Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie TR-03109

Anhang C: Public Key Infrastruktur für Smart Meter Gateways

Version: 0.20 - Stand 10.10.2011

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Smart Meter Gateway (SM-GW) ist die zentrale Kommunikationseinheit in der Infrastruktur eines Messsystems. Das Gateway kommuniziert im lokalen Bereich beim Endkunden mit den elektronischen Zählern (Local Metrological Network, LMN-Bereich), mit Geräten aus dem Home Area Network (HAN-Bereich) und im Wide Area Network (WAN-Bereich) mit autorisierten Marktteilnehmern. Außerdem ermöglicht das SM-GW die Verbindungsaufnahme von lokalen Geräten des HANs über das WAN mit autorisierten Marktteilnehmern.

Für die Verbindung des SM-GWs zu einem autorisierten Marktteilnehmer im WAN ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dann stets über einen verschlüsselten, integritätsgesicherten Kanal. Zudem werden zu sendende Daten vom SM-GW zusätzlich auf Datenebene verschlüsselt und signiert.

In dem vorliegenden Dokument wird die Architektur der Smart Meter - Public Key Infrastruktur (SM-PKI) spezifiziert, welche die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner sicherstellt. Die SM-PKI bildet damit die Grundlage für die Absicherung der Kommunikation in der Infrastruktur.

Des Weiteren werden in dieser Technischen Richtlinie die Mindestanforderungen an die Interoperabilität und die Sicherheit der PKI aufgestellt, die in der Zertifizierungsrichtlinie (Certificate Policy, CP) für die SM-PKI berücksichtigt werden müssen. Es werden Profile für die einzusetzenden Zertifikate und Sperrlisten vorgegeben. Ferner werden Protokolle für die Beantragung und Zustellung von Zertifikaten spezifiziert.

1.1 Einordnung des Dokuments

Das vorliegende Dokument spezifiziert die Architektur sowie die Mindestanforderungen an die Interoperabilität und Sicherheit der SM-PKI. Darüber hinaus sind die folgenden Dokumente für die SM-PKI zu berücksichtigen:

- **Technische Richtlinie BSI TR-03109 [1]:**

  Diese TR spezifiziert Sicherheitsanforderungen und Interoperabilitätseigenschaften an die Kommunikationseinheit von Messsystemen, beschreibt die Rollen der Marktteilnehmer in der Infrastruktur von Messsystemen und liefert damit die Grundlage für die SM-PKI.

- **Technische Richtlinie TR-03109 Anhang: Kryptographische Vorgaben für die Infrastruktur von Messsystemen [2]**:

  In diesem Anhang zur Technischen Richtlinie werden die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur von Messsystemen im Energiesektor beschrieben. Insbesondere wird dort definiert, welche kryptographischen Algorithmen und Schlüssellängen für die Zertifikate in der SM-PKI eingesetzt werden müssen.

- **Certificate Policy** der Root-CA (Root-CP):

  In der Certificate Policy werden organisatorische und technische Anforderungen für das Anerkennen, Ausstellen,Verwalten, Benutzen, Zurückziehen und Erneuern von Zertifikaten zur Kommunikation zwischen SM-GW und Marktteilnehmern spezifiziert. Die Certificate Policy wird von der Root-CA erstellt und hat die Mindestanforderungen aus dem hier vorliegenden Dokument zu berücksichtigen.

1.2 Abkürzungen

Abkürzung	Begriff
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Certificate
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List (Zertifikatssperrliste)
Enc	Encryption
ENu	Endnutzer (Dazu gehören externe Marktteilnehmer, GW-Administrator und SM-GW)
GW	Gateway
GWA	Gateway-Administrator
HAN	Home Area Network
HSM	High Security Module
KM	Kryptografiemodul
LMN	Local Metrological Network
EMT	Externer Marktteilnehmer
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PP	Protection Profile (Common Criteria)
RA	Registration Authoritiy
Sign	Signature
SM-GW	Smart Meter Gateway
SM-PKI	Smart Meter - Public Key Infrastruktur (SM-PKI)
TLS	Transport Layer Security
TR	Technische Richtlinie
WAN	Wide Area Network
Z	Zertifikat

2 Architektur der PKI

Die SM-PKI hat die folgende dreistufige hierarchische Struktur:

- **Hoheitlicher Vertrauensanker (Root-CA)**
- **Endnutzerzertifizierung (Sub-CA)**
- **Endnutzer: Marktteilnhmer, GW-Admin und SM-GW**

In Abbildung 1 ist die hierarchische Struktur der PKI exemplarisch dargestellt. Die Rolle der Instanzen wird im Folgenden genauer erläutert.

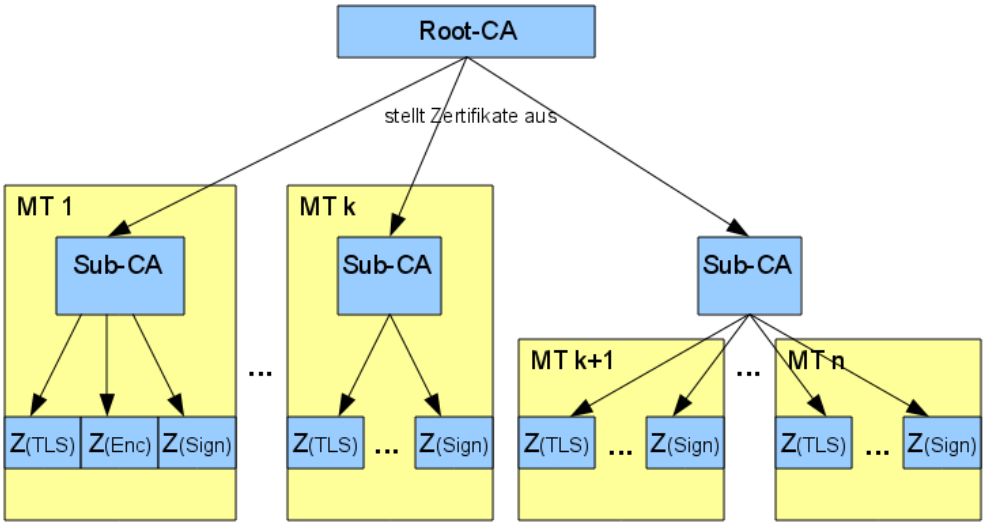

Abbildung 1: Architektur der PKI (Beispiel)

2.1 Root-CA

2.1.1 Beschreibung

Die **Root-CA** bildet den Vertrauensanker der PKI. Sie stellt Zertifikate für die Sub-CAs aus.

Die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten werden von der Root-CA in einer Certificate Policy (Root-CP) unter Berücksichtigung der in diesem Dokument vorgegebenen Mindestanforderungen festgelegt.

2.1.2 Zertifikate der Root-CA

Die Root-CA besitzt ein Root-Zertifikat *C(Root)*. Es bildet den Trust-Point der PKI und ist bei der Root-CA erhältlich.

Das initiale Root-Zertifikat ist mit dem privaten Schlüssel des Zertifikats selbst-signiert. Folgende Root-Zertifikate werden sowohl als selbst-signierte Zertifikate als auch Link-Zertifikate, jeweils signiert mit dem privaten Schlüssel des vorhergehenden Root-Zertifikats, veröffentlicht.

Der private Schlüssel des Root-Zertifikats wird dazu eingesetzt die Sub-CA Zertifikate zu signieren.

Zertifikat	***Signatur des Zertifikats***	***Funktion***
C(Root)	Initial: Selbst-signiert Nicht-Initial: Sowohl selbst-signiert als auch signiert mit dem privaten Schlüssel des vorigen Root-Zertifikats	Signatur der Sub-CA-Zertifikate

Tabelle 1: Zertifikate der Root-CA

2.1.3 Rückruflisten der Root-CA

Die Root-CA ist verantwortlich für die Erstellung, Pflege und Bereitstellung aktueller Listen zurückgerufener Root-CA- und Sub-CA-Zertifikate.

2.2 Sub-CA

2.2.1 Beschreibung

Eine **Sub-CA** ist eine Organisationseinheit, welche Zertifikate für die Endnutzer ausstellt. Jede Sub-CA wird dazu von der Root-CA zur Ausstellung von Kommunikationszertifikaten für die Endnutzer autorisiert.

Eine Sub-CA kann unternehmensintern bei einem Marktteilnehmer oder unternehmensübergreifend betrieben werden. Dementsprechend kann eine Sub-CA ausschließlich einen Marktteilnehmer mit Zertifikaten versorgen oder für mehrere Endnutzer zuständig sein.

Jede Sub-CA muss eine Zertifikatspolicy (Sub-CP) erstellen und dabei die übergeordnete Root-CP beachten.

2.2.2 Zertifikate einer Sub-CA

Eine Sub-CA besitzt ein Zertifikat *C(Sub-CA)*. Dieses wird der Sub-CA von der Root-CA ausgestellt. Der private Schlüssel des Sub-CA-Zertifikats dient zur Signatur von Endnutzer-Zertifkaten.

Zertifikat	*Signatur des Zertifikats*	*Funktion*
C(Sub-CA)	Privater Schlüssel zu *C(Root)*	Signatur von Endnutzerzertifikaten

Tabelle 2: Zertifikate einer Sub-CA

2.2.3 Rückruflisten einer Sub-CA

Jede Sub-CA ist verantwortlich für die Erstellung, Pflege und Bereitstellung aktueller Listen der von ihr ausgestellten zurückgerufenen Endnutzerzertifikate.

2.3 Endnutzer: Externe Marktteilnehmer, GW-Administrator und SM-GW

2.3.1 Beschreibung

Den Endnutzern werden Zertifikate von ihren Sub-CAs unter Berücksichtigung der Vorgaben dieser Technischen Richtlinie ausgestellt. Der Besitz dieser Zertifikate ist die Voraussetzung für eine mögliche Kommunikation zwischen den Marktteilnehmern und den SM-GWs.

Es gibt verschiedene Typen von Endnutzern:

- **Externe Marktteilnehmer (EMT)**
- **Gateway-Administrator (GWA)**
- **Smart Meter Gateway (SM-GW)**

Zu den externen Marktteilnehmer gehören im Kontext der PKI alle Marktteilnehmer, die potentielle Kommunikationspartner eines Smart Meter Gateway im WAN sind, d.h. Verteilnetzbetreiber, Messstellenbetreiber, Messdienstleister und Lieferanten.

Der wichtigste Kommunikationspartner eines SM-GW, und daher in diesem Dokument gesondert hervorgehoben, ist der Gateway-Adminstrator (siehe [1]). Der Gateway-Administrator ist dafür verantwortlich seine SM-GWs zu konfigurieren und zu überwachen und übernimmt in der PKI die Management-Funktionenen des SM-GWs, welche dieses nicht selbst ausführen kann.

2.3.2 Zertifikatstypen

Die Zertifikate werden zum sicheren Datenaustausch von autorisierten Marktteilnehmern und dem Smart Meter Gateway eingesetzt. Da die Übermittlung von Daten zwischen SM-GW und einem Marktteilnehmer auch über dritte Marktteilnehmer (Messstellenbetreiber) erfolgen kann, muss einerseits die Kommunikationsverbindung abgesichert werden, andererseits müssen die Daten auf Inhaltsebene für den Endempfänger verschlüsselt und signiert werden.

Es gibt also verschiedene Verwendungszwecke für die Zertifikate. Im Folgenden werden die von der Sub-CA ausgestellten Zertifikate und deren Verwendungzwecke beschrieben:

- **TLS-Zertifikate**: Gegenseitige Authentisierung zwischen Smart Meter Gateway und autorisierten Marktteilnehmern sowie Aufbau eines eines verschlüsselten, integritätgesicherten TLS-Kanals zwischen beiden.
- **Verschlüsselungszertifikate**: Ende-zu-Ende-Verschlüsselung von Daten für den Endempfänger (Datenebene, unabhängig von TLS-Verbindungen).
- **Signaturzertifikate**: Erstellung / Prüfung von elektronischen Signaturen.

Pro Verwendungszweck müssen jeweils separate Schlüsselpaare verwendet werden. Ein privater Schlüssel darf ausschließlich für den im Zertifikat definierten Verwendungszweck genutzt werden.

2.3.3 Zertifikate eines externen Marktteilnehmer

Ein externer Marktteilnehmer erhält die benötigten Zertifikate von seiner Sub-CA.

Er muss ein TLS-Zertifikat besitzen, sofern er direkt mit einem SM-GW kommunizieren will. Er muss stets ein Verschlüsselungszertifikat besitzen. Der Besitz eines Signaturszertifikats ist optional.

Zertifikat	***Signatur des Zertifikats***	***Funktion***	***m/c/o***
$C_{TLS}(EMT)$	Privater Schlüssel zu *C(Sub-CA)*	Authentisierung beim Kommunikationspartner und Aufbau eines verschlüsselten, integritätsgesicherten Kanals	c
$C_{Enc}(EMT)$	Privater Schlüssel zu *C(Sub-CA)*	Verschlüsselung für den EMT	m
$C_{Sign}(EMT)$	Privater Schlüssel zu *C(Sub-CA)*	Signatur des EMT	o

Tabelle 3: Zertifikate eines Marktteilnehmers

Autorisierte Marktteilnehmer: Ist ein Marktteilnehmer autorisiert mit einem SM-GW zu kommunizieren (autorisierter Marktteilnehmer), so werden die benötigten, gültigen Zertifikate vom GWA auf dem SM-GW installiert (Zur Beschreibung siehe [1]). Die Installation sowie die Prüfung der Gültigkeit der Zertifikate eines EMT ist Aufgabe des GWA. Erlischt die Autorisierung eines EMT zur Kommunikation mit dem SM-GW oder wird das Zertifikat des EMT zurückgerufen, so müssen durch den GWA unverzüglich vom SM-GW gelöscht werden.

2.3.4 Zertifikate eines Gateway-Administrators

Der GWA besitzt ein TLS-, ein Verschlüsselungs- und ein Signaturzertifkat, welche ihm von seiner Sub-CA ausgestellt werden.

Zertifikat	*Signatur des Zertifikats*	*Funktion*	*m/c/o*
$C_{TLS}(GWA)$	Privater Schlüssel zu *C(Sub-CA)*	TLS-Zertifikat von GW-Administrator	m
$C_{Enc}(GWA)$	Privater Schlüssel zu *C(Sub-CA)*	Verschlüsselung für GW-Administrator	m
$C_{Sign}(GWA)$	Privater Schlüssel zu *C(Sub-CA)*	Signatur von GW-Administrator	m

Tabelle 4: Zertifikate des GWAs

Besitzt der GWA auch gleichzeitig die Rolle eines EMT, so sind keine getrennten Zertifikate für Rollen als EMT bzw. als GWA notwendig.

2.3.5 Zertifikate eines Smart Meter Gateways

Jedem SM-GW werden folgende Zertifikate der zugehörigen Sub-CA ausgestellt. Die Zertifikate werden zusammen mit den zugehörigen privaten Schlüsseln bei Produktion auf einem Kryptographiemodul (KM) des SM-GWs gespeichert.

Zertifikat	*Signatur des Zertifikats*	*Funktion*	*m/c/o*
$C_{TLS}(SM\text{-}GW)$	Privater Schlüssel zu *C(Sub-CA)*	TLS-Zertifikat des SM-GWs	m
$C_{Enc}(SM\text{-}GW)$	Privater Schlüssel zu *C(Sub-CA)*	Verschlüsselung für SM-GWs	m
$C_{Sign}(SM\text{-}GW)$	Privater Schlüssel zu *C(Sub-CA)*	Signatur des SM-GWs	m

Tabelle 5: Zertifikate des SM-GWs

Bemerkung (informativ): Außerdem werden schon bei Produktion das TLS-, das Verschlüsselungs- und das Signatur-Zertifikat auf dem Sicherheitsmodul des SM-GWs gespeichert, um die Authentifikation des GWA durch das SM-GW sicherstellen zu können (siehe auch [1]).

2.3.6 Rückruf von Zertifikaten

-tbd-

2.4 Übersicht der PKI-Teilnehmer und Aufgabenstellungen

Folgende Aufgabenstellungen sind in der PKI gegeben.

- Zertifizierungsstelle

  Stellt Zertifikate für sich oder eine untergeordnete Instanz aus.
- Registrierungsstelle

  Führt die Identifizierung und Authentisierung einer untergeordneten Instanz durch.

- Zertifikatsnehmer

  Bezieht Zertifikate für sich oder von einer übergeordneten Stelle.

- Zertifikatsnutzer

  Verwendet Zertifikate für deren Aufgabenstellung. Hierbei wird zwischen der Nutzung zum Ausstellen von Zertifikaten und der Absicherung der Kommunikation unterschieden.

In der folgenden Tabelle ist eine Übersicht der PKI-Teilnehmer und deren Aufgaben dargestellt.

Instanz der PKI	***Zert.-Stelle***	***Reg.-Stelle***	***Zert.-Nehmer***	***Zert.-Nutzer***	
				Ausstellen	***Kommunikation***
Root-CA	■	■	■	■	
Sub-CA	■	■	■	■	
Endnutzer			■		■

Tabelle 6: Aufgaben der Instanzen in der PKI

2.4.1 Zertifizierungsstellen

In der folgenden Tabelle sind die Zertifizierungsstellen (Certification Authority, CA) und die hiervon ausgegebenen Zertifikate aufgeführt.

PKI-Instanz	**Auszustellende Zertifikate**
Root-CA	*C(Root)*, *C(Sub-CA)*
Sub-CA	C_{TLS}*(ENu)*, C_{Enc}*(ENu)*, C_{Sign}*(ENu)*

2.4.2 Registrierungsstellen

Registrierungsstellen (Registration Authority, RA) führen vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung und Authentifizierung des Antragstellers durch. Die zur Identifizierung und Authentifizierung erforderlichen Prozesse werden in der Certificate Policy der Root-CA festgelegt.

- Die Root-CA betreibt eine RA zur Identifizierung und Authentifizierung der antragstellenden Sub-CAs.
- Jede Sub-CAs muss über eine RA verfügen, um eine Identifizierung und Authentifizierung der Antragssteller von Kommunikationszertifikaten durchzuführen.

3 Zertifikate und Sperrlisten

In diesem Kapitel wird ein Überblick über die Struktur der Zertifikate und Sperrlisten gegeben sowie Datenformate und organisatorische Prozesse beschrieben, die im Zusammenhang mit der Verwendung von Zertifikaten anfallen.

3.1 Struktur der Zertifikate und Sperrlisten

Die Zertifikate bzw. Sperrlisten der SM-PKI sind X.509-Zertifikate bzw. X.509-Sperrlisten gemäß den Vorgaben aus [3].

- Das Zertifikatsprofil wird in Anhang 5.1 spezifiziert.
- Der Signaturalgorithmus, die Domain-Parameter und Schlüssellängen, die in den Zertifikaten zu verwenden sind, werden von [2] vorgegeben.
- Innerhalb einer Zertifikatskette können verschiedene Signaturalgorithmen, Domain-Parameter oder Schlüssellängen verwendet werden (siehe [2]). Folgezertifikate (insbesondere Link-Root-Zertifikate) können zu anderen Algorithmen, Parametern und Schlüssellängen wechseln.
- Als Format für die Sperrlisten soll das Profil aus Anhang 5.2 verwendet werden.

3.2 Zertifikatslaufzeiten

Jedes in der SM-PKI verwendete Zertifikat besitzt eine Gültigkeitszeit und Verwendungszeit für den zugehörigen privaten Schlüssel, welche im Zertifikat angegeben werden.

Die folgende Tabelle 7 gibt die Zertifikatslaufzeiten sowie die Verwendungszeiten der zugehörigen privaten Schlüssel verbindlich vor.

Zertifikat	*Gültigkeitszeit*	*Private Key Usage Period*
Root-Zertifikat	10 Jahre	5 Jahre
Sub-CA-Zertifikat	9 Jahre	3 Jahre
Endnutzerzertifikate	2 Jahre	2 Jahre

Tabelle 7: Zertifikatslaufzeiten

3.3 Zertifikatsupdates

-tbd-

3.4 Zertifikatsvalidierung

Validierungsmodell

Die Validierung der Zertifikate basiert auf dem Schalenmodell.

4 Sicherheit

4.1 Schlüssellängen und kryptografische Algorithmen

Die zu verwendenden kryptographischen Algorithmen und Schlüssellängen sind in [2] spezifiziert. Diese Technische Richtlinie wird fortlaufend aktualisiert unter Berücksichtigung des aktuellen Technologie- und Wissensstands.

4.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

Folgende Systeme der SM-PKI müssen kryptographische Hardwaremodule, sogenannte Kryptographiemodule (KM)**,** zur Generierung, Speicherung und Nutzung des jeweiligen privaten Schlüssels verwenden.

PKI-Instanz	*System*	*Nutzung*
Root-CA	CA	Zertifikatsausstellung
Sub-CA	CA	Zertifikatsausstellung
Endnutzer	EMT	Authentisierung, Verschlüsselung und Integritätssicherung der Kommunikationsverbindungen.
	GWA	Konfiguration des SM-GW. Signatur der Befehle und Berechtigungsprofile.
	SM-GW	Authentisierung, Verschlüsselung und Integritätssicherung der Kommunikationsverbindungen.

Tabelle 8: Übersicht Kryptographiemodule in der SM-PKI

Die Kryptographiemodule können unterschiedlicher Bauart sein und müssen nach folgenden Common Criteria Protection Profiles (PPs) durch das BSI zertifiziert sein.

Root-CA/ Sub-CA / EMT /GWA

- High Security Module (HSM): PP-Cryptographic Modules "moderate“ [4]
- Chipkarten: PP-Secure Signature-Creation Device [5].

SM-GW:

- Chipkarte: PP-Sicherheitsmodule [6].

4.2.1 Erzeugung von Schlüsselpaaren

Das jeweilige kryptographische Schlüsselpaar muss in einem sicheren Kryptographiemodul generiert werden.

Der technische Zugriff auf die Kryptografiemodule aller Zertifikatsnehmer ist durch ein Geheimnis geschützt (Passwort, PIN, o.ä.), welches nur die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptographiemodul, insbesondere zur Schlüsselerzeugung, ist auf ein Minimum an Operatoren beschränkt.

Die Generierung von Schlüsseln durch die Root-CA und auf Sub-CA Ebene erfordert die Einhaltung des 4-Augenprinzips. Zusätzlich muss die Generierung in einer sicheren Umgebung erfolgen.

4.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Prinzip der gegenseitigen Kontrolle muss bei der Zertifikatsausstellung durchgesetzt werden. Ein Operator für die Zertifikatsausstellung darf kein Operator bei der RA sein.

4.3 Physikalische und organisatorische Sicherheitsanforderungen

-tbd-

5 Anhang: Profile für Zertifikate und CRLs

Die Zertifikate, die in dieser PKI ausgegeben werden, sind X.509 Zertifikate und müssen konform zum folgenden Zertifikatsprofil sein.

Dabei wird im Weiteren folgende Terminologie verwendet:

- m (mandatory): Das Feld muss vorhanden sein.
- x (do not use): Das Feld sollte nicht vorhanden sein
- c (conditional): Verwendung des Feldes hängt von Bedingungen ab.
- o (optional): Das Feld kann vorhanden sein.

5.1 Zertifikatsprofile

5.1.1 Zertifikatskörper

Der Zertifkatskörper eines X.509-Zertifikate besitzt gemäß [3] folgende Struktur:

Zertifikatsfeld	*Referenz in [3]*	*m/x/c /o*	*Bemerkung*
`Certificate`	4.1.1		
`TBSCertificate`	4.1.1.1	m	Siehe Tabelle 10.
`SignatureAlgorithm`	4.1.1.2	m	Siehe Abschnitt 5.1.1.1.
`SignatureValue`	4.1.1.3	m	Datenformat: Siehe [7], 4.1.1.3. Wert: Abhängig vom gewählten SignatureAlgorithm

Tabelle 9: Zertifikatskörper

Tabelle 10 gibt die Struktur des Feldes `TBSCertificate` verbindlich vor.

Zertifikatsfeld	*Referenz in [3]*	*m/x/c /o*	*Bemerkung*
`TBSCertificate`	4.1.2	m	
`version`	4.1.2.1	m	Wert: 'v3'
`serialNumber`	4.1.2.2	m	Wert: Eindeutige Nummer bestimmt von der CA (nicht länger als 20 Octets)
`signature`	4.1.2.3	m	Wert: Wie im Feld SignatureAlgorithm.
`Issuer`	4.1.2.4	m	Siehe Abschnitt 5.1.1.2.
`validity`	4.1.2.5	m	Wert: Die Gültigkeitszeiten der Zertifikate sind in Kapitel 3.2 angegeben.
`subject`	4.1.2.6	m	Wert: Siehe Abschnitt 5.1.1.4.
`subjectPublicKey-Info`	4.1.2.7	m	Siehe Abschnitt 5.1.1.3
`issuerUniqueID`	4.1.2.8	x	
`subjectUniqueID`	4.1.2.8	x	
`extensions`	4.1.2.9	m	Kapitel 5.1.2 gibt die vorhandenen Extensions an.

Tabelle 10: Struktur des Feldes `TBSCertificate`

5.1.1.1 SignatureAlgorithm

Durch die Datenstruktur SignatureAlgorithm wird nach [3] der Signaturalgorithmus des Zertifikats angegeben. Dieser besteht aus der folgenden Datenstruktur:

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

Der Wert von `algorithm` wird von [8], Kapitel 3, verbindlich vorgegeben. Das Feld `parameters` bleibt leer.

5.1.1.2 Issuer

-tbd-

5.1.1.3 SubjectPublicKeyInfo

Das Feld `SubjectPublicKeyInfo` muss folgende Struktur besitzen (siehe [9]) :

```
SubjectPublicKeyInfo ::= SEQUENCE {
     algorithm            AlgorithmIdentifier,
```

```
        subjectPublicKey      BIT STRING
    }
```

Die OID in `algorithm` muss den Wert 1.2.840.10045.2.1 (id-ecPublicKey) haben. Als EC-Parameter ist gemäß [9] die Variante `namedCurve` zu verwenden. In Abschnitt 5.4 sind die OIDs der von dieser Technischen Richtlinie unterstützten Elliptischen Kurven aufgelistet.

Für die aktuell zu verwendenden Werte siehe [8], Kapitel 3, 4 und 7.

5.1.1.4 Subject

-tbd-

5.1.2 Extensions

Folgende Erweiterungen können in den Zertifikaten verwendet werden.

1. `AuthorityKeyIdentifier`
   - Extension-ID (OID): 2.5.29.35
   - Kritisch: Nein
   - Beschreibung: Der `authorityKeyIdentifier` wird benutzt, um verschiedene öffentliche Schlüssel desselben Zertifikatsherausgebers unterscheiden zu können.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	m

   - Wert: Der `KeyIdentifier` wird mit Methode 1 gemäß [3], 4.2.1.1 berechnet, d.h. er besteht aus dem SHA-1-Wert des Feldes `subjectPublicKey` (ohne tag, length und number of unused bits) aus dem Zertifikat des Zertifikatsherausgebers.
2. `SubjectKeyIdentifier`
   - Extension-ID (OID): 2.5.29.14
   - Kritisch: Nein
   - Beschreibung: Der dient zur Identifikation eines Zertifikats mit einem spezifischen öffentlichen Schlüssel.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	o	o

   - Wert: Der `KeyIdentifier` wird mit Methode 1 gemäß [3], 4.2.1.1 berechnet, d.h. er besteht aus dem SHA-1-Wert des Felds `subjectPublicKey` (ohne tag, length und number of unused bits) des Zertifikatsinhabers.
3. `KeyUsage`
   - Extension-ID (OID): 2.5.29.15
   - Kritisch: Ja
   - Beschreibung: Die Extension `KeyUsage` ist in [3], 4.2.1.1 spezifiziert. Sie gibt an für welche Zwecke der zertifizierte öffentliche Schlüssel verwendet werden darf.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C_{TLS}(ENu)*	*C_{Enc}(ENu)*	*C_{Sign}(ENu)*
m/o/x	m	m	m	m	m

- Wert: Folgende Bits sind in den einzelnen Zertifikaten gesetzt:

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C_{TLS}(ENu)*	*C_{Enc}(ENu)*	*C_{Sign}(ENu)*
Gesetzte Bits	KeyCert-Sign, cRL-Sign	KeyCert-Sign, cRL-Sign	DigitalSi-gnature	KeyEnci-pherment, KeyAgree-ment	DigitalSi-gnature

4. `PrivateKeyUsagePeriod`

- Extension-ID (OID): 2.5.29.16
- Kritisch: Nein
- Beschreibung: Die Extension `PrivateKeyUsagePeriod` wird in [3], 4.2.1.1 spezifiziert. Sie gibt die Gültigkeitszeit des zum Zertifikat gehörenden privaten Schlüssel an.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C_{TLS}(ENu)*	*C_{Enc}(ENu)*	*C_{Sign}(ENu)*
m/o/x	m	m	o	o	o

- Wert: Die einzutragenen Verwendungszeiten des privaten Schlüssels werden von Kapitel 3.2 vorgegeben.

5. `CertificatePolicies`

- Extension-ID (OID): 2.5.29.32
- Kritisch: Nein
- Beschreibung: Diese Extension (spezifiziert in [3], 4.2.1.4) gibt Informationen über die zugrundeliegende Zertifikatspolicy, nach der das Zertifikat ausgestellt wurde.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	m

- Wert: **-tbd-**

6. `SubjectAltNames`

- Extension-ID (OID): 2.5.29.17
- Kritisch: Nein
- Beschreibung: Diese Extension (Definition siehe [3], 4.2.1.6) enthält weitergehende Informationen über `Subject`.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	m

- Wert: `SubjectAltName` muss genau den rfc822Name des Subjects enthalten

7. `IssuerAltName`

- Extension-ID (OID): 2.5.29.18

- Kritisch: Nein
- Beschreibung: Diese Extension (spezifiziert in [3], 4.2.1.7) …?

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	m

- Wert: IssuerAltName muss aus dem rfc822Name und einem uniformRecourceIdentifier des Issuers bestehen..

8. `BasicConstraints`

- Extension-ID (OID): 2.5.29.19
- Kritisch: Ja
- Beschreibung: Diese Extension (spezifiziert in [3], 4.2.1.9) gibt an, ob es sich bei dem gegebenen Zertifikat um eine CA handelt und wie viele CAs in folgen können.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	x

- Werte: Die Extension hat in den einzelnen Zertifikaten folgende Werte:

Zertifikat	*C(Root)*	*C(Sub-CA)*
`cA`	TRUE	TRUE
`pathLen-Constraint`	1	0

9. `ExtendedKeyUsage`

- Extension-ID (OID): 2.5.29.37
- Kritisch: Nein
- Beschreibung: Dieser Extension (spezifiziert in [3], 4.2.1.13) gibt an wo und wie die CRL erhalten werden kann. s in folgen können.

Zertifikat	*C(Root)*	*C(Sub-CA)*	C_{TLS}*(ENu)*	C_{Enc}*(ENu)*	C_{Sign}*(ENu)*
m/o/x	x	x	m	x	x

- Werte: Die Extension hat in den einzelnen Zertifikaten folgend

Zertifikat	C_{TLS}*(MT)*	C_{Enc}*(GWA)*	C_{Sign}*(SM-GW)*
Wert	TLS-Web-Client-Authentifikation (1.3.6.1.5.5.7.3.2)	TLS-Web-Client-Authentifikation (1.3.6.1.5.5.7.3.2)	TLS-Webserver-Authentifikation (1.3.6.1.5.5.7.3.1) TLS-Web-Client-Authentifikation (1.3.6.1.5.5.7.3.2)

10. `CRLDistributionPoints`

- Extension-ID (OID): 2.5.29.19
- Kritisch: Nein

- Beschreibung: Diese Extension (spezifiziert in [3], 4.2.1.13) gibt an wo und wie die CRL erhalten werden kann.

Zertifikat	*C(Root)*	*C(Sub-CA)*	*C(ENu)*
m/o/x	m	m	m

11. `AuthorityInformationAccess`

- Extension-ID (OID): 1.3.6.1.5.5.7.1.1
- Kritisch: Nein
- Beschreibung: Diese Extension optional
- Wert: **-tbd-**

5.2 CRL-Profile

-tbd-

5.3 Zertifkatsrequests

Zum Update von Zertifikaten werden Zertifikatsrequests verwendet.

-tbd-

5.4 Elliptische Kurven

Von dieser Technischen Richtlinie werden Brainpool- und NIST-Kurven über Primkörpern unterstützt.

- Die OBJECT IDENTIFIER der Brainpool-Kurven sind in [10] und [11] spezifiziert.
- Die OBJECT IDENTIFIER der NIST-Kurven über Primkörpern sind in [12], Kapitel A.2.1 spezifiziert.

6 Protokolle für das Management von Zertifikaten und CRLs

In diesem Kapitel werden Kommunikationsprotokolle für das Management von Zertifikaten spezifiziert.

-tbd-

Literaturverzeichnis

[1] BSI TR-03109, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, 2011

[2] BSI TR-03109 Anhang: Kryptographische Vorgaben für die Infrastruktur von Messsystemen, 2011

[3] D. Cooper, S. Santesson, S. Farrell, S. Boyen, R. Housley, W. Polk , RFC 5280: Internet X.509 Public Key Infrastructures - Certificates and Certificate Revocation List (CRL) Profiles , 2008

[4] BSI: , Protection Profile - Cryptografic Modules, Security Level "Moderate" ,

[5] , Protection Profile - Secure Signature-Creation Device, ,

[6] BSI BSI-CC-PP-xxxx, Protection Profile for the Security Module of a Smart Metering System, 2011

[7] ANSI X9.62 , Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algirithm (ECDSA), 2005

[8] BSI TR-03109, Anhang: Kryptographische Vorgaben für die Infrastruktur von Messsystemen, 2011

[9] S. Turner, R. Housley, T. Polk , RFC 5480: Elliptic Curve Cryptography Subject Public Key Information,

[10] BSI TR-03111, Elliptic Curve Cryptography, 2011

[11] M. Lochter, J. Merkle , RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010

[12] Standards for Efficient Cryptography Group , SEC 2: Recommended Elliptic Curve Domain Parameters. , 1999