
C_12370_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderungen in gemSpec_IDP_Sek.....	3
2.1 Änderungen in Kapitel 4.1 Entity Statement des sektoralen IDP.....	3
3 Änderungen in gemSpec_IDP_FD.....	4
3.1 Änderungen in Kapitel 4.3 Entity Statements.....	4
4 Änderungen in Steckbriefen.....	5
4.1 Änderungen in gemAnbT_IDP-Sek_KTR_ATV.....	5
4.2 Änderungen in gemAnbT_IDP-Dienst_ATV, gemAnbT_Aktensystem_ePA_ATV, gemAnbT_TIM_ATV, gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID, AnbT_TI-M_ePA_ATV, gemAnbT_eRp_FD_ATV	5

1 Änderungsbeschreibung

Die Spezifikationen für die Handhabung von Verschlüsselungs- und Signaturschlüsseln lassen derzeit Raum für betriebliche Probleme, die aus der korrekten Auswahl des zu nutzenden Schlüssels und der Verwendung von Schlüsseln, deren PrK auf der anderen Seite nicht mehr vorliegt.

Daher soll als neue übergreifende Festlegung UUIDv7 [[RFC9562#name-uuid-version-7](#)] als Format für Key-Identifizier "kid" festgelegt und die Vorhaltdauer des private Key Materials angepasst werden.

UUIDv7 erlaubt die zeitliche Einordnung eines Schlüssels und kann daher zuverlässig bei der Selektion des zu nutzenden Schlüssels gleichen Typs helfen.

2 Änderungen in gemSpec_IDP_Sek

2.1 Änderungen in Kapitel 4.1 Entity Statement des sektoralen IDP

Nach A_226622

neu:

A_28195 -Anbieter sek IDP KTR - Schlüssel-Identifizier im JWK-Format

Der Anbieter sektoraler IDP KTR MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [[RFC9562#name-uuid-version-7](#)] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln. [\leq ,Anb_IDP-Sek_KTR,Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

Nach A_22710

neu:

A_28196 -Anbieter sek IDP KTR - Schlüsselwechselphase - Nutzbarkeit der ENC-Schlüssel

Der Anbieter sektoraler IDP KTR MUSS sicherstellen, dass die privaten Schlüssel von Schlüsselpaaren, deren Zweck die Verschlüsselung ist, systemintern noch mindestens 24 Stunden und maximal 48 Stunden zur Entschlüsselung verwendet werden können, nachdem die Schlüssel aus dem Entity Statement oder einem daraus referenzierten JSON Web Key Set depubliziert wurden. [\leq ,Anb_IDP-Sek_KTR,Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

3 Änderungen in gemSpec_IDP_FD

3.1 Änderungen in Kapitel 4.3 Entity Statements

Vor A_24607

neu:

A_28208 -Schlüssel-Identifizier im JWK-Format

Der Anbieter des Fachdienstes MUSS sicherstellen, dass bei der Bereitstellung neuer Schlüssel im JSON Web Key Set (JWKS) Format die Key Identifier der Schlüssel im UUID7-Format [RFC9562#name-uuid-version-7] vorliegen, die den Zeitpunkt der Schlüsselerzeugung widerspiegeln. [≤, Anw_DiGA, Anb_eRp_FD, Anb_Integ_PAT, digi_ID_OGR, Anb_Aktensystem_ePA, Anb_TIM_FD, Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

Nach A_24607

neu:

A_28209 -Schlüsselwechsel - Nutzbarkeit der Encryption-Schlüssel

Der Anbieter eines Fachdienstes MUSS sicherstellen, dass die privaten Schlüssel von Schlüsselpaaren, deren Zweck die Verschlüsselung ist, systemintern noch mindestens 24 Stunden und maximal 48 Stunden zur Entschlüsselung verwendet werden können, nachdem die Schlüssel aus dem Entity Statement oder einem daraus referenzierten JSON Web Key Set depubliziert wurden. [≤, Anw_DiGA, Anb_eRp_FD, Anb_Integ_PAT, digi_ID_OGR, Anb_Aktensystem_ePA, Anb_TIM_FD, Sich.techn. Eignung: Anbietererklärung, organ./betriebl. Eignung: Anbietererklärung]

4 Änderungen in Steckbriefen

4.1 Änderungen in gemAnbT_IDP-Sek_KTR_ATV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_IDP-Dienst]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehen.

Tabelle 1: Anforderungen zur betrieblichen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28195	Schlüssel-Identifizier im JWK-Format	gemSpec_IDP_Sek
A_28196	Schlüsselwechselphase - Nutzbarkeit der ENC-Schlüssel	gemSpec_IDP_Sek

Tabelle 2: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28195	Schlüssel-Identifizier im JWK-Format	gemSpec_IDP_Sek
A_28196	Schlüsselwechselphase - Nutzbarkeit der ENC-Schlüssel	gemSpec_IDP_Sek

4.2 Änderungen in gemAnbT_IDP-Dienst_ATV, gemAnbT_Aktensystem_ePA_ATV, gemAnbT_TIM_ATV, gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID, AnbT_TI- M_ePA_ATV, gemAnbT_eRp_FD_ATV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabellen der Originaldokumente. Alle Anforderungen der Tabellen der Originaldokumente, die in der folgenden Tabellen nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 3: Anforderungen zur betrieblichen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208	Schlüssel-Identifizier im JWK-Format	gemSpec_IDP_FD
A_28209	Schlüsselwechsel - Nutzbarkeit der Encryption-Schlüssel	gemSpec_IDP_FD

Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28208	Schlüssel-Identifizier im JWK-Format	gemSpec_IDP_FD
A_28209	Schlüsselwechsel - Nutzbarkeit der Encryption-Schlüssel	gemSpec_IDP_FD