Änderung in gemSpec_Krypt (C_10861)

In Abschnitt [gemSpec_Krypt#2.1.1.2] wird vor Anforderung A_19083 die folgende Anforderung eingefügt (und dem Konnektor zugewiesen):

A_22220 - Konnektor: zulässige Algorithmen und Domainparameter bei Zertifikatsprüfungen
Ein Konnektor KANN bei einer Zertifikatsprüfung alle im SOGIS-Katalog [SOGIS-2020] als zulässig aufgeführten kryptographischen Signaturverfahren inkl. der dem jeweiligen Verfahren zugehörigen Domainparametern (Mindestschlüssellängen, Kurvenparameter etc.) für eine Zertifikatsprüfung verwenden. Die Angaben aus [gemSpec_Krypt#Tab_KRYPT_002 und _002a (und auch _003 und _003a)] können als Mindestvorgaben verstanden werden.**[**<=**]**

weiter werden folgende editorische Änderungen vorgenommen

1.

In Tab_KRYPT_003 in der vorletzten und letzten Tabellenzeile wird jeweils wie folgt geändert:

> ...
>
> zulässig bis ~~Ende 2022~~ vgl. Angabe in [SOG-IS-2020]
>
> ....
>
> zulässig bis ~~Ende 2024~~ vgl. Angabe in [SOG-IS-2020]
>
> ...

2.

In Abschnitt 6.1 wird ein informativer Satz wie folgt korrigiert:

> Aus dem gemeinsamen ECDH-Geheimnis ~~wird~~ werden mittels einer HKDF ~~ein~~ zwei AES-Schlüssel abgeleitet (A_16943-*).

Änderungen in gemProdT_Konnektor

Tabelle 1: Anforderungen für CC-Evaluierung

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22220	Konnektor: zulässige Algorithmen und Domainparameter bei Zertifikatsprüfungen	