Inhaltsverzeichnis

1 Änderungsbeschreibung....2
2 Änderung in gemSpec_IDP_Dienst....3
3 Änderung in gemSpec_IDP_Frontend....11
4 Änderung in gemSpec_Perf....15
5 Änderungen in Steckbriefen....16
5.1 Änderungen in gemAnbT_IDP-Dienst....16
5.2 Änderungen in gemProdT_IDP-Dienst_PTV....16

1 Änderungsbeschreibung

Lt. Beschluss soll die Möglichkeit zu Nutzung von Biometrie aus der eRP-App ausgebaut werden. Die Spezifikation zum IDP-Dienst muss dazu bereinigt werden.

2 Änderung in gemSpec_IDP_Dienst

- Referenzen auf *auth_pair_endpoint* und *uri_pair* entfernen
- Anforderungen anpassen
  - A_20699-03 anpassen
  - A_20458-03 anpassen
- Texte anpassen
  - Tabelle 3: TAB_IDP_DIENST_0003 Bezeichnungen der extern genutzten Schlüssel und Adressen des IDP-Dienstes
  - Abschnitt 5.4 Pairing-Endpunkt
  - Anpassung Abschnitt 7.7 Aufbau des Discovery Document
  - Abschnitt 8 Anhang C - Datenformate und Kommunikationsprotokolle im Zusammenhang mit alternativen Authentisierungsverfahren

Es folgende Anforderungen entfernt:

- A_21404 - Bewertung von Typen mobiler Endgeräte durch den IdP-Dienst
- A_21405 - Management der Gerätetypen und ihrer Einstufung
- A_21406 - Anforderungen an Transaktionalität der Freischaltung der Einstufung von Gerätetypen
- A_21407 - Vorhalten von Backup-Daten zur Einstufung von Gerätetypen
- A_21408 - Exportierbarkeit der Datenbasis zur Einstufung von Gerätetypen
- A_21409 - Anforderung an die Revisionssicherheit des Managements der Datenbasis zur Einstufung von Gerätetypen
- A_21410 - Registrierung des Pairing-Endpunkts und des Authenticator-Moduls am IdP-Dienst
- A_21429-02 - Erweiterung des Authorization-Endpunkts: Realisierung verschiedener Authentifizierungsmethoden
- A_21415 - Registrierungsfunktion des IdP-Dienstes: Datenformate und Syntax zur Kommunikation mit dem Authenticator-Modul
- A_21411 - Registrierungsfunktion des IdP-Dienstes: Fehlermeldungen
- A_21412 - Registrierungsfunktion des IdP-Dienstes: Registrierung
- A_21413 - Registrierungsfunktion des IdP-Dienstes: Prüfung des Scope
- A_21419 - Registrierungsfunktion des IdP-Dienstes: Anforderung an die Authentifizierung des Nutzers
- A_21420 - Registrierungsfunktion des IdP-Dienstes: Entschlüsselung der Registrierungsdaten
- A_21421-01 - Registrierungsfunktion des IDP-Dienstes: Validierung der signierten Pairing-Daten
- A_21422 - Registrierungsfunktion des IdP-Dienstes: Validierung des Zusammenhangs von ACCESS_TOKEN und Pairing-Daten

- A_21470 - Registrierungsfunktion des IdP-Dienstes: Prüfung des Zusammenhangs zwischen Pairing-Daten und übermittelten Authentifizierungszertifikat
- A_21423 - Registrierungsfunktion des IdP-Dienstes: Bewertung des Gerätetyps
- A_21424 - Registrierungsfunktion des IdP-Dienstes: Speicherung der Pairing-Daten
- A_21426 - Registrierungsfunktion des IdP-Dienstes: Nicht-Speicherung des übermittelten Authentifizierungszertifikats
- A_21427 - Registrierungsfunktion des IdP-Dienstes: Rückmeldung an den Nutzer
- A_21449 - Erweiterung des Authorization-Endpunkts: Datenmodell und Syntax zur Kommunikation mit dem Authenticator-Modul
- A_21428 - Erweiterung des Authorization-Endpunkts: Fehlermeldungen
- A_21432 - Erweiterung des Authorization-Endpunkts: Prüfung der vorliegenden Gerätedaten
- A_21433 - Erweiterung des Authorization-Endpunkts: Validierung des Authentifizierungszertifikats
- A_21434 - Erweiterung des Authorization-Endpunkts: Auslesen der gespeicherten Pairing-Daten
- A_21435 - Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der gespeicherten Pairing-Daten
- A_21437 - Erweiterung des Authorization-Endpunkts: Bewertung der Gültigkeit des öffentlichen Schlüssels in den Pairing-Daten
- A_21438 - Erweiterung des Authorization-Endpunkts: Validierung der mathematischen Integrität der signierten Authentication_Data-Struktur
- A_21439 - Erweiterung des Authorization-Endpunkts: Zu unterstützende Algorithmen zur Prüfung der mathematischen Integrität der signierten Authentication_Data-Struktur
- A_21440 - Erweiterung des Authorization-Endpunkts: Produktion des Authorization Code und eines SSO_TOKEN
- A_21450 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Datenmodell und Syntax zur Kommunikation mit dem Authenticator-Modul
- A_21441 - Inspektions- und Deregistrierungsfunktion des IDP-Dienstes: Fehlermeldungen
- A_21445-02 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des "ACCESS_TOKEN"
- A_21452 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Rückgabe der Pairing-Daten
- A_21447 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Annahme des Kommandos zur Deaktivierung des Pairings
- A_21448 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Deaktivierung des identifizierten Pairing-Datensatzes
    - A_21454 - Performance - IdP-Dienst - Deregistrierung eines Pairings

Es werden folgende Kapitel entfernt:

- 5.4 Pairing-Endpunkt
- 8 Anhang C - Datenformate und Kommunikationsprotokolle im Zusammenhang mit alternativen Authentisierungsverfahren

99 Es wird in Kapitel "3.2 Begriffsdefinition" angepasst:

100 Alt:

101 **Tabelle 1: TAB_IDP_DIENST_0003 Bezeichnungen der extern genutzten Schlüssel und**
102 **Adressen des IDP-Dienstes**

	PUK	private Key	Adressen
Authorization-Endpunkt (AUTH)	PuK_IDP_SIG - für die Signaturprüfung desCHALLENGE_TOKEN, des AUTHORIZATION_CODE und des SSO_TOKEN - kodiert in einem FD.SIG-Zertifikat PuK_IDP_ENC - für die Verschlüsselung der signierten Challenge durch das Authenticator-Modul PuK_IDP_SIG_Sek - Wird für die Authentisierung gegenüber einem sektoralen IDP dort registriert PuK_IDP_TLS - Wird für die Authentisierung innerhalb der Föderation registriert	PrK_IDP_SIG - zum Signieren des CHALLENGE_TOKEN des AUTHORIZATION_CODE und des SSO_TOKEN PrK_IDP_ENC - zum Entschlüsseln der signierten Challenge PrK_IDP_SIG_Sek - Für die Authentisierung gegenüber einem sektoralen IDP PrK_IDP_TLS - Wird für die TLS Authentisierung innerhalb der Föderation verwendet	URI_AUTH (authorization_endpoint) URI_AUTH_SSO (sso_endpoint) URI_AUTH_3RD (third_party_endpoint)
Discovery-Endpunkt (DISC)	PuK_DISC_SIG - für die Signaturprüfung des Discovery Document - kodiert in einem FD.SIG-Zertifikat	PrK_DISC_SIG - zum Signieren des Discovery Document	URI_DISC
Token-Endpunkt (TOKEN)	PuK_IDP_SIG - für die Signaturprüfung des ID_TOKEN und des ACCESS_TOKEN - kodiert in einem FD.SIG-Zertifikat PuK_IDP_ENC	PrK_IDP_SIG - zum Signieren des ID_TOKEN und des ACCESS_TOKEN	URI_TOKEN(token_endpoint)

	- für die Verschlüsselung des KEY_VERIFIER durch das Anwendungsfrontend	PrK_IDP_ENC - für die Entschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang	
Pairing-Endpunkt (PAIR)	PuK_IDP_ENC - für die Verschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang	PrK_IDP_ENC - für die Entschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang	URI_PAIR

Neu:

Tabelle 2: TAB_IDP_DIENST_0003 Bezeichnungen der extern genutzten Schlüssel und Adressen des IDP-Dienstes

	PUK	private Key	Adressen
Authorization-Endpunkt (AUTH)	PuK_IDP_SIG - für die Signaturprüfung desCHALLENGE_TOKEN, des AUTHORIZATION_CODE und des SSO_TOKEN - kodiert in einem FD.SIG-Zertifikat PuK_IDP_ENC - für die Verschlüsselung der signierten Challenge durch das Authenticator-Modul PuK_IDP_SIG_Sek - Wird für die Authentisierung gegenüber einem sektoralen IDP dort registriert PuK_IDP_TLS - Wird für die Authentisierung innerhalb der Föderation registriert	PrK_IDP_SIG - zum Signieren des CHALLENGE_TOKEN des AUTHORIZATION_CODE und des SSO_TOKEN PrK_IDP_ENC - zum Entschlüsseln der signierten Challenge PrK_IDP_SIG_Sek - Für die Authentisierung gegenüber einem sektoralen IDP PrK_IDP_TLS - Wird für die TLS	URI_AUTH (authorization_endpoint) URI_AUTH_SSO (sso_endpoint) URI_AUTH_3RD (third_party_endpoint)

		Authentisierung innerhalb der Föderation verwendet	
Discovery-Endpunkt (DISC)	PuK_DISC_SIG - für die Signaturprüfung des Discovery Document - kodiert in einem FD.SIG-Zertifikat	PrK_DISC_SIG - zum Signieren des Discovery Document	URI_DISC
Token-Endpunkt (TOKEN)	PuK_IDP_SIG - für die Signaturprüfung des ID_TOKEN und des ACCESS_TOKEN - kodiert in einem FD.SIG-Zertifikat PuK_IDP_ENC - für die Verschlüsselung des KEY_VERIFIER durch das Anwendungsfrontend	PrK_IDP_SIG - zum Signieren des ID_TOKEN und des ACCESS_TOKEN ~~PrK_IDP_ENC~~ ~~- für die Entschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang~~	URI_TOKEN(token_endpoint)
~~Pairing-Endpunkt (PAIR)~~	~~PuK_IDP_ENC~~ ~~- für die Verschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang~~	~~PrK_IDP_ENC~~ ~~- für die Entschlüsselung des ACCESS_TOKEN für den Pairing-Vorgang~~	~~URI_PAIR~~

Es wird in Kapitel "5.1.1 Aufbau des Discovery Documents" angepasst:

Alt:

A_20458-03 - Inhalte des Discovery Document
Der Anbieter des IDP-Dienstes MUSS am Discovery-Endpunkt sowohl im internen als auch im externen Discovery Document gemäß [RFC8414#section-2] mindestens die folgenden Attribute als URI angeben:

- "issuer" (hier ist der IdP-Dienst erreichbar),
- "signed_jwks_uri" (für den Abruf der öffentlichen Schlüssel und Zertifikate von "PUK_IDP_ENC“ sowie "PUK_IDP_SIG“ entsprechend TAB_IDP_DIENST_0003 [RFC7517] – identifiziert anhand der "kid“-Parameter und des "alias" (puk_idp_enc / puk_idp_sig)),
- "uri_disc" (URI, unter welcher das Discovery Document bereitgestellt wird),
- "authorization_endpoint" (URI des Dienstes und des öffentlichen Verschlüsselungsschlüssels des Authorization-Endpunktes gemäß [RFC6749]),

- "sso_endpoint“ (URI des Authorization-Endpunktes für Requests mit SSO Token),
- "auth_pair_endpoint“ (URI des Authorization-Endpunktes für Requests mit Pairing-Daten),
- "token_endpoint" (URI des Token-Endpunktes gemäß [RFC6749])

Neu:

A_20458-04 - Inhalte des Discovery Document
Der Anbieter des IDP-Dienstes MUSS am Discovery-Endpunkt sowohl im internen als auch im externen Discovery Document gemäß [RFC8414#section-2] mindestens die folgenden Attribute als URI angeben:

- "issuer" (hier ist der IdP-Dienst erreichbar),
- "signed_jwks_uri" (für den Abruf der öffentlichen Schlüssel und Zertifikate von "PUK_IDP_ENC“ sowie "PUK_IDP_SIG“ entsprechend TAB_IDP_DIENST_0003 [RFC7517] – identifiziert anhand der "kid“-Parameter und des "alias" (puk_idp_enc / puk_idp_sig)),
- "uri_disc" (URI, unter welcher das Discovery Document bereitgestellt wird),
- "authorization_endpoint" (URI des Dienstes und des öffentlichen Verschlüsselungsschlüssels des Authorization-Endpunktes gemäß [RFC6749]),
- "sso_endpoint“ (URI des Authorization-Endpunktes für Requests mit SSO Token),
- ~~"auth_pair_endpoint“ (URI des Authorization-Endpunktes für Requests mit Pairing-Daten),~~
- "token_endpoint" (URI des Token-Endpunktes gemäß [RFC6749])

Es wird in Kapitel "5.2.1 Authorization-Endpunkt Eingangsdaten" angepasst:

Alt:

A_20699-03 - Annahme von CHALLENGE_TOKEN: Authentication_Data-Struktur
Der Authorization-Endpunkt MUSS:

- entweder das mit dem Zertifikat der Smartcard des Nutzers signierte und durch das Authenticator-Modul mittels `PuK_IDP_ENC` verschlüsselte `CHALLENGE_TOKEN`
- oder – im Fall der Verwendung von alternativen Authentisierungsmitteln – die mit dem privaten Schlüssel des Endgeräts signierte und durch das Authenticator-Modul mittels `PuK_IDP_ENC` verschlüsselte Authentication_Data-Struktur

annehmen. Er MUSS in beiden Fällen anhand des im Header vorhandenen exp-Claim die Token anhand der Systemzeit auf zeitliche Gültigkeit prüfen. Sind diese nicht mehr gültig, MUSS der Authentifizierungsvorgang abgebrochen werden. Im Fall der Gültigkeit MÜSSEN diese mit dem PrK.IDP.ENC entschlüsselt werden.

Neu:

A_20699-04 - Annahme von CHALLENGE_TOKEN: Authentication_Data-Struktur
Der Authorization-Endpunkt MUSS:

- ~~entweder das mit dem Zertifikat der Smartcard des Nutzers signierte und durch das Authenticator-Modul mittels `PuK_IDP_ENC` verschlüsselte `CHALLENGE_TOKEN`~~
- ~~oder – im Fall der Verwendung von alternativen Authentisierungsmitteln – die mit dem privaten Schlüssel des Endgeräts signierte und durch das Authenticator-Modul mittels `PuK_IDP_ENC` verschlüsselte Authentication_Data-Struktur~~

das mit dem Zertifikat der Smartcard des Nutzers signierte und durch das Authenticator-Modul mittels PuK_IDP_ENC verschlüsselte CHALLENGE_TOKEN annehmen.

Er MUSS ~~in beiden Fällen~~ anhand des im Header vorhandenen exp-Claim die Token anhand der Systemzeit auf zeitliche Gültigkeit prüfen. Sind diese nicht mehr gültig, MUSS der Authentifizierungsvorgang abgebrochen werden. Im Fall der Gültigkeit MÜSSEN diese mit dem PrK.IDP.ENC entschlüsselt werden.

Es wird in Kapitel "7.7 Aufbau des Discovery Document" angepasst:

Alt:

```
{...
}
.
{
   "authorization_endpoint": "[URL des Authorization Endpunkts.]",
   "federation_authorization_endpoint": "[URL des Authorization Endpunkt für
Anfragen an IDP der Föderation - dieser ist nur im Internet verfügbar]",
   "auth_pair_endpoint": "[URL des Pairing-Authorization-Endpunkts - dieser ist
nur im Internet verfügbar]",
   "third_party_authorization_endpoint" : "[URL des third_party-Authorization-
Endpunkts - dieser ist nur im Internet verfügbar]",
   "sso_endpoint": "[URL des SSO-Authorization Endpunkts.]",
   "uri_pair": "[URL des Pairing-Endpunkts.]",
   "token_endpoint": "[URL des Authorization-Endpunkts.]",
   "uri_disc": "[URL des Discovery Document.]",
   ...
}
.<SIGNATURE>
```

Neu:

```
{
 ...
}
.
{
   "authorization_endpoint": "[URL des Authorization Endpunkts.]",
   "federation_authorization_endpoint": "[URL des Authorization Endpunkt für
Anfragen an IDP der Föderation - dieser ist nur im Internet verfügbar]",
   "auth_pair_endpoint": "[URL des Pairing-Authorization-Endpunkts - dieser ist
nur im Internet verfügbar]",
   "third_party_authorization_endpoint" : "[URL des third_party-Authorization-
Endpunkts - dieser ist nur im Internet verfügbar]",
   "sso_endpoint": "[URL des SSO-Authorization Endpunkts.]",
   "uri_pair": "[URL des Pairing-Endpunkts.]",
   "token_endpoint": "[URL des Authorization-Endpunkts.]",
   "uri_disc": "[URL des Discovery Document.]",
   ...
}
.<SIGNATURE>
```

3 Änderung in gemSpec_IDP_Frontend

Es werden folgende Anforderungen entfernt:

- A_21515 - Authenticator-Modul: Registrierung
- A_21573 - Anbieten der Option zur Registrierung von alternativen Authentisierungsmitteln
- A_21574 - Warnhinweise an den Nutzer
- A_21575 - Bezug eines ACCESS_TOKEN zur Einleitung des Registrierungsprozesses
- A_21576 - Löschung bestehender alternativer Authentisierungsmittel
- A_21577 - Verbot der Erhebung und Speicherung von Referenzmerkmalen zur Authentifizierung des Nutzers durch das Authenticator-Modul
- A_21578 - Sicherstellung des Vorliegens einer geeigneten Umgebung zur Speicherung von biometrischen Referenzmerkmalen
- A_21579 - Sicherstellung des Vorliegens einer geeigneten Umgebung zur Speicherung von biometrischen Referenzmerkmalen
- A_21580 - Ausschluss von Eigenimplementierungen zur Schlüsselverwaltung
- A_21581 - Verfügbarkeit von kryptographischen Algorithmen
- A_21582 - Lokale Authentisierung des Nutzers vor Anwendung des PrK_SE_AUT zur Authentisierung
- A_21583 - Qualitative Anforderungen an lokale Authentisierungsmittel
- A_21584 - Verwendung von Geräte-eigenen Mechanismen zur Authentisierung des Nutzers
- A_21585 - Beschränkung der Nutzung des PrK_SE_AUT auf das Authenticator-Modul
- A_21586 - Löschung des PrK_SE_AUT als Reaktion auf Systemereignisse
- A_21587 - Beschränkung des PrK_SE_AUT auf Signaturbildung
- A_21588 - Erzeugung eines Key-Identifiers für das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT gegenüber dem IdP-Dienst
- A_21589 - Erzeugung des Schlüsselpaars PrK_SE_AUT/PuK_SE_AUT
- A_21590 - Beschränkung der Nutzung des PrK_SE_AUT auf Authentisierung gegenüber dem IdP-Dienst
- A_21591 - Erhebung von Geräteinformationen
- A_21592 - Signatur der Pairing-Daten
- A_21593 - Produktion der Registrierungsdaten
- A_21416 - Authenticator-Modul: Einleiten der Registrierung
- A_21414 - Authenticator-Modul: Umschlüsselung des "ACCESS_TOKEN" für Pairing-Endpunkt
- A_21417 - Authenticator-Modul: Übertragung der Registrierungsdaten
- A_21595 - Lokale Speicherung des C.CH.AUT
- A_21596 - Speicherung des vom Nutzer vergebenen Namen des Geräts

- A_21597 - Information des Nutzers
- A_21598 - Löschung von lokalen Daten bei Fehlschlag
- A_21599 - Anbieten der Option zur Verwendung von alternativen Authentisierungsmitteln
- A_21430 - Authenticator-Modul: Authorization-Request bei Verwendung von alternativen Authentisierungsmitteln
- A_21600 - Einholen von aktuellen Geräteinformationen
- A_21431 - Authenticator-Modul: Übermittelung von Authentifizierungsdaten zur Verwendung von alternativen Authentisierungsmitteln
- A_21601 - Reaktion auf Fehlermeldungen des Authorization-Endpunkts
- A_21602 - Ermöglichung der Inspektion von lokal gespeicherten Daten
- A_21603 - Ermöglichung der Löschung von alternativen Authentisierungsmitteln und lokal gespeicherten Daten
- A_21604 - Hinweise an den Nutzer bei der lokalen Löschung von alternativen Authentisierungsmitteln und lokal gespeicherten Daten
- A_21605 - Realisierung der Inspektions- und Deregistrierungsfunktion am Authenticator-Modul
- A_21442 - Inspektions- und Deregistrierungsfunktion des IDP-Dienstes: Authentisierung des Nutzers
- A_21443 - Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Verschlüsselung des ACCESS_TOKEN
- A_21444 - Authenticator-Modul: Übertragung des "ACCESS_TOKEN"
- A_21608 - Option zur Deaktivierung einzelner Pairing-Daten
- A_21446 - Authenticator-Modul: Übermittelung eines Kommandos zur Deregistrierung
- A_21607 - Abbildung der Pairing-Daten auf der Nutzeroberfläche des Authenticator-Moduls
- A_21617 - Anzeige des Ergebnisses der Deregistrierung

Es werden folgende Kapitel entfernt:

- 7.7 Nutzung von alternativen Authentisierungsmitteln

Es wird in Kapitel "7.2.1 Schnittstellendefinition" angepasst:

Alt:

A_20700-07 - Authenticator-Modul: Signatur der "CHALLENGE"
Das Authenticator-Modul MUSS die vom Authorization-Endpunkt empfangene CHALLENGE_TOKEN mit dem Zertifikat C.CH.AUT aus der Smartcard des Nutzers signieren. Hierbei wird der über die CHALLENGE_TOKEN gebildete HASH-Wert zur Signatur überreicht (siehe Abschnitt9.3.7.3 Signiervorgang in diesem Dokument).

Im Fall der Authentisierung mit einem alternativen Authentisierungsmittel signiert das Authenticator-Modul die folgenden Daten mithilfe des PrK_SE_AUT:

- das vom Authorization-Endpunkt bezogene `CHALLENGE-TOKEN`,
- das auf dem Gerät gespeicherte Authentifizierungszertifikat C.CH.AUT,
- den Key-Identifier für das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT,

- die aktuell erhobenen Geräteinformationen,
- die Art des vom Nutzer verwendeten, lokalen Authentisierungsmittels zur Freischaltung der Anwendung des Schlüssels PrK_SE_AUT.

Es MUSS hierbei eine Datenstruktur vom Typ "Signed_Authentication_Data" produzieren. Der zur Signatur zu verwendende Algorithmus MUSS ECDSA mit SHA-256 sein. Das Feld`amr` MUSS hierbei wie folgt in Abhängigkeit der vom Nutzer verwendeten Methode belegt werden:

Tabelle 3: Belegung des`amr`-Claims durch das Authenticator-Modul

Art	Authentication-Method-Reference ("amr")
Biometrisch	["mfa","hwk","generic-biometric"]
PIN	["mfa","hwk","kba"]
Passwort	["mfa","hwk","kba"]
Muster	["mfa","hwk","kba"]

Neu:

A_20700-08 - Authenticator-Modul: Signatur der "CHALLENGE"
Das Authenticator-Modul MUSS die vom Authorization-Endpunkt empfangene CHALLENGE_TOKEN mit dem Zertifikat C.CH.AUT aus der Smartcard des Nutzers signieren. Hierbei wird der über die CHALLENGE_TOKEN gebildete HASH-Wert zur Signatur überreicht (siehe Abschnitt9.3.7.3 Signiervorgang in diesem Dokument).

Im Fall der Authentisierung mit einem alternativen Authentisierungsmittel signiert das Authenticator-Modul die folgenden Daten mithilfe des PrK_SE_AUT:

- das vom Authorization-Endpunkt bezogene `CHALLENGE-TOKEN`,
- das auf dem Gerät gespeicherte Authentifizierungszertifikat C.CH.AUT,
- den Key-Identifier für das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT,
- die aktuell erhobenen Geräteinformationen,
- die Art des vom Nutzer verwendeten, lokalen Authentisierungsmittels zur Freischaltung der Anwendung des Schlüssels PrK_SE_AUT.

Es MUSS hierbei eine Datenstruktur vom Typ "Signed_Authentication_Data" produzieren. Der zur Signatur zu verwendende Algorithmus MUSS ECDSA mit SHA-256 sein. Das Feld`amr` MUSS hierbei wie folgt in Abhängigkeit der vom Nutzer verwendeten Methode belegt werden:

Tabelle 4: Belegung des`amr`-Claims durch das Authenticator-Modul

Art	Authentication-Method-Reference ("amr")
~~Biometrisch~~	~~["mfa","hwk","generic-biometric"]~~
PIN	["mfa","hwk","kba"]
Passwort	["mfa","hwk","kba"]

Muster	["mfa","hwk","kba"]

283

4 Änderung in gemSpec_Perf

Weitere Anpassungen sind in [gemSpec_Perf] notwendig, da Use Cases wegfallen.
Etwa A_22013-04 in Tabelle 21: Tab_gemSpec_Perf_Berichtsformat_IDP

- Wegfall UC_8

5 Änderungen in Steckbriefen

5.1 Änderungen in gemAnbT_IDP-Dienst

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

Tabelle 5: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20458-03~~	Inhalte des Discovery Document	gemSpec_IDP_Dienst
A_20458-04	Inhalte des Discovery Document	gemSpec_IDP_Dienst

5.2 Änderungen in gemProdT_IDP-Dienst_PTV

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

Tabelle 6: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20699-03~~	Annahme von CHALLENGE_TOKEN: Authentication_Data-Struktur	gemSpec_IDP_Dienst
A_20699-04	Annahme von CHALLENGE_TOKEN: Authentication_Data-Struktur	gemSpec_IDP_Dienst