Public Key Service

Profil der qualifizierten Attributzertifikate

Version: 2.0
Stand: 01.08.2017
Status: Freigegeben

Öffentliches Dokument

Business flexibility T · · Systems · · ·

Impressum

Herausgeber
T-Systems International GmbH

Dateiname	Dokumentennummer	Dokumentenbezeichnung
PKS Zertifikatsprofil qual Attr v2.doc		Spezifikation

Version	Stand	Status
2.0	01.08.2017	Freigegeben

Kurzinfo
Zertifikatsprofil der qualifizierten PKS Attribut-Zertifikate

Inhaltsverzeichnis

1 Einleitung

Seit Umsetzung der eIDAS Verordnung werden keine weiteren Attributzertifikate mehr produziert. Diese sind nicht mehr Bestandteil der eIDAS Verordnung und dürfen daher für qualifizierte Zertifikate nicht weiter angeboten werden.

Dieses Dokument bleibt erhalten um das Zertifikatsprofil von in der Vergangenheit produzierten Attributzertifikaten zu dokumentieren.

Die in dem jeweiligen Zertifikattyp enthaltenen Daten werden ausgehend von der jeweils grundlegenden Struktur gemäß X.509 [X509] erläutert. Dabei werden die Felder und mögliche Inhalte, sowie die zu verwendenden Datentypen festgelegt.

2 Profil der Attributzertifikate

Der Aufbau des Attributzertifikates entspricht der Norm X.509_v3 und hat die folgenden Syntax.

```
AttributeCertificate ::= SEQUENCE
{
        acInfo       AttributeCertificateInfo
        signature  Algorithm  AlgorithmIdentifier
        signatureValue    BIT STRING
}

AttributeCertInfo ::= SEQUENCE
{
      version     AttCertVersion DEFAULT v1
      subject   CHOICE
        {
          baseCertificateID [0] EXPLICIT IssuerSerial
          subjectName     [1] EXPLICIT GeneralNames
        }
      issuer         GeneralNames
      signature         AlgorithmIdentifier
      serialNumber      CertificateSerialNumber
      attrCertValidityPeriod AttCertValidityPeriod
      attributes           SEQUENCE OF Attribute
      issuerUniqueID       UniqueIdentifier OPTIONAL
      extensions           Extensions OPTIONAL
}
```

2.1 Übersicht über die Felder des Attributzertifikates

Die folgende Tabelle zeigt alle möglichen Felder innerhalb des Zertifikates, die von TeleSec genutzt werden. Die Extensions werden zusätzlich mit P (Pflicht, immer vorhanden), B (bedingt Pflicht) oder O (optional) gekennzeichnet.

Name des Feldes	Bedeutung	Wert
Version	Versionsnummer für die verwendete Attributzertifikatsstruktur	0 (Version 1), Default (wird nicht kodiert)
Subject	Referenz auf den Inhaber des Zertifikates mittels der Zertifikatsnummer und dem Herausgeber des Basiszertifikates	Herausgeber: C=DE / O=Deutsche Telekom AG / OU=T-TeleSec / CN=TeleSec SigG CA 1:PN Zertifikatsnummer: 1234
Issuer	Name des Herausgebers des Zertifikates	z.B. C=DE / O=Deutsche Telekom AG / OU=T-TeleSec / CN=TeleSec SigG CA 1:PN
Signature	Algorithmus der Signatur des Zertifikates	RSA-PSS
SerialNumber	Eindeutige Zertifikatsnummer innerhalb der CA	z.B. 1235
AttrCertValidityPeriod	Gültigkeitszeitraum des Attributzertifikates	z.B. vom 02.04.2002 09:20:23 bis zum 02.04.2005 09:20:23
Attributes	Inhalt des Attributzertifikats	z.B. Prokura für Person x erlaubt oder Identifikationsdaten: sn=Mustermann, gn=Herbert, dateAtBirth=08.11.1963, placeOfBirth=Musterhausen
SignatureAlgorithm	Algorithmus, mit dem das Attributzertifikat signiert worden ist	RSA-PSS
SignatureValue	Signatur des Attributzertifikates	BIT STRING

Extensions			Bemerkung
AuthorityKeyIdentifier	P	Informationen zur Identifizierung des öffentlichen Schlüssels des Aussteller-Zertifikates	keyIdentifier = OCTET STRING mit einer Länge von 20 Bytes
CertificatePolicy	P	Information, unter welchen Bedingungen das Zertifikat erstellt wurde und unter welchen Bedingungen es genutzt werden darf	Wert isismtt-cp-sigconform und die URL der CPS
AuthorityInfoAccess	P	Liefert die Adresse (URL) des OCSP-Servers für die Prüfung von Zertifikaten.	http://pks.telesec.de/ocspr
QCStatement	P	Indikator dafür, dass es sich um ein qualifiziertes Zertifikat handelt. Eine Selbstbeschränkung (QcEuLImitValue) kann mit diesem Feld hier nicht vorgenommen werden.	ID = id_etsi_qcs_qcCompliance

2.2 Das Feld Version

Dieses Feld gibt die Versionsnummer der Struktur des Attributzertifikats an. Der Wert ist immer 0 (Default, Version 1) und wird im Attributzertifikat nicht kodiert.

2.3 Das Feld Subject

Das Feld `subject` enthält Informationen über den Inhaber des Zertifikates. Die Daten werden in dem Feld `baseCertificateID` vom Typ `IssuerSerial` gespeichert.

```
IssuerSerial ::= SEQUENCE
{
    issuer        GeneralNames
    serial        CertificateSerialNumber
```

```
    issuerUID       UniqueIdentifier OPTIONAL
}
```

Das Feld `issuer` enthält genau den DName des Issuers des Basiszertifikates. Die Zertifikatsnummer des Basiszertifikates wird im Feld `serial` abgelegt.

Das Feld `issuerUID` wird nicht verwendet.

2.4 Das Feld Issuer

In diesem Feld wird der Herausgeber des Attributzertifikates abgelegt. Der Datentyp ist GeneralNames und enthält genau den einen DName des Herausgebers.

Anmerkung:

Der Inhalt des Feldes Issuer wird aus dem Subject-Feld des CA-Zertifikates entnommen von dem das Attributzertifikat später unterschrieben werden soll.

2.5 Das Feld Signature

Dieses Feld enthält den Signaturalgorithmus mit dem das Attributzertifikat von der Zertifizierungsstelle unterschrieben worden ist.

Der Inhalt dieses Feldes hat folgende Struktur:

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

Folgender Algorithmus wird verwendet:

- RSA-PSS {1.2.840.113549.1.1.10} ab 10.12.2015
- sha256WithRsaEncryption {1.2.840.113549.1.1.11} ab 31.12.2007
- vor 31.12.2007 sha1WithRSAEncryption

Das Feld `parameters` kann zusätzliche Parameter des Algorithmus enthalten.

Für den Algorithmus RSA-PSS werden hier die verwendeten Hashalgorithmen zur Erstellung des PSS-Paddings eingetragen. Für qualifizierte Zertifikate werden vom Trust Center der Deutschen Telekom AG dort sha256 Hashwerte (OID: 2.16.840.1.101.3.4.2.1) verwendet.

Für die Signaturverfahren sha1WithRSAEncryption und sha256WithRSAEncryption wird dieser Parameter nicht benötigt, deshalb ist dieses Feld Null (explizit NULL).

2.6 Das Feld SerialNumber

In diesem Feld wird die Zertifikatsnummer abgelegt. Diese Zertifikatsnummer muss innerhalb des Zertifizierungsbereiches (gleicher Issuer) eindeutig sein. Der Datentyp der Zertifikatsnummer ist INTEGER und muss immer positiv sein. Die maximale Länge des kodierten Wertes darf 20 Bytes (1 <= Zertifikatsnummer < 2^{159}) nicht überschreiten.

2.7 Das Feld AttrCertValidityPeriod

In diesem Feld wird der Gültigkeitszeitraum des Attributzertifikates eingetragen. Der Inhalt des Feldes hat folgende Syntax:

```
AttrCertValidityPeriod ::= SEQUENCE
{
    notBeforeTime     GeneralizedTime
    notAfterTime    GeneralizedTime
}
```

Die Uhrzeit wird immer im Format YYYYMMDDHHMMSSZ kodiert werden. Die Gültigkeit des Attributzertifikates endet immer mit der Gültigkeit des Basis-Zertifikates.

2.8 Das Feld Attributes

Dieses Feld wird zum Einfügen zusätzlicher Informationen über bzw. Einschränkungen für den Zertifikatsinhaber verwendet.

In Kapitel 3 wird eine Profilierung der Attributzertifikate für unterschiedliche Verwendungszwecke durchgeführt. Dort wird auch festgelegt, welche Attribute in welchem Typ von Attributzertifikat vorhanden sein müssen oder dürfen.

```
Attributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
Attribute ::= SEQUENCE
{
 type      AttributeType
 values    SET OF AttributeValue
}
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
```

Die folgenden Attribute werden unterstützt:

- Restriction:

  Dieses Attribut wird für die Aufnahme von Einschränkungen in das Zertifikat verwendet.

  Die Extension Restriction hat die folgende Datenstruktur:

  ```
  RestrictionSyntax ::= DirectoryString
  ```

  Die Länge des Strings wird auf 1000 Zeichen beschränkt. Der Inhalt der Extension `Restriction` wird als PrintableString kodiert.

- AdditionalInformation

  Dieses Attribut wird für die Integration von Informationen mit nicht einschränkendem Charakter in das Zertifikat verwendet.

  Die Extension AdditionalInformation hat die folgende Datenstruktur:

  ```
  AdditionalInformationSyntax ::= DirectoryString
  ```

  Die Länge des Strings wird auf 2000 Zeichen beschränkt. Der Inhalt der Extension `AdditionalInformation` wird als PrintableString kodiert.

2.9 Das Feld Extensions

Die Extensions dienen zur Erweiterung der im Attributzertifikat 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 das Zertifikat als ungültig betrachten muss, wenn er die Extension nicht auswerten kann.

2.9.1 Die Extension AuthorityKeyIdentifier (vorgeschrieben)

Diese Extension dient zur eindeutigen Identifizierung des Ausstellerzertifikates, mit dem das Benutzerzertifikat unterschrieben worden ist.

Diese Extension wird als nicht kritisch markiert.

Die Extension AuthorityKeyIdentifier hat folgende Datenstruktur:

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

```
 authorityCertSerialNumber [2]  IMPLICIT  CertificateSerialNum-
 ber
                                                          OPTIO-
                                                             NAL
}
```

Das Feld `keyIdentifier` enthält einen eindeutigen Wert zur Identifizierung des öffentlichen Schlüssels des Herausgebenden CA-Zertifikats. Der Wert enthält den mit dem Algorithmus SHA-1 (160 bit) 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.

2.9.2 Die Extension AuthorityInfoAccess (vorgeschrieben)

Diese Extension enthält eine URL, unter der ein OCSP-Server für die Zertifikatsprüfung angesprochen werden kann.

Diese Extension wird als nicht kritisch markiert.

Die Extension AuthorityInfoAccess hat folgenden Aufbau:

```
AuthorityInfoAccessSyntax ::=
             SEQUENCE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE
{
       accessMethod   OBJECT IDENTIFIER
       accessLocation    GeneralName
}
```

Als Zugriffsmethode wird im Feld `accessMethod` der Wert `id-ad-ocsp` verwendet. Der Zugriffsort wird über eine URL im Feld `accessLocation` beschrieben.

2.9.3 Die Extension CertificatePolicies (vorgeschrieben)

Diese Extension legt die Bedingungen fest, unter denen das Zertifikat herausgegeben wurde und unter denen es verwendet werden darf.

Diese Extension wird als nicht kritisch markiert.

```
CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF
                                                PolicyInformation
PolicyInformation ::= SEQUENCE
{
 policyIdentifier     CertPolicyId
policyQualifiers     SEQUENCE SIZE (1..MAX) OF
PolicyQualifierInfo OPTIONAL
}
CertPolicyId ::= OBJECT IDENTIFIER
PolicyQualifierInfo ::= SEQUENCE
{
 policyQualifierId PolicyQualifierId
 qualifier       ANY DEFINED BY policyQualifierId
}
PolicyQualifierId ::= OBJECT IDENTIFIER {id-qt-cps | id-qt-
unotice}
```

Als `policyIdentifier` wird immer id-isismtt-cp-sigconform {1 3 36 8 1 1} ohne zusätzliche `PolicyQualifierInfo`

2.9.4 Die Extension QCStatements (vorgeschrieben)

Mit dieser Extension wird festgelegt, dass es sich um ein qualifiziertes Zertifikat handelt.

Diese Extension wird als nicht kritisch markiert.

Die Extension QCStatements hat folgenden Aufbau:

```
QCStatements ::= SEQUENCE OF QCStatement
QCStatement ::= SEQUENCE
{
 statementId       ObjectIdentifier
 statementInfo        ANY DEFINDED BY statementId OPTIONAL
}
```

Als `statementId` wird der folgende Wert verwendet:

- id-etsi-qcs-QcCompliance zeigt an, dass es sich um ein qualifiziertes Zertifikat handelt, dessen CertificatePolicy konform zu ETSI TS 101 456 v1.1.1 ist und muss vorhanden sein.

2.10 Das Feld SignatureAlgorithm

Dieses Feld enthält den Algorithmus, mit dem das Zertifikat von der Zertifizierungsstelle unterschrieben worden ist. Der Inhalt und die Kodierung sind identisch mit dem Feld Signature (siehe Kapitel 2.5).

2.11 Das Feld SignatureValue

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

Der Typ des Feldes `signatureValue` ist BIT STRING.

3 Typen von Attributzertifikaten

Attributzertifikate werden in die folgenden Typen unterstützt:

- Attributzertifikat für sonstige Einschränkungen
- Attributzertifikat für Prokura
- Attributzertifikat für die Erlaubnis zur Ausübung von bestimmten Tätigkeiten
- Attributzertifikat für allgemeine Zusatzinformationen.

In den folgenden Kapiteln werden die in den unterschiedlichen Attributzertifikattypen enthaltenen Attribute näher beschrieben.

3.1 Das Attributzertifikat für sonstige Einschränkungen

Dieser Attributzertifikatstyp kann für die Einschränkung von anderen Vorgängen wie den oben beschriebenen verwendet werden. Es kann eine Einschränkung in Textform mit bis zu 1000 Zeichen formuliert und in das Zertifikat übernommen werden.

Dieses Attributzertifikat enthält das folgende Attribut:

- restrictions (vorgeschrieben).

3.2 Das Attributzertifikat für allgemeine Zusatzinformationen

Dieser Attributzertifikatstyp kann für die Integration von

- Vertretungsmacht für einen Dritten (Prokura),
- berufsbezogenen Angaben oder
- beliebiger Informationen ohne einschränkende Wirkung

verwendet werden.

Es kann eine Information in Textform mit bis zu 2000 Zeichen formuliert und in das Zertifikat übernommen werden.

Dieses Attributzertifikat enthält das folgende Attribut:

additionalInformation (vorgeschrieben).

Anhang A: Verwendete Attributtypen

Name des Attributs	Object Identifier	ASN.1 String Typ	maximale Länge
commonName	{id-at 3}	UTF8	64
surName	{id-at 4}	UTF8	64
givenName	{id-at 42}	UTF8	64
serialNumber	{id-at 5}	PrintableString	64
title	{id-at 12}	UTF8	64
organizationName	{id-at 10}	UTF8	64
organizationalUnitName	{id-at 11}	UTF8	64
BusinessCategory	{id-at 15}	UTF8	128
localityName	{id-at 7}	UTF8	128
stateOrProvinceName	{id-at 8}	UTF8	128
countryName	{id-at 6}	PrintableString	2 (ISO 3166 Code)
distinguishedNameQualifier	{id-at 46}	PrintableString	64
initials	{id-at 43}	UTF8	64
generationQualifier	{id-at 44}	UTF8	64
eMailAddress	{pkcs-9 1}	IA5String	128
domainComponent	{0 9 2342 19200300 100 1 25}	IA5String	definiert in RFC 2247
postalAddress	{id-at 16}	SEQUENCE SIZE (1..6) OF UTF8	6 * 30, Verwendung wird in RFC 3039 beschrieben
pseudonym	{pkix 9 3}	UTF8	64
dateOfBirth	{id-pda 1}	GeneralizedTime	15
placeOfBirth	{id-pda 2}	UTF8	128
gender	{id-pda 3}	PrintableString SIZE (1)	Inhalt: „M“ oder „F“
countryOfCitizenship	{id-pda 4}	PrintableString	2 (ISO 3166 Code)
countryOfResidence	{id-pda 5}	PrintableString	2 (ISO 3166 Code)
nameAtBirth	{id-isismtt-at 14}	UTF8	64

Für die UTF8-Kodierung wird einen Auszug aus dem UTF8-Zeichensatz verwendet, der nur ANSI / ISO 8859-1 Zeichen (Unicode Latin-1 Seite) enthält. Andere Zeichen, die nicht in diesem Zeichensatz enthalten sind, dürfen nicht benutzt werden.

Abkürzungsverzeichnis

CA	Certification Authority
eIDAS	EU Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
HTTP	Hypertext Transmission Protocol
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol

Literaturverzeichnis

[COMMON-PKI]	COMMON-PKI Core Specification, Version 2.0, 20. Januar 2009
[X509]	Recommendation X.509: The Directory – Authentication Frame