CRL-Profil und Spezifikation, Version 2.3.2

Bundesärztekammer, Berlin

	Datum	Name, Abteilung, Firma
Autor, Ansprechpartner		Georgios Raptis
Status (HPC-Projektbüro)	06.05.2010	Freigegeben

Versionshistorie				
Version	**Datum**	**Bearbeiter**	**Änderungen**	**Bemerkungen**
0.1	15.06.06	Georgios Raptis		Initiale Version Dokument finalisiert, ready for QS
0.1.1	16.06.06	Raptis	Redaktionelle Korrekturen	Eigene QS, ready for extQS
0.1.2	11.07.06	Raptis	Kompromiss für ReasonCodes	
0.1.3	11.07.06	Schladweiler	QS	
2.3.1	10.03.09	Raptis	Konsolidierung zum Paket V2.3.1 Berücksichtigung Common-PKI 2.0 und neue RFCs	Delta-CRLs bleiben optional ReasonCodes SOLLEN nicht eingesetzt werden, bei begründeten Ausnahmen werden die Rahmenbedingungen festgelegt
2.3.1	23.03.09 29.05.09	Beyer	QS	
2.3.2	03.03.10	Georgios Raptis	CRLs sind optional aber empfohlen	Lt. Mitteilung der gematik vom 17.02.2010

Inhalt

TABELLENVERZEICHNIS 5

1 EINLEITUNG 6

2 KONZEPTE UND FESTLEGUNGEN 8

3 PROFIL DER CRLS, ÜBERSICHT UND INHALTE 9

3.1 Struktur der CRL 9

3.2 Struktur der tbsCertList 10

3.3 revokedCertificates mit CRLEntryExtensions 11

3.4 CRL-Extensions 12

4 LITERATUR 13

Tabellenverzeichnis

Tabelle 1: Grundstruktur: `CertificateList` 9

Tabelle 2: Struktur der tbsCertList....10

Tabelle 3: Struktur von revokedCertificates inkl. CRLEntryExtensions....11

Tabelle 4: Struktur der CRL-Extensions....12

1 Einleitung

In diesem Dokument werden die Profile der Sperrlisten im Bereich der elektronischen Arztausweise definiert sowie allgemeine Spezifikationsrichtlinien festgelegt. Die Struktur und die Inhalte der hier spezifizierten CRLs folgen die Empfehlungen des IETF RFC5280 [extern1] und der Common-PKI-Spezifikation [extern2].

Es können CRLs sowohl für qualifizierte publicKey- und Attributzertifikate als auch für alle nicht-qualifizierte Zertifikate eingesetzt werden.

Die Bereitstellung von CRLs ist für alle Zertifikatsklassen optional, jedoch empfohlen.

Prüfkomponenten, die CRLs auswerten, müssen für qualifizierte Zertifikate die Vorgaben des Signaturgesetzes insbesondere für das Gültigkeitsmodell (Kettenmodell) beachten, für nicht-qualifizierte Zertifikate die Vorgaben aus [leoGemPolicy] umsetzen.

Der Wert einer CRL ist im SigG-Kontext sowie auch für Authentisierungs- und Verschlüsselungszertifikate, die für e-Arztausweise den SigG-Anforderungen genügen müssen, zumindest für eine erste Überprüfung eines Zertifikates, zweifelhaft. Der Grund ist, dass ausgestellte Zertifikate, die nicht im Verzeichnisdienst freigeschaltet wurden, nicht in einer CRL aufgenommen werden können, obwohl sie ungültig sind. Eine Verweigerung zur Freischaltung kann z. B. entstehen, wenn der Empfänger die Chipkarte nie bekommen hat (jemand hat die Karte abgefangen) oder wenn die Transport-PIN gebrochen war. Solche Zertifikate sind mathematisch korrekt aber formal „nicht existent“ und somit ungültig. Die qualifizierten Signaturzertifikate können auch dann nicht in der CRL aufgenommen werden, weil damit suggeriert würde, dass sie bis zur Sperrung gültig wären (eine rückwirkende Sperrung ist laut SigG nicht zulässig). Es wird somit hingewiesen, dass eine CRL-Prüfung nicht ausreicht, um die Gültigkeit eines Zertifikates zu einem bestimmten Zeitpunkt zu ermitteln. Eine OCSP-Prüfung hingegen liefert die notwendige Information „vorhanden“ und ist somit erforderlich. Wenn allerdings ein Zertifikat einmal als „vorhanden“ über OCSP deklariert wurde, ist in der Folge eine CRL-Prüfung ausreichend.

Das o. g. Problem ist auch für die nicht-qualifizierten Zertifikate relevant, zumindest für die Zeit von der Produktion bis verlässliche Informationen über den Status der Chipkarte vorliegen. So können AUTH und ENC Zertifikate, dessen Träger-Chipkarte von einem Angreifer abgefangen wurde, (d. h. das zugehörige Signaturzertifikat wird im Verzeichnisdienst nie freigeschaltet), in die CRL aufgenommen werden. Bis zu diesem Zeitpunkt kann die Karte aber missbräuchlich für bspw. Authentisierungen verwendet werden. Der Überprüfer von ENC und AUTH-Zertifikaten trägt das Risiko dafür, wenn er sich ausschließlich auf eine CRL verlässt und das OCS-Protokoll nicht einsetzt.

Der CRL-Issuer kann sich im SigG-Kontext ändern. Dies ist z. B. möglich, wenn die Person, auf die das Zertifikat personalisiert ist, gestorben ist und somit auch nicht mehr unterschreiben kann. Laut SigG/SigV ist es nicht zulässig, ein bereits vergebenes Pseudonym (z. B. CRL-Signer 1:PN) einer zweiten Person zuzuordnen. Der DistinguishedName im Feld cRLSigner ist jedoch fest. Auch für ENC und AUTH-Zertifikaten ist es möglich, dass ein anderer CRL-Signer, als der im CRL-DP Eingetragene, die CRL unterschreiben muss. Dies ist dann der Fall, wenn ein Trustcenter aus Gründen der Hochverfügbarkeit zwei Standorte betreibt und Chipkarten/HSMs mit nicht-kopierbaren Schlüsseln einsetzt. Der zweite Standort muss dann einen anderen CRLSigner einsetzen als der erste Standort. Folgender Lösungsweg wird dafür

sowohl für Qualifizierte als auch für alle nicht-qualifizierten-Zertifikate definiert, gemäß Common-PKI Spezifikation [extern2] Part 9 S. 27ff:

Der Überprüfer einer CRL soll die CRL mittels dem URL im CRL-DP herunterladen und mit den in Common-PKI beschriebenen Validierungsalgorithmen überprüfen. Wenn der CRLSigner, der die CRL unterschrieben hat, nicht identisch ist mit dem CRLSigner, der im Zertifikat eingetragen ist, dann soll überprüft werden, ob das Zertifikat (dessen Gültigkeit mit Hilfe der CRL geprüft wird) und der CRLSigner, der die CRL signiert hat, aus der selben Zertifizierungshierarchie stammen. Wenn dies der Fall ist und auch alle anderen Prüfschritte positiv verlaufen, dann soll die CRL als gültig betrachtet werden.

2 Konzepte und Festlegungen

- Es werden indirekte CRLs ausgestellt.
- Alle auf dem eArztausweis enthaltenen X.509-Zertifikate (inklusive Attributzertifikate) sind stets gemeinsam zu sperren. Es ist zu vermeiden, dass sich diese Zertifikate in unterschiedlichen Zuständen befinden.
- Für qualifizierte Zertifikate (publicKey oder Attributzertifikate) werden qualifiziert signierte CRLs eingesetzt. Für ENC und AUTH-Zertifikate werden CRLs ausgestellt, die von nicht-qualifizierten CRL-Signer-Zertifikaten unterschrieben werden. Diese werden durch die Root-Instanz der Bundesärztekammer ausgestellt.
- Es steht einem Trustcenter frei, unterschiedliche CRLs für publicKey- und Attributzertifikate auszustellen. Ebenso können mehrere CRLs in mehreren CRL-Distribution-Points veröffentlicht werden, die jeweils für eine bestimmte Anzahl von Zertifikaten eingesetzt werden. Es darf jedoch nur eine CRL in einem CRL-DP aufgenommen werden.
- CRLs müssen gemäß Verzeichnisdienstkonzept für e-Arztausweise per LDAP veröffentlicht werden. Sie können auch über andere Protokolle, z. B. http, veröffentlicht werden; dies liegt im Ermessen des Trustcenters.
- Ein Trustcenter kann optional Delta-CRLs ausstellen. Diese (und die zugehörigen Full-CRLs) müssen Common-PKI-konform sein.
- In den CRL-Einträgen dürfen keine ReasonCodes aufgenommen werden. Der Grund dafür ist, dass ReasonCodes im Kontext der eArztausweise keine Relevanz im Sinne einer unterschiedlichen Behandlung der Zertifikate abhängig vom ReasonCode besitzen. D. h. eine SigG-konforme Signatur ist grundsätzlich gültig, wenn sie vor der Sperrung getätigt wurde, egal ob nachher die Karte gestohlen, verloren oder das Vertragsverhältnis gekündigt wurde. Authentisierungen sind immer als ungültig zu betrachten, unabhängig von den Sperrgründen des AUTH-Zertifikats. Außerdem können ReasonCodes datenschutzrechtlich problematische Informationen liefern (z. B. Entzug der Approbation, Verlust der Karte, Rechnung nicht bezahlt usw.). Da es also für eine Zertifikatsprüfung irrelevant ist, welcher ReasonCode aufgeführt wird, erfüllt die Aufnahme von ReasonCodes keinen ersichtlichen Zweck und soll daher entfallen. Ist dies aus technischen Gründen sehr schwierig, können ausnahmsweise CRLs für eArztausweise die ReasonCodes "unspecified", „affiliationChanged“, „superseded“ und „cessationOfOperation“ enthalten. 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.
- Die CRLs müssen den Anforderungen der „Gemeinsamen Policy für die Herausgabe der HPC“ [leoGemPolicy] insbesondere bezüglich des Archivierungszeitraums entsprechen.
- Rückwirkende Sperrungen sind auch für ENC/AUTH-Zertifikate nicht zulässig. Ebenso unzulässig ist, eine Sperrung rückgängig zu machen. Zertifikate „on Hold“ zu halten ist nicht vorgesehen.

3 Profil der CRLs, Übersicht und Inhalte

Folgende Elemente müssen in den CRLs unterstützt und aufgenommen werden, es sei denn, sie sind in den u.g. Tabellen als optional gekennzeichnet. Elemente, die hier nicht aufgeführt werden, dürfen in einer CRL nicht aufgenommen werden. Leere Elemente dürfen in den CRLs nicht aufgenommen werden. Die ASN.1-Struktur der Elemente kann aus dem RFC5280 [extern1] und der Common-PKI-Spezifikation [extern2] entnommen werden.

3.1 Struktur der CRL

Struktur	Semantik	Inhalt
CertificateList		
tbsCertList	Inhalt der Sperrliste (CRL), DER-kodiert, wird vom CRLSigner signiert	siehe Tabelle 2
signatureAlgorithm	OID des Algorithmus inkl. ggf. zugehörige Parameter für die Signatur der Sperrliste	Zulässige Algorithmen nach jeweils aktuellem amtlichen Algorithmenkatalog [extern4]. Es werden die Algorithmen verwendet, die auch für die X.509-Zertifikate der eArztausweise verwendet werden.
signatureValue	Signatur der `tbsCertList`	BIT STRING

Tabelle 1: Grundstruktur: `CertificateList`

3.2 Struktur der tbsCertList

Struktur	Semantik	Inhalt
tbsCertList		
Version	Version des CRL-Formats	1 (CRLv2)
Signature	OID des Algorithmus inkl. ggf. zugehörige Parameter für die Signatur der Sperrliste	Zulässige Algorithmen nach jeweils aktuellem amtlichen Algorithmenkatalog, s. o.
Issuer	Distinguished Name des CRL-Ausstellers	Die Struktur muss exakt den SubjectDN des CRLSigners entsprechen (inkl. Kodierung, Reihenfolge usw.) so dass die Hashwerte beider Strukturen (Issuer der CRL und SubjectDN des CRLSigners) gleich sind
thisUpdate	Zeitpunkt der Erzeugung der CRL (UTC-Time bis zum Jahr 2049, ab 2050 GeneralizedTime)	Zeitpunkt der Erzeugung der CRL
nextUpdate	Die nächste planmäßige CRL wird nicht später als zum Zeitpunkt „nextUpdate“ ausgestellt. Ein Trustcenter/ZDA muss eine neue CRL sofort (d. h. unabhängig vom nextUpdate) ausstellen, wenn ein Zertifikat gesperrt wird. Kodierung wie thisUpdate	Die nächste planmäßige CRL wird nicht später als zum Zeitpunkt „nextUpdate“ ausgestellt.
revokedCertificates	Liste der gesperrten Zertifikate, mit CRLEntryExtensions	siehe Tabelle 3
crlExtensions	Für die CRL relevante Extensions	siehe Tabelle 4

Tabelle 2: Struktur der tbsCertList

3.3 revokedCertificates mit CRLEntryExtensions

Struktur	Semantik	Inhalt
revokedCertificates		
userCertificate	Seriennummer des gesperrten Zertifikats	CertificateSerialNumber
revocationDate	Zeitpunkt der Sperrung	Time: Datum und Uhrzeit, bis 2049 UTCTime, ab 2050 GeneralizedTime
crlEntryExtensions	Extensions, die für den Eintrag des gesperrten Zertifikats relevant sind	s.u.
crlEntryExtensions		
CertificateIssuer	KRITISCHE EXTENSION. Aussteller des gesperrten Zertifikats	DN exakt wie der SubjectDN des CA-Zertifikats inkl. Kodierung, Reihenfolge usw., so dass die Hashwerte beider Strukturen gleich sind
Die CRLEntryExtensions ReasonCode, HoldInstructionCode und InvalidityDate dürfen nicht gesetzt werden		

Tabelle 3: Struktur von revokedCertificates inkl. CRLEntryExtensions

3.4 CRL-Extensions

Struktur	Semantik	Inhalt
crlExtensions		
AuthorityKeyIdentifier	Key Identifier vom öffentlichen Schlüssel des CRLSigner-Zertifikates	nur keyIdentifier = OCTET STRING, 20 Bytes, SHA-1 aus dem public-key ohne Tag- und Längen-bytes (s.[extern2])
CRLNumber	Seriennummer der CRL	positiver INTEGER, 20 OCTETS mit Vorzeichen (MSB), streng monoton steigend (Ausnahme: s. DeltaCRLs)
DeltaCRLIndicator	KRITISCHE EXTENSION. Kennzeichnet die CRL als Delta-CRL. Darf nur in Delta-CRLs aufgenommen werden	s. u.
IssuingDistributionPoint	KRITISCHE EXTENSION. In dieser Spezifikation: Informationen, dass es sich um eine indirekte CRL handelt	s. u.
DeltaCRLIndicator		
BaseCRLNumber	Nummer der zugehörigen Full-CRL. Wenn eine Delta-CRL ausgestellt wird, muss auch eine zugehörige Full-CRL ausgestellt werden, die alle gesperrte Zertifikate enthält (also auch die Zertifikate in der Delta-CRL) und die gleiche CRL-Seriennummer hat.	CRLNumber der zugehörigen Full-CRL
IssuingDistributionPoint		
indirectCRL	Kennzeichnet die CRL als eine indirekte CRL, d.h. der Aussteller der CRL ist nicht der Aussteller der gesperrten Zertifikate	[4] BOOLEAN TRUE

Tabelle 4: Struktur der CRL-Extensions

4 Literatur

[extern1] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W., Request for Comments (RFC) 5280, May 2008.

[extern2] Common PKI Specification for Interoperable Applications, T7 & TeleTrusT, Version 2.0, 20.01.2009

[extern4] 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.

[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