Funktionale Spezifikation der OCSP Responder für die PKI der e-Arztausweise Version 2.3.2

Bundesärztekammer, Berlin

	Datum	Name, Abteilung, Firma
Autor, Ansprechpartner		Georgios Raptis
Status (HPC-Projektbüro)	12.05.11	Freigegeben

Versionshistorie

Version	Datum	Bearbeiter	Änderungen	Bemerkungen
0.1	28.03.06	Georgios Raptis (RS)		Initiale Version
0.1.0	03.04.06	RS	Dokument finalisiert	QS erforderlich
0.1.1	20.06.06	RS	weitere SHA-Algorithmen, Migrationspfad für RevocationReason	Einarbeitung der Kommentare der ZDAs
0.1.2	04.07.06	RS	Kompromiss für RevocationReasons	nach Abstimmung mit ZDAs
0.1.3	31.08.06	Schladweiler	QS	
2.3.1	10.03.09 29.05.09	Georgios Raptis	Konsolidierung zum Paket V2.3.1	
2.3.2	12.05.11	Dirk Schladweiler	Aktualisierung der Referenzen	

Inhalt

1 Einleitung

Die Bundesärztekammer, als Arbeitsgemeinschaft der Landesärztekammern, plant die Zulassung interessierter Zertifizierungsdiensteanbieter, welche diese unter Einhaltung verschiedener Kriterien zur Ausgabe der elektronischen Arztausweise berechtigt.

Der elektronische Arztausweis enthält verschiedene Schlüssel und Zertifikate, beispielsweise für die qualifizierte elektronische Signatur, die Authentifizierung, die Verschlüsselung und für die Card-2-Card-Authentifizierung zur elektronischen Gesundheitskarte des Patienten.

Dieses Dokument beschreibt die funktionale Spezifikation der OCSP-Responder für die PKI der elektronischen Arztausweise. Die Spezifikation muss von zugelassenen Zertifizierungsdiensteanbietern implementiert werden, um die Zertifikate der elektronischen Arztausweise nachprüfbar und ggf. abrufbar zu halten.

In der Phase der Test- und Pilotierung des elektronischen Arztausweises werden Signaturzertifikate auf fortgeschrittenem Niveau eingesetzt. Die Anforderungen an die Verzeichnisdienste in der Test- und Pilotierungsphase unterscheiden sich nicht von denen der Wirkbetriebsphase, in welcher obligatorisch mit Signaturzertifikaten und Attributzertifikaten auf qualifiziertem Niveau mit Anbieter-Akkreditierung gearbeitet werden muss. Im Folgenden wird der Terminus „qualifizierte Zertifikate“ synonym für Signatur- und Attributzertifikate und „nicht-qualifizierte Zertifikate“ für die Verschlüsselungs- und Authentisierungszertifikate verwendet.

Für die Nachprüfbarkeit von Zertifikaten soll das OCS-Protokoll verwendet werden. Dies gilt auch für die nicht-qualifizierten Zertifikate. Für qualifizierte Signatur- und Attributzertifikate müssen die Zertifikate nach entsprechender Anfrage in der OCSP-Response mitgeliefert werden. Dies ist notwendig, um die Last der Anfragen, die bei der Überprüfung von eRezepten (schätzungsweise 0,8 bis 1,2 Milliarden pro Jahr bei einer Signaturprüfung pro eRezept, evtl. auch deutlich mehr) zu minimieren.

Für die Struktur der PKI liegt das „Rahmenvertragsmodell“ der Bundesärztekammer zugrunde. Es gibt damit ein Root-Zertifikat der Bundesärztekammer, das CA-Zertifikate für kommerzielle zugelassene Trustcenter ausstellt. Von diesen CA-Zertifikaten werden die nicht-qualifizierten Authentisierungs- und Verschlüsselungszertifikate der Ärzte abgeleitet. Zusätzlich existiert auf jeden eArztausweis ein qualifiziertes Signatur- und eventuell ein qualifiziertes Attributzertifikat, die von einem qualifizierten CA-Zertifikat eines ZDA ausgestellt wurden und zu einem Root-Zertifikat der Bundesnetzagentur validiert werden können. Das Root-Zertifikat der Bundesärztekammer zertifiziert mit Hilfe von Cross-Zertifikaten die qualifizierten CA-Zertifikate der zugelassenen ZDA. Ein Validierungspfad für die Signatur- und Attributzertifikate kann somit auch bis zum Root-Zertifikat der Bundesärztekammer gebildet werden. Es ist damit für alle Zertifikate ersichtlich, dass sie von einem eArztausweis stammen und den Anforderungen aus SGB V §291a erfüllen.

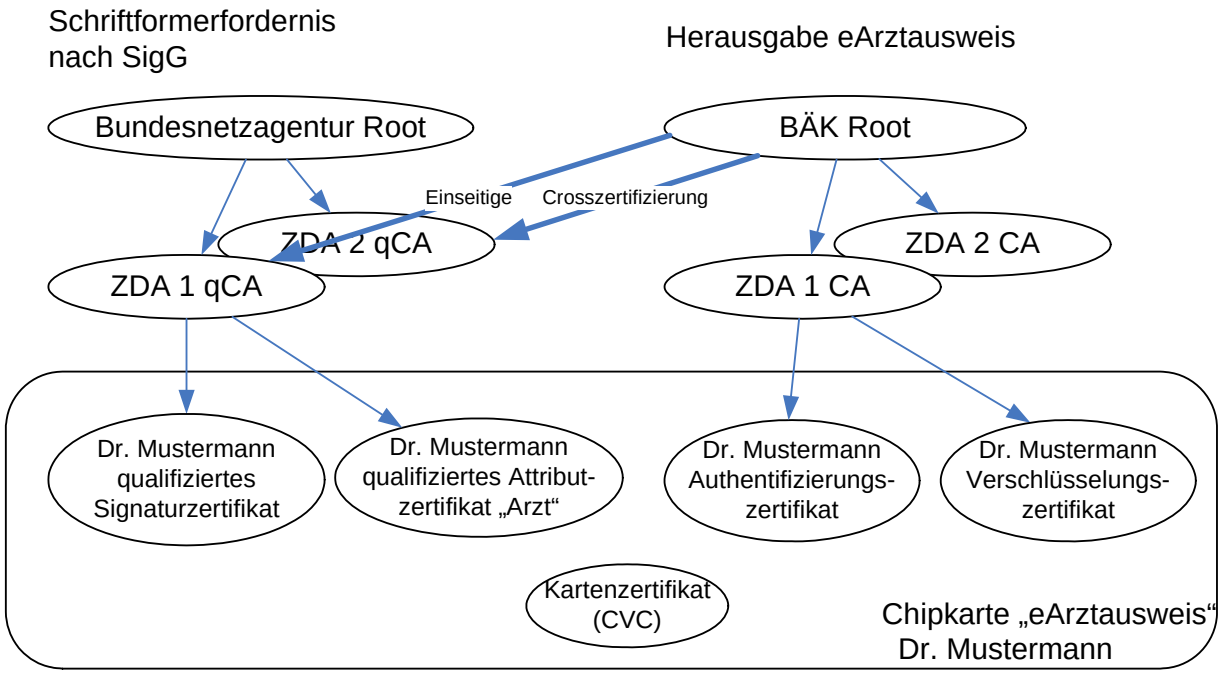

Abbildung 1: Zertifizierungsstruktur

1.1 Grundsätze

Alle Zertifikate müssen grundsätzlich nachgeprüft werden können. Die Nachprüfbarkeit der Zertifikate wird über das OCS-Protokoll realisiert. Qualifizierte Signatur- und Attributzertifikate werden über OCSP-Responder soweit zulässig abrufbar und (stets) nachprüfbar gehalten. Es muss möglich sein, in einer einzigen OCSP-Abfrage und zugehöriger OCSP-Antwort gleichzeitig ein qualifiziertes Signatur- und ein qualifiziertes Attributzertifikat abzurufen und nachzuprüfen.

Es gibt über die verschiedenen zugelassenen Zertifizierungsdiensteanbieter hinweg keine zentrale Datenhaltung oder zentraler OCSP-Responder oder OCSP-Proxy. Jeder ZDA betreibt seine eigene OCSP-Responder, ggf. getrennt für qualifizierte und nicht-qualifizierte Zertifikate. Die Adresse des zuständigen OCSP-Responders für die Überprüfung eines Zertifikates ist im Zertifikat selbst (Extension authorityInfoAccess, s. [baekCerts]) und in einer TSL der Bridge-CA der gematik enthalten.

1.2 Antwortverhalten des OCSP-Responders

Ein OCSP-Responder stellt die „Nachprüfbarkeit“ (s. Begriff im SigG) der Zertifikate sicher. D.h., wenn man das Zertifikat oder relevante Teile davon kennt, kann man seinen Status

abfragen. Der Status eines qualifizierten Zertifikates im Kontext der elektronischen Arztausweise kann lauten:

- „good“: D.h. das Zertifikat ist vorhanden und nicht gesperrt. Als Nachweis dafür muss der OCSP-Responder den Hashwert des DER-kodierten Zertifikats in der OCSP-Extension `certHash` liefern.
- „unknown“, D.h. das Zertifikat ist nicht bekannt.
- „revoked at <date and time>“, d.h. das Zertifikat ist bekannt und wurde am Zeitpunkt <date and time> gesperrt. Der Hashwert des DER-kodierten Zertifikats in der OCSP-Extension `certHash` muss als Nachweis der Existenz geliefert werden.

Es ist ersichtlich, dass der OCSP-Responder keine Informationen über die Gültigkeit von Zertifikaten liefert, sondern nur über deren Status. So antwortet ein OCSP-Responder z.B. mit „good“ für ein abgelaufenes Zertifikat, das vorhanden und nicht gesperrt ist, welches aber zum Zeitpunkt der Anfrage nicht mehr gültig ist. Es ist Aufgabe des Clients, die Gültigkeit eines Zertifikates zu einem bestimmten Zeitpunkt auf Grund der Informationen, die er vom Verzeichnisdienst bekommt und des zugrunde liegenden Gültigkeitsmodells zu ermitteln. Dem OCSP-Responder „unbekannte“ Zertifikate sind ungültig, auch wenn sie mathematisch gültig sind.

Bei Signaturzertifikaten und Attributzertifikaten muss der OCSP-Responder auf Verlangen und soweit zulässig (im Rahmen der e-Arztausweise werden alle Signatur- und Attributzertifikate abrufbar gehalten) das Zertifikat liefern. Dies resultiert aus den Anforderungen der noch offenen Spezifikation des eRezeptes (das Signaturzertifikat soll nicht im signierten eRezept enthalten sein, nur dessen IssuerDN und Seriennummer). Der Client, der die Signatur eines eRezeptes prüfen möchte, kann aus dem Rezept (nach gegenwärtigem Meinungsstand) nur die Seriennummer des signierenden Zertifikats und seinen Aussteller extrahieren. Diese Informationen sind ausreichend, um eine OCSP-Anfrage zu starten und in einem Arbeitsschritt sowohl das Signaturzertifikat als auch ggf. das Attributzertifikat als auch entsprechende Statusinformationen zu bekommen. Voraussetzung dafür ist, dass die „statischen“ Root- und CA-Zertifikate, von denen die angefragten Zertifikate abgeleitet sind, dem Client vorliegen, damit er die Hashwerte vom DN und öffentlichen Schlüssel bilden kann.

Es wird davon ausgegangen, dass der Hashwert vom IssuerDN des angefragten Zertifikates stets mit dem Hashwert vom SubjectDN seines Ausstellers übereinstimmt (!).

1.3 Funktionale Anforderungen für den OCSP-Responder

Es existiert kein zentraler OCSP-Responder. Jedes zugelassene Trustcenter betreibt seine eigene OCSP-Responder. Ein Anwender (d.h. eine Applikation) muss das Zertifikat haben, dessen Status er erfahren möchte (Ausnahme: Signatur- und Attributzertifikate). Die Information, welcher OCSP-Responder für das Zertifikat anzufragen sei, ist in der „AuthorityInfoAccess“-Extension im Zertifikat oder ggf. in einer TSL enthalten. Im Bereich der Telematik-Infrastruktur des Gesundheitswesens müssen TSL-Informationen über die Zuständigkeit von OCSP-Responder, falls vorhanden, prioritär behandelt werden. Dies ist

aufgrund von Sicherheitsanforderungen des mit der gematik abgestimmten Gültigkeitsmodells notwendig. Die Extension „authorityInfoAccess“ wird trotzdem im Zertifikat aufgenommen, um Kompatibilität mit existierenden Clients außerhalb des Gesundheitswesens und Konformität zur Common-PKI-Spezifikation ([externCommonPKI]) zu wahren.

- Zugelassene Zertifizierungsdiensteanbieter müssen Signatur- und Attributzertifikate in der OCSP-Response (in einer einzigen OCSP-Response) auf Nachfrage (Extension in der OCSP-Request: `RetrieveIfAllowed`) mitliefern können. In der OCSP-Response wird dafür die Extension `RequestedCertificate` verwendet. Für Authentisierungszertifikate ist dies nicht zulässig, für Verschlüsselungszertifikate ist dies optional. Clients müssen solche OCSP-Responses bei gesetzter `RetrieveIfAllowed`-Extension verarbeiten können.
- Es ist zulässig für die Nachprüfbarkeit und ggf. Abrufbarkeit von nicht-qualifizierten Zertifikaten, ein HSM für die Signatur der OCSP-Responses zu verwenden. Das HSM muss mindestens nach CC EAL4 „hoch“ oder FIPS 140-2 Level 3 oder vergleichbar sicherheitsevaluiert sein. Der ZDA ist für die Sicherheit eines HSM-betriebenen OCSP-Responders verantwortlich.
- Ein OCSP-Responder kann aus Sicherheitsgründen die Anzahl von Statusauskünften pro Anfrage (d.h. die Anzahl `Requests` in der `requestList`) beschränken. Jedoch müssen mindestens zwei `Requests` in einer `requestList` unterstützt werden, damit ein Signaturzertifikat und ein Attributzertifikat in einer Anfrage geprüft und ggf. geliefert werden können. Wenn der OCSP-Responder die Anfrage, bei mehr als zwei angefragten Zertifikate, nicht zurückweist, dann muss er für alle angefragten Zertifikate den Status und ggf. die Zertifikate selbst liefern.
- Ein OCSP-Responder, der für nicht-qualifizierte Zertifikate Statusinformationen liefert, muss die OCSP-Responses mit einem OCSP-Signer-Zertifikat unterschreiben, das von der Root-Instanz der Bundesärztekammer ausgestellt wurde. OCSP-Responder, die für qualifizierte Zertifikate zuständig sind, verwenden qualifizierte OCSP-Signer-Zertifikate, die von der Bundesnetzagentur ausgestellt worden sind.
- Es müssen OCSP-Requests ohne Signatur des Anfragenden unterstützt werden. Signierte OCSP-Requests dürfen nicht zurückgewiesen werden.
- In OCSP-Responses soll bei gesperrten Zertifikaten kein `revocationReason` gesetzt werden[1]. Ist dies aus technischen Gründen sehr schwierig, können ausnahmsweise OCSP-Responder für alle gesperrten Zertifikate der eArztausweise mit "unspecified", „affiliationChanged“, „superseded“ und „cessationOfOperation“ antworten. Unter keinen Umständen dürfen die ReasonCodes „keyCompromise“, „cACompromise“, „certificateHold“, „removeFromCRL“, „privilegeWithdrawn“ und „aACompromise“ verwendet werden. Falls ein ZDA ReasonCodes verwendet, ist er für die Einhaltung damit verbundener datenschutzrechtlicher Bestimmungen selbst verantwortlich.
- Für die Antwortzeiten für OCSP-Requests, die nicht-qualifizierte Zertifikate betreffen, gelten dieselben Anforderungen wie für OCSP-Requests, die qualifizierte Zertifikate

[1] Gründe für den Verzicht auf ReasonCodes im Kontext der eArztausweise: s. Analyse im Dokument „CRL-Profil und Spezifikation“

betreffen. Darüber hinaus können weitere Service Level Agreements mit garantierten Antwortzeiten sowohl für qualifizierte als auch für nicht-qualifizierte Zertifikate abgeschlossen und unterstützt werden.

Als Gültigkeitsmodell für die qualifizierte Attribut- und Signaturzertifikate gilt das Kettenmodell; für alle nicht-qualifizierten Zertifikate (auch für Authentisierungs- und Verschlüsselungszertifikate) wird das mit der gematik abgesprochene und in der gemeinsame Policy der Leistungsträger beschriebene „Kompromissmodell“ festgelegt. Nach diesem Modell erfolgt die Prüfung der nicht-qualifizierten Zertifikate nach dem Kettenmodell, die Ausstellung jedoch nach den Maßgaben des Schalenmodells, so dass kein nicht-qualifiziertes Zertifikat länger als sein Aussteller gültig sein darf. Es wird auf die entsprechende Dokumente (s.[baekValidityModel]) verwiesen. D.h. ein OCSP-Responder muss für ein nicht-gesperrtes bekanntes Zertifikat mit „good“ antworten, auch wenn das Root- oder CA-Zertifikat inzwischen gesperrt wurde (auch wenn der Sperrgrund möglicherweise „unspecified“ lautet oder nicht ermittelt werden kann).

Der OCSP-Responder muss konform zur Common-PKI v2.0 Spezifikation [externCommonPKI] und insbesondere zum SigG-Profil (Part 9) sein. Das SigG-Profil gilt explizit auch für die nicht-qualifizierten Authentisierungs- und Verschlüsselungszertifikate; insbesondere muss der Hashwert des angefragten Zertifikates als Nachweis der Existenz geliefert werden. Für qualifizierte Signatur- und Attributzertifikate müssen zudem die optionale Erweiterungen „`RetrieveIfAllowed`“ und „`RequestedCertificate`“ unterstützt werden.

Ein Client muss eine OCSP-Anfrage stellen, wenn die Gültigkeit eines Zertifikats zu einem bestimmten Zeitpunkt ermittelt werden soll. Es reicht nicht aus, zu prüfen, ob ein mathematisch gültig signiertes Zertifikat nicht in der CRL aufgeführt ist, weil es sein könnte, dass das Zertifikat „nicht bekannt“ ist (wenn z.B. die zugehörige Chipkarte abgefangen und missbräuchlich genutzt wurde). Dies gilt auch für die Authentisierungs- und Verschlüsselungszertifikate. Wurde jedoch ein Zertifikat einmal mittels eines OCSP-Responses als „bekannt“ ermittelt, kann dessen Status künftig über die zugehörige CRL ermittelt werden.

1.4 Problematik der zulässigen Algorithmen

Bezüglich Hash- und Signaturalgorithmen für OCSP-Responder, die für nicht-qualifizierte Zertifikate zuständig sind, gelten gleiche Anforderungen an Sicherheit und kryptographische Stärke wie für OCSP-Responder, die für qualifizierte Zertifikate OCSP-Responses liefern.

Die Anforderungen des jeweils aktuellen amtlichen Algorithmenkatalogs (z.Z. [extern3]) gelten auch für Signaturen und – soweit von der Bundesnetzagentur für qualifizierte Zertifikate gefordert – für die Extension `certHash` (Nachweis der Existenz des Zertifikats) von OCSP-Responses. Demnach ist SHA-1 zumindest für die Signatur nicht mehr zulässig.

2 Literatur

[externCommonPKI] Common PKI Specification for Interoperable Applications, T7 & TeleTrusT, Version 2.0, 20.01.2009

[extern3] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17.11.2008, veröffentlicht am 27.01.2009 im Bundesanzeiger Nr. 13 S. 346, Bundesnetzagentur. http://www.bundesnetzagentur.de/media/archive/15549.pdf

[baekCerts] Zertifikatsprofile für X.509 Basiszertifikate; Version 2.3.2; 12.05.11

[leoGemPolicy] Gemeinsame Policy für die Herausgabe der HPC; Version 0.9.3w2; 03.03.06; Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, Kassenzahnärztliche Bundesvereinigung, Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH

[baekValidityModel] Gültigkeitsmodell der elektronischen Arztausweise und Laufzeit der Zertifikate; Version 2.3.1; 29.05.09