gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Richtlinie für die Herausgabe der Prüfkarten des Typs eGK

Version:	1.0.0
Revision:	
Stand:	07.12.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemRL_PK_eGK]

Dokumentinformationen

Änderungen zur Vorversion

Ersterstellung des Dokuments.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	07.12.18		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Ziel dieses Dokuments ist es, die Prozesse für die Ausstellung und Sperrung von nicht-qualifizierten X.509-Zertifikaten (TSP-X.509 nonQES) im Rahmen der Ausgabe von Prüfkarten des Typs eGK (im weiteren Verlauf des Dokuments als Prüfkarte eGK bezeichnet) angelehnt an [gemRL_TSL_SP_CP] zu beschreiben.

1.2 Zielgruppe

Das Dokument richtet sich an Anwender von Prüfkarten des Typs eGK.

1.3 Geltungsbereich

Dieses Dokument enthält Informationen zur Erstellung und Sperrung von Zertifikaten der Prüfkarten eGK in der Produktivumgebung der TI. Die entsprechenden Prozesse und konkrete Vorgaben werden durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokuments

In der Richtlinie [gemRL_TSL_SP_CP] der gematik werden die Sicherheitsanforderungen hinsichtlich der Erzeugung, Verwaltung und Sperrung von nicht-qualifizierten X.509-Zertifikaten definiert. Die vorliegende Certificate Policy ersetzt diese nicht.

Anforderungen an den Anbieter des TSL-Dienstes werden in der Spezifikation des TSL-Dienstes [gemSpec_TSL] beschrieben.

Anforderungen an die Anbieter von CV-Zertifikaten (TSP-CVC) werden in der Spezifikation des TSP CVC beschrieben [gemSpec_CVC_TSP]. In dieser Certificate Policy werden CV-Zertifikate (Card Verifiable Certificates) als informativ betrachtet.

Für den Trust Service Provider Prüfkarte eGK wird im Verlauf des Dokuments der Begriff „TSP-X509 nonQES“ verwendet. Generelle Anforderungen an alle TSP-X509 nonQES bzgl. der Antragstellung, Erzeugung und Sperrung von X.509-Personen-, Organisations-, Komponenten-, Signer-Zertifikaten sowie die Bereitstellung der Zertifikatsstatusinformation sind in [gemSpec_X.509_TSP] beschrieben.

Sämtliche geltende Anforderungen an die personalisierte Prüfkarte eGK sind in der Spezifikation [gemSpec_PK_eGK] beschrieben.

2 Einleitung fachlicher Teil

2.1 Überblick

Die Prüfkarte eGK ist eine speziell ausgestattete elektronische Gesundheitskarte. Mit der Prüfkarte eGK kann der Dienstleister vor Ort (DVO) die erfolgreichen Online-Anbindung bspw. einer Praxis an die TI verifizieren. Darüber hinaus kann mithilfe der Prüfkarte eGK kontrolliert werden, ob das verwendete Primärsystem auf die eGK fehlerfrei zugreift und die Versichertenstammdaten korrekt ausliest und anzeigt.

Die Prüfkarte eGK hat die Eigenschaften einer echten Versichertenkarte (eGK). Aber durch geeignete Maßnahmen der elektrischen und optischen Personalisierung werden der Missbrauch und die Verwechselung mit einer echten eGK der PU (Echtkarte eGK) ausgeschlossen.

Die Benutzung der Prüfkarte eGK kann durch Kartensperrung unterbunden werden.

3 Identifizierung und Authentifizierung

3.1 Namensregeln

3.1.1 Arten von Namen

Detaillierte Vorgaben zur Namensvergabe in Zertifikaten von Prüfkarten eGK sind [gemSpec_PK_eGK] und [gemProdT_PK_eGK] zu entnehmen.

3.1.2 Aussagekraft von Namen

Generelle Vorgaben an die Namensregeln und Formate sind im Dokument „Spezifikation PKI“ [gemSpec_PKI#4.1] beschrieben. Abweichungen hiervon sind [gemSpec_PK_eGK] zu entnehmen.

3.1.3 Notwendigkeit für aussagefähige und eindeutige Namen

Die Zertifikate von Prüfkarten eGK werden durch die Vorgaben der gematik zur Namensvergabe deutlich als solche kenntlich gemacht (siehe Kapitel 6 Format der Zertifikate). Die Namen sind aber nicht eindeutig, sondern für alle Prüfkarten eGK gleich.

3.1.4 Anonymität oder Pseudonyme von Zertifikatsnehmern

Die Verwendung der pseudonymen Zertifikate C.CH.AUTN und C.CH.ENCV ist für Prüfkarten eGK optional.

3.2 Überprüfung der Identität

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Ein TSP-X.509 nonQES muss für die Ausgabe von Zertifikaten der Prüfkarten eGK auf Prozesse und Vorgaben, die eine Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer gewährleisten, verzichten.

Ein TSP-X.509 nonQES muss zur Benennung von Zertifikatsnehmern von Zertifikaten der Prüfkarten eGK die Auftragsdaten der gematik verwenden, welche keinen Bezug zu echten Personen oder Organisationen haben. Details sind [gemSpec_PK_eGK] zu entnehmen.

4 Betriebliche Maßnahmen

4.1 Zertifikatsausgabe

Die X.509-Zertifikate einer PK eGK werden im Gegensatz zu den eGK von Versicherten von einer separaten SubCA abgeleitet.

Die selbstsignierten CA-Zertifikate werden für die Aufnahme in die TSL dem Anbieter des TSL-Dienstes zur Verfügung gestellt.

4.2 Zertifikatserneuerung

Die Erneuerung von Zertifikaten der Prüfkarten eGK ist nicht vorgesehen.

4.3 Zertifikatsänderung

4.3.1 Sperrung und Suspendierung von Zertifikaten der Prüfkarte eGK

Eine Suspendierung/Desuspendierung von X.509-Zertifikaten der Prüfkarten eGK ist nicht vorgesehen.

Nur Sperrberechtigte dürfen eine Sperrung von Endanwenderzertifikaten vornehmen.

Als sperrberechtigt ist nur die gematik vorgesehen.

4.3.2 Bedingungen für eine Sperrung

Die gematik kann EE-Zertifikate der Prüfkarten eGK jederzeit ohne Angabe von Gründen sperren.

Der Besteller ist verpflichtet bei Verlust einer oder mehrerer Prüfkarten eGK diesen unverzüglich an die gematik zu melden.

4.3.3 Verfahren für einen Sperrantrag

Für die Kartensperrung senden Sie bitte eine E-Mail an betrieb@gematik.de mit dem Betreff „Kartensperrung Prüfkarte eGK“ und den folgenden Daten:

- Name des Käufers bzw. Inhabers der Prüfkarte eGK
- Name des Sperrantragstellers, falls nicht der Käufer bzw. Inhaber selbst die Sperrung beantragt
- Kartennummer

Ihre Daten werden geprüft und die Sperrung wird veranlasst.

Eine einmal gesperrte Prüfkarte eGK kann nicht wieder entsperrt werden. Eine weitere Nutzung ist somit ausgeschlossen.

4.3.4 Online-Verfügbarkeit von Sperrinformationen

Die in der PK eGK personalisierten X.509-Zertifikate sind während ihres Gültigkeitszeitraumes jederzeit mittels OCSP in der TI validierbar.

5 Sicherheitsmaßnahmen

Da die Zertifikatsnehmer von Zertifikaten der Prüfkarten eGK keine realen Personen oder Organisationen sind, werden trotz des Einsatzes der Prüfkarten eGK in der Produktivumgebung, keine besonderen Sicherheitsanforderungen gestellt.

Ein TSP-X.509 nonQES soll die Gültigkeitsdauer eines ausgestellten Zertifikats der Prüfkarte eGK gemäß den Vorgaben an die Gültigkeitsdauer von Zertifikaten, die für den Einsatz in der Produktivumgebung vorgesehen und vom gleichen Typ sind, begrenzen.

5.1 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Nutzungsdauer von Zertifikaten der Prüfkarten eGK soll nach [gemSpec_Krypt] auf maximal 5 Jahre beschränkt werden. Diese Vorgabe wird für die Endbenutzerzertifikate umgesetzt.

Die Gültigkeit der CA- und Endbenutzerzertifikate kann zudem durch die Verwendung einer TSL während des laufenden Betriebs weiter eingeschränkt werden, da die TSL in diskreten Zeitabständen aktualisiert und veröffentlicht wird. Hierdurch kann ein zu einer kürzeren Gültigkeitsdauer der Zertifikate äquivalentes Sicherheitsniveau erreicht werden.

6 Format der Zertifikate

Ein TSP-X.509 nonQES muss für die Ausstellung von Zertifikaten der Prüfkarten eGK das Zertifikatsprofil von Zertifikaten, die für den Einsatz in der Produktivumgebung vorgesehen und vom gleichen Typ sind, verwenden.

Die Festlegung der Datenformate und Zertifikatsprofile erfolgt in [gemSpec_PKI]. Abweichungen hiervon sind [gemSpec_PK_eGK] zu entnehmen.

Es gibt keine personalisierten Daten. Die Zertifikate aller Prüfkarten eGK werden identisch mit den folgenden Inhalten erstellt:

- organizationName: *Test GKV-SV*
- givenName: *Dienstleister vor*
- surname: *Ort*
- commonName: *Dienstleister vor Ort*

Anhang C – Verzeichnisse

C1 – Abkürzungen

Kürzel	Erläuterung
CA	Certificate Authority
eGK	Elektronische Gesundheitskarte
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PKI	Publik Key Infrastructure
QES	Qualifizierte elektronische Signatur
TI	Telematikinfrastruktur
TSL	Trust-Service Status List
TSP	Trust-Service Provider
TSP-X.509 nonQES	Trust-Service Provider für nicht-qualifizierte X.509-Anwenderzertifikate

C2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

C3 – Referenzierte Dokumente

C3.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

[Quelle]	Herausgeber: Titel
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_Krypt]	gematik: Spezifikation Kryptographie (bis Release 0.5.3: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur)
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_X.509_TSP]	gematik: Spezifikation Trust Service Provider X.509
[gemSpec_PK_eGK]	gematik: Spezifikation für Prüfkarten eGK der Generation 2.1
[gemProdT_PK_eGK]	gematik: Produkttypsteckbrief Prüfvorschrift Prüfkarte eGK