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.

Änderungsbedarf in gemSpec_PKI

Dokument	Referenz	Anpassung
gemKPT_PKI_TIP	2.7.3 Kartenherausgeber	Kartenherausgeber (Gesellschafterorganisationen (ORG), Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller) sind für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig. ⌦ **TIP1-A_2094 Rollenautorisierung von TSP durch Kartenherausgeber** Die Kartenherausgeber MÜSSEN die von ihnen beauftragten TSP bzgl. der Einbringung von Zertifikatsattributen für Rollen (Zugriffsprofile) in die Zertifikate autorisieren.⌫ ⌦ **TIP1-A_2098 Umsetzung von Sperraufträgen durch Berechtigte** TSP-X.509QES und TSP-X.509nonQES MÜSSEN für die von ihm herausgegebenen Zertifikate Sperraufträge umsetzen, unter Anwendung der Berechtigungen gemäß Tab_PKI_107 sowie nach Authentifizierung und Berechtigungsprüfung der beauftragenden Person oder Organisationseinheit.⌫ **Tabelle 1: Tab_PKI_107 Übersicht der PKI-spezifischen Sperrgründe** [illegible] | [illegible] | [illegible] | Zertifikate der Kartenarten

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung

Sperrberechtigte Stellen *)		HBA	HBA	SMC-B	SMC-B	SMC-B		
	eGK	QES	nonQES	LEI	ORG	KTR	gSMC-K	FD, ZD
LE		1a	1a	1a				
med. Institution				1a				
Hersteller							1b	
Anbieter **)								1b, 3
Herausgebende LEO **)		2,5	2,5	2,5	2			
Zertifikatsnehmende LEO					1a			
GKV-Spitzenverband **)					2	2		
KTR **)	1a, 2				1a	1a		
gematik		3	3	3	3	3	1c,3	1c,3
BNetzA		4						

1a) Jederzeit ohne Angabe von Gründen

1b) Eventgetriggert im Rahmen eines definierten Incident-Prozesses mit den zuständigen und betroffenen

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung
		Parteien 1c) Jederzeit ohne Angabe von Gründen für Zertifikate, die für den Produkttyp Service Monitoring erstellt wurden 2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy 3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung 4) Verlust des Qualifikationsstatus des VDA für QES gemäß [eIDAS] 5) Wegfall oder Entzug geforderter Eigenschaften des VDA für QES /TSP gemäß Sektor-Zulassung *) Berechtigung für organisatorische Sperrungen gilt nur für den jeweiligen Herausgeber der Zertifikate **) In herausgeberspezifischen Policies können weitere Sperrgründe definiert sein.
gemRL_TSL_SP_CP	5.9.1 Bedingungen für eine Sperrung	⌦ **GS-A_4219 Sperrung von Anwenderzertifikaten** Ein TSP-X.509 nonQES MUSS für die von ihm herausgegebenen Anwenderzertifikate Sperraufträge umsetzen, unter Anwendung der Berechtigungen gemäß Tab_PKI_305 sowie nach Authentifizierung und Berechtigungsprüfung der beauftragenden Person oder Organisationseinheit.⌫ **Tabelle 2: Tab_PKI_305 Übersicht der PKI-spezifischen Sperrgründe** Zertifikate der Kartenarten

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung

Sperrberechtigte Stellen *)	eGK	HBA nonQES	SMC-B LEI	SMC-B ORG	SMC-B KTR	gSMC-K	FD, ZD
LE		1a	1a				
med. Institution			1a				
Hersteller						1b	
Anbieter **)							1b, 3
Herausgebende LEO **)		2,5	2,5	2			
Zertifikatsnehmende LEO				1a			
GKV-Spitzenverband **)				2	2		
KTR **)	1a, 2			1a	1a		
gematik		3	3	3	3	1c,3	1c,3

1a) Jederzeit ohne Angabe von Gründen

1b) Eventgetriggert im Rahmen eines definierten Incident-Prozesses mit den zuständigen und betroffenen

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung
		Parteien 1c) Jederzeit ohne Angabe von Gründen für Zertifikate, die für den Produkttyp Service Monitoring erstellt wurden 2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy 3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung 5) Wegfall oder Entzug geforderter Eigenschaften des VDA/TSP gemäß Sektor-Zulassung *) Berechtigung für organisatorische Sperrungen gilt nur für den jeweiligen Herausgeber der Zertifikate **) In herausgeberspezifischen Policies können weitere Sperrgründe definiert sein.
gemSpec_X.509_TSP	Tab_PKI_511	Gemäß Tabelle Tab_PKI_511 gelten folgende Zuständigkeiten für die berechtigte Antragstellung der X.509-Zertifikatstypen: **Tabelle 3: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate** (siehe unten)

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.NK.VPN	Hersteller	gematik	Konnektor
C.NK.VPN	Diensteanbieter, gematik	gematik	Service Monitoring

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung			
		C.SAK.AUT	Hersteller	gematik	Konnektor
		C.AK.AUT	Hersteller	gematik	Konnektor
		C.SMKT.AUT	Hersteller	gematik	Kartenterminal
		C.FD.TLS-C	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
		C.FD.TLS-C	Diensteanbieter, gematik	gematik	Service Monitoring
		C.FD.TLS-S	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
		C.CM.TLS-CS	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
		C.ZD.TLS-C *)	Diensteanbieter	gematik	Zentraler Dienst
		C.ZD.TLS-S	Diensteanbieter	gematik	Zentraler Dienst
		C.VPNK.VPN	Diensteanbieter	gematik	VPN-Zugangsdienst
		C.VPNK.VPN-SIS	Diensteanbieter	gematik	VPN-Zugangsdienst
		C.GEM.OCSP	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
		C.GEM.CRL	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
		C.HP.AUT	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer

© gematik – öffentlich_Entwurf

Dokument	Referenz	Anpassung

C.HP.ENC	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer
C.HCI.AUT	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle
C.HCI.ENC	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle
C.HCI.OSIG	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations-Geschäftsstelle/Betriebsstätte Kostenträgergeschäftsstelle

**) geplant*

Die Abbildung Abb_PKI_515 stellt die Zuständigkeiten der Rollen bei der Antragsstellung der Komponenten- und Signerzertifikate dar.

© gematik – öffentlich_Entwurf

Änderungsbedarf in gemSpec_Perf

4.2 Produkttypen der zentralen Zone der TI-Plattform

⌦ **GS-A_4155 Performance – zentrale Dienste – Verfügbarkeit**

Die Produkttypen Namensdienst, Sicherheitsgateway Bestandsnetze, VPN-Zugangsdienst, OCSP-Proxy, TSP-X.509QES (Komponente OCSP-Responder), TSP-X.509nonQES (Komponente OCSP-Responder), gematik-Root-CA (Komponente OCSP-Responder), Verzeichnisdienst, Service Monitoring und die Störungsampel MÜSSEN zur Hauptzeit eine Verfügbarkeit von 99,9% und zur Nebenzeit von 99% für alle Operationen der technischen Schnittstellen aufweisen.

Wartungsfenster dürfen nur in der Nebenzeit liegen. Genehmigte Wartungsfenster werden nicht als Ausfallzeit gewertet.

Hauptzeit ist Montag bis Freitag von 6 bis 22 Uhr sowie Samstag und Sonntag von 6 bis 20 Uhr. Alle übrigen Stunden der Woche sind Nebenzeit. Bundeseinheitliche Feiertage werden wie Sonntage behandelt, alle übrigen Feiertage wie Werktage.

Der Anschluss an das zentrale Netz muss über die Anschlussoption „Hohe Verfügbarkeit“ erfolgen. ⌫

⌦ **GS-A_5028 Performance – zentrale Dienste – Verfügbarkeit Produktivbetrieb**

Die Produkttypen Namensdienst, Sicherheitsgateway Bestandsnetze, VPN-Zugangsdienst, OCSP-Proxy, TSP-X.509QES (Komponente OCSP-Responder), TSP-X.509nonQES (Komponente OCSP-Responder), Verzeichnisdienst, Service Monitoring, ~~die~~ Störungsampel und das Zentrale Netz der TI MÜSSEN perspektivisch in der Produktivphase eine Verfügbarkeit zwischen 99,9% und 99,99% anbieten können.⌫

4.2.6 Produkttyp Service Monitoring

Für den Produkttypen Service Monitoring gelten folgende Anforderungen: [GS-A_4155], [GS-A_5028], [GS-A_3055],[GS-A_3058], [GS-A_4145].

© gematik – öffentlich_Entwurf