



## **Authentisierung/Authentifizierung**

Überblick über die Client- und Dienstauthentisierung im Kontext der elektronischen Fallakte

**Editor: Olaf Rode**

Dokumenten-ID: Authentisierung/ Authentifizierung  
Verantwortlich: Fraunhofer ISST  
Status: Release  
Version: 1.2.0.02  
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 GENANNTE 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	11.07.07	Alle	Erste Version	OR
0.7	23.07.07	Alle	Überarbeitung	OR
1.2	29.02.08	Alle	Anpassung an Architekturänderungen	OR

## Statushistorie

Status	Datum	Bemerkungen	Bearbeiter
In Erstellung	11.07.07	Erste Version	OR
Draft	23.07.07	Fertigstellung für Review	OR
PreFinal	29.02.08	PreFinal	OR
Final	03.03.08	Fertigstellung für Veröffentlichung	OR

## Inhalt

<b>1</b>	<b>Einleitung</b>	<b>5</b>
1.1	Zielgruppe	5
1.2	Referenzierte Spezifikationen und Standards	5
1.3	Konventionen	6
<b>2</b>	<b>Grundlagen</b>	<b>7</b>
2.1	Begriffsdefinitionen	7
2.2	Authentisierung auf verschiedenen Ebenen des OSI-Referenzmodells	7
<b>3</b>	<b>Authentisierung auf Anwendungsebene</b>	<b>8</b>
3.1	Direkte zertifikatsbasierte Authentisierung	8
3.2	Zertifikatsgestützte Authentisierungsnachweise	9
<b>4</b>	<b>Authentisierung auf Transportebene</b>	<b>10</b>
<b>5</b>	<b>Weitere Anforderungen</b>	<b>12</b>
5.1	Certificate Validation / Certificate Path Validation	12
5.2	Umgang mit privaten Schlüsseln	12
5.3	Algorithmen	13
<b>6</b>	<b>Literatur</b>	<b>14</b>



## 1 Einleitung

Authentisierung und Authentifizierung bilden zwei der zentralen Mechanismen, um den im Sicherheitskonzept formulierten Schutzziele (Integrität, Vertraulichkeit, Nicht-Abstreitbarkeit) gerecht zu werden. Insbesondere der sichere Aufbau von Kommunikationskanälen zwischen den einzelnen Komponenten der eFA-Architektur stellt hohe Ansprüche an die zum Einsatz kommenden Verfahren. Nur mit – im Hinblick auf den Schutzbedarf – angemessenen und leistungsfähigen Lösungen kann den ausnahmslos hohen Datenschutzanforderungen entsprochen werden.

Der Fokus des Dokuments liegt auf der Beschreibung der zertifikatsbasierten bzw. zertifikatsgestützten Authentisierung und Authentifizierung von Personen, Diensten und IT-Systemen. Es soll gezeigt werden, in welcher Form X.509-Public-Key-Zertifikate als Identitätsnachweis zum Einsatz kommen können und wie die eindeutige und verlässliche Überprüfung der entsprechenden Nachweise sichergestellt werden kann.

Im Rahmen der Darstellung wird sowohl auf den sicheren Aufbau von Kommunikationskanälen zwischen den Komponenten eines Providers als auch den Komponenten verschiedener Providern eingegangen. Dabei wird grundsätzlich zwischen zertifikatsbasierten Authentisierungsmechanismen auf Anwendungs- und Transportschicht unterschieden.

Alternative Verfahren wie beispielsweise die Authentifizierung anhand von Kerberos-Tickets sind nicht Bestandteil der Betrachtung.

### 1.1 Zielgruppe

Diese Spezifikation richtet sich vorrangig an Unternehmen und Personen, die sich für die Implementierung der eFA-Architektur in konkrete Anwendungen und Produkte verantwortlich zeigen. Es wird insbesondere auf die technischen und organisatorischen Anforderungen im Umfeld der Authentifizierung/Authentisierung eingegangen.

### 1.2 Referenzierte Spezifikationen und Standards

Dieses Dokument basiert auf einer Reihe international anerkannter Standards und Quasistandards. Dazu gehören:

- Common ISIS-MTT Specifications for Interoperable PKI Applications. Part 5: Certificate Path Validation [*ISISMTT\_5-1.1*]
- IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication Profile (ATNA) [*IHE-ITI-TF-1\_4.0*]
- The Transport Layer Security (TLS) Protocol [*RFC4346*]
- ISO/IEC 9594-8:2005 - Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [*ISO/IEC\_9594-8\_2005*]

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

- PKI und X.509 Zertifikatsprofile [*eFA\_PKI-1.2*]
- eFA Sicherheitsarchitektur [*eFA\_SA-1.2*]
- eCR Cryptographic Keys and Algorithms [*eCR\_Crypt-1.1.9*]

### 1.3 Konventionen

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



## 2 Grundlagen

### 2.1 Begriffsdefinitionen

Innerhalb des Dokuments wird zwischen den Begriffen Authentisierung und Authentifizierung unterschieden. Folgende Definitionen finden Anwendung: [eGov\_Glossar]

---

**Authentisierung**

---

„Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, in dem bestätigt wird, dass er tatsächlich derjenige ist, der er vorgibt zu sein.“

---

**Authentifizierung**

---

„Unter einer Authentifizierung versteht man die Prüfung einer Authentisierung, d. h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.“

---

### 2.2 Authentisierung auf verschiedenen Ebenen des OSI-Referenzmodells

Die Struktur des OSI-Referenzmodells [ISO/IEC\_7498-1] bietet die Möglichkeit die Authentisierung auf verschiedenen Ebenen des Modells zu realisieren. Von Bedeutung sind dabei insbesondere die Verfahren auf Schicht 3 und 4 (Vermittlungsschicht/ Transportschicht) sowie Schicht 7 (Anwendungsschicht).

Die serviceorientierte Architektur der elektronischen Fallakte siedelt Authentisierung und Authentifizierung standardmäßig auf Schicht 7 an. Dies ermöglicht die gegenseitige Authentifizierung der Dienste an den jeweiligen Endpunkten. (Ende-zu-Ende-Sicherheit)

Nur unter bestimmten Umständen, ist die Verwendung von Verfahren auf Transport- oder Vermittlungsebene notwendig. (Punkt-zu-Punkt-Sicherheit) Kapitel 3 und 4 werden entsprechende Szenarien vorstellen und eine Zuordnung innerhalb des Modells vornehmen.

## 3 Authentisierung auf Anwendungsebene

Grundsätzlich erfolgt die Authentisierung von Nutzern und Diensten im Kontext der elektronischen Fallakte auf Basis von WS-Security. Neben der vorherrschenden Verwendung von zertifikatsgestützten Authentisierungs- und Autorisierungsnachweisen (z. B. SAML-Assertions) für den Aufbau von Vertrauensbeziehungen, spielt bei einigen Komponenten auch die direkte zertifikatsbasierte Authentisierung eine entscheidende Rolle.

### 3.1 Direkte zertifikatsbasierte Authentisierung

Grundlage der zertifikatsbasierten Authentisierung auf Anwendungsebene ist das für WS-Security im X.509 Certificate Token Profile [WSS\_CTP-1.1] definierte X.509 Authentication Framework. **[MUST]** Insbesondere für die beiden folgenden Szenarien ist es von großer Bedeutung.

---

#### Authentisierung zwischen Client und Identity Provider

---

Zwingende Voraussetzung für die Nutzung der eFA-Dienste durch den Client ist die erfolgreiche Authentifizierung durch den Identity Provider. Grundsätzlich empfiehlt sich der Einsatz von X.509-Public-Key-Zertifikaten. **[SHOULD]** Von dieser Empfehlung sollte nur in begründeten Ausnahmefällen abgewichen werden. Kommen andere Mechanismen zum Einsatz, so müssen diese ein vergleichbares Sicherheitsniveau gewährleisten. **[MUST]**

Die Ausgestaltung der verwendeten Clientzertifikate muss den Vorgaben der veröffentlichten Zertifikatsprofile für „Clientauthentisierungszertifikate“ [eFA\_PKI-1.2] entsprechen. **[MUST]**

---

#### Authentisierung zwischen Diensten

---

Auch Dienste müssen sich gegenseitig authentifizieren. Vorgeschriebenes Verfahren ist die zertifikatsbasierte Authentisierung auf Grundlage des X.509 Certificate Token Profile. **[MUST]**

Die Ausgestaltung der verwendeten Dienstzertifikate muss den Vorgaben der veröffentlichten Zertifikatsprofile für „eCR-Servicezertifikate“ [eFA\_PKI-1.2] entsprechen. **[MUST]**

---

Innerhalb des X.509 Certificate Token Profiles werden keinerlei Mechanismen benannt, die für die Überprüfung der Gültigkeit des X.509-Public-Key-Zertifikats zum Einsatz kommen. Um die Sicherheit des Authentifizierungsverfahrens zu gewährleisten, ist die Festlegung bestimmter Testkriterien dennoch zwingend erforderlich. Kapitel 5.1 definiert Richtlinien, an denen sich die Zertifikatsüberprüfung orientieren muss.



### 3.2 Zertifikatsgestützte Authentisierungsnachweise

Kernidee der eFA-Sicherheitsarchitektur ist die Verwendung von Authentisierungs- und Autorisierungsnachweisen in Form von SAML-Assertions. [eFA\_SA-1.2] Sie dienen dem Aufbau von Vertrauensbeziehungen zwischen einzelnen eFA-Komponenten. Grundlage für die Einbettung der Nachweise in den Security-Header der innerhalb der Kommunikation verwendeten SOAP-Nachrichten ist das für WS-Security spezifizierte SAML Token Profile 1.1. **[MUST]** Einen detaillierten Überblick über Aufbau und Verwendung der verschiedenen Assertions bietet [eFA\_SA-1.2].

Die Sicherheit der Nachweise basiert weitestgehend auf zertifikatsgestützten asymmetrischen Kryptographieverfahren (Signatur der Nachweise, Verschlüsselung von Proof-of-Possession-Tokens). Für die zum Einsatz kommenden Zertifikate gelten daher die gleichen Anforderungen wie für die zertifikatsbasierte Authentisierung, d. h. wird ein Nachweis durch einen der eFA-Dienste generiert und durch ein zertifiziertes, asymmetrisches Schlüsselpaar geschützt, so muss das zugehörige Zertifikat den Vorgaben der veröffentlichten Zertifikatsprofile für „eCR-Servicezertifikate“ [eCR\_Profile-1.0] entsprechen. **[MUST]**

Um die Authentizität der einzelnen Authentisierungs- und Autorisierungsnachweise sicherzustellen, ist u. a. auch die Überprüfung der Gültigkeit der Zertifikate bzw. Zertifizierungspfade zwingend erforderlich. Kapitel 5.1 definiert Richtlinien, an denen sich die Überprüfung orientieren muss. **[MUST]**

## 4 Authentisierung auf Transportebene

Um dem im Sicherheitskonzept definierten Schutzbedarf zu entsprechen, bietet die Authentifizierung auf Anwendungsebene in Verbindung mit Mechanismen wie WS-Secure-Conversation [WS\_SC-1.3] meist einen angemessenen Schutz. Unter bestimmten Umständen ist es jedoch notwendig auf ergänzende Mechanismen zurückzugreifen. Dies gilt insbesondere dann, wenn sich die kommunizierenden Komponenten innerhalb verschiedener Sicherheitskontexte befinden.

Bevorzugter Mechanismus im Umfeld der elektronischen Fallakte ist die in RFC4346 beschriebene Transport Layer Security (TLS) [RFC4346]. **[SHOULD]** Von dieser Empfehlung sollte nur in begründeten Ausnahmefällen abgewichen werden. Kommt TLS zum Einsatz, muss die beidseitige (mutual), zertifikatsbasierte Authentisierung genutzt werden, d. h. sowohl Client als auch Server weisen ihre Identität anhand von X.509-Public-Key-Zertifikaten nach. **[MUST]**

Eine Authentisierung und Verschlüsselung mit TLS kommt insbesondere in folgenden Szenarien in Betracht:

---

### Kommunikation zwischen Diensten verschiedener Provider (P2P)

---

Die Authentisierung und Verschlüsselung der Kommunikation auf Anwendungsebene erfüllt nicht vollständig die formulierten Sicherheitsanforderungen. Beispielsweise ist die verschlüsselte Übertragung von Webservice-endpunktadressen nicht ohne weiteres möglich. Um einer Profilbildung bei der Übertragung über unsichere Netze vorzubeugen, muss die Verbindung zusätzlich über TLS authentisiert und gesichert (verschlüsselt) werden. **[MUSS]** Von dieser Festlegung darf nur abgewichen werden, wenn andere Mechanismen, die ein vergleichbares Schutzniveau garantieren (z. B. IPsec), zum Einsatz kommen.

Die Ausgestaltung der verwendeten Zertifikate muss den Vorgaben der veröffentlichten Zertifikatsprofile für „SSL-Serverzertifikate“ [eFA\_PKI-1.2] entsprechen. **[MUST]**

---

### Kommunikation zwischen Client und eFA-Diensten

---

Erfolgt die Kommunikation des Clients mit einzelnen eFA-Diensten über unsichere Netze gelten die gleichen Anforderungen wie bei der Peer-To-Peer-Kommunikation. (s.o.). **[MUST]**

Die Ausgestaltung der verwendeten Zertifikate muss den Vorgaben der veröffentlichten Zertifikatsprofile für „Clientauthentisierungszertifikate“ bzw. „SSL-Serverzertifikate“ [eFA\_PKI-1.2] entsprechen. **[MUST]**

---

### Kommunikation zwischen Client und Daten haltenden Systemen (KIS, VPA)

---

Wird die Nachrichtenübertragung nicht auf Anwendungsebene geschützt muss der Kommunikationskanal grundsätzlich über TLS authentisiert und gesichert werden. **[MUST]** Von dieser Festlegung darf nur abgewichen werden, wenn andere Mechanismen, die ein vergleichbares Schutzniveau garantieren (z. B. IPsec), zum Einsatz kommen.

Die Ausgestaltung der verwendeten Zertifikate muss den Vorgaben der veröffentlichten Zertifikatsprofile für „Clientauthentisierungszertifikate“ bzw. „SSL-Serverzertifikate“ [eFA\_PKI-1.2] entsprechen. **[MUST]**

---



Innerhalb der TLS-Spezifikation werden keinerlei Anforderungen an die Zertifikatsvalidierung gestellt. Entscheidungen über die Gültigkeit müssen von den auf TLS aufsetzenden Komponenten getroffen werden. Kapitel 5.1 definiert Richtlinien, an denen sich die Validierung der Zertifikate bzw. Zertifizierungspfade orientieren muss. **[MUST]**

## 5 Weitere Anforderungen

Es existiert eine Vielzahl von Rahmenbedingungen, die bei der zertifikatsbasierten Authentisierung und Authentifizierung beachtet werden muss. Dazu gehören u. a. die Überprüfung der Gültigkeit von Zertifikaten und Zertifizierungspfaden sowie die Verwaltung kryptographischer Schlüssel. Die folgenden Abschnitte definieren konkrete Richtlinien, die den Umgang mit diesen Problemen erleichtern sollen.

### 5.1 Certificate Validation / Certificate Path Validation

Die Überprüfung der Gültigkeit eines Zertifikats stellt einen wesentlichen Bestandteil der sicheren Authentifizierung dar. Nur wenn sie erfolgreich war, d. h. das Zertifikat verifiziert werden konnte, kann der entsprechende Dienst, das System oder der Nutzer erfolgreich authentifiziert werden.

Der Umfang des Validierungsprozesses ist dabei sehr stark vom Bezugsort des Zertifikats abhängig. Stammt es aus einer als sicher geltenden Quelle, ist nur eine überschaubare Anzahl von Validierungsschritten notwendig (z. B. Überprüfung von CRLs, OCSP-Request). Wurde es aus einer öffentlichen, potentiell unsicheren Quelle bezogen, muss der gesamte Zertifizierungspfad bis hoch zu einem Sicherheitsanker validiert werden. Der Sicherheitsanker repräsentiert dabei immer ein Element (z. B. Zertifizierungsstellenzertifikat), das auf sicherem Weg bezogen wurde und als vertrauenswürdig angesehen werden kann.

Weder in der TLS-Spezifikation noch in den Festlegungen zum X.509 Certificate Token Profile finden sich Aussagen zur Zertifikats- bzw. Zertifizierungspfadvalidierung. Beide Dokumente verweisen explizit auf extern zu treffende Regelungen.

Die ISIS-MTT Spezifikation beschreibt in Part 5 *[ISISMTT\_5-1.1]* einen Algorithmus zur Validierung von Zertifizierungspfaden. Die Gültigkeitsüberprüfung für Zertifikate im Umfeld der elektronischen Fallakte muss sich an diesen Vorgaben orientieren. **[MUST]**

### 5.2 Umgang mit privaten Schlüsseln

Die veröffentlichten Zertifikatsprofile sehen die Nutzung von RSA-Schlüsseln innerhalb der einzelnen Zertifikatstypen vor. Während das Zertifikat (und somit auch der öffentlichen Teil des Schlüsselpaares) uneingeschränkt veröffentlicht werden kann, muss der private Schlüssel umfassend geschützt werden. Nur so



kann sichergestellt werden, dass ausschließlich berechnete Dienste, Personen und Systeme erfolgreich authentifiziert werden.

An den Umgang mit privaten Schlüsseln werden die folgenden Anforderungen gestellt:

---

#### **Speichern privater Schlüssel**

---

Die unverschlüsselte Ablage von privaten Schlüsseln auf IT-Systemen stellt ein hohes Sicherheitsrisiko dar. Gelingt es einer unberechtigten Person Zugriff auf das System zu erhalten, kann der Schlüssel u. U. problemlos ausgelesen und somit kompromittiert werden. Private Schlüssel müssen daher immer verschlüsselt gespeichert werden. **[MUST]**

Für fast alle Softwareprodukte existieren mehrere Möglichkeiten die entsprechenden Schlüssel zu schützen:

- Microsoft bietet unter Windows die Möglichkeit private Schlüssel verschlüsselt zu speichern. Der Zugriff auf die Objekte erfolgt über die MS Crypto API. Das Schutzniveau für die einzelnen Schlüssel lässt sich individuell festlegen.
- Im Rahmen von Java werden zumeist JKS-Files (Java Key Stores) für die Aufbewahrung der Schlüssel verwendet. Sowohl der JKS-Container als solches, als auch die einzelnen privaten Schlüssel lassen sich durch Passwörter sichern.
- Eine weitere Möglichkeit ist die Ablage von privaten Schlüsseln in passwortgeschützten PKCS#8- oder PKCS#12-Containern.

---

#### **Übertragen privater Schlüssel**

---

Für die Übermittlung privater Schlüssel gelten dieselben Einschränkungen wie für deren Speicherung. Sie dürfen ausschließlich in verschlüsselter Form übertragen werden. **[MUST]**

Als Austauschformat sollte PKCS#12 verwendet werden. **[SHOULD]** Neben dem Schlüsselmaterial können zusätzlich auch Zertifikate und Sperrlisten gespeichert werden.

---

#### **Freischalten (entschlüsseln) privater Schlüssel**

---

Die Entschlüsselung privater Schlüssel für die erstmalige Verwendung nach einem erneuten Systemstart muss durch die bewusste Handlung einer berechtigten Person erfolgen. **[MUST]** Dazu zählt u. a. die Anmeldung am System bzw. die Eingabe eines Passwortes. Vollständig automatisierte Verfahren sind nicht zulässig. **[MUST NOT]**

---

#### **Hardware Security Module (HSM)**

---

Die Verwendung von HSMs im Umfeld kryptographischer Operationen gewährleistet ein höheres Schutzniveau, als softwarebasierte Lösungen. Der Einsatz entsprechender Hardware ist für die elektronische Fallakte jedoch optional. **[MAY]**

---

## **5.3 Algorithmen**

Festlegungen zu den zu verwendenden Algorithmen und minimalen Schlüssel-längen finden sich in [eCR\_Crypt-1.1.9] und [eFA\_PKI-1.2].

## 6 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\_PKI-1.2] Fraunhofer ISST: Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: PKI und X.509 Zertifikatsprofile. Version 1.2 vom Juni 2007.
- [eFA\_SA-1.1] Fraunhofer ISST: Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Sicherheitsarchitektur. Version 1.1 vom Juli 2006.
- [eFA\_SA-1.2] Fraunhofer ISST: Spezifikation einer Architektur zum einrichtungsübergreifenden Austausch von Patientendaten: Security Architecture. Version 1.2 vom Februar 2008.
- [eGov\_Glossar] Bundesamt für Sicherheit in der Informationstechnik: Das E-Government-Glossar. Version X.Y vom Januar 2006.
- [IHE-ITI-TF-1\_4.0] IHE: IT Infrastructure technical Framework Vol. 1 Integration Profiles. Revision 4.0 vom 22. August 2007.
- [ISISMTT\_5-1.1] T7, Teletrust: Common ISIS-MTT Specifications for Interoperable PKI Applications. Part 5: Certificate Path Validation. Version 1.1 vom 16. März 2004.
- [ISO/IEC\_7498-1] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 7498-1 - Information technology – Open Systems Interconnection – Basic reference Model: The Basic Model, 1994.
- [ISO/IEC\_9594-8] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 9594-8:2005 - Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2005.



- [PKCS#8-1.2] RSA Laboratories: Private-Key Information Syntax Standard. Version 1.2 vom 1. November 1993.
- [PKCS#12-1.0] RSA Laboratories: Personal Information Exchange Syntax. Version 1.0 vom 24 Juni 1999.
- [RFC4346] Dierks, T.; Rescorla, E.: The Transport Layer Security (TLS) Protocol. Version 1.1 vom April 2006.
- [WSS\_CTP-1.1] OASIS: Web Service Security – X.509 Certificate Token Profile 1.1. Version 1.1 vom Februar 2006.
- [WS\_SC-1.3] OASIS: Web Service – Secure Conversation 1.3. Version 1.3 vom März 2007.
- [WSS\_STP-1.1] OASIS: Web Service Security – SAML Token Profile 1.1. Version 1.1 vom Februar 2006.