ChangeLog SM-Test-PKI

Aktualisiert: 2017-10-25

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-Test-BSI-Root- und -Sub-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

Konkretisierung der Umsetzung, Auswirkung (optional)

Inhalt

2017-10-25
Information / Systemänderung

Anpassung der Systeme der SM-Test-Root-CA an die aktuellen Spezifikationen

Die Systeme der SM-Test-Root-CA wurden an die aktuell gültigen Spezifikationen angepasst. Insbesondere erfolgte die Umstellung von O = SM-Test-PKI auf O = SM-Test-PKI-DE.

Nicht den aktuellen Spezifikationen entsprechende Requests werden abgelehnt. Insbesondere ist es nicht mehr möglich Zertifikate mit dem Attribut O = SM-Test-PKI zu beantragen.

Bestehende Zertifikate mit O = SM-Test-PKI können weitergenutzt und für Folge-Requests verwendet werden. Die Tests im Rahmen der Registrierung bei einer Sub-CA können bis zum 01.03.2018 auch auf Basis dieser Zertifikate durchgeführt werden.

Ab dem 01.03.2018 dürfen in der SM-Test-PKI ausschließlich Zertifikate gem. den aktuell gültigen Spezifikationen ausgegeben werden.

Bestehende Zertifikate auf Basis der alten Spezifikationen bleiben auch nach dem 01.03.2018 gültig, dürfen aber entsprechend nicht mehr zur Ausstellung weiterer („alter“) Zertifikate verwendet werden.

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

2017-10-23
Information / Systemänderung

Parallelbetrieb der Webservice-Schnittstelle in den Versionen 1.3.0 und 1.3.1

Im Rahmen der Umstellung der Testsysteme der SM-Test-PKI wurde ein Parallelbetrieb der Webservice-Schnittstelle in den Versionen 1.3.0 sowie 1.3.1 installiert.

Die bisherigen WebService URLs werden auf den WebService der Version 1.3.0 der jeweiligen CA umgeleitet und können weiterverwendet werden sofern der Client „ HTTP 307 Temporary Redirect“ unterstützt. Der Parallelbetrieb endet am 01.03.2018.

Die neuen Zugriffsparameter finden Sie in der folgenden Tabelle:

CA	Version	URL
SM-Test-Root-CA	1.3.0	root.test.sm-pki.telesec.de/smrootcat/130/services/SM-RootCA-ProtocolService
SM-Test-Root-CA	1.3.1	root.test.sm-pki.telesec.de/smrootcat/131/services/SmartMeterService
SM-Test-BSI-Sub-CA	1.3.0	bsi-subca.test.sm-pki.telesec.de/smsubcat/130/services/SM-SubCA-ProtocolService
SM-Test-BSI-Sub-CA	1.3.1	bsi-subca.test.sm-pki.telesec.de/smsubcat/131/services/SmartMeterService

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.

2016-12-19
Information

Anforderungen an die Zufallszahlengenerierung beim Einsatz von Kryptografiemodulen SM-Test-PKI

Die Certificate Policy, Anhang C.1 definiert für den Einsatz von Kryptgrafiemodulen das Sicherheitsniveau Security Level 1 gemäß dem Dokument "Key Lifecycle Security Requirements". Die unter Security Level 1 definierten Anforderungen an die Zufallszahlengenerierung für Kryptografiemodule in der SM-Test-PKI gelten nur als EMPFEHLUNG.

- CP Version 1.1, Anhang C.1; Key Life Cycle Security Requirements 1.0.1

2016-04-19
Systemänderung

Änderung bzgl. Session-Regnegotiaton bei TLS-Verbindungen SM-Test-BSI-Sub-CA

Serverseitig initiiertes Session-Renegotiation bei TLS Verbindungen mit der Webservice-Schnittstelle wurde unterbunden.

- TR-03116-3, Stand 04.04.2016, Kapitel 4.1.1

* Der Webserver initiiert bei TLS Verbindungen kein Session-Renegotiation.

2016-04-19
Systemänderung

Änderung bzgl. der vom Server übermittelten Zertifikatskette bei TLS-Verbindungen SM-Test-BSI-Sub-CA

Die Sortierreihenfolge der vom Server ausgelieferten Zertifikatskette bei TLS Verbindungen mit der Webservice-Schnittstelle wurde gem. den Vorgaben des IETF RFC 5246
angepasst. Das Root-Zertifikat wurde aus der Zertifikatskette entfernt.

- IETF RFC 5246, Section 7.4.2

* Der Webserver liefert bei TLS Verbindungen die Zertifikatskette gem. den Vorgaben des RFC 5246 sortiert und ohne das Root-Zertifikat aus.

2015-11-10
Information / Systemänderung

Geänderte Validierung von Zertifikatsrequests mit Autorisierungssignatur SM-Test-BSI-Sub-CA

Ein Zertifikatsrequest mit Autorisierung durch eine dritte Partei muss in EncapsulatedContentInfo entweder den content type id-CertReqMsgs-with-outerSignature oder id-CertReqMsgs enthalten. Daraus folgt: signedAttrs MUSS gemäß RFC 5652 verwendet werden, da die TR-03109-4 als content type von EncapsulatedContentInfo nicht id-data, sondern id-CertReqMsgs bzw. id-CertReqMsgs-with-outerSignature verlangt.

- TR-03109-4 Version 1.1.1, Anhang C; IETF RFC 5652

* Es wurde eine Valdierung bzgl. der Verwendung von SignedAttr implementiert. Requests, die SignedAttrs nicht berücksichtigen, werden vom System abgelehnt.