SRQ - Specification Related Question

SRQ-ID: 1125

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	Anpassung an die normativen Vorgaben und Korrektur bzgl. Sicherheitsgutachten
zu Dokument / Datei (evtl. ersetzt SRQ)	gemTSL_SP_CP, SRQ_0913
Version	1.2.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kapitel 1, 2.5, 2.1, 3.1, 3.1.1, 3.1.3, 3.3.7 (eingefügt), 3.3.8, 4, 4.1.1, 5.1.4, 6.1, 6.9

Stichwort: Anpassung an die normativen Vorgaben und Korrektur bzgl. Sicherheitsgutachten

Frage:

Welche für den Basis-Rollout relevanten Änderungen haben sich in der Certificate Policy der gematik ergeben, auch in Bezug auf die Vorgaben an das Sicherheitskonzept für TSP und das zugehörige Sicherheitsgutachten?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	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		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Teil 1: spezifischer Bezug zu Sicherheitskonzept / Sicherheitsgutachten

Kapitel 1 Zusammenfassung

Für eine Public Key Infrastruktur (PKI) ist die Einschätzung der Vertrauenswürdigkeit der ausgestellten Zertifikate durch die Empfänger von Nachrichten oder Transaktionen von entscheidender Bedeutung. Dieses Dokument beschreibt die dazu notwendigen Sicherheitsrichtlinien (Policy). Die Dokumentenstruktur dieser Certification Policy lehnt sich an die Empfehlungen des [RFC3647] an. ~~und vereinigt somit inhaltlich sowohl die Elemente einer Certification Policy als auch eines trifft die Vorgaben für mehr technisch-organisatorisch orientiertes Certificate Practice Statement (CPS) bzw. das Sicherheitskonzept des.~~

Aussteller von Zertifikaten (Trust-Service Provider, TSP), die innerhalb der Telematik-infrastruktur eingesetzt werden sollen, MÜSSEN die Anforderungen dieser Policy erfüllen und dieses durch die Erstellung eines spezifischen ~~CPS~~ Sicherheitskonzepts nachweisen.

Der Nachweis gegenüber der gematik MUSS durch die Vorlage eines ~~„Certification Practice Statements“~~ Sicherheitsgutachtens auf Basis des Sicherheitskonzepts erfolgen. Nur nach erfolgter Genehmigung nimmt der gematik TSL-Service Provider den TSP in die zentrale Trust-service Status List auf.

Kapitel 2.5 Abgrenzung des Dokumentes

[...]

Die Details zum Ablauf der Registrierungsbedingungen und -prozesse für die Zertifikate der Versicherten sind durch die Kostenträger zu definieren und im jeweiligen ~~„Certification Practise Statement“ bzw.~~ Sicherheitskonzept darzulegen.

Für die Zertifikate der HPC gelten ~~zusätzlich~~ die Anforderungen aus ~~[BÄK_POL]~~ [CP-HPC] in der jeweils gültigen Fassung.

[...]

Kapitel 3.1 Überblick

Alle an der Telematikinfrastruktur (TI) beteiligten Trustcenter, genauer ausgedrückt „Trust-Service Provider“ (TSP) müssen aus Gründen des Datenschutzes ein Mindestsicherheitsniveau einhalten. Dieses ~~wird~~ muss anhand eines vom TSP für diesen Zweck erstellten Sicherheitskonzepts nachgewiesen werden ~~„Certification Practice Statements“ durch die gematik oder von ihr Beauftragte geprüft~~ Das von einem unabhängigen Gutachter erstellte Sicherheitsgutachten muss bestätigen, dass der TSP das Mindestsicherheitsniveau erfüllt und dies in einem Sicherheitskonzept ausreichend beschrieben hat. Auf dieser Basis erfolgt die Aufnahme des Root- bzw. des CA-Zertifikats des TSP in eine signierte XML-Liste, die „Trust-Service Status List“ (TSL)

Kapitel 3.1.1 Ziel dieser Policy

Der Prozess der Aufnahme in die gematik TSL orientiert sich grundsätzlich an den Wertmaßstäben

- technische Konformität und
- angemessene und vergleichbare Sicherheitslevel.

Das vorliegende Dokument adressiert vorrangig den zweiten Wertmaßstab, da die entsprechenden Vorgaben zur Konformität durch andere Dokumente vorgegeben werden. Ein Herausgeber von Zertifikaten (TSP), der in die „Trust-service Status List“ der gematik

aufgenommen werden will, MUSS ~~zukünftig~~ ein ~~eigenes CPS~~ Sicherheitskonzept erstellen, ~~das mit dieser Gliederung nach RFC 3647 konform ist.~~ Dieses dient der Erfüllung der folgenden Ziele:

- ~~Der formale Aufbau nach dem international anerkannten Rahmenwerk nach RFC 3647 verbessert die Transparenz und Vergleichbarkeit gegenüber der bisher üblichen Praxis. Durch das Dokument wird eine sichtbare Vergleichbarkeit der Policies und damit der Sicherheitsniveaus erreicht.~~

- In der Erklärung zur Aufnahme eines TSP in die gematik TSL sind für die teilnehmende PKI und deren Architektur Mindestanforderungen formuliert. Diese CP präzisiert einerseits diese Mindestanforderungen, andererseits bietet diese Policy die Möglichkeit, dass die Selbsterklärung auf die Erfüllung dieser Policy verweist. So kann eine Aktualität der geforderten Sicherheitslevels erzielt werden.

- Das vorliegende Dokument bzw. seine teilnehmerspezifische Ausprägung bietet die Möglichkeit, als Referenzdokument für vertragliche Regelungen zwischen den Nachfragern (z. B. Kostenträgern) und Anbietern (z. B. Kartenpersonalisierern) von Trust-Services zu dienen (geeignet als Basis für Ausschreibungen und Verträge).

Kapitel 3.1.3 Der gematik-TSL-Service Provider und seine Teilnahmebedingungen

Absatz 4

Die Einhaltung der Mindestanforderungen zur Aufnahme in die gematik TSL MUSS ~~MÜSSEN~~ durch den TSP mit ~~in~~ einem ~~eigenen~~ ~~Sicherheitskonzept~~ Sicherheitsgutachten ~~berücksichtigt~~ nachgewiesen sein, welches auf das Sicherheitskonzept Bezug nimmt. Begründete Abweichungen sind nach ausdrücklicher Bestätigung durch die gematik möglich.

Kapitel 4 Allgemeine Maßnahmen

Ist der TSP ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung nach SigG, genügt statt Vorlage des ~~Sicherheitskonzepts~~ Sicherheitsgutachtens die Vorlage der entsprechenden Akkreditierung sowie eine Erklärung, die Maßnahmen des Sicherheitskonzepts anzuwenden.

Dieser Grundsatz gilt für dieses und alle weiteren Kapitel dieses Dokuments.

Kapitel 6.1 Zertifikatsantrag durch TSP (TSP + Root-TSP)

Letzter Absatz

Ist der TSP ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung nach SigG, genügt statt Vorlage des ~~Sicherheitskonzepts~~ Sicherheitsgutachtens die Vorlage der entsprechenden Akkreditierung sowie die Erklärung, die Maßnahmen des Sicherheitskonzepts anzuwenden.

Teil 2: weitere Änderungen

Kapitel 2.1 Zielsetzung und Einordnung des Dokumentes

Der folgende Text wird als 1. Absatz hinzugefügt:

Diese Policy trifft Vorgaben sowohl für TSP, die als Root-Instanz fungieren, als auch für diejenigen, die innerhalb einer Zertifizierungshierarchie nachgeordnet sind und Aussteller von Zertifikaten für eGK und SMC-B sind. Des Weiteren werden Aussagen bzgl. der Erstellung von

Endnutzer-Zertifikaten getroffen. Der Geltungsbereich der jeweiligen Vorgaben ist aus der Kapitelüberschrift ersichtlich.

3.3.7 gematik (neues Kapitel)

Die gematik trifft mit dem vorliegenden Dokument als Policy Authority die Vorgaben für die Aufnahme eines TSP in den Vertrauensraum der TSL. In Aufgabenteilung und enger Absprache mit den Leistungserbringerorganisationen trifft sie die Vorgaben für den Aufbau der auf den jeweiligen Kartentypen eGK, SMC-B und HBA eingesetzten X.509- Zertifikate. Weiterhin fungiert die gematik als Registrierungsinstanz für den gematik TSL-SP.

~~**3.3.7 Andere Teilnehmer**~~ **3.3.8 Andere Teilnehmer**

Kapitel 4.1.1 Verzeichnisse (TSP + Root-TSP)

Anforderung an TSP bezüglich OCSP-Responder.

Der TSP MUSS den Zertifikatsnutzern Zugriff auf Gültigkeitsinformationen in Form eines OCSP-Responders zur Verfügung stellen.

Kapitel 5.1.4 Notwendigkeit für aussagefähige und eindeutige Namen

Bei der Vergabe von Namen (Nutzer- oder PKI-Zertifikate) ~~muss~~ MUSS sichergestellt sein, dass der gewählte distinguishedName des Zertifikatsnehmers innerhalb des ausstellenden TSP eindeutig ist. Durch die Verwendung der Namensform in Kapitel 5.1.2 wird die Eindeutigkeit sichergestellt. Der ausstellende TSP MUSS sicherstellen, dass die Daten in dieser Form aufbereitet werden. Die Integrität und Vollständigkeit der Daten liegt in der Hoheit der Herausgeber der Zertifikate ~~jeweiligen Registrierungsstellen (bei Versicherten ist dies der Kostenträger)~~.

Kapitel 6.9 Sperrung und Suspendierung von Zertifikaten (TSP + Root-TSP + Endanwender)

Es wird die Sperrung und Suspendierung von Zertifikaten näher beschrieben.

Der TSP muss den Sperrberechtigten einen Sperrdienst zur Verfügung stellen.

A4. Referenzierte Dokumente

[...]

Weitere Referenzen

[CP-HPC]	Gemeinsame Policy für die Ausgabe der HPC Version: 1.0.0 vom 08.06.2009 Object Identifier: 1.2.276.0.76.4.62 {policy-hba-010000-cp} http://www.baek.de/downloads/CP_HPC_v1.0.0_19062009.pdf
~~[BÄK_POL]~~	~~Bundesärztekammer (03.03.2006/08.02.2006): Gemeinsame Policy für die Herausgabe der HPC, inkl. Anlage zum Gültigkeitsmodell V0.9.3; Rechtliches Niveau und rechtliche Einordnung der ausgestellten Zertifikate sowie Anhang zum Gültigkeitsmodell (Kompromissmodell)~~