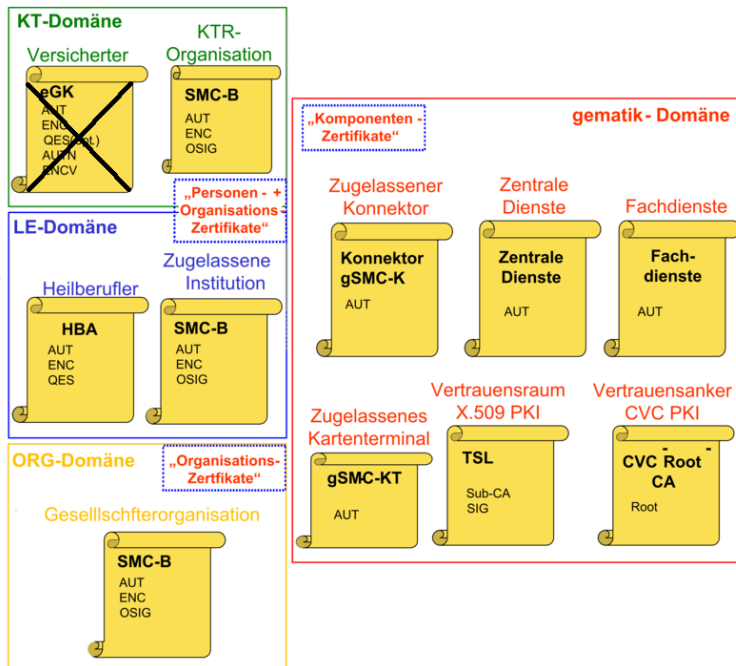


## Änderung in gemKPT\_PKI\_TIP

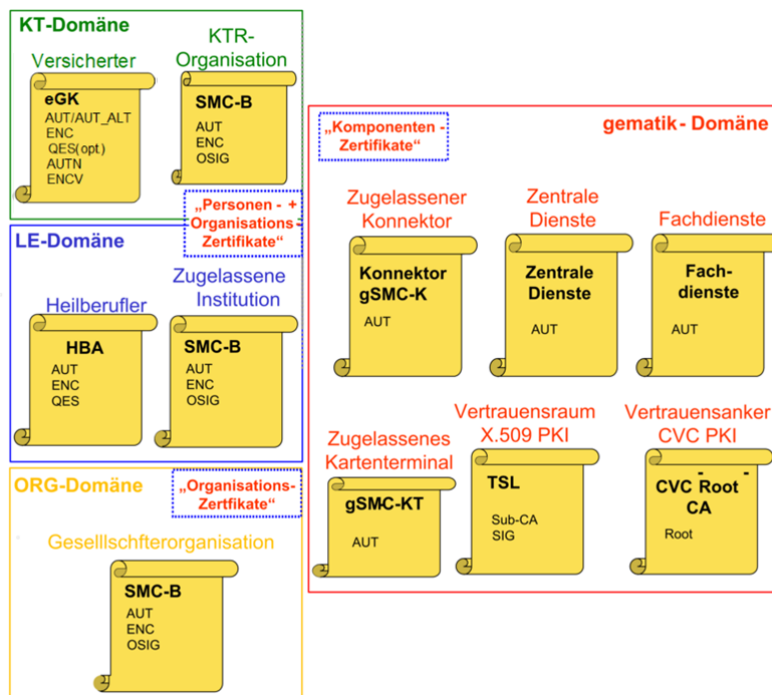
### 1.1 Kapitel 2.6 Verantwortliche Instanzen

(...)

Alt:



neu:



---

## 2 1.1 Kapitel 4.5 OCSP-Dienste

---

(...)

OCSP-Dienste für QES-Zertifikate müssen den Vorgaben von [eIDAS] genügen. Dies beinhaltet Konformität der OCSP-Zertifikatsprofile mit [RFC6960]. Wegen der Ausstellung der End-Entity-Zertifikate nach Kettenmodell kann wie oben erläutert die Vorgabe in [RFC6960#4.2.2.2] zur Ableitung der OCSP-Signer-Zertifikate nicht streng erfüllt werden.

Durch die Forderung nach der dauerhaften Prüfbarkeit für qualifizierte Signaturen auch bei Beendigung des Betriebs können folgende Fälle eintreten (vgl. [VDG§16], [VDV§4]):

- Die Bereitstellung der OCSP-Statusauskünfte wird von einer anderen qualifizierten CA übernommen. Diese qualifizierte CA kann auch von einem anderen qualifizierten Vertrauensdiensteanbieter betrieben werden oder
- die Bereitstellung der OCSP-Statusauskünfte wird von der Bundesnetzagentur übernommen. Für diesen Zweck stellt die Bundesnetzagentur ein dauerhaftes Verzeichnis (DA:VE) respektive OCSP-Signer und OCSP-Responder bereit.

DA:VE erteilt Auskunft zum Widerruf von Zertifikaten der Bundesnetzagentur und von Zertifikaten von Vertrauensdiensteanbietern, die ihren Betrieb gemäß § 16 Abs. 1 VDG bzw. § 13 Abs. 2 SigG eingestellt haben. Die technische Umsetzung basiert auf dem OCSP-Protokoll nach [RFC6960].

Aufgrund der fachlichen Gegebenheiten sind bei der Nutzung von DA:VE einige technische Besonderheiten zu beachten:

- Die OCSP-Antworten werden nicht für jede OCSP-Anfrage neu erzeugt, sondern liegen vorgefertigt und signiert vor.
- Sofern vorhanden, verwendet das System die ursprünglichen OCSP-Antworten der Anbieter, die den Betrieb eingestellt haben. Anderenfalls nutzt das System OCSP-Antworten, die von der Bundesnetzagentur signiert sind.
- Der Vertrauensstatus der zur Signatur der OCSP-Antworten gehörigen Zertifikate ist über die deutsche Vertrauensliste prüfbar. Dies gilt auch für die Zertifikate der Bundesnetzagentur.
- Bei OCSP-Anfragen zu Zertifikaten, die der Bundesnetzagentur nicht vorliegen, erfolgt anstelle der OCSP-Antwort „unknown“ eine Fehlermeldung (Quelle: Bundesnetz Agentur).

### 2.1.1 Kapitel 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Ärzte-ZV]	Zulassungsverordnung für Vertragsärzte (Ärzte-ZV) Zulassungsverordnung für Vertragsärzte auf der Grundlage des Artikel 9 des Gesetzes zur Verbesserung der Versorgungsstrukturen in der gesetzlichen Krankenversicherung (GKV-Versorgungsstrukturgesetz – GKV-VStG) vom 28.12.2011 (BGBl. I S. 3016)
[CP-HPC]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, gematik GmbH, Bezirksregierung Münster – eGBR, Deutscher Handwerkskammertag e.V. (14.09.2023): Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie Heilberufsausweis (Version 2.3.0) <a href="https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zertifizierungsrichtlinien#c4198">https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zertifizierungsrichtlinien#c4198</a>
(...)	(...)
[VDV]	Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV), Bundesministerium für Wirtschaft und Energie. Stand: 15.02.2019 <a href="https://www.gesetze-im-internet.de/vdv/BJNR011400019.html">https://www.gesetze-im-internet.de/vdv/BJNR011400019.html</a>

### Änderung in gemSpec\_PKI

### 2.1.2 Kapitel 11.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[SOG-IS]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.2, January 2020 <a href="https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf">https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf</a>
[BSI-TR-03110]	BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 20.03.2012 <a href="https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/TR-03110_node.html">https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/TR-03110_node.html</a>

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR-03111]	BSI (2012): Elliptic Curve Cryptography, Version 2.0 <a href="https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03111/TR-03111_node.html">https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03111/TR-03111_node.html</a>
[BSI-CC-PP-0098]	BSI (21.05.2021): Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor. Version 1.4 Neu: BSI-CC-PP-0098-V3-2021 BSI (03.07.2019): Common Criteria Schutzprofil (Protection Profile) Schutzprofil 2: Anforderungen an den Konnektor. Version 1.5.9 <a href="https://www.commoncriteriaportal.org/files/ppfiles/pp0098V3a_pdf.pdf">https://www.commoncriteriaportal.org/files/ppfiles/pp0098V3a_pdf.pdf</a>
[CP-HPC]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, gematik GmbH, Bezirksregierung Münster – eGBR, Deutscher Handwerkskammertag e.V. (14.09.2023): Gemeinsame Policy für die Ausgabe der Heilberufsausweise – Zertifikatsrichtlinie Heilberufsausweis (Version 2.3.0) <a href="https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zertifizierungsrichtlinien#c4198">https://fachportal.gematik.de/schnelleinstieg/downloadcenter/zertifizierungsrichtlinien#c4198</a>
[DIN5008]	DIN 5008 (2005): Schreib- und Gestaltungsregeln für die Textverarbeitung
(...)	