Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Grund der Änderung

Die gematik hat nach den beim 36C3 aufgedeckten Sicherheitsmängeln bei der Ausgabe von HBA und SMC-B den gesetzlichen Auftrag erhalten (PDSG §311), die Sicherheit der in der Telematikinfrastruktur genutzten Identifikations- und Authentifizierungsverfahren, insbesondere der Karten und Ausweise (gemäß §§ 291 und 340) sowie deren Ausgabeprozesse zu koordinieren, zu überwachen und bei Sicherheitsmängeln verbindliche Vorgaben zu machen.

Um diesem Auftrag nachzukommen, werden Änderungen an den Spezifikationen bzw. an der gematik Certificate Policy [gemRL_TSL_SP_CP] in der folgenden Form vorgenommen.

Die grün, gelb oder rot markierten Anpassungen haben Auswirkungen auf die Anbieter HBA und/oder Anbieter SMC-B. Hierbei wird der Spezialfall „Einsatz eines HSM" anstelle der Ausgabe von Karten nicht berücksichtigt. Einzelne Afo sind in diesem Fall nicht anwendbar. Der Ausschluss dieser erfolgt über die jeweiligen Anbietertypsteckbriefe. Zum aktuellen Zeitpunkt betrifft dies folgende Afo innerhalb der [gemRL_TSL_SP_CP]: A_20115, A_20971, A_20972, A_20973, A_20966.

Hinweis: Die gelb markierten Textstellen sind bereits in Release 4.0 über den Änderungseintrag C_10061 in die Dokumente eingeflossen. Die grün markierten Textstellen stellen die Anpassungen des Changes C_10298 für das Hotfix dar. Die rot markierten Textstellen wurden im Rahmen der Kommentierung zum 26.11.2020 angepasst.

Änderung in gemRL_TSL_SP_CP:

[...]

1.4 Abgrenzung des Dokuments

~~Die vorliegende Certificate Policy ist auf Zertifikate für HBAs in der Produktivumgebung nicht anwendbar.~~ Als führende Certificate Policy für HBAs ~~Für diese~~ gilt weiterhin die „Gemeinsame Policy für die Ausgabe der HPC" [CP-HPC]. Einzelne übergeordnete Anforderungen zum Herausgabeprozess für HBAs sind zusätzlich in dem vorliegenden Dokument geregelt.

Für sämtliche Zertifikate der HBA (nonQES, Pseudo-QES) in der Test- und Referenzumgebung gelten die Festlegungen dieser Certificate Policy gemäß Anhang B.

Anforderungen an den Anbieter des TSL-Dienstes (in Vorversionen des Dokumentes als „TSL-SP" bezeichnet) werden in der Spezifikation des TSL-Dienstes [gemSpec_TSL] beschrieben.

Anforderungen an die Vertrauensdiensteanbieter (VDA) qualifizierter X.509-Zertifikate (TSP-X.509 QES) werden in [eIDAS] festgelegt.

Anforderungen an die Anbieter von CV-Zertifikaten (TSP-CVC) werden in der Spezifikation des TSP-CVC beschrieben [gemSpec_CVC_TSP]

[…]

2.1.3 Rahmen dieser Richtlinie

Diese Richtlinie trifft Vorgaben sowohl für TSPs, die als Root-Instanz (gematik Root-CA) fungieren, als auch für TSPs, die innerhalb einer Zertifizierungshierarchie nachgeordnet sind (TSP-X.509 nonQES). Für den TSP-X509 nonQES werden zudem Anforderungen bzgl. der Erstellung von Endnutzer-Zertifikaten gestellt. Sofern in dieser Richtlinie Anforderungen an einzelne Sicherheitsmaßnahmen nicht spezifiziert und nicht durch andere normative Dokumente der gematik gefordert werden, sind diese mindestens an die entsprechenden Maßnahmenkataloge des [BSI_2020] und der internationalen Rahmenwerke [ISO27001] und [ISO27002] anzulehnen.

[…]

Umbenennung des folgenden Kapitels:

4.2 ~~Erstmalige~~ Überprüfung der Identität

Neues Unterkapitel mit dem darunter folgenden Inhalt:

4.2.7 Sicherheit der Herausgabeprozesse für Karten sowie Personen- und Organisations-Zertifikate

Umbenennung der Anforderung

A_20112-02 – Sichere Identifizierung von Zertifikatsnehmern

Ein Anbieter HBA und Anbieter SMC-B MUSS die Herausgabeprozesse derart gestalten, dass eine sichere eindeutige Identifizierung des Zertifikatsnehmers im Rahmen des Antragsprozesses sichergestellt ist. Eine Antragstellung durch einen Vertreter oder Bevollmächtigten ist nur für die SMC-B zulässig. <=

Die Identifikation bei Antragstellung erfolgt stets als natürlichen Person, welche im Falle HBA mit der juristischen Person des Antragstellers identisch ist. Im Falle der SMC-B ist durch den Kartenherausgeber eine Prüfung auf Berechtigung der Antragstellung der natürlichen Person für die juristische Person durchzuführen. Die einzusetzenden Identifikationsverfahren sind zwischen dem Anbieter, Kartenherausgeber, der Bundesnetzagentur (nur HBA) und der gematik vorab abzustimmen. Grundsätzlich sind die Prozesse der Identifikation des Zertifikatsnehmers an [TR_3107] anzupassen und gemäß des Abschnitts 3.2.1 [TR_3107] für das Vertrauensniveau „hoch" umzusetzen.

Hierbei werden die Anforderungen aus 3.5.2 der [TR_3107] an die Herausgeber als abdingbar betrachtet. Insbesondere besteht für die Herausgeber keine Notwendigkeit eine Zertifizierung nach [BSI_2020] oder [ISO27001] vorzuweisen. Zusätzlich wird die Tabelle 5, Abschnitt 5.3 [TR-3107] als nicht abschließend betrachtet. Die Nutzung der eID-Funktion ist möglich, jedoch nicht erforderlich.

Werden Identifikationsverfahren mit bestehenden Zertifizierungen nach [eIDAS] oder ETSI verwendet, können diese Zertifizierungen berücksichtigt werden. Bei nicht vorliegenden Einstufung des Vertrauensniveaus nach [eIDAS LoA] oder [TR_3107] ist lediglich eine Einstufung des Vertrauensniveaus im Rahmen des

Sicherheitsgutachtens durch den Sicherheitsgutachter erforderlich. Eine Zertifizierung des Sicherheitsniveaus oder des gesamten Identifikationsverfahrens wird nicht verlangt.

~~Wird eines der unten aufgeführten Identifikationsverfahren eingesetzt, so ist eine Information an die gematik ausreichend.~~

~~Die im Folgenden aufgeführten Identifikationsverfahren sind aufgeteilt nach den in A_20112 aufgeführten Teil-Prozessschritten und stellen bespielhaft aber nicht abschließend sichere Verfahren dar. Die abschließende erfolgt dabei im Rahmen eines Sicherheitsgutachtens.~~

~~Identifikationsverfahren bei Beantragung:~~

~~Sichere Identifikationsverfahren können dabei im Rahmen der Beantragung von Karten und Zertifikaten sein:~~

- ~~PostIdent~~
- ~~KammerIdent~~
- ~~VideoIdent~~
- ~~sonstiges eIDAS-konformes Verfahren~~
- ~~Verifikation durch den Herausgeber oder den Anbieter über dritten Kanal (z.B. sichere E-Mail, Telefon, Fax)~~
- ~~Starke Authentisierung mit QES-Zertifikat einer Vorgänger-Karte (nur im Falle HBA)~~
- ~~Starke Authentisierung mit QES-Zertifikat einer mindestens gleichwertigen anderen Karte (z.B. nPA).~~

~~Die Identifikationsverfahren müssen im Falle HBA den eIDAS-konformen und von der Bundesnetzagentur zugelassenen Verfahren entsprechen.~~

~~Im Rahmen der Beantragung ist ergänzend beispielweise auch eine Beantragung über das Antragsportal mit durch den Kartenherausgeber vorbefüllten Antragsdaten möglich. Wenn dabei eine Sperrung der vorbefüllten Adressdaten für den Antragssteller implementiert ist, ist das auch als sicheres Verfahren zu betrachten.~~

Entfall der Anforderung

~~A_20113 – Auslieferung von Karten an verifizierte Adressen~~

~~Ein Anbieter HBA und ein Anbieter SMC-B MUSS sicherstellen, dass personalisierte Karten und die entsprechenden PIN-Briefe nur an verifizierte Adressen ausgeliefert werden. <=~~

~~Die Auslieferung des HBA ist aufgrund der darauf enthaltenen QES-Zertifikate integraler Bestandteil der eIDAS-konformen Prozesse des Anbieters. Die Auslieferung ist dabei nur an die Adresse zulässig, die im Rahmen des Identifikationsprozesses bei Beantragung angegeben wurde.~~

Im Fall der SMC-B erfolgt die Verifikation der Lieferadresse anhand der zur jeweiligen Institution vorliegenden Daten des Kartenherausgebers.

Verifikationsverfahren bei Auslieferung:

Sichere Verifikationsverfahren können dabei im Rahmen der Auslieferung sowohl von Karten als auch der PINs sein:

- Bestätigung der Lieferadresse durch den Herausgeber
- Einschreiben eigenhändig (oder gleichwertiges Verfahren)
- Verifikation bei persönlicher Übergabe durch vertrauenswürdigen Dienstleister
- sonstiges eIDAS-konformes Verfahren
- Verifikation durch den Herausgeber oder den Anbieter über dritten Kanal (z.B. sichere E-Mail, Telefon, Fax)

Die Bestätigung der Lieferadresse durch den Herausgeber kann durch die Bereitstellung eines mit der Lieferadresse vorbefüllten Antrages erfolgen. Desweiteren kann dies über einen dritten Kanal (z.B. sichere E-Mail, telefonische Auskunft) durch den Kartenherausgeber erfolgen.

Identifikationsverfahren bei Freischaltung:

Sichere Identifikationsverfahren können im Rahmen der Freischaltung von Karten und Zertifikaten sein:

- Einschreiben eigenhändig (oder gleichwertiges Verfahren)
- VideoIdent
- sonstiges eIDAS-konformes Verfahren
- Verifikation durch den Herausgeber oder den Anbieter über dritten Kanal (z.B. sichere E-Mail, Telefon, Fax)
- starke Authentisierung mit QES-Zertifikat einer Vorgänger-Karte (nur im Falle HBA)
- starke Authentisierung mit QES-Zertifikat einer mindestens gleichwertigen anderen Karte

Entfall der Anforderung

A_20114 – Identifikationsverfahren in zwei von drei Schritten

Ein Anbieter HBA und ein Anbieter SMC-B MUSS im Rahmen des sicheren Gesamtprozesses für die Kartenherausgabe sicherstellen, dass eine Auslieferung an alternative Lieferadresse nur dann erfolgt, wenn diese bereits bei der Beantragung vom Zertifikatsnehmer angegeben wurde. Zusätzlich MUSS eine sichere Identifizierung des Empfängers als Zertifikatsnehmer (bei HBA oder SMC-B) oder als zur Entgegennahme berechtigter Vertreter (nur SMC-B) bei Übergabe erfolgen. mindestens in zwei der drei Prozessschritte (Beantragung, Auslieferung, Freischaltung) eines der dabei in diesem Kapitel aufgeführten sicheren Identifikations- bzw. Verifikationsverfahren verwenden. <=

Neue Anforderung

A_20979 – Alternative Identifikation des Antragstellers bei Übergabe

Ein Anbieter HBA und ein Anbieter SMC-B DARF von der Anforderung A_20112-02 abweichen und die Identifikation des Antragsstellers, unter Einhaltung der Anforderungen aus A_20112-02 an die Identifikation des Antragsstellers, ausschließlich bei der Übergabe durchführen. <=

Es sind durch den Anbieter technische und/oder organisatorische Maßnahmen zur Unterbindung massenhafter, unberechtigter Antragsstellungen zu implementieren.

Neue Anforderung
A_20971 – Nachverfolgbarkeit beim Versand von Karten und PIN-Briefen
Ein Anbieter HBA und Anbieter SMC-B MUSS die Nachverfolgbarkeit beim Versand von Karten und PIN-Briefen sicherstellen. <=

Nachverfolgbarkeit bedeutet unter anderem, dass die Zustellung dokumentiert und für den Versender auch nachvollziehbar ist. Eine persönliche Identifikation des Empfängers kann gegeben sein, ist jedoch nicht zwingend erforderlich.

Neue Anforderung
A_20972 – Keine Nachsendung von Karten und PIN-Briefen
Ein Anbieter HBA und ein Anbieter SMC-B MUSS sicherstellen, dass Karten und PIN-Briefe nicht durch z.B. Nachsendeaufträge an andere Adressen als die in der Antragstellung angegebene übermittelt werden. <=

Neue Anforderung
A_20973 – Unveränderbarkeit der Versandadresse
Ein Anbieter HBA und ein Anbieter SMC-B MUSS sicherstellen, dass während des Gesamtprozesses der Kartenherausgabe eine Veränderung der Versandadresse, welche im Rahmen der Antragstellung angegeben wurde, durch Dritte ausgeschlossen ist. <=

Sollte eine Zustellung nach A_20971 fehlschlagen, darf der Anbieter zur Vermeidung eines Neustarts des Prozesses (inkl. Sperrung und Vernichtung der nicht zugestellten Karte) auf eine ihm bereits bekannte, verifizierte und eindeutig zum Antragssteller zugehörige Adresse ausweichen. Dies kann unter anderem die Meldeadresse (gemäß Ausweisdokument) bei HBA oder die Betriebsanschrift (z.B. Krankenhaus/Apotheke) bei SMC-B sein.

Neue Anforderung
A_20966 – Sicherheit des Gesamtprozesses

Im Gesamtprozess der Kartenherausgabe MUSS ein Anbieter HBA und Anbieter SMC-B sicherstellen, dass private Schlüssel vor der Verwendung durch unberechtigte Dritte geschützt werden. <=

Die abschließende Bewertung der Sicherheit des Gesamtprozesses durch das Zusammenwirken der Identifikationsverfahren in den Teil-Prozessschritten erfolgt dabei mittels eines Sicherheitsgutachtens im Rahmen der Anbieterzulassung.

A_20115 – Herausgabe von Nachfolgekarten

Ein Anbieter HBA und Anbieter SMC-B MUSS sicherstellen, dass eine Herausgabe von Nachfolgekarten ohne erneute Identifizierung des Zertifikatsnehmers nicht möglich ist. <=

Die bereits ausgegebenen Karten können im Identifikationsverfahren bei der Bestellung von Nachfolgekarten im Rahmen der Antragstellung verwendet werden, soweit technisch möglich. Hierbei muss sichergestellt sein, dass die Identifikation mittels der bestehenden Karte mindestens das Sicherheitsniveau gemäß A_20112-02 erreicht.

A_20116 – Sicherung eines Beantragungs-Portals

Wenn der Anbieter HBA und Anbieter SMC-B ein Online-Portal zur Beantragung, Freischaltung oder Sperrung von Zertifikaten und Karten verwendet, MUSS er dieses gesichert und nach dem aktuellen Stand der Technik bereitstellen. <=

[...]

12.4.2 Weitere Dokumente

[eIDAS LoA] → DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

[BSI_2020] → Edition 2020 des IT-Grundschutz-Kompendiums https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html

[TR_3107] → TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

~~[BSI_2005]~~

~~[ISO17799]~~

[ISO27001] → ISO/IEC 27001:2013 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques

[ISO27002] → ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security