ChangeLog SM-Root-CA

Aktualisiert: 2024-03-12

Aktuell gültige Spezifikationen

Folgende Spezifikation sind aktuell gültig und auf der Webseite des BSI (www.bsi.bund.de/SM-PKI) abrufbar:

- TR-03109-4 (Version 1.2.1)
- TR-03129-4 (Version 1.3.1)
- Certificate Policy der Smart Metering PKI (Version 1.1.2)

Einleitung

Dieses ChangeLog wird im Auftrag des BSI veröffentlicht und enthält abgestimmte Informationen zu Klarstellungen und Korrekturen bzgl. der aktuell gültigen Spezifikationen. Soweit nicht anders angegeben, sind diese Anpassungen ab dem Zeitpunkt der Veröffentlichung gültig und verbindlich und werden in das nächste Release der jeweiligen Spezifikation übernommen.

Des Weiteren wird in diesem Dokumente über konkrete Systemänderungen bei der SM-Root-CA informiert.

Struktur

Das Dokument wird fortlaufend, umgekehrt chronologisch erweitert. Die Einträge sind einheitlich wie folgt aufgebaut:

Datum des Eintrags [Format: JJJJ-MM-DD]
Art des Eintrags [Systemänderung / Information]

Überschrift
Erklärender Kurztext

Ursprung, Quelle, Referenz (optional)

Konkretisierung der Umsetzung, Auswirkung (optional)

Inhalt

2024-03-12
Information / Prozessänderung

Aktualisierung des Eintrags von 2023-09-01
Veröffentlichung von Zertifikaten der AS/4 gestützten Martkommunikation (EMT.MAK) durch die Sub-CAs der SM-Root-CA

Die Befristung bis zum 01.04.2024 entfällt. Die Regelung zur Veröffentlichung von EMT-MAK-Zertifikaten (siehe Eintrag von 2023-09-01) gilt bis auf Widerruf.

2024-01-25
Information

DB Energie GmbH als Vergabestelle von Marktpartner-IDs im Anwendungsbereich des deutschen Bahnstromnetzes

Zusätzlich zu den in der SM-PKI CP unter 3.2.2.2 genannten Betreibern von Codenummernverzeichnissen, kann auch die DB Energie GmbH Zuteilungsurkunden zur autorisierten Nutzung von Marktpartner-IDs ausstellen.

Das Codenummernverzeichnis der DB Energie GmbH ist unter folgender Adresse als PDF abrufbar:

https://www.dbenergie.de/resource/blob/4570920/63809a49d6ddc9e64097da722016b2f9/Datei-Marktpartner-IDs-data.pdf

- CP Version 1.1.2

2024-01-08
Information

Klarstellung zu SubjectAltNames bei Zertifikaten der AS/4 gestützten Martkommunikation (EMT.MAK)

Teilnehmer der Marktkommunikation (mit EMT.MAK-Zertifikaten) müssen gem. SM-PKI CP, A.7.1 die Adresse ihres AS4-Webservices verpflichtend im SubjectAltName angeben. Die AS4-Adresse MUSS dem Typ uniformResourceIdentifier entsprechen.

Der Antragsteller ist für die Richtigkeit der Angaben und die Einhaltung etwaiger Vorgaben aus den Festlegungen zur Marktkommunikation selbst verantwortlich. Eine Prüfung durch die RA der Sub-CA ist nicht erforderlich.

Die Angaben im SubjectAltName gelten als technische/betriebliche Angaben und DÜRFEN gem. SM-PKI CP Kap. 4.7 im Rahmen der Schlüsselerneuerung (d. h. Bei Folge-zertifikaten) geändert werden

- CP Version 1.1.2

2023-09-01 (Update 2024-03-06)
Information / Prozessänderung

Veröffentlichung von Zertifikaten der AS/4 gestützten Martkommunikation (EMT.MAK) durch die Sub-CAs der SM-Root-CA

Die Sub-CAs der Smart Metering PKI werden verpflichtet, ab dem 20.09.2023 alle ausgestellten EMT-MAK-Zertifikate (mit CN: <org>.EMT.MAK[<extension>]) auf ihren Webseiten zum Download zur Verfügung zu stellen.

Sub-CAs, die keine EMT-MAK-Zertifikate verwalten, teilen dies auf ihren Webseiten mit.

Die Bereitstellung der EMT-MAK-Zertifikatstripel erfolgt zusammengefasst in einer Datei im "LDAP Data Interchange Format" (LDIF). Die LDIF-Datei muss die Zertifikate in Base64-ASCII Codierung (analog PEM-Format) enthalten.

Die LDIF-Datei wird wöchentlich am Mittwoch bzw. dem darauffolgenden Werktag (Montag bis Freitag) aktualisiert. Im Zeitraum vom 21.12.2023 bis 02.01.2024 findet keine Aktualisierung statt.

~~Diese Regelung ist befristet bis zum 01.04.2024 und gilt nicht für die SM-Test-PKI~~
Diese Regelung gilt bis auf Widerruf und nicht für die SM-Test-PKI.

- CP Version 1.1.2

2023-09-01
Information

Aktualisierung des Eintrags von 2020-03-12
Regelungen für das Testen im Rahmen einer SMGW CC-Re-Zertifizierung unter Wirkbedingungen

Die Limitierung der Tests auf bis zu acht SMGW entfällt.
Die maximal zulässige Dauer der Tests wird von 2 auf 12 Monate angehoben.

2022-10-20
Information

Routinemäßige Erneuerung von Zertifikaten der SM-Root-CA

Die folgenden Zertfikate der SM-Root-CA wurden routinemäßig erneuert:

C(Root)
CCRL-S(Root)
CTLS-S(Root)
CTLS(Root)
Link-C(Root)

Die Zertifikate wurden im Downloadbereich der SM-Root-CA Webseite veröffentlicht.

- CP Version 1.1.1, TR-03109-4 Version 1.2.1

2021-11-04
Information

Routinemäßige Erneuerung von Zertifikaten der SM-Root-CA

Die folgenden Zertfikate der SM-Root-CA wurden routinemäßig erneuert:

C_{TLS-S}(Root)
C_{TLS}(Root)

Die Zertifikate wurden im Downloadbereich der SM-Root-CA Webseite veröffentlicht.

- CP Version 1.1.1, TR-03109-4 Version 1.2.1

2021-10-05
Information / Systemänderung

Routinemäßiger Austausch von Zertifikaten der SM-Root-CA:

Die SM-PKI Spezifikationen sehen die regelmäßige Neuausstellung sowie den Austausch der von der SM-Root-CA verwendeten Zertifikate vor.

Die Schlüssel-/Zertifikatsgenerierungszeremonie für die Erneuerung der Zertifikate

C_{TLS-S}(Root)
C_{TLS}(Root)

ist für Ende Oktober 2021 geplant.

Die Veröffentlichung der erzeugten Zertifikate erfolgt zum 01.11.2021.
Die Inbetriebnahme der Zertifikate erfolgt zeitversetzt am 04.11.2021.

- CP Version 1.1.1, TR-03109-4 Version 1.2.1

Zur Signierung des neuen C_{TLS-S}(Root) Zertifikats wird das derzeit verwendeten C(Root) Zertifikat (SN2) verwendet.

Das neue C_{TLS}(Root) Zertifikat wird im Anschluss erzeugt und mit dem neuen C_{TLS-S}(Root) Zertifikat signiert.

2020-03-12 (Update 2023-09-01)
Information

Regelungen für das Testen im Rahmen einer SMGW CC-Re-Zertifizierung unter Wirkbedingungen

Im Rahmen der CC-Re-Zertifizierung soll es einem GWH unter Nutzung der SM-PKI und in Zusammenarbeit mit einem oder mehreren GWA möglich sein, vor Abschluss der Re-Zertifizierung den Firmwareupdate-Prozess sowie den Wirkbetrieb mit der noch nicht abschließend zertifizierten Firmware zu testen. Voraussetzung für die Durchführung dieser Tests ist ein laufendes SMGW CC-Re-Zertifizierungsverfahren des GWH beim BSI. Des Weiteren müssen die nachfolgenden Anforderungen beim GWH und den weiteren Akteuren erfüllt sein:

- Die Tests dürfen ausschließlich im abgesicherten Testbereich des GWA durchgeführt werden.

- Die Durchführung der Tests muss dokumentiert werden. In der Dokumentation müssen insb. die Gateway-IDs der verwendeten SMGWs, die weiteren Akteure und die durchlaufenen Stationen festgehalten werden. Die Unterlagen müssen der Verfahrensdokumentation der SMGW CC-Re-Zertifizierung hinzugefügt werden.

- Der GWH muss dem GWA das FW-Image über einen gesicherten Kanal zur Verfügung stellen. Hierüber muss die Authentizität und Integrität des Updates gewährleistet werden. Der GWA darf für die Testdurchführung die noch in Zertifizierung befindliche Firmware in seiner Wirkumgebung hochladen und die vorher dokumentierten Geräte damit updaten. Eine darüberhinausgehende Verwendung des FW-Image ist nicht zulässig.

  ~~Die Tests dürfen insgesamt auf bis zu acht SMGW durchgeführt werden.~~

- Die im Rahmen der Tests zu verwendenden SMGW müssen sich VOR Durchführung des Firmware-Updates im zertifizierten Zustand befinden.

- Die SMGW müssen bereits personalisiert sein und es müssen insbesondere Wirk-Zertifikate aufgebracht sein.

- Nach dem Update auf die nicht zertifizierte Firmware, darf ein SMGW den abgesicherten Testbereich des GWA nur verlassen, wenn ~~dessen~~ die Zertifikate des SMGW zuvor vom zugehörigen GWA gesperrt wurden.

- Die Tests dürfen maximal ~~2~~ 12 Monate dauern, danach muss die Entsorgung der SMGWs erfolgen, sofern die Re-Zertifizierung nicht erfolgreich abgeschlossen wurde.

2019-12-19
Information

Konkretisierung der SM-PKI CP bzgl. der SMGW-G Zertifikate

Anhang A, Abs. 3 der SM-PKI CP wird wie folgt ergänzt:

- Zertifikate des Typs SMGW-G dürfen in Ausnahmefällen mehrfach mit identischem CN sowie der Seriennummer 0 ausgestellt werden (z.B. um zu verhindern, dass SMGW Hardware durch ein Vorkommnis während der Konfiguration beim GWH unbrauchbar wird)

Eine Mehrfachzertifizierung von Schlüsselmaterial ist in jedem Fall unzulässig.

Die Ausnahmeregelung ist ab sofort gültig und wird im Rahmen der nächsten Aktualisierung in die SM-PKI Certificate Policy übernommen.

- CP Version 1.1.1, Anhang A, Abs. 3

2019-10-08
Information

Terminverschiebung: Routinemäßiger Austausch der Zertifikate der SM-Root-CA

Die routinemäßige Neuausstellung sowie der Austausch der von der SM-Root-CA verwendeten Zertifikate verschiebt sich aus organisatorischen Gründen.

Die Veröffentlichung der erzeugten Zertifikate erfolgt bis zum 11.11.2019.
Die Inbetriebnahme der Zertifikate erfolgt zeitversetzt am 02.12.2019.

2019-09-02
Information / Systemänderung

Routinemäßiger Austausch der Zertifikate der SM-Root-CA

Die SM-PKI Spezifikationen sehen die regelmäßige Neuausstellung sowie den Austausch der von der SM-Root-CA verwendeten Zertifikate vor.

Die dazu notwendige Schlüssel-/Zertifikatsgenerierungszeremonie ist für Oktober 2019 geplant.

Die Veröffentlichung der erzeugten Zertifikate erfolgt bis zum 14.10.2019.
Die Inbetriebnahme der Zertifikate erfolgt zeitversetzt am 18.11.2019.

- CP Version 1.1.1, TR-03109-4 Version 1.2.1

Bitte installieren Sie den neuen Vertrauensanker rechtzeitig (bis zu dem genannten Stichtag der Inbetriebnahme) auf Ihren an der SM-PKI teilnehmenden Systemen um Probleme bei der Zertifikatsvalidierung zu vermeiden.

Der Zugriff auf die Web Service Schnittstelle sowie den Verzeichnisdienst ist ab dem 18.11.2019 nur noch unter Berücksichtigung der neuen Zertifikate möglich. Insbesondere die Signierung der SM-Root-CA Sperrliste erfolgt ab dem 18.11.2019 ausschließlich durch das neue CRL-S Zertifikat.

2018-12-10
Information

Anpassung der Regelungen für ALC-Tests im Rahmen einer SMGW CC-Zertifizierung unter Wirkbedingungen

Die zulässige Anzahl an Prototyp-SMGWs in der Wirkumgebung wird von fünf auf acht angehoben.

Die Regelungen für die ALC-Tests vom 14.11.2017 werden entsprechend wie folgt angepasst:

- Der GWH darf einmalig im Rahmen der CC-Zertifizierung mit seinem Wirk-Zertifikat **acht** (bisher fünf) Prototyp-SMGWs produzieren, um die ALC-Tests durchzuführen.

- Der GWH muss dabei sicherstellen, dass nur Gütesiegel-Zertifikate aus der SM-PKI für **acht** (bisher fünf) Prototyp-SMGWs bezogen werden.

- Nach der Produktion der **acht** (bisher fünf) Prototyp-SMGW dürfen die Tests maximal 2 Monate dauern, danach muss die Entsorgung der Prototyp-SMGWs erfolgen. Ist die CC-Zertifizierung bis dahin nicht abgeschlossen, müssen auch die GWH-Zertifikate gesperrt werden. Nach Abschluss der CC-Zertifizierung ist dann ein initialer Zertifikats-Request erforderlich.

Die übrigen Regelungen für ALC-Tests bleiben unverändert.

2018-12-05
Information

Erneuerung des TLS-Zertifikats der SM-Root-CA (SM-Root.CA.TLS)

Das TLS-Zertifikat der SM-Root-CA (SM-Root.CA.TLS) wurde routinemäßig erneuert.

Der Austausch des Zertifikats bei der Web-Service Schnittstelle sowie dem LDAP Verzeichnis der SM-Root-CA erfolgt am 06.12.2018.

Das aktuelle TLS-Zertifikat (SM-Root.CA.TLS, SN2) finden sie im Downloadbereich der SM-Root-CA.

2018-03-01
Systemänderung

Anpassungen im Rahmen der Übergangsfrist zum ausschließlich spezifikationskonformen Betrieb der SM-PKI

- Anpassung des DN bei dem Verzeichnisdienst von "dc=Certificates, dc=SM-PKI" zu "dc=Certificates, dc=SM-PKI-DE"
- Anpassung der WebService Schnittstelle
  URL: https://root.sm-pki.telesec.de/smrootca/services/SmartMeterService

- CP Version 1.1.1, TR-03109-4 Version 1.2.1, TR-03129-4 Version 1.3.1

2017-11-14
Information

Regelungen für ALC-Tests im Rahmen einer SMGW CC-Zertifizierung unter Wirkbedingungen

Die ALC-Tests (Class ALC = Life-Cycle Support) sollen es einem GWH unter Nutzung der SM-PKI ermöglichen, seine Lifecycle-Prozesse zum SMGW unter Wirkbedingungen zu erproben. Voraussetzung für die Durchführung der Tests ist ein laufendes SMGW CC-Zertifizierungsverfahren beim GWH. Des Weiteren müssen die nachfolgenden Sicherheits-anforderungen beim GWH und den weiteren Lifecycle-Akteuren für die ALC-Tests erfüllt sein:

- Das Vorort-Audit der Produktionsumgebung beim GWH im Rahmen der CC-Zertifizierung zum SMGW muss erfolgreich abgeschlossen sein.
- Der Prüfbericht zum ALC-Baustein im Rahmen der CC-Zertifizierung des SMGW muss von der Zertifizierungsstelle abgenommen sein.
- Der GWH benötigt ein Schreiben seiner CC-Prüfstelle, dass die zuvor genannten Bedingungen erfüllt wurden.
- Der GWH muss die Registrierung bei einer Sub-CA bis auf den Abschluss der CC-Zertifizierung erfolgreich durchlaufen haben. Das Schreiben der Prüfstelle muss der Sub-CA übermittelt werden.
- Auf Basis des Schreibens darf eine Sub-CA für den GWH Zertifikate aus der SM-PKI ausstellen, auch wenn die CC-Zertifizierung des SMGW noch nicht vollständig abgeschlossen wurde.
- Der GWH darf einmalig im Rahmen der CC-Zertifizierung mit seinem Wirk-Zertifikat fünf Prototyp-SMGWs produzieren, um die ALC-Tests durchzuführen.

- Der GWH muss dabei sicherstellen, dass nur Gütesiegel-Zertifikate aus der SM-PKI für fünf Prototyp-SMGWs bezogen werden.

- Den Rahmen für die Erprobung des Lifecycles bildet das abgenommene ALC-Konzept, das von allen Akteuren eingehalten werden muss. Es dürfen keine abrechungsrelevanten Daten von den Prototyp-SMGWs verarbeitet werden.

- Nach der Produktion der fünf Prototyp-SMGW dürfen die Tests maximal 2 Monate dauern, danach muss die Entsorgung der Prototyp-SMGWs erfolgen. Ist die CC-Zertifizierung bis dahin nicht abgeschlossen, müssen auch die GWH-Zertifikate gesperrt werden. Nach Abschluss der CC-Zertifizierung ist dann ein initialer Zertifikats-Request erforderlich.

- Die Auslieferung der Prototyp-SMGWs zur Durchführung der weiteren Tests darf ausschließlich an einen zertifizierten GWA erfolgen, der bereits bei einer Sub-CA registriert wurde.
- Alle Tests nach der Auslieferungen dürfen ausschließlich in der sicheren Umgebung des GWA durchgeführt werden.

- Nach der Personalisierung des Prototyp-SMGW bei Inbetriebnahme (Aufbringen der Wirk-Zertifikate) darf ein Prototyp-SMGW die sichere GWA-Umgebung nur verlassen, wenn dessen Zertifikate zuvor vom zugehörigen GWA gesperrt wurden.

- Die Durchführung der ALC-Tests muss dokumentiert werden. In der Dokumentation müssen insb. die Gateways-IDs der Prototyp-SMGWs, die weiteren Akteure und die durchlaufenen Stationen festgehalten werden. Die Unterlagen müssen der Verfahrensdokumentation der SMGW CC-Zertifizierung hinzugefügt werden.

2017-09-13
Information

Umstellung der Testsysteme der Root-CA auf die aktuellen Spezifikationen.

Die Umstellung der Testsysteme der SM-Root-CA (SM-Test-PKI) auf die aktuellen Spezifikationen ist für KW42/2017 geplant.

Aus Gründen der Abwärtskompatibilität steht die Webservice-Schnittstelle zunächst parallel, sowohl in der Version 1.3.1 also auch in der Version 1.3. zur Verfügung. Die Webservice-Schnittstelle nach Version 1.3 entfällt zum Ende der Übergangszeit.

Im Rahmen der Umstellung werden neue Zertifikate mit O=SM-Test-PKI-DE erzeugt. Diese sowie weitere Informationen (z.B. URLs der Webservices) werden zu gegebener Zeit auf den Webseiten bzw. im ChangeLog der SM-Test-PKI veröffentlicht.

2017-09-13
Information

Verlängerung der Übergangsregelung zur Umsetzung der Web-Service-Schnittstelle gem. TR-03129-4 und zur Suspendierung.

Die mit der Meldung 2017-05-18 bekanntgegebene Übergangsfrist wird bis zum 01.03.2018 verlängert.

2017-06-22
Information

Ergänzende Hinweise zu Kapitel 1.3.3.4, SM-PKI Policy (Externer Marktteilnehmer)

Über den Webauftritt des BSI wurden zusätzliche Hinweise bzgl. der externen Marktteilnehmer (EMT) veröffentlicht.
Diese Informationen ergänzen das Kapitel 1.3.3.4 der SM-PKI Policy und gelten ggf. vorrangig.

- Webauftritt des BSI, „Fragen und Antworten zum Themenbereich der SM-PKI“
- TR-03109-4, Version 1.2, Stand 09.12.2016
- Certificate Policy der Smart Metering PKI, Version 1.1, Stand 09.12.2016

2017-05-18
Information

Übergangsregelung zur Umsetzung der Web-Service-Schnittstelle gemäß TR-03129-4 und zur Suspendierung von Zertifikaten

Übergangsweise kann bis zum 01.01.2018 die Web-Service-Schnittstelle gemäß TR-03109-4 Version 1.1.1 weiterhin genutzt werden.

Entsprechend muss die Suspendierung von Zertifikaten erst bis zum genannten Termin unterstützt werden.

Der Zeitpunkt für die Umstellung bzw. für die Realisierung der Suspendierung und Nutzung der neuen Web-Service-Schnittstelle gemäß TR-03129-4 und CP V1.1 kann von den Sub-CAs innerhalb der Frist selbst gewählt werden.

Die Root-CA und die Testsysteme der Root werden vorerst die Web-Service-Schnittstelle gemäß TR-03109-4 Version 1.1.1 weiter betreiben. Die Umstellungszeitpunkte für die einzelnen Systeme werden rechtzeitig bekanntgegeben.

- TR-03109-4, Version 1.2, Stand 09.12.2016
- Certificate Policy der Smart Metering PKI, Version 1.1, Stand 09.12.2016

2017-01-11
Information

Übergangsregelung zur Umsetzung von Anforderungen aus den überarbeiteten Spezifikationen

Mit der Veröffentlichung der überarbeiteten Spezifikationen (TR-03109-4 / CP) gilt ein Übergangszeitraum für die Umsetzung der sich daraus ergebenden Anforderungen von 6 Monaten. Dies beinhaltet bei einer Sub-CA insbesondere die Anpassung der Sub-CA Certificate Policy.

Die Registrierung eines PKI-Teilnehmers auf Basis der zuvor veröffentlichten Spezifikationen ist im Übergangszeitraum möglich.

- TR-03109-4, Version 1.2, Stand 09.12.2016
- Certificate Policy der Smart Metering PKI, Version 1.1, Stand 09.12.2016

2016-12-09
Information

Aktualisierte Spezifikationen, Übergangszeitraum für die Implementierung der Funktion „Suspendierung"

Mit Veröffentlichung der neuen Spezifikationen (TR/CP) gilt ein Übergangszeitraum für die Implementierung der Funktion "Suspendierung" von 6 Monaten. Innerhalb dieser Frist ist eine Registrierung als Sub-CA auch dann möglich, wenn die Funktion "Suspendierung" noch nicht realisiert wurde.Anschließend muss die Funktion, konform zu den Spezifikationen, von einer Sub-CA unterstützt werden.

- TR-03109-4, Stand 09.12.2016, Version 1.2, Kapitel 4.3
- Certificate Policy der Smart Metering PKI, Version 1.1, Stand 09.12.2016, Kapitel 4.8.2