Public Key Service

Profil der Sperrlisten für nicht qualifizierte Zertifikate

Version: 1.0
Stand: 27.07.2018
Status: Freigegeben

Business flexibility T · · Systems · · ·

Impressum

Herausgeber
T-Systems International GmbH

Dateiname	Dokumentennummer	Dokumentenbezeichnung
PKS Sperrlistenprofil v2.0.doc		

Version	Stand	Status
1.0	27.07.2018	Freigegeben

Kurzinfo
Dieses Dokument beschreibt das Sperrlistenprofil für nicht qualifizierte Zertifikate der Dienstleistung Public Key Service

Änderungshistorie

Version	Stand	Änderungen / Kommentar
1.0	27.07.2018	1. Version

Inhaltsverzeichnis

1 Einleitung 1

2 Profil der Sperrliste 2

2.1 Übersicht über die Felder der Sperrliste 3

2.2 Die Felder der Struktur CertificateList 4

2.2.1 Das Feld tbsCertList 4

2.2.2 Das Feld signatureAlgorithm 4

2.2.3 Das Feld signatureValue 4

2.3 Die Felder der Struktur TBSCertList 5

2.3.1 Das Feld version 5

2.3.2 Das Feld signature 5

2.3.3 Das Feld issuer 5

2.3.4 Das Feld thisUpdate 6

2.3.5 Das Feld nextUpdate 6

2.3.6 Das Feld revokedCertificates 6

2.3.7 Das Feld crlExtensions 7

1 Einleitung

Dieses Dokument beschreibt den Aufbau von Sperrlisten. Die darin enthaltenen Daten werden ausgehend von der jeweils grundlegenden Struktur gemäß X.509 erläutert. Dabei werden die Felder und mögliche Inhalte, sowie die zu verwendenden Datentypen festgelegt.

Die Sperrliste dient zur Überprüfung der vom Public Key Service herausgegebenen nicht qualifizierten Zertifikate.

2 Profil der Sperrliste

Der generelle Aufbau der Sperrliste entspricht der Norm X.509 und hat folgende Struktur:

```
CertificateList ::= SEQUENCE
{
        tbsCertList         TBSCertList
        signatureAlgorithm      AlgorithmIdentifier
        signatureValue        BIT STRING
}

TBSCertList ::= SEQUENCE
{
        version       Version OPTIONAL
        signature        AlgorithmIdentifier
        issuer        Name
        thisUpdate          Time
        nextUpdate          Time OPTIONAL
        revokedCertificates ::= SEQUENCE
        {
          userCertificate    CertificateSerialNumber
          revocationDate     TIME
          crlEntryExtensionsExtensions OPTIONAL
        }
        crlExtensions      [0] EXPLICIT Extensions Optional
}
```

Die Datentypen der verwendeten Felder der Sperrliste und deren mögliche Inhalte werden in den folgenden Kapiteln erläutert.

2.1 Übersicht über die Felder der Sperrliste

Die folgende Tabelle zeigt alle möglichen Felder innerhalb der Sperrliste, die von TeleSec genutzt werden. Nicht verwendete Felder werden in der Tabelle nicht aufgeführt.

In Tabelle 1 werden die Felder der Struktur `CertificateList` dargestellt.

Name der Feldes	Bedeutung	Wert
tbsCertList	Inhalt der Sperrliste	siehe Tabelle 2
signatureAlgorithm	Algorithmus der Signatur der Sperrliste	sha-256WithRsaEncryption
signatureValue	Signatur der Sperrliste	BIT STRING

Tabelle 1: Inhalt der Struktur `CertificateList`

Die folgende Tabelle stellt die Felder der Struktur `TBSCertList` dar. Diese Struktur befindet sich zusammen mit der Signatur und dem dazu verwendeten Algorithmus in der kodierten Sperrliste.

Name des Feldes	Bedeutung	Wert
version	Versionsnummer für die verwendete Sperrlisten-struktur	1 (Version 2)
signature	Algorithmus der Signatur der Sperrliste	sha-256WithRsaEncryption
issuer	Name des Herausgebers der Sperrliste	z.B. C=DE / O=T-Systems International GmbH / OU=Trust Center Deutsche Telekom / CN=TeleSec PKS CA 7:PN
thisUpdate	Erstellungsdatum der Sperrliste	z.B. 02.04.2018 09:20:23 GMT
nextUpdate	Nächte Aktualisierung der Sperrliste	z.B. 02.04.2018 10:20:23 GMT
revokedCertificates	Liste der Zertifikatsnummern gesperrten Zertifikate einschließlich Sperrdatum	z.B. Zertifikatsnummer 123456, Sperrdatum 01.04.2018 20:23:57 GMT
CrlExtensions		
authorityKeyIdentifier	Informationen zur Identifizierung des öffentlichen Schlüssels des Aussteller-Zertifikates	z.B. keyIdentifier = OCTET STRING mit einer Länge von 20 Bytes
crlNumber	Laufende Nummer der Sperrliste	z.B. 1357

Tabelle 2: Inhalt der Struktur `TBSCertList`

2.2 Die Felder der Struktur CertificateList

2.2.1 Das Feld tbsCertList

siehe Kapitel 2.3

2.2.2 Das Feld signatureAlgorithm

Das Feld `signatureAlgorithm` enthält den Signaturalgorithmus, der von der CA für die Erstellung der Sperrliste benutzt wird. Der Inhalt dieses Feldes hat folgende Struktur:

```
AlgorithmIdentifier ::= SEQUENCE
{
     algorithm       OBJECT IDENTIFIER
     parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

Folgender Algorithmus wird verwendet:

sha-256WithRsaEncryption {1.2.840.113549.1.1.11}

Das Feld `parameters` kann zusätzliche Parameter des Algorithmus enthalten. Für den verwendeten Algorithmus (RSA) werden sie jedoch nicht benötigt, deshalb ist dieses Feld Null (explizit NULL).

2.2.3 Das Feld signatureValue

Das Feld `signatureValue` enthält die Signatur der Sperrliste, die von der Zertifizierungsstelle erzeugt worden ist.

Der Typ des Feldes `signatureValue` ist BIT STRING.

2.3 Die Felder der Struktur TBSCertList

2.3.1 Das Feld version

In dem Feld `version` wird die Version der Datenstruktur der Sperrliste kodiert. Alle Sperrlisten müssen die Versionsnummer v2 haben, da nur in dieser Version Extensions enthalten sein dürfen. Der Datentyp von `version` ist INTEGER und hat immer den Wert 1 (entspricht v2).

2.3.2 Das Feld signature

Das Feld `signature` enthält den Bezeichner des Signaturalgorithmus, der von der CA für die Erstellung der Sperrliste benutzt wird. Der Inhalt und die Struktur dieses Feldes sind identisch mit dem Feld `signatureAlgorithm` (siehe Kapitel 2.2.2).

2.3.3 Das Feld issuer

In dem Feld `issuer` wird der Name des Herausgebers abgelegt. Der Inhalt dieses Feldes muss exakt mit dem Inhalt des Subject-Feldes des CA-Zertifikates übereinstimmen, von dem die Sperrliste unterschrieben worden ist.

Folgende Attribute werden verwendet:

- countryName (vorgeschrieben)
- organizationName (vorgeschrieben)
- organizationalUnitName (optional)
- commonName (optional)

Das Feld hat die folgende Datenstruktur:

```
Name ::= CHOICE {RDNSequence}

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE

{

   type      AttributeType
```

```
   value      AttributeValue
}

AttributeType ::== OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
```

2.3.4 Das Feld thisUpdate

In diesem Feld wird das Generierungsdatum der Sperrliste eingetragen. Der Inhalt des Feldes hat folgende Syntax:

```
Time ::= CHOICE
{
      utcTime    UTCTime
      generalizedTime GeneralizedTime
}
```

Die Uhrzeit wird bis zum Jahr 2049 als UTCTime kodiert werden. Ab dem Jahr 2050 wird die Kodierung GeneralizedTime verwendet.

2.3.5 Das Feld nextUpdate

In diesem Feld wird der Zeitpunkt eingetragen, zu dem die nächste aktualisierte Sperrliste spätetstens erstellt wird. Dieser Zeitpunkt darf nicht als Gültigkeitsende der Sperrliste betrachtet werden. Der Inhalt des Feldes hat die gleiche Syntax: wie das Feld `thisUpdate` (siehe Kapitel 2.3.4). Dieses Feld ist optional, es ist aber immer vorhanden.

2.3.6 Das Feld revokedCertificates

Dieses Feld enthält die Liste der gesperrten Zertifikate. Zu jedem gesperrten Zertifikat gibt es einen Eintrag mit Zertifikatsnummer, Sperrzeitpunkt.

Der Inhalt des Feldes hat folgende Syntax:

```
revokedCertificates ::= SEQUENCE OF SEQUENCE
{
   userCertificate      CertificateSerialNumber
   revocationDate       TIME
   crlEntryExtensions   Extensions OPTIONAL
}
```

Das Feld `userCertificate` enthält die Zertifikatsnummer des gesperrten Zertifikats.

Der Sperrzeitpunkt wird in dem Feld `revocationDate` als GMT-Zeit abgelegt.

Das Feld `crlEntryExtension` wird nicht verwendet.

2.3.7 Das Feld crlExtensions

Die Extensions dienen zur Erweiterung der in der Sperrliste enthaltenen Daten. Es gibt mehrere verschiedene Extensions, die in den folgenden Unterkapiteln aufgeführt werden.

Die Extensions haben folgende Syntax:

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE
{
   extnId       OBJECT IDENTIFIER
   critical        BOOLEAN DEFAULT FALSE
   extnValue       OCTET STRING
}
```

Der Wert `extnId` gibt mit Hilfe eines Object Identifiers den Typ der in `extnValue` enthaltenen Extension an. Das Flag `critical` zeigt an, ob die Extension als kritisch markiert worden ist. Wenn `critical` auf TRUE gesetzt wird, bedeutet dies, dass der Client die Sperrliste als ungültig betrachten muss, wenn er die Extension nicht auswerten kann.

2.3.7.1 Die Extension AuthorityKeyIdentifier

Diese Extension dient zur eindeutigen Identifizierung des Ausstellerzertifikates, mit dem die Sperrliste unterschrieben worden ist.

Diese Extension wird als nicht kritisch markiert und ist immer vorhanden.

Die Extension AuthorityKeyIdentifier hat folgende Datenstruktur:

```
AuthorityKeyIdentifier ::= SEQUENCE
{
   keyIdentifier        [0] IMPLICIT KeyIdentifier OPTIONAL
   authorityCertIssuer    [1] IMPLICIT GeneralNames OPTIONAL
   authorityCertSerialNumber [2] IMPLICIT CertificateSerialNumber
OPTIONAL
}
```

Das Feld `keyIdentifier` enthält einen eindeutigen Wert zur Identifizierung des öffentlichen Schlüssels des Herausgebenden CA-Zertifikats. Der Wert enthält den mit dem Algorithmus SHA-256 berechneten Hashwert über den subjectPublicKey des CA-Zertifikates (ohne die Bytes Tag, Länge und nicht benutzte Bits).

Die Felder `authorityCertIssuer` und `authorityCertSerialNumber` werden nicht verwendet.

2.3.7.3 Die Extension CrlNumber

Diese Extension enthält eine positive Seriennummer (maximal 20 Bytes), die von der Zertifizierungsstelle fortlaufend für die Sperrlisten vergeben wird.

Diese Extension wird als nicht kritisch markiert und ist immer vorhanden.

Die Syntax der Extension ist `Integer`.

Abkürzungsverzeichnis

CA	Certification Authority
CRL	Certificate Revocation List
HTTP	Hypertext Transmission Protocol
LDAP	Lightweight Directory Access Protocol
PN	Pseudonym