</b>	(M)	Issuer der Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3



Participant Object Fallakte [0..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.6.2 RecReg.setRecordMetadata / RecReg.getRecordMetadata / RecReg.setRecordState /RecReg.getRecordState / RecReg.getRecordStateHistory

Event [1..1]	<b>EventID</b>	(M)	EV (5610610, ECR, „RecReg.setRecordMetadata“) (5610615, ECR, „RecReg.getRecordMetadata“) (5610620, ECR, „RecReg.setRecordState“) (5610625, ECR, „RecReg.getRecordState“) (5610630, ECR, „RecReg.getRecordStateHistory“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create) „U“ (Update) „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3



Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniquelIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

### 4.6.3 RecReg.registerRecord

Event [1..1]	<b>EventID</b>	(M)	EV (5610635, ECR, „RecReg.registerRecord“)
	<b>EventActionCode</b>	(M)	EV „U“ (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der der Anfrage zugrunde liegenden Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	FALSE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
Active Participant Dedicated Service [1..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzert.
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UsersRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

## 4.7 ECR Folder Registry (FldReg)

### 4.7.1 FldReg.getFolderList

Event [1..1]	<b>EventID</b>	(M)	EV (5610705, ECR, „FldReg.getFolderList“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
Active Participant ID Service [0..1]	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniquelIdentifier)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3
Participant Object Folder [0..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelIdentifier)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.7.2 FldReg.setFolderMetadata / FldReg.setFolderState / FldReg.getFolderState / FldReg.getFolderStateHistory / FldReg.getFolderStateCollection / FldReg.getFolderStateHistoryCollection

Event [1..1]	<b>EventID</b>	(M)	EV (5610710, ECR, „FldReg.setFolderMetadata“) (5610735, ECR, „FldReg.setFolderState“) (5610740, ECR, „FldReg.getFolderState“) (5610745, ECR, „FldReg.getFolderStateHistory“) (5610755, ECR, „FldReg.getFolderStateCollection“) (5610760, ECR, „FldReg.getFolderStateHistoryCollection“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create) „U“ (Update) „R“ (Read/View/Query, Print)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
	Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)
<b>AlternateUserID</b>		(M)	Issuer der Access Assertion
<b>UserName</b>		(O)	Vgl. Kapitel 3
<b>UserIsRequestor</b>		(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
<b>RoleIDCode</b>		(O)	Vgl. Kapitel 3
<b>NetworkAccessPoint TypeCode</b>		(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
<b>NetworkAccessPointID</b>		(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object Folder [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelidentifier)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.7.3 FldReg.resumeRecord / FldReg.suspendRecord

Event [1..1]	<b>EventID</b>	(M)	EV (5610715, ECR, „FldReg.resumeRecord“) (5610720, ECR, „FldReg.suspendRecord“)
	<b>EventActionCode</b>	(M)	EV „U“ (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
Participant Object Fallakte [0..1]	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
<b>PODetail</b>	(O)	Vgl. Kapitel 3	

#### 4.7.4 FldReg.createAndRegisterRecord

Event [1..1]	<b>EventID</b>	(M)	EV (5610725, ECR, „FldReg.createAndRegisterRecord“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
Participant Object Fallakte [0..1]	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
<b>PODetail</b>	(O)	Vgl. Kapitel 3	

#### 4.7.5 FldReg.registerFolder

Event [1..1]	<b>EventID</b>	(M)	EV (5610630, ECR, „FldReg.registerFolder“)
	<b>EventActionCode</b>	(M)	EV „U“ (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der für die Anfrage zugrunde liegenden Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	FALSE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant Service [1..1]	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
Participant Object Fallakte [1..1]	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
<b>POQuery</b>	(O)	Vgl. Kapitel 3	

Participant Object Folder [1..1]	<b>PODetail</b>	(O) Vgl. Kapitel 3
	<b>POTypeCode</b>	(M) EV 2 (system)
	<b>POTypeCodeRole</b>	(M) EV 3 (report)
	<b>PODataLifeCycle</b>	(O) Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M) EV (5616070, ECR, „ECRFolderUniqueIdentifier“)
	<b>POSensitivity</b>	(O) Vgl. Kapitel 3
	<b>POID</b>	(M) OID des zu registrierenden Folders
	<b>POName</b>	(O) Vgl. Kapitel 3
	<b>POQuery</b>	(O) Vgl. Kapitel 3
	<b>PODetail</b>	(O) Vgl. Kapitel 3

## 4.8 ECR Document Registry (DocReg)

### 4.8.1 DocReg.createAndRegisterFolder

<b>Event</b> [1..1]	<b>EventID</b>	(M)	EV (5610805, ECR, „DocReg.createAndRegisterFolder“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
<b>Active Participant</b> eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
<b>Audit Source</b> [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
<b>Participant Object</b> Fallakte [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616060, ECR, „ECRRecordUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID der elektronischen Fallakte
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

Participant Object Folder [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des angelegten Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.8.2 DocReg.getInfoObjectList / DocReg. getInfoObjectListCollection

Event [1..1]	<b>EventID</b>	(M)	EV (5610810, ECR, „DocReg.getInfoObjectList“) (5610850, ECR, „Doc- Reg.getInfoObjectListCollection“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzli- cher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAc- cessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifi- kats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object Folder [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des ausgewählten Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.8.3 DocReg.suspendFolder / DocReg.resumeFolder

Event [1..1]	EventID	(M)	EV (5610815, ECR, „DocReg.suspendFolder“) (5610820, ECR, „DocReg.resumeFolder“)
	EventActionCode	(M)	EV “U” (Update)
	EventDateTime	(M)	Vgl. Kapitel 3
	EventOutcomeIndicator	(M)	Vgl. Kapitel 3
	EventTypeCode	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	UserID	(M)	UUID der vorgelegten Access Assertion
	AlternateUserID	(M)	Issuer der Access Assertion
	UserName	(O)	Vgl. Kapitel 3
	UserIsRequestor	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	RoleIDCode	(O)	Vgl. Kapitel 3
	NetworkAccessPoint TypeCode	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	NetworkAccessPointID	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	UserID	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	AlternateUserID	(O)	Vgl. Kapitel 3
	UserName	(O)	Vgl. Kapitel 3
	UserIsRequestor	(O)	TRUE
	RoleIDCode	(O)	Vgl. Kapitel 3
	NetworkAccessPoint TypeCode	(M)	Vgl. Kapitel 3
	NetworkAccessPointID	(M)	Vgl. Kapitel 3
Audit Source [1..1]	Audit Enterprise Site ID	(O)	Vgl. Kapitel 3
	Audit Source ID	(M)	Vgl. Kapitel 3
	Audit Source Type Code	(O)	Vgl. Kapitel 3

Participant Object Folder [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des ausgewählten Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.8.4 DocReg.setInformationObjectState / DocReg.getInformationObjectState / DocReg.getInformationObjectStateHistory / DocReg.getInformationObjectStateCollection / DocReg.getInformationObjectStateHistoryCollection

Event [1..1]	<b>EventID</b>	(M)	EV (5610825, ECR, „DocReg.setInformationObjectState“) (5610830, ECR, „DocReg.getInformationObjectState“) (5610835, ECR, „DocReg.getInformationObjectStateHistory“) (5610855, ECR, „DocReg.getInformationObjectStateCollection“) (5610860, ECR, „DocReg.getInformationObjectStateHistoryCollection“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Print/Query) “U” (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPointTypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3

<b>Audit Source</b> [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
<b>Participant Object Information Object</b> [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616080, ECR, „ECRInformationObjectUniqueIdentifier)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des ausgewählten InformationObjects
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.8.5 DocReg.registerInformationObject

Event [1..1]	<b>EventID</b>	(M)	EV (5610740, ECR, „DocReg.registerInformationObject“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der für die Anfrage zugrunde liegenden Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	FALSE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant Dedicated Service [1..1]	<b>NetworkAccessPointID</b>	(O)	Vgl. Kapitel 3
	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
Participant Object Information Object [1..1]	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616080, ECR, „ECRInformationObjectUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des zu registrierenden InformationObjects
	<b>POName</b>	(O)	Vgl. Kapitel 3
<b>POQuery</b>	(O)	Vgl. Kapitel 3	

Participant Object Folder [1..1]	<b>PODetail</b>	(O) Vgl. Kapitel 3
	<b>POTypeCode</b>	(M) EV 2 (system)
	<b>POTypeCodeRole</b>	(M) EV 3 (report)
	<b>PODataLifeCycle</b>	(O) Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M) EV (5616070, ECR, „ECRFolderUniquelIdentifier“)
	<b>POSensitivity</b>	(O) Vgl. Kapitel 3
	<b>POID</b>	(M) OID des ausgewählten Folders
	<b>POName</b>	(O) Vgl. Kapitel 3
	<b>POQuery</b>	(O) Vgl. Kapitel 3
	<b>PODetail</b>	(O) Vgl. Kapitel 3
Participant Object Fallakte [1..1]	<b>POTypeCode</b>	(M) EV 2 (system)
	<b>POTypeCodeRole</b>	(M) EV 3 (report)
	<b>PODataLifeCycle</b>	(O) Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M) EV (5616060, ECR, „ECRRecordUniquelIdentifier“)
	<b>POSensitivity</b>	(O) Vgl. Kapitel 3
	<b>POID</b>	(M) OID der elektronischen Fallakte
	<b>POName</b>	(O) Vgl. Kapitel 3
	<b>POQuery</b>	(O) Vgl. Kapitel 3
	<b>PODetail</b>	(O) Vgl. Kapitel 3

## 4.9 ECR Document Repository (DocRep)

### 4.9.1 DocRep.createAndRegisterInformationObject

Event [1..1]	<b>EventID</b>	(M)	EV (5610905, ECR, „DocReg.createAndRegisterInformationObject“)
	<b>EventActionCode</b>	(M)	EV „C“ (Create)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3

Participant Object Folder [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616070, ECR, „ECRFolderUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des Folders
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3
Participant Object Information Object [1..1]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616080, ECR, „ECRInformationObjectUniquelidentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des angelegten Information Objects
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

#### 4.9.2 DocRep.getInformationObject / DocRep.getInformationObjectCollection

Event [1..1]	<b>EventID</b>	(M)	EV (5610910, ECR, „DocReg.getInformationObject“) (5610915, ECR, „DocReg.getInformationObjectCollection“)
	<b>EventActionCode</b>	(M)	EV „R“ (Read/View/Query/Print)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
Participant Object Information Object [1..n]	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616080, ECR, „ECRInformationObjectUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des Information Objects
	<b>POName</b>	(O)	Vgl. Kapitel 3
	<b>POQuery</b>	(O)	Vgl. Kapitel 3
	<b>PODetail</b>	(O)	Vgl. Kapitel 3

### 4.9.3 DocRep.resumeInformationObject / DocRep.suspendInformationObject

Event [1..1]	<b>EventID</b>	(M)	EV (5610920, ECR, „DocReg.resumeInformationObject“) (5610925, ECR, „DocReg.suspendInformationObject“)
	<b>EventActionCode</b>	(M)	EV „U“ (Update)
	<b>EventDateTime</b>	(M)	Vgl. Kapitel 3
	<b>EventOutcomeIndicator</b>	(M)	Vgl. Kapitel 3
	<b>EventTypeCode</b>	(O)	Vgl. Kapitel 3
Active Participant eFA-Client [1..1]	<b>UserID</b>	(M)	UUID der vorgelegten Access Assertion
	<b>AlternateUserID</b>	(M)	Issuer der Access Assertion
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE → Client ruft Operation direkt auf FALSE → Client ruft Operation indirekt auf (→dann zusätzlicher Active Participant)
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn der Client die Operation aufruft)
	<b>NetworkAccessPointID</b>	(MC)	Vgl. Kapitel 3 (Das Feld ist verpflichtend, wenn NetworkAccessPointTypeCode gesetzt ist)
Active Participant ID Service [0..1]	<b>UserID</b>	(M)	Subject des für die Authentisierung genutzten Dienstzertifikats
	<b>AlternateUserID</b>	(O)	Vgl. Kapitel 3
	<b>UserName</b>	(O)	Vgl. Kapitel 3
	<b>UserIsRequestor</b>	(O)	TRUE
	<b>RoleIDCode</b>	(O)	Vgl. Kapitel 3
	<b>NetworkAccessPoint TypeCode</b>	(M)	Vgl. Kapitel 3
Audit Source [1..1]	<b>NetworkAccessPointID</b>	(M)	Vgl. Kapitel 3
	<b>Audit Enterprise Site ID</b>	(O)	Vgl. Kapitel 3
	<b>Audit Source ID</b>	(M)	Vgl. Kapitel 3
Participant Object Information Object [1..n]	<b>Audit Source Type Code</b>	(O)	Vgl. Kapitel 3
	<b>POTypeCode</b>	(M)	EV 2 (system)
	<b>POTypeCodeRole</b>	(M)	EV 3 (report)
	<b>PODataLifeCycle</b>	(O)	Vgl. Kapitel 3.
	<b>POIDTypeCode</b>	(M)	EV (5616080, ECR, „ECRInformationObjectUniqueIdentifier“)
	<b>POSensitivity</b>	(O)	Vgl. Kapitel 3
	<b>POID</b>	(M)	OID des Information Objects



---

<b>POName</b>	(O) Vgl. Kapitel 3
<b>POQuery</b>	(O) Vgl. Kapitel 3
<b>PODetail</b>	(O) Vgl. Kapitel 3

---

## 5 Literatur

- [eCR\_Crypt-1.1.9] Fraunhofer ISST: Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Cryptographic Keys and Algorithms. Version 1.1.9.02 vom Juni 2007.
- [eFA\_AA-1.2] Fraunhofer ISST: *Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Application Architecture*. Version 1.2 vom Februar 2008.
- [eFA\_DS-1.2.1.2] Fraunhofer ISST: *Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Datenschutzkonzept*. Version 1.2.1.2 vom 25.09.2007.
- [eFA\_SK-1.1.9.1] Fraunhofer ISST: *Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Sicherheitskonzept*. Version 1.1.9.1 vom 07.01.2008.
- [eFA\_SA-1.2] Fraunhofer ISST: *Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Security Architecture*. Version 1.2 vom Februar 2008.
- [DICOM\_AT] Digital Imaging and Communications in Medicine (DICOM): *Supplement 95 – Audit Trail Messages*. Version vom 18. Juni 2004.
- [IHE-ITI-TF-1\_4.0] IHE: IT Infrastructure technical Framework Vol. 1 Integration Profiles. Revision 4.0 vom 22. August 2007.
- [RFC3881] Marshall, G.: *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*. Version 1.0 vom September 2004.
- [RFC3195] Marshall, G.: *Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*. Version 1.0 vom September 2004.



[XML\_Schema-1.1 D Peterson et al: *XML Schema*. Version 1.1, W3C Recommendation, Februar 2006.  
<http://www.w3.org/XML/Schema>

## A XML-Schema

---

```

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="AuditMessage">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="EventIdentification" type="EventIdentificationType" />
        <xs:element name="ActiveParticipant" maxOccurs="unbounded">
          <xs:complexType>
            <xs:complexContent>
              <xs:extension base="ActiveParticipantType" />
            </xs:complexContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="AuditSourceIdentification"
type="AuditSourceIdentificationType" maxOccurs="unbounded" />
        <xs:element name="ParticipantObjectIdentification"
type="ParticipantObjectIdentificationType" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:complexType name="EventIdentificationType">
    <xs:sequence>
      <xs:element name="EventID" type="CodedValueType" />
      <xs:element name="EventTypeCode" type="CodedValueType" minOccurs="0"
maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="EventActionCode" use="optional">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="C">
            <xs:annotation>
              <xs:appinfo>Create</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="R">
            <xs:annotation>
              <xs:appinfo>Read</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="U">
            <xs:annotation>
              <xs:appinfo>Update</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="D">
            <xs:annotation>
              <xs:appinfo>Delete</xs:appinfo>
            </xs:annotation>
          </xs:enumeration>
          <xs:enumeration value="E">
            <xs:annotation>

```

---

---

```

        <xs:documentation>Execute</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="EventDateTime" type="xs:dateTime" use="required" />
<xs:attribute name="EventOutcomeIndicator" use="required">
  <xs:simpleType>
    <xs:restriction base="xs:string" />
  </xs:simpleType>
</xs:attribute>
</xs:complexType>
<xs:complexType name="AuditSourceIdentificationType">
  <xs:sequence>
    <xs:element name="AuditSourceTypeCode" minOccurs="0" maxOccurs="unbounded">
      <xs:complexType>
        <xs:complexContent>
          <xs:restriction base="CodedValueType">
            <xs:attribute name="code" use="required">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="1">
                    <xs:annotation>
                      <xs:appinfo>End-user display device, diagnostic display</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="2">
                    <xs:annotation>
                      <xs:appinfo>Data acquisition device or instrument</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="3">
                    <xs:annotation>
                      <xs:appinfo>Web server process</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="4">
                    <xs:annotation>
                      <xs:appinfo>Application server process</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="5">
                    <xs:annotation>
                      <xs:appinfo>Database server process</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="6">
                    <xs:annotation>
                      <xs:appinfo>Security server, e.g., a domain controller</xs:appinfo>
                    </xs:annotation>
                  </xs:enumeration>
                  <xs:enumeration value="7">
                    <xs:annotation>
                      <xs:documentation>ISO level 1-3 network component</xs:documentation>
                    </xs:annotation>
                  </xs:enumeration>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:restriction>
        </xs:complexContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:documentation>

```

---

---

```

        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="8">
        <xs:annotation>
            <xs:appinfo>ISO level 4-6 operating software</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="9">
        <xs:annotation>
            <xs:appinfo>External source, other or unknown type</xs:appinfo>
        </xs:annotation>
    </xs:enumeration>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
</xs:restriction>
</xs:complexContent>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="AuditEnterpriseSiteID" type="xs:string" use="optional" />
<xs:attribute name="AuditSourceID" type="xs:string" use="required" />
</xs:complexType>
<xs:complexType name="ActiveParticipantType">
    <xs:sequence minOccurs="0">
        <xs:element name="RoleIDCode" type="CodedValueType" minOccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
    <xs:attribute name="UserID" type="xs:string" use="required" />
    <xs:attribute name="AlternativeUserID" type="xs:string" use="optional" />
    <xs:attribute name="UserName" type="xs:string" use="optional" />
    <xs:attribute name="UserIsRequestor" type="xs:boolean" use="optional" default="true" />
    <xs:attribute name="NetworkAccessPointID" type="xs:string" use="optional" />
    <xs:attribute name="NetworkAccessPointTypeCode" use="optional">
        <xs:simpleType>
            <xs:restriction base="xs:unsignedByte">
                <xs:enumeration value="1">
                    <xs:annotation>
                        <xs:appinfo>Machine Name, including DNS name</xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="2">
                    <xs:annotation>
                        <xs:appinfo>IP Address</xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="3">
                    <xs:annotation>
                        <xs:appinfo>Telephone Number</xs:appinfo>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
    </xs:attribute>
</xs:complexType>
<xs:complexType name="ParticipantObjectIdentificationType">
    <xs:sequence>

```

---

---

```

<xs:element name="ParticipantObjectTypeCode">
  <xs:complexType>
    <xs:complexContent>
      <xs:restriction base="CodedValueType">
        <xs:attribute name="code" use="required">
          <xs:simpleType>
            <xs:restriction base="xs:string" />
          </xs:simpleType>
        </xs:attribute>
      </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
</xs:element>
<xs:choice minOccurs="0">
  <xs:element name="ParticipantObjectName" type="xs:string" minOccurs="0" />
  <xs:element name="ParticipantObjectQuery" type="xs:base64Binary" minOccurs="0"
/>
</xs:choice>
<xs:element name="ParticipantObjectDetail" type="TypeValuePairType" minOccurs="0"
maxOccurs="unbounded" />
</xs:sequence>
<xs:attribute name="ParticipantObjectID" type="xs:string" use="required" />
<xs:attribute name="ParticipantObjectTypeCode" use="optional">
  <xs:simpleType>
    <xs:restriction base="xs:unsignedByte">
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:appinfo>Person</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="2">
        <xs:annotation>
          <xs:appinfo>System object</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="3">
        <xs:annotation>
          <xs:appinfo>Organization</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="4">
        <xs:annotation>
          <xs:appinfo>Other</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectTypeCodeRole" use="optional">
  <xs:simpleType>
    <xs:restriction base="xs:unsignedByte">
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:appinfo>Patient</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="2">
        <xs:annotation>

```

---

---

```

        <xs:appinfo>Location</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="3">
    <xs:annotation>
        <xs:appinfo>Report</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="4">
    <xs:annotation>
        <xs:appinfo>Resource</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="5">
    <xs:annotation>
        <xs:appinfo>Master file</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="6">
    <xs:annotation>
        <xs:appinfo>User</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="7">
    <xs:annotation>
        <xs:appinfo>List</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="8">
    <xs:annotation>
        <xs:appinfo>Doctor</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="9">
    <xs:annotation>
        <xs:appinfo>Subscriber</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="10">
    <xs:annotation>
        <xs:appinfo>Guarantor</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="11">
    <xs:annotation>
        <xs:appinfo>Security User Entity</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="12">
    <xs:annotation>
        <xs:appinfo>Security User Group</xs:appinfo>
    </xs:annotation>
</xs:enumeration>
<xs:enumeration value="13">
    <xs:annotation>
        <xs:appinfo>Security Resource</xs:appinfo>
    </xs:annotation>
</xs:enumeration>

```

---

---

```

<xs:enumeration value="14">
  <xs:annotation>
    <xs:appinfo>Security Granularity Definition</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="15">
  <xs:annotation>
    <xs:appinfo>Provider</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="16">
  <xs:annotation>
    <xs:appinfo>Report Destination</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="17">
  <xs:annotation>
    <xs:appinfo>Report Library</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="18">
  <xs:annotation>
    <xs:appinfo>Schedule</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="19">
  <xs:annotation>
    <xs:appinfo>Customer</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="20">
  <xs:annotation>
    <xs:appinfo>Job</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="21">
  <xs:annotation>
    <xs:appinfo>Job Stream</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="22">
  <xs:annotation>
    <xs:appinfo>Table</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="23">
  <xs:annotation>
    <xs:appinfo>Routing Criteria</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
<xs:enumeration value="24">
  <xs:annotation>
    <xs:appinfo>Query</xs:appinfo>
  </xs:annotation>
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
</xs:attribute>

```

---

---

```

<xs:attribute name="ParticipantObjectDataLifeCycle" use="optional">
  <xs:simpleType>
    <xs:restriction base="xs:unsignedByte">
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:appinfo>Origination / Creation</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="2">
        <xs:annotation>
          <xs:appinfo>Import / Copy from original</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="3">
        <xs:annotation>
          <xs:appinfo>Amendment</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="4">
        <xs:annotation>
          <xs:appinfo>Verification</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="5">
        <xs:annotation>
          <xs:appinfo>Translation</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="6">
        <xs:annotation>
          <xs:appinfo>Access / Use</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="7">
        <xs:annotation>
          <xs:appinfo>De-identification</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="8">
        <xs:annotation>
          <xs:appinfo>Aggregation, summarization, derivation</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="9">
        <xs:annotation>
          <xs:appinfo>Report</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="10">
        <xs:annotation>
          <xs:appinfo>Export / Copy to target</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="11">
        <xs:annotation>
          <xs:appinfo>Disclosure</xs:appinfo>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:attribute>

```

---

---

```

    <xs:enumeration value="12">
      <xs:annotation>
        <xs:appinfo>Receipt of disclosure</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="13">
      <xs:annotation>
        <xs:appinfo>Archiving</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="14">
      <xs:annotation>
        <xs:appinfo>Logical deletion</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="15">
      <xs:annotation>
        <xs:appinfo>Permanent erasure / Physical destruction</xs:appinfo>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="ParticipantObjectSensitivity" type="xs:string" use="optional"
/>
/>
</xs:complexType>
<xs:complexType name="CodedValueType">
  <xs:attribute name="code" type="xs:string" use="required" />
  <xs:attributeGroup ref="CodeSystem" />
  <xs:attribute name="displayName" type="xs:string" use="optional" />
  <xs:attribute name="originalText" type="xs:string" use="optional" />
</xs:complexType>
<xs:complexType name="TypeValuePairType">
  <xs:attribute name="type" type="xs:string" use="required" />
  <xs:attribute name="value" type="xs:base64Binary" use="required" />
</xs:complexType>
<xs:attributeGroup name="CodeSystem">
  <xs:attribute name="codeSystem" type="OID" use="optional" />
  <xs:attribute name="codeSystemName" type="xs:string" use="optional" />
</xs:attributeGroup>
<xs:simpleType name="OID">
  <xs:restriction base="xs:string">
    <xs:whiteSpace value="collapse" />
    <xs:pattern value="[0-2]((\\.0)|\\. [1-9][0-9]*)*" />
  </xs:restriction>
</xs:simpleType>
</xs:schema>

```

## B Code System (Event ID)

Code System Name	Code Value	Display Name
ECR	5610010	Audit Recording Started
ECR	5610020	Audit Recording Stopped
ECR	5610100	Identity Provider Function (IdtPrv) → <b>don't use</b>
ECR	5610105	IdtPrv.authenticate
ECR	5610200	Admission Token Service Function (AdmTokSvc) → <b>don't use</b>
ECR	5610205	AdmTokSvc.requestAdmissionTokenCollection
ECR	5610210	AdmTokSvc.requestAdmissionTokenSelection
ECR	5610215	AdmTokSvc.requestAdmissionToken
ECR	5610400	Access Token Service Function (AccTokSvc) → <b>don't use</b>
ECR	5610405	AccTokSvc.requestAccessToken
ECR	5610410	AccTokSvc.requestCreationToken
ECR	5610415	AccTokSvc.registerRecord
ECR	5610500	Policy Token Service Function (PolTokSvc) → <b>don't use</b>
ECR	5610505	PolTokSvc.requestPolicyToken
ECR	5610510	PolTokSvc.resolveAccessToken
ECR	5610600	Record Registry Function (RecReg) → <b>don't use</b>
ECR	5610605	RecReg.getRecordList
ECR	5610610	RecReg.setRecordMetadata
ECR	5610615	RecReg.getRecordMetadata
ECR	5610620	RecReg.setRecordState
ECR	5610625	RecReg.getRecordState
ECR	5610630	RecReg.getRecordStateHistory
ECR	5610635	RecReg.registerRecord
ECR	5610600	Folder Registry Functions (FldReg) → <b>don't use</b>
ECR	5610705	FldReg.getFolderList
ECR	5610710	FldReg.setFolderMetadata
ECR	5610715	FldReg.resumeRecord
ECR	5610720	FldReg.suspendRecord
ECR	5610725	FldReg.createAndRegisterRecord

ECR	5610730	FldReg.registerFolder
ECR	5610735	FldReg.setFolderState
ECR	5610740	FldReg.getFolderState
ECR	5610745	FldReg.getFolderStateHistory
ECR	5610750	FldReg.getFolderListCollection
ECR	5610755	FldReg.getFolderStateCollection
ECR	5610760	FldReg.getFolderStateHistoryCollection
ECR	5610800	Document Registry Function (DocReg) → <b>don't use</b>
ECR	5610805	DocReg.createAndRegisterFolder
ECR	5610810	DocReg.getInformationObjectList
ECR	5610815	DocReg.suspendFolder
ECR	5610820	DocReg.resumeFolder
ECR	5610825	DocReg.setInformationObjectState
ECR	5610830	DocReg.getInformationObjectState
ECR	5610835	DocReg.getInformationObjectStateHistory
ECR	5610840	DocReg.registerInformationObject
ECR	5610850	DocReg.getInformationObjectListCollection
ECR	5610855	DocReg.getInformationObjectStateCollection
ECR	5610860	DocReg.getInformationObjectStateHistoryCollection
ECR	5610900	Document Repository Function (DocRep) → <b>don't use</b>
ECR	5610905	DocRep.createAndRegisterInformationObject
ECR	5610910	DocRep.getInformationObject
ECR	5610915	DocRep.getInformationObjectCollection
ECR	5610920	DocRep.resumeInformationObject
ECR	5610925	DocRep.suspendInformationObject

## C Code System (Event Outcome Indicator)

Code System Name	Code Value	Display Name
ECR	5611000	Success
ECR	5612000	Security Data Error
ECR	5612100	Credential Error
ECR	5612110	Invalid Assertion
ECR	5612120	Invalid Certificate
ECR	5612200	Message Protection Error
ECR	5612210	Decryption Error
ECR	5612220	Signature Error
ECR	5613000	Application Data Error
ECR	5613100	Minor Failure
ECR	5613200	Serious Failure
ECR	5613300	Major Failure
ECR	5614000	Transmission Error



## D Code System (Partition Object ID Type Code)

<b>Code System Name</b>	<b>Code Value</b>	<b>Display Name</b>
ECR	5616010	Identity Assertion UUID
ECR	5616020	AdmissionTokenCollection UUID
ECR	5616030	Admission Assertion UUID
ECR	5616040	Access Assertion UUID
ECR	5616050	Policy Assertion UUID
ECR	5616060	ECRRecordUniquelIdentifier
ECR	5616070	ECRFolderUniquelIdentifier
ECR	5616080	ECRInformationObjectUniquelIdentifier
ECR	5616090	ECRPolicyUID