
C_12301_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Allgemeine Änderungen in gemSpec_IDP_FedMaster, gemSpec_IDP_Sek, gemSpec_IDP_FD.....	3
3 Änderung in gemSpec_IDP_Dienst.....	5
4 Änderung in gemSpec_IDP_Sek.....	8
5 Änderung in gemSpec_IDP_FD.....	13
6 Änderung in gemSpec_IDP_Frontend.....	18
7 Änderungen in Steckbriefen.....	21
7.1 Änderungen in gemProdT_IDP-Dienst_PTV.....	21
7.2 Änderungen in gemProdT_IDP_Sek.....	21
7.3 Änderungen in gemAnbT_IDP-Sek_KTR_ATV.....	21
7.4 Änderungen in gemProdT_Aktensystem_ePA_PTV, gemProdT_IDP-Dienst_PTV, gemProdT_PoPP_Service_PTV, gemProdT_TI-M_FD_ePA_PTV.....	22
7.5 Änderungen in gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID.....	22
7.6 Änderungen in gemAnbT_Aktensystem_ePA_ATV, gemAnbT_TI-M_ePA_ATV, gemAnbT_IDP-Dienst_ATV, gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID	22

1 Änderungsbeschreibung

- Die Anforderungen A_21421, A_21425 und A_21445 enthalten ungültige Verweise auf andere Dokumente. Diese Verweise müssen entfernt werden.
- In den Spezifikationen sind teilweise fehlerhafte Beispiele und Links vorhanden:
 - gemSpec_IDP_Dienst
 - gemSpec_IDP_FedMaster
 - gemSpec_IDP_Sek
 - gemSpec_IDP_FD
 - gemSpec_IDP_Frontend
- Die Anforderungen zu den Entity Statements verweisen auf Tabellen im Anhang. Inhaltsänderungen bei den Tabellen werden dadurch nicht als Änderung der Anforderung wahrgenommen. Deshalb werden die normativen Inhalte der Entity Statements mit in die Anforderung aufgenommen, der Verweis auf den Anhang entfällt.

2 Allgemeine Änderungen in gemSpec_IDP_FedMaster, gemSpec_IDP_Sek, gemSpec_IDP_FD

In der Spezifikation befinden sich Beispiele für URIs mit http. Bitte überprüfen, an welchen Stellen nun mehr https verwendet werden soll. Beispiele:

- gemSpec_IDP_FedMaster
 - ersetze überall http://master0815.de durch https://app-ref.federationmaster.de
 - prüfe und korrigiere Links
 - 2.2 Detaillierter Überblick
 - Tabelle "Anwendungsfall "Monitoring der TLS-Zertifikate der VAU"
 - 5.5.2 Weitere Dokumente
- gemSpec_IDP_Sek
 - ersetze überall http://master0815.de durch https://app-ref.federationmaster.de
 - Prüfe und korrigiere Links
 - Hinweis zu
 - A_22692, A_22512, A_22989,
 - A_22649, A_27598, A_25753
 - 6.5.1 Dokumente der gematik
 - 6.5.2 Weitere Dokumente
 - Links zu den [RFC...]
 - Links zu [OpenID Connect ...]
 - Links zu [OpenID Connect ...]
 - Links zu [OAuth 2.0 ...]
 - Link zu [OWASP Top Ten]
- gemSpec_IDP_Dienst
 - ersetze überall http: durch https:
 - Prüfe und korrigiere Links
 - A_19874, A_19877,
 - Hinweis
 - A_20440
 - 6.5.2 Weitere Dokumente
 - Links zu den [RFC...]
- gemSpec_IDP_FD
 - Prüfe und korrigiere Links
 - 6.5.2 Weitere Dokument

- Tabelle "AB_IDP_FD_0005 Inhalte des Claim für Leistungserbringerinstitutionen (SMC-B)"
- Tabelle "TAB_IDP_FD_0004 Inhalte des Claims für Leistungserbringer (HBA)"
- Tabelle "TAB_IDP_FD_0003 Inhalte der Claims für Versicherte"
- A_23080, A_27076, A_24932, AF_10118, A_23047, A_23048, AF_10117, A_23030
- Hinweis zu A_23500
- Links zu den [RFC...]
- Anmerkung zu organization_name in Tabelle "Body Entity Statement des Federation Master" (gemSpec_IDP_Sek)
- A_23185-01 - Zuordnung zu "VZD-FHIR" entfällt. Die Anforderung wurde fälschlicher Weise zugeordnet, "VZD-FHIR" ist nicht Teil der TI-Föderation.

3 Änderung in gemSpec_IDP_Dienst

Kapitel "5.4.2.5.2 Spezifikation" wird wie folgt angepasst:

- **A_21421** - redaktionelle Änderung*

Der Pairing-Endpunkt MUSS die in den übermittelten Registrierungsdaten enthaltenen Pairing-Daten extrahieren und MUSS die Signatur des Nutzers zu den Pairing-Daten prüfen. Die Prüfung des Authentifizierungszertifikats MUSS hierbei auf Basis der aktuellen Systemzeit des Pairing-Endpunkts als Referenzzeit und gemäß [gemSpec_PKI], **Abschnitt 8.3.1.1 „TUC_PKI_018“** erfolgen. Der IdP-Dienst MUSS zur Validierung alle Algorithmen unterstützen, die im Zusammenhang mit den Authentisierungsmitteln verwendet werden, die zur Authentisierung am IdP-Dienst zugelassen sind (siehe [gemSpec_IDP_Frontend], **Abschnitt 3**). Hierbei MÜSSEN die Vorgaben aus **Abschnitt 9.3.4** [gemSpec_IDP_Frontend] beachtet werden. Andere Algorithmen DÜRFEN NICHT unterstützt werden. Kann die Authentizität der Pairing-Daten nicht belegt werden oder ist das übermittelte Authentifizierungszertifikat zum aktuellen Zeitpunkt ungültig oder gesperrt, MUSS der Pairing-Endpunkt die Anfrage mit der Fehlermeldung REG.1 beenden. Unter "Authentifizierungszertifikat" wird ein Zertifikat des Typs C.CH.AUT verstanden.

Alt:

A_21421 -Registrierungsfunktion des IdP-Dienstes: Validierung der signierten Pairing-Daten

Der Pairing-Endpunkt MUSS die in den übermittelten Registrierungsdaten enthaltenen Pairing-Daten extrahieren und MUSS die Signatur des Nutzers zu den Pairing-Daten prüfen. Die Prüfung des Authentifizierungszertifikats MUSS hierbei auf Basis der aktuellen Systemzeit des Pairing-Endpunkts als Referenzzeit und gemäß [gemSpec_PKI], Abschnitt 8.3.1.1 „TUC_PKI_018“ erfolgen. Der IdP-Dienst MUSS zur Validierung alle Algorithmen unterstützen, die im Zusammenhang mit den Authentisierungsmitteln verwendet werden, die zur Authentisierung am IdP-Dienst zugelassen sind (siehe [gemSpec_IDP_Frontend], Abschnitt 3). Hierbei MÜSSEN die Vorgaben aus Abschnitt 9.3.4 [gemSpec_IDP_Frontend] beachtet werden. Andere Algorithmen DÜRFEN NICHT unterstützt werden. Kann die Authentizität der Pairing-Daten nicht belegt werden oder ist das übermittelte Authentifizierungszertifikat zum aktuellen Zeitpunkt ungültig oder gesperrt, MUSS der Pairing-Endpunkt die Anfrage mit der Fehlermeldung REG.1 beenden. Unter "Authentifizierungszertifikat" wird ein Zertifikat des Typs C.CH.AUT verstanden. [\leq , IDP-D, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

Neu:

A_21421-01 -Registrierungsfunktion des IDP-Dienstes: Validierung der signierten Pairing-Daten

Der Pairing-Endpunkt MUSS die in den übermittelten Registrierungsdaten enthaltenen Pairing-Daten extrahieren und die Signatur des Nutzers zu den Pairing-Daten prüfen. Die Prüfung des Authentifizierungszertifikats MUSS hierbei auf Basis der aktuellen Systemzeit des Pairing-Endpunkts als Referenzzeit und gemäß [gemSpec_PKI] erfolgen. Der IDP-Dienst MUSS zur Validierung alle Algorithmen unterstützen, die im Zusammenhang mit den Authentisierungsmitteln verwendet werden, die zur Authentisierung am IDP-Dienst zugelassen sind (siehe [gemSpec_IDP_Frontend]). Hierbei MÜSSEN die Vorgaben aus [gemSpec_IDP_Frontend] beachtet werden. Andere Algorithmen DÜRFEN NICHT

unterstützt werden. Kann die Authentizität der Pairing-Daten nicht belegt werden oder ist das übermittelte Authentifizierungszertifikat zum aktuellen Zeitpunkt ungültig oder gesperrt, MUSS der Pairing-Endpunkt die Anfrage mit der Fehlermeldung REG.1 beenden. Unter "Authentifizierungszertifikat" wird ein Zertifikat des Typs C.CH.AUT verstanden.

[<=, IDP-D, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

"A_21425- redaktionelle Änderung, relevante Afos sind ohnehin IDP-D zugewiesen" wird mit "A_21445 - Inspektions- und Deregistrierungsfunktion des IDP-Dienstes: Validierung und Verarbeitung des ACCESS_TOKEN" zusammengefasst zu A_21445_02

A_21425 entfällt

Kapitel "5.4.2.7.3 Spezifikation" wird wie folgt angepasst:

Alt:

A_21445 - Inspektions- und Deregistrierungsfunktion des IDP-Dienstes: Validierung und Verarbeitung des ACCESS_TOKEN

Der Pairing-Endpunkt MUSS das bezogene ACCESS_TOKEN mit dem privaten Schlüssel PrK.IDP.ENC entschlüsseln. Das zur Entschlüsselung des ACCESS_TOKEN zu verwendende Verfahren ist ECDH-ES. ~~Die Prüfung des ACCESS_TOKEN erfolgt wie in [gemSpec_IDP_FD] beschrieben.~~ Sofern das ACCESS_TOKEN ungültig ist, MUSS dem Authenticator-Modul die Fehlermeldung AC.1 übermittelt werden.

Neu:

A_21445-02 -Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des "ACCESS_TOKEN"

Der Pairing-Endpunkt MUSS die verschlüsselten Registrierungsdaten und den übermittelten ACCESS_TOKEN annehmen. Der Pairing-Endpunkt MUSS das bezogene ACCESS_TOKEN mit dem privaten Schlüssel PrK.IDP.ENC entschlüsseln. Das zur Entschlüsselung des ACCESS_TOKEN zu verwendende Verfahren ist ECDH-ES. Sofern das ACCESS_TOKEN ungültig ist, MUSS dem Authenticator-Modul die Fehlermeldung AC.1 übermittelt werden. [<=, IDP-D, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

4 Änderung in gemSpec_IDP_Sek

Kapitel "4.1 Entity Statement des sektoralen IDP" wird wie folgt angepasst:

Alt:

A_22643 -Entity Statement des sektoralen IDP

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß[OpenID Connect Federation 1.0#entity-statement] bereitstellen und im Internet verfügbar machen. Mindestens die in den Tabellen "Header Entity Statement des sektoralen IDP" und "Body Entity Statement des sektoralen IDP" in[~~ML-132850--Missing cross-reference~~] genannten Daten und Werte MÜSSEN im Entity Statement enthalten sein. [\leq , IDP-Sek, funkt. Eignung: Test Produkt/FA]

Neu:

Der Verweis auf eine Tabelle im Anhang wird abgelöst durch die Tabelle in der Anforderung selbst.

A_22643-01 -Entity Statement des sektoralen IDP

Der sektorale IDP MUSS ein selbst signiertes Entity Statement gemäß[OpenID federation 1.0#name-entity-statement] bereitstellen und im Internet verfügbar machen. Das Entity Statement MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 1: Header des Entity Statement des sektoralen IDP

Name	Werte / Wertebereich
alg	string, zulässiger Wert "ES256"
kid	string Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string zulässiger Wert "entity-statement+jwt"

Tabelle 2 :Allgemeine Attribute im well-known-Dokument des sektoralen IDP

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]
sub	string, URL nach [RFC1738]
iat	number,

	Alle time-Werte in Sekunden seit 1970,[RFC7519#section-2]
exp	number, Alle time-Werte in Sekunden seit 1970,[RFC7519#section-2]
jwks	Set von JWK [RFC7517]
authority_hints	[string] zulässiger Wert: iss aus dem Entity Statement des Federation Master
metadata	string, zulässiger Wert: "openid_provider"

Tabelle 3 : Attribute des Metadatenblocks openid_provider im well-known-Dokument des sektoralen IDP

Name	Werte
issuer	string, URL nach [RFC1738]
signed_jwks_uri	string, URL nach [RFC1738]
authorization_endpoint	string, URL nach [RFC1738]
token_endpoint	string, URL nach [RFC1738]
pushed_authorization_request_endpoint	string, URL nach [RFC1738]
client_registration_types_supported	[string] zulässiger Wert: "automatic"
subject_types_supported	[string] zulässiger Wert: "pairwise"
response_types_supported	[string] zulässiger Wert: "code"
scopes_supported	[string], Wertebereich: "openid", "<weitere Scopes nach A_22989*>"

claims_supported	[string], Wertebereich: "<Claims nach A_22989*>"
claims_parameter_supported	boolean, Wertebereich: true/false
response_modes_supported	[string] zulässiger Wert: "query"
grant_types_supported	[string] zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean, Wertebereich: true/false
token_endpoint_auth_methods_supported	[string] erforderlicher Wert: "self_signed_tls_client_auth"
request_authentication_methods_supported	JSON-Objekt, zulässige Werte: "ar": ["none"], "par": ["self_signed_tls_client_auth"]
id_token_signing_alg_values_supported	[string] erforderlicher Wert: "ES256"
id_token_encryption_alg_values_supported	[string] erforderlicher Wert: "ECDH-ES"
id_token_encryption_enc_values_supported	[string] erforderlicher Wert: "A256GCM"
user_type_supported	[string] zulässiger Wert: "IP" (Insured Person)
ti_features_supported {	
id_token_version_supported	[string] zulässige Werte in Liste: "1.0.0", "2.0.0"

Tabelle 4 :Attribute des Metadatenblocks federation_entity im well-known-Dokument des Authorization Server des Fachdienstes

Name	Werte / Wertebereich
organization_name	String (max. 128 Zeichen)

	Wertebereich: ^[ÄÖÜäöüß\w\ \.\&\+*V/]{1,128}\$
--	--

[<=, IDP-Sek, funkt. Eignung: Test Produkt/FA]

Neu - Bekanntgabe der Änderungen bisher nicht explizit gefordert

A_27988 -Bekanntgabe von Änderungen im Entity Statement - Anbieter sek IDP KTR

Der Anbieter sektoraler IDP KTR MUSS geplante Änderungen der folgenden Claims im Entity Statement vor deren Veröffentlichung bei dem Federation Master über einen organisatorischen Prozess beantragen:

- Änderungen des Schlüsselsets, mit dem das Entity Statement signiert wird - jwks,
- Änderungen des in der TI-Föderation propagierten Organisationsnamens - *federation_entity.organization_name*.

[<=, Anb_IDP-Sek_KTR, organ./betriebl. Eignung: Betriebshandbuch]

Kapitel "4.2.2 PAR - Endpunkt" wird wie folgt angepasst:

Alt:

A_22966-01 -Prüfung eingehender Pushed Authorization Request durch den sektoralen IDP

Der sektorale IDP MUSS die eingehende Pushed Authorization Request validieren und invalide Request gemäß [\[OAuth 2.0 Pushed Authorization Requests#section-2.3\]](#) mit einer Fehlermeldung quittieren. Die Validierung des eingegangenen Pushed Authorization Request schließt die Prüfung der im Request enthaltenen Werte für redirect_uri, Scope und Claims gegen die für den Fachdienst zulässigen (d.h. bei der Registrierung gemeldeten) Werte ein.

[<=, IDP-Sek, funkt. Eignung: Test Produkt/FA]

Neu - Präzisierung, dass die Informationen aus der Teilnehmerauskunft zu entnehmen sind

A_22966-02 -Prüfung eingehender Pushed Authorization Request durch den sektoralen IDP

Der sektorale IDP MUSS eingehende Pushed Authorization Requests validieren und invalide Requests gemäß [\[OAuth 2.0 Pushed Authorization Requests#section-2.3\]](#) mit einer Fehlermeldung ablehnen.

Die Validierung eines eingegangenen Pushed Authorization Request MUSS die Prüfung der im Request enthaltenen Werte für redirect_uri, scope und claims beinhalten. Dabei müssen redirect_uri, scope und claims aus dem Pushed Authorization Request eine Teilmenge der Werte sein, die der Federation Master für diesen Fachdienst in der Teilnehmerauskunft liefert (siehe A_23413-*).

[<=, IDP-Sek, funkt. Eignung: Test Produkt/FA]

Kapitel "7.1.4 Detailinformationen zum App-App-Flow" wird wie folgt angepasst:

Tabelle "Body Entity Statement des Federation Master"

organization_name	String (max. 128 Zeichen) Wertebereich:	"RISE GmbH" "Federation"	Nach [OpenID Federation 1.0] wird der Claim im Entity Statement durch eine
-------------------	--	-----------------------------	--

	^[ÄÖÜäöüß\w\ \-\.\&\+*V]{1,128}\$	Master"	menschenlesbare Repräsentation der Organisation gefüllt. welche di e Entity "OpenID-Provider " gehört.
--	-------------------------------------	---------	--

Tabelle "Body Entity Statement des sektoralen IDP"

organization_name	String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüß\w\ \-\.\&\+*V]{1,128}\$	"gematik sektoraler IDP" , "AOK Bayern" "Techniker Krankenkasse"	Nach [OpenID Federation 1.0] wird der Claim im Entity Statement durch eine menschenlesbare Repräsentation der Organisation gefüllt. welche di e Entity "OpenID-Provider " gehört.
-------------------	--	---	--

Tabelle "Body Entity Statement des sektoralen IDP"

organization_name	String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüß\w\ \-\.\&\+*V]{1,128}\$	"RISE GmbH"	Nach [OpenID Federation 1.0] wird der Claim im Entity Statement durch eine menschenlesbare Repräsentation der Organisation gefüllt. welche di e Entity "OpenID-Provider " gehört.
-------------------	--	----------------	--

5 Änderung in gemSpec_IDP_FD

Kapitel "4.3 Entity Statements" wird wie folgt angepasst:

Alt:

A_23034 -Entity Statement veröffentlichen

Authorization-Server MÜSSEN über sich ein, ES256 signiertes, Entity Statement gemäß [\[OpenID Connect Federation 1.0#rfc.section.6\]](#) unter ".well-known/openid-federation" veröffentlichen. Das Entity Statement ist maximal 24h gültig. [≤, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, extNutz_GID, Anb_IDP-D, IDP-D, PoPP_Service, digi_ID_OGR, funkt. Eignung: Herstellererklärung, organ./betriebl. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test Produkt/FA]

Neu:

Der Verweis auf eine Tabelle im Anhang wird abgelöst durch die Tabelle in der Anforderung selbst.

A_23034-01 -Entity Statement veröffentlichen

Authorization Server MÜSSEN unter „.well-known/openid-federation“ ein über sich Auskunft gebendes, mit ES256 signiertes Entity Statement gemäß [\[OpenID federation 1.0#name-obtaining-federation-entity\]](#) veröffentlichen. Dieses Entity Statement muss die Metadaten openid_relying_party und federation_entity als Relying Party der TI-Föderation enthalten. Das Entity Statement ist maximal 24 Stunden gültig. Es MUSS mindestens die in der folgenden Tabelle aufgeführten Metadaten enthalten:

Tabelle 5: Header des Entity Statement des Fachdienstes

Name	Werte / Wertebereich
alg	string, zulässiger Wert: "ES256"
kid	string Es wird empfohlen, den JWK Thumbprint gemäß [RFC7638] als kid zu verwenden.
typ	string zulässiger Wert: "entity-statement+jwt"

Tabelle 6 :Allgemeine Attribute im well-known-Dokument des Authorization Server des Fachdienstes

Name	Werte / Wertebereich
iss	string, URL nach [RFC1738]
sub	string, URL nach [RFC1738]

iat	number, Alle time-Werte in Sekunden seit 1970,[RFC7519#section-2]
exp	number, Alle time-Werte in Sekunden seit 1970,[RFC7519#section-2]
jwks	Set von JWK [RFC7517]
authority_hints	[string] zulässiger Wert: iss aus dem Entity Statement des Federation Master
metadata	string, zulässiger Wert: "openid_relying_party"

Tabelle 7 :Attribute des Metadatenblocks openid_relying_party im well-known-Dokument des Authorization Server des Fachdienstes

Name	Werte
signed_jwks_uri	string, URL nach [RFC1738]
client_name	string, Wertebereich: ^[ÄÖÜäöüß\w\ \.\&\+*\V/]{1,128}\$
redirect_uris	[string], Wertebereich: Bei der Registrierung des Fachdienstes hinterlegte redirect_uris
response_types	[string] zulässiger Wert: "code"
client_registration_types	[string] zulässiger Wert: "automatic"
grant_types	[string] zulässiger Wert: "authorization_code"
require_pushed_authorization_requests	boolean zulässiger Wert: true
token_endpoint_auth_method	string, zulässiger Wert: "self_signed_tls_client_auth"
default_acr_values	[string] zulässiger Wertebereich: "gematik-ehealth-loa-high", "gematik- ehealth-loa-substantial"
id_token_signed_response_alg	string, zulässiger Wert: "ES256"
id_token_encrypted_response_alg	string, zulässiger Wert: "ECDH-ES"
id_token_encrypted_response_enc	string, zulässiger Wert: "A256GCM"
scope	string
ti_features_supported {	
id_token_version_supported	[string] zulässige Werte in Liste:

	"1.0.0", "2.0.0"
--	------------------

Tabelle 8 :Attribute des Metadatenblocks federation_entity im well-known-Dokument des Fachdienstes Authorization Server

Name	Werte / Wertebereich
organization_name	String (max. 128 Zeichen) Wertebereich: ^[ÄÖÜäöüß\w\ \.\&\+*V]{1,128}\$

[<=, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, extNutz_GID, IDP-D, PoPP_Service, digi_ID_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung, funkt. Eignung: Test Produkt/FA]

Hinweis: Beispiel des Entity Statement eines Fachdienst Authorization Server sind im Anhang zu [gemSpec_IDP_Sek] dargestellt.

Neu - Bekanntgabe der Änderungen bisher nicht explizit gefordert

A_27989 -Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation

Anbieter eines Authorization Server in der TI-Föderation MÜSSEN geplante Änderungen folgender claims im Entity Statement vor Veröffentlichung dem Federation Master über einen organisatorischen Prozess beantragen:

- Änderungen des Schlüsselsets, mit dem das Entity Statement signiert wird - jwks,
- Änderungen des in der TI-Föderation propagierten Organisationsnamens - federation_entity.organization_name,
- Änderungen des Namens der Anwendung - openid_relying_party.client_name.

[<=, Anw_DiGA, Anb_IDP-D, Anb_TI-M_ePA, digi_ID_OGR, Anb_Aktensystem_ePA, extNutz_TI-Dienste_allg, organ./betriebl. Eignung: Anbietererklärung]

Neu - Zusätzlicher Hinweis zu A_27505 aufgrund der Möglichkeit von Synchronisationsproblemen durch Cache von Entity Statements

A_27505 -Signalisierung der unterstützten TI-Feature-Versionen durch einen Fachdienst der TI-Föderation

Ein Fachdienst der TI-Föderation MUSS in seinem Entity Statement im Metadatenblock openid_relying_party in einem Claim ti_features_supported signalisieren, welche spezifischen Versionen der TI-Föderation unterstützt werden. Im Claim ti_features_supported MUSS ein Fachdienst die Unterstützung der in Tabelle "Durch einen Fachdienst unterstützte TI-Features" genannten Claims signalisieren.

Tabelle 9 : Durch einen Fachdienst unterstützte TI-Features

claim	Wertebereich	Beschreibung
id_token_version_supported	[string], zulässige Werte in Liste: "1.0.0", "2.0.0"	Mit A_22867-* und A_23207-* ändert sich die Syntax des vom sektoralen IDP ausgestellten ID_TOKEN nicht abwärtskompatibel. Für einen Übergangszeitraum muss

		<p>ein Fachdienst die beiden Versionen:</p> <ul style="list-style-type: none">• 1.0.0 nach A_22867-01 und A_23207-02,• 2.0.0 nach A_27591 und A_27592, unterstützen.
--	--	---

【<=, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, SigD, extNutz_GID, IDP-D, PoPP_Service, digi_ID_OGR, funkt. Eignung: Herstellererklärung, organ./betriebl. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung】

Hinweis 1: Ob die Token Response vom sektoralen IDP einen ID_TOKEN der Version 1.0.0 oder 2.0.0 enthält, wird im JWT Header unter "version=1.0.0" bzw. "version=2.0.0" signalisiert. Das Fehlen dieses Tags im JWT Header ist als "version=1.0.0" zu interpretieren.

Hinweis 2: Ist id_token_version_supported im Entity Statement einer Relying Party nicht gesetzt, so unterstützt diese nur ID_TOKEN

Version "1.0.0" gemäß A_23129-04, A_22867-01, A_23207-02 (default).

Hinweis 3: Falls im JWT-Header der Token Response vom sektoralen IDP der Wert für "version=2.0.0" gesetzt ist, jedoch diese Version im Entity Statement des sektoralen IDP, welches der Fachdienst zuletzt geladen hat, nicht unter id_token_version_supported gelistet ist, so kann dies durch eine veraltete Version des Entity Statement im Cache des Fachdienstes begründet sein. Der Fachdienst muss in diesem Fall das aktuelle Entity Statement vom sektoralen IDP aktualisieren.

6 Änderung in gemSpec_IDP_Frontend

Kapitel "7.2.1 Schnittstellendefinition" wird wie folgt angepasst:

Alt:

A_20601-01 -Authenticator-Modul: Übergabe des Authorization-Request an den Authorization-Endpunkt

Das Authenticator-Modul MUSS den Authorization-Request, welchen dieses vom Anwendungsfrontend erhalten hat, an den Authorization-Server des IDP-Dienstes schicken. Der Authorization-Request MUSS folgende Parameter enthalten:

- "response_type"
- "scope"
- "client_id"
- "redirect_uri"
- "code_challenge"(Hashwert des "code_verifier") [RFC7636]
- "code_challenge_method"HASH-Algorithmus (S256) [RFC7636]
- "state" (State-Parameter)
- "nonce" (Nonce des ID_TOKEN gemäß [OpenID Connect Core])

[<=, eRp_FdV, Sich.techn. Eignung: Produktgutachten]

Neu:

A_20601-02 -Authenticator-Modul: Übergabe des Authorization Request an den Authorization-Endpunkt

Das Authenticator-Modul MUSS den Authorization Request, ~~welchen dieses vom~~einem Anwendungsfrontends ~~erhalten hat~~, an den Authorization Server des IDP-Dienstes schicken. Der Authorization Request MUSS folgende Parameter enthalten, ~~wenn es eine Authentifizierung über den IDP-Dienst unterstützt:~~

- "response_type"
- "scope"
- "client_id"
- "redirect_uri"
- "code_challenge"(Hashwert des "code_verifier") [RFC7636]
- "code_challenge_method"HASH-Algorithmus (S256) [RFC7636]
- "state" (State-Parameter)
- "nonce" (Nonce des ID_TOKEN gemäß [OpenID Connect Core])

[<=, eRp_FdV, Sich.techn. Eignung: Produktgutachten]

7 Änderungen in Steckbriefen

7.1 Änderungen in gemProdT_IDP-Dienst_PTV

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

Tabelle 10: Anforderungen zur funktionalen Eignung "Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21445-02	[Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des "ACCESS_TOKEN"]	gemSpec_IDP_Dient

Tabelle 11: Anforderungen zur sicherheits technische Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21445-02	[Inspektions- und Deregistrierungsfunktion des IdP-Dienstes: Validierung und Verarbeitung des "ACCESS_TOKEN"]	gemSpec_IDP_Dient

7.2 Änderungen in gemProdT_IDP_Sek

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

Tabelle 12: Anforderungen zur funktionalen Eignung "Test Produkt/FA"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22643-01	[Entity Statement des sektoralen IDP]	gemSpec_IDP_Sek

7.3 Änderungen in gemAnbT_IDP-Sek_KTR_ATV

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

Tabelle 13: Anforderungen zur organ./betriebl.Eignung "Betriebshandbuch"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_27988	[Bekanntgabe von Änderungen im Entity Statement eines sektoralen IDP der TI-Föderation]	gemSpec_IDP_Sek

7.4 Änderungen in gemProdT_Aktensystem_ePA_PTV, gemProdT_IDP-Dienst_PTV, gemProdT_PoPP_Service_PTV, gemProdT_TI-M_FD_ePA_PTV

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

Tabelle 14: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23034-01	[Entity Statement veröffentlichen]	gemSpec_IDP_FD

7.5 Änderungen in gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID

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

Tabelle 15: Anforderungen zur funktionalen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23034-01	[Entity Statement veröffentlichen]	gemSpec_IDP_FD

7.6 Änderungen in gemAnbT_Aktensystem_ePA_ATV, gemAnbT_TI-M_ePA_ATV, gemAnbT_IDP-Dienst_ATV, gemAnw_DiGA, gemAnw_OGR, gemAnw_PAT_GID

Anmerkung: Die Anforderungen der folgenden Tabelle stellt einen Auszug dar und verteilt sich innerhalb der Tabellen der Originaldokumente. Alle Anforderungen der Tabellen der

Originaldokumente, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 16: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_27989	[Bekanntgabe von Änderungen im Entity Statement einer Relying Party der TI-Föderation]	gemSpec_IDP_FD