SRQ - Specification Related Question

SRQ-ID: 1202

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemX.509_TSP]
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	4.2.1, 5.2.1, 5.2.3, 5.2.6, 5.3.1, 5.3.3

Stichwort: Änderungen/Ergänzungen für Basis-Rollout

Frage:

Welche Änderungen/Ergänzungen werden für den Basis-Rollout vorgenommen?

Betrifft:

Gültig ab	07.4.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Der SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	offen	voraussichtl. Zeitpunkt	
Anmerkungen:	Dieser SRQ enthält unter anderem Maßnahmen, die sich aus dem Sicherheitsgutachten ergeben haben.		
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Es wurden folgenden Änderungen/Ergänzungen vorgenommen:

- Anforderungen zur Umsetzung des 4-Augen-Prinzips für die Übergabe der Zertifikate des TSP an den TSL-SP zur Aufnahme in die TSL wurden aufgenommen
  (Kap. 4.2.1)
- Anforderungen zur Identifizierung des Antragstellers einer PKI-Registrierung (TSL-TSP) wurden aufgenommen.
  (Kap. 5.2.1, 5.2.3, 5.2.6, 5.3.1, 5.3.3)

4.2.1 gematik

Die gematik ist verantwortlich für die Gestaltung der PKI der X.509-Zertifikate. Sie übernimmt unter anderem die folgenden Aufgaben:

- Beauftragung und Kontrolle des gematik-TSL-Service-Provider,
- Registrierung eines TSP [gemTSL_SP_CP],
- ggf. Widerruf der Registrierung eines TSP [gemTSL_SP_CP],
- bei Bedarf Kontrolle eines TSP [gemTSL_SP_CP],
- Vorgabe der Algorithmen und Schlüssellängen für das Generieren der X.509-Zertifikate [gemX.509_eGK], [gemX.509_SMCB],
- Entscheidung über Generationswechsel beim gematik-TSL-SP [gemTSL_SP_CP] und
- gematik-Test-TSL.

Die gematik MUSS sicherstellen, dass nach der Registrierung eines TSPs das 4-Augen-Prinzip bei der Übergabe von Zertifikaten des TSP umgesetzt wird.

5.2 Verfahren für einen Produktiv-TSP

5.2.1 Antrag auf Registrierung

[...]

Das Sicherheitsgutachten muss bestätigen, dass der TSP die Mindestanforderungen aus [gemTSL_SP_CP] erfüllt und dies in einem Sicherheitskonzept ausreichend beschrieben hat. Das Sicherheitsgutachten muss von einem durch die gematik anerkannten Gutachter stammen (Liste der Gutachter ist auf den Seiten der gematik veröffentlicht). Bei

akkreditierten CAs bestätigt die Selbsterklärung, dass der Betrieb des TSP unter denselben Sicherheitsbedingungen erfolgt.

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug~~ unterschrieben sein. Es muss überprüft werden, ob die unterzeichnende Person gemäß Handelsregisterauszug eine Zeichnungsbefugnis für das entsprechende Unternehmen besitzt. Falls Nein, darf der Antrag nicht weiter bearbeitet werden und das ISMS der gematik muss über den Vorfall informiert werden.

Um sicher zu stellen, dass es sich beim unterzeichnenden Antragssteller auch wirklich um die behauptete Person handelt, MUSS diese sicher identifiziert werden. Zudem muss sichergestellt werden, dass die Integrität und Authentizität des Antrags nicht verletzt wurde, also auch genau der Antrag bearbeitet wird, den der Antragsteller intendiert hat.

Die Registrierungsstelle der gematik MUSS für die sichere Identifizierung des zeichnungsberechtigten Antragsstellers mindestens eines der folgenden, grundsätzlich geeigneten, Verfahren einsetzen:

1. Persönliche Übergabe

Hierbei erfolgt die persönliche Übergabe des Antrags durch den Antragsteller an die zuständigen Mitarbeiter in der gematik und die Identifikation per Personalausweis oder Reisepass durch die Mitarbeiter der gematik. Der zuständige Mitarbeiter der gematik muss die Unterschrift des Antrags mit der Unterschriftenprobe auf dem präsentierten Ausweisdokument vergleichen. Die festgestellte Identität wird anschließend mit den Angaben im Handelsregisterauszug verglichen und damit überprüft ob die identifizierte Person zeichnungsbefugt ist.

2. Nutzung des Postident-Verfahrens

Hierbei übersendet der Antragsteller den Antrag und die notwendigen Unterlagen im Rahmen des Postident-Verfahrens an die Registrierungsstelle der gematik. Er muss sicherstellen, dass die Integrität der übergebenen Dokumente bis zum Zeitpunkt der Übergabe an die Postident durchführenden Stelle sicher gestellt ist. Bei der Übergabe wird von der Postident durchführenden Stelle die Identität des Antragstellers per Personalausweis oder Reisepass festgestellt und die abgegebenen, in einem Umschlag verschlossenen Unterlagen werden mit dieser Identität (inkl. einer Unterschriftenprobe) verbunden. Die Unterschrift auf den Antragsunterlagen muss nach Eingang in der Registrierungsstelle von den Mitarbeitern der gematik mit der Unterschriftenprobe aus dem Postident-Verfahren überprüft werden. Die Angaben zur Identität des Antragsstellers aus dem Postident-Verfahren werden mit den Angaben im Handelsregisterauszug verglichen und überprüft, ob die entsprechende Person zeichnungsbefugt ist.

3. Nutzung qualifizierter elektronischer Signaturen

Hier wird der Antrag per qualifizierter elektronischer Signatur vom Antragsteller unterschrieben. Die Signatur des Antrags muss von den Mitarbeitern der gematik überprüft werden. So wird die Integrität und die Authentizität (bez. der Antragstellenden Person) des Antrags sichergestellt. Die Mitarbeiter der gematik müssen anhand der im qualifizierten Zertifikat enthaltenden Angaben überprüfen, ob es sich bei der mit dem Zertifikat verbundenen natürlichen Person um dieselbe Person handelt, die im Handelsregisterauszug als zeichnungsberechtigte Person aufgeführt ist.

Weitere Hinweise zur Verwendung erhalten Sie auf der Homepage der gematik (www.gematik.de) unter der Rubrik „Zertifikatsherausgeber“.

[…]

5.2.3 Änderung einer Registrierung

[...]

Liegen Änderungen vor, die für das Sicherheitskonzept relevant sind, muss der Änderungsmitteilung ein neues Sicherheitsgutachten beigefügt werden. Dieses Sicherheitsgutachten muss bestätigen, dass die Mindestanforderungen aus [gemTSL_SP_CP] auch nach den Änderungen erfüllt werden.

Ggf. können die Änderungen zu einem Widerruf der Registrierung führen (siehe 5.2.4).

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug ((oder entsprechend vorgelegter Vertretungsvollmacht)~~ unterschrieben sein.

Für die Identifizierung des Antragstellers gelten die gleichen Vorgaben wie bei der erstmaligen Registrierung (siehe Abschnitt 5.2.1).

[…]

5.2.6 Verlängerungsantrag

Der TSL-Service-Provider generiert jedes Jahr eine komplett neue Version der Trust-service Status List. Dazu erhält er von der gematik die Registrierungsanträge (Folgeanträge) der TSPs.

Im laufenden Jahr werden bei Registrierungsanträgen neue TSP-Einträge generiert und der vorhandenen Version der TSL hinzugefügt.

~~Die Gültigkeit der Erstregistrierung gilt für das Jahr der Registrierung und das Folgejahr. Danach muss spätestens 3 Monate vor Ablauf der registrierte TSP einen Verlängerungsantrag (siehe Vorgaben Formulare) stellen.~~ Die Gültigkeitsdauer der Registrierung eines TSPs beträgt 2 Jahre. Spätestens 3 Monate vor Ablauf muss der registrierte TSP einen Verlängerungsantrag stellen. Dieser bestätigt, dass der Betrieb weiterhin gemäß der bei der erstmaligen Registrierung nachgewiesenen Sicherheitsbedingungen geführt wird. Das Formular muss vollständig ausgefüllt werden.

Alle Formulare des Antrages auf Verlängerung einer Registrierung und die beigefügten Unterlagen MÜSSEN rechtsverbindlich unterschrieben sein.

Der Antrag auf Verlängerung der Registrierung eines TSPs KANN (abweichend zum Vorgehen der erstmaligen Registrierung) von dem benannten „Leiter TSP“ gestellt werden. Für die Identifizierung des Antragstellers gelten dieselben Vorgaben wie bei der erstmaligen Registrierung (siehe Abschnitt 5.2.1).

Unter diesen Voraussetzungen kann das Schlüsselpaar des TSP im Kontext „Einführung der Gesundheitskarte“ weiter verwendet werden.

5.3 Verfahren für einen Test-TSP

5.3.1 Antrag auf Registrierung

[...]

Die Kopie des Registerauszugs muss von dem aktuellen Eintrag des Betreibers in dem zuständigen Register (Handelsregister, Vereinsregister, etc.) stammen. Aus diesem müssen die folgenden Informationen hervorgehen:

- Hauptsitz des Betreibers (Einschränkungen siehe 5.1.1),
- Gesellschafter des Betreibers,
- zeichnungsberechtigte Personen.

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug ((oder entsprechend vorgelegter Vertretungsvollmacht)~~ unterschrieben sein.

Für die Identifizierung des Antragstellers gelten die gleichen Vorgaben wie bei Registrierung eines Produktiv-TSP (siehe Abschnitt 5.2.1).

[…]

5.3.3 Änderung einer Registrierung

[...]

Die Änderungen sind durch entsprechende Nachweise, z. B. neuer Registerauszug, nachzuweisen.

Ggf. können die Änderungen zu einem Widerruf der Registrierung führen (siehe 5.3.4).

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug ((oder entsprechend vorgelegter Vertretungsvollmacht)~~ unterschrieben sein.

Für die Identifizierung des Antragstellers gelten die gleichen Vorgaben wie bei Registrierung eines Produktiv-TSP (siehe Abschnitt 5.2.1).