
C_12182_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_IDP_Sek.....	3
3 Änderung in gemSpec_IDP_FD.....	13
4 Änderungen in Steckbriefen.....	16
4.1 Änderungen in gemProdT_..._PTVx.y.z-n.....	16

1 Änderungsbeschreibung

Im Rahmen der Besprechung des Kommentar BSI_01 (Kommentierung zu IDP_24.10) wurde ein Vorschlag erarbeitet, der die Anmerkungen des BSI löst. Der Vorschlag löst außerdem eine proprietäre durch eine standardkonforme Lösung ab.

2 Änderung in gemSpec_IDP_Sek

Änderungen im Kapitel "4.3.2 Authentifizierungsverfahren"

Ergänzung Hinweis zur beschränkten Gültigkeit der Anforderung A_23129-04

A_23129-04 - Identifikation des Authentifizierungsverfahren

Der sektorale IDP MUSS den Claim amr im ID_TOKEN entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 1: Codierung der Authentisierungsverfahren

Authentifizierungsverfahren	Wert des amr Claim	zulässiges Niveau (acr)
Authentifizierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high
Authentifizierung mittels elektronischem Identitätsnachweises (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high
Authentisierungsverfahren mit Einwilligung für ein Single Sign-On (SSO)	urn:telematik:auth:sso	gematik-ehealth-loa-high gematik-ehealth-loa-substantial
Authentisierungsverfahren mit Einwilligung zum Zugriff auf Daten mit hohem Schutzbedarf	urn:telematik:auth:mEW	gematik-ehealth-loa-substantial
Authentifizierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang)	urn:telematik:auth:guest:eGK	gematik-ehealth-loa-high
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial

[<=, IDP-Sek, Sich.techn. Eignung: Produktgutachten]

Hinweis: Die Anforderung gilt noch befristet bis zur vollständigen Umsetzung der Anforderungen A_27590, A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation.

Die neue Anforderung A_27590 löst die bestehende A_23129-04 nach einer Übergangszeit ab.

Neu:

A_27590 - Codierung der Authentisierungsverfahren im Claim "amr" des ID_TOKEN

Der sektorale IDP MUSS den Claim amr im ID_TOKEN entsprechend dem durchgeführten Authentisierungsverfahren nach folgender Tabelle befüllen.

Tabelle 2: Codierung der Authentisierungsverfahren

Authentisierungsverfahren	Wert des amr Claim	zulässiges Niveau (acr)
Authentisierung mittels eGK und PIN	urn:telematik:auth:eGK	gematik-ehealth-loa-high
Authentisierung mittels elektronischem Identitätsnachweis (Online-Ausweisfunktion)	urn:telematik:auth:eID	gematik-ehealth-loa-high
Authentisierung mittels Gerätebindung und System-PIN	urn:telematik:auth:systemPIN	gematik-ehealth-loa-high
Authentisierung mittels Gerätebindung und Anwendungs-PIN	urn:telematik:auth:appPIN	gematik-ehealth-loa-high
Authentisierung mittels eGK und PIN ohne Prüfung Gerätebindung (Gastzugang)	urn:telematik:auth:guest:eGK	gematik-ehealth-loa-high
Authentisierung mittels Gerätebindung und Biometrie	urn:telematik:auth:biometric	gematik-ehealth-loa-substantial
Anderes Authentisierungsverfahren	urn:telematik:auth:other	gematik-ehealth-loa-high und gematik-ehealth-loa-substantial

【<=, IDP-Sek, Sich.techn. Eignung: Produktgutachten】

Ergänzung Hinweis zur beschränkten Gültigkeit der Anforderung A_22867-01

A_22867-01 - Signalisierung der Verwendung des Authentisierungsverfahrens "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS den Claim amr um den Wert "urn:telematik:auth:mEW" erweitern, wenn der Fachdienst eine Authentifizierung des Nutzers auf dem Niveaugematik-ehealth-loa-high angefragt hat, der Nutzer jedoch ein Authentisierungsverfahren auf dem Niveau gematik-ehealth-loa-substantial verwendet hat. Die Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf MUSS vorliegen. 【<=, IDP-Sek, funkt. Eignung: Herstellererklärung】

Hinweis: Die Anforderung gilt noch befristet bis zur vollständigen Umsetzung der Anforderungen A_27590, A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation.

Die neue Anforderung A_27591 löst die bestehende A_22867-01 nach einer Übergangszeit ab.

Neu:

A_27591 - Signalisierung der Einwilligung durch den Nutzer in "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Der sektorale IDP MUSS in den Custom Claim urn:telematik:auth:consent den Wert loa-substantial ergänzen, wenn der Fachdienst eine Authentisierung des Nutzers auf dem Niveau gematik-ehealth-loa-high angefragt, der Nutzer jedoch ein Authentisierungsverfahren auf dem Niveau gematik-ehealth-loa-substantial verwendet hat und die Einwilligung des Anwenders zur Nutzung dieses Verfahrens zum Zugriff auf Daten mit hohem Schutzbedarf vorliegt. [\leq , IDP-Sek, funkt. Eignung: Herstellererklärung]

Änderungen im Kapitel "4.3.2.3 Unterstützung Single-Sign-On (SSO) auf Anwendungsebene"

Ergänzung Hinweis zur beschränkten Gültigkeit der Anforderung A_23207-02

A_23207-02 - Single-Sign-On (SSO) als Authentifizierungsverfahren

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS im claim acr das Niveau beauskunften, welcher dem der vorhergehenden Authentisierung entspricht. Der claim amr MUSS um den Wert urn:telematik:auth:sso gemäß der Tabelle "Codierung der Authentisierungsverfahren" erweitert werden. [\leq , IDP-Sek, Sich.techn. Eignung: Produktgutachten]

Hinweis: Die Anforderung gilt noch befristet bis zur vollständigen Umsetzung der Anforderungen A_27590, A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation.

Die neue Anforderung A_27592 löst die bestehende A_23207-02 nach einer Übergangszeit ab. Der claim urn:telematik:auth:interactive in A_27592 ist so ausgeprägt, dass die geplanten technischen Erweiterungen damit ebenfalls abgebildet werden können.

Neu:

A_27592 - Signalisierung Single-Sign-On (SSO) als Authentifizierungsverfahren im ID_TOKEN

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS im ID_TOKEN im Claim acr das Niveau bestätigen, welches dem der vorhergehenden Authentifizierung entspricht. Der Custom Claim urn:telematik:auth:interactive MUSS im ID_TOKEN auf den Wert silent gesetzt werden, wenn eine SSO-Authentisierung ohne Benutzerinteraktion durchgeführt wurde. [\leq , IDP-Sek, Sich.techn. Eignung: Produktgutachten]

A_27598 - Unterstütze Versionen der von sektoralen IDPs ausgestellten ID_TOKEN

Der sektorale IDP MUSS den Claim `metadata.openid_relying_party.ti_features_supported.id_token_version_supported` aus dem Entity Statement des anfragenden Fachdienstes auswerten und die jeweils höchste von beiden Seiten unterstützte Version für das auszugebene ID_TOKEN auswählen. Gibt es keine passende Übereinstimmung der unterstützten ID_TOKEN Versionen, so MUSS der IDP die höchste von ihm unterstützte ID_TOKEN Version benutzen. [≤, IDP-Sek, funkt. Eignung: Herstellererklärung]

Hinweis: Wird vom anfragenden Fachdienst nur die Version "1.0.0" supportet, so muss der sektorale IDP ein ID_TOKEN gemäß A_22867- ausstellen. Wird vom anfragenden Fachdienst die Version "2.0.0" supportet, so muss der sektorale IDP ein ID_TOKEN gemäß A_27593 ausstellen.*

Änderungen in "7.1.4 Detailinformationen zum App-App-Flow" - (11) Der Authorization Server erhält vom Token-Endpunkt des IDP einen ID_TOKEN und ACCESS_TOKEN mit den gewünschten Claims, der mit dem öffentlichen Schlüssel aus der Registrierung verschlüsselt ist

HTTP-200:

- Content-Type=application/json,
- Cache-Control=no-store,
- Pragma=no-cache,
- TI-ID-Token-Version=1.0.0 (wenn im ID-Token die Claims gemäß A_23202-02 befüllt sind),
- TI-ID-Token-Version=2.0.0 (wenn im ID-Token die Claims gemäß A_27593 befüllt sind).

Änderungen in Tabelle 43

- Ergänzung der Custom Claims "urn:telematik:auth:consent" und "urn:telematik:auth:interactive"
- Entfernen überflüssiger Einträge
- Textuelle Überarbeitung

Body Claims für den ID_TOKEN des sektoralen IDP

Name	Werte, Wertebereich	Beispiel	Anmerkungen
iss	string, URL nach [RFC1738]	https://idp4711.de	Adresse des sektoralen IDP / reicht als Authentizitätsnachweis
sub	string	"UserC3PO-666"	Beliebig, aber eindeutig je Nutzer und fest je Fachdienst. Wird als pseudonymer Identifier

			verwendet und ist einzig relevanter Claim für Dienste, die keine Nutzerdaten erhalten sollen oder wollen.
iat	number, Alle time Werte in Sekunden seit 1970, [RFC 7519 Sect.2]	1645565035	2022-02-22 22:23:55
exp	number, Alle time Werte in Sekunden seit 1970, [RFC 7519 Sect.2]	1645565335	Zeitliche Gültigkeit des Token von 5 Minuten
aud	string, URL nach [RFC1738]	"https:// Fachdienst007.de"	Die client_id des Fachdienstes - dieser hat die Anfrage gestellt.
nonce	string, max. 512 Zeichen	274312:dj83hs9s	
acr	string, "gematik- ehealth-loa- high", "gematik- ehealth-loa- substantial"	gematik-ehealth-loa- highsubstantial	Authentisierungsniveau, auf dem sich der Versicherte authentisiert hat.
amr	string, abschließend nach A_23129 A_27590 defin ierten Werten	urn:telematik:auth:bi ometric	Authentisierungsmethode, mit der sich der Versicherte authentisiert hat.
urn:telematik:auth:consent	[string] zulässige Werte in Liste: "loa- substantial"	["loa-substantial"]	Optional, wenn der Nutzer der Herabsetzung des Vertrauensniveau zugestimmt hat.
urn:telematik:auth:inte	string, zulässige	"silent"	Optional, wenn der Nutzer ohne

ractive	Werte: "silent"		Interaktion (durch SSO) authentifiziert wurde.
urn:telematik:claims:profession	OID	1.2.276.0.76.4.49	Claim belegt mit OID des Versicherten, abhängig von Scope/Claims
urn:telematik:claims:given_name	max. 64 Zeichen	-	Claim belegt mit dem Vornamen des Versicherten, abhängig von Scope/Claims
urn:telematik:claims:family_name	max. 64 Zeichen		UTF8String[RFC3629]
urn:telematik:claims:organization	max. 64 Zeichen	-	Claim belegt mit IK-Nummer der Kasse, abhängig von Scope/Claims
urn:telematik:Claims:id	10 Zeichen (für KVNR)	-	Claim belegt mit KVNR des Versicherten, abhängig von Scope/Claims
Claims gemäß A_22989* - "Scope" und "Claims" des sektoralen IDP für Versicherte		"urn:telematik:Claims:id" : <KVNR des Versicherten>	Das ID-Token enthält die Claims, welche der Fachdienst im PAR angefragt hat und die der sektorale IDP beauskunften kann.

Neue Anforderung

A_27506 - Signalisierung der unterstützten TI-Features durch einen sektoralen IDP der TI-Föderation

Ein sektoraler IDP MUSS in seinem Entity Statement im Metadatenblock openid_provider in einem Claim ti_features_supported signalisieren, welche spezifischen Versionen der TI-Föderation unterstützt werden. Im Claim ti_features_supported MUSS der sektorale IDP aktuell die Unterstützung der in

Tabelle "Durch einen sektoralen IDP unterstützte TI-Features" genannten Claims signalisieren.

Tabelle 3 : Durch einen sektoralen IDP 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 ein sektoraler IDP die beiden Versionen: <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.
sso_version_supported	[string], Zulässige Werte in Liste: "epafdv_controlled", "idp_controlled"	Das SSO auf ePA-FdV Anwendungsebene ändert sich von einer Version, in der das ePA-FdV die SSO-Präferenzen kontrolliert. Diese Version wird durch eine Version abgelöst, in welcher die sektoralen IDP die SSO-Präferenzen kontrollieren. Für einen Übergangszeitraum muss ein sektoraler IDP die beiden Versionen: <ul style="list-style-type: none"> • epafdv_controlled, • idp_controlled, unterstützen.

[<=, IDP-Sek, funkt. Eignung: Herstellererklärung]

Hinweis 1: Ist id_token_version_supported im Entity Statement eines sektoralen IDP nicht gesetzt, so unterstützt dieser nur ID Token Version "1.0.0" gemäß A_23129-04, A_22867-01, A_23207-02 (default).

Hinweis 2: Ist sso_version_supported im Entity Statement eines sektoralen IDP nicht gesetzt, so unterstützt dieser nur SSO-Version "epafdv_controlled" gemäß A_23129-04, A_22867-01, A_23207-02 (default).

Neues Kapitel: "9 Anhang D - Verfahrensbeschreibung zur Migration nicht abwärtskompatibler Änderungen in der TI-Föderation"

Nicht abwärtskompatible Änderungen in der TI-Föderation betreffen oft alle Teilnehmer der TI-Föderation. Eine zeitgleiche Produktivsetzung solcher Änderungen (Big Bang) ist

sehr risikoreich und unrealistisch. Es ist notwendig, solche Änderungen über eine Zeitspanne (Übergangszeit) durchführen zu können, ohne dass die Funktion der beteiligten Systeme beeinträchtigt wird.

Analog zum Vorgehen in der Softwareentwicklung ist es notwendig, abzulösende Artefakte als "deprecated" oder "befristet" zu markieren. Jedem nutzenden Teilnehmer wird so signalisiert, dass die Unterstützung für dieses Artefakt zeitlich begrenzt und eine Umstellung auf aktuellere Versionen notwendig ist.

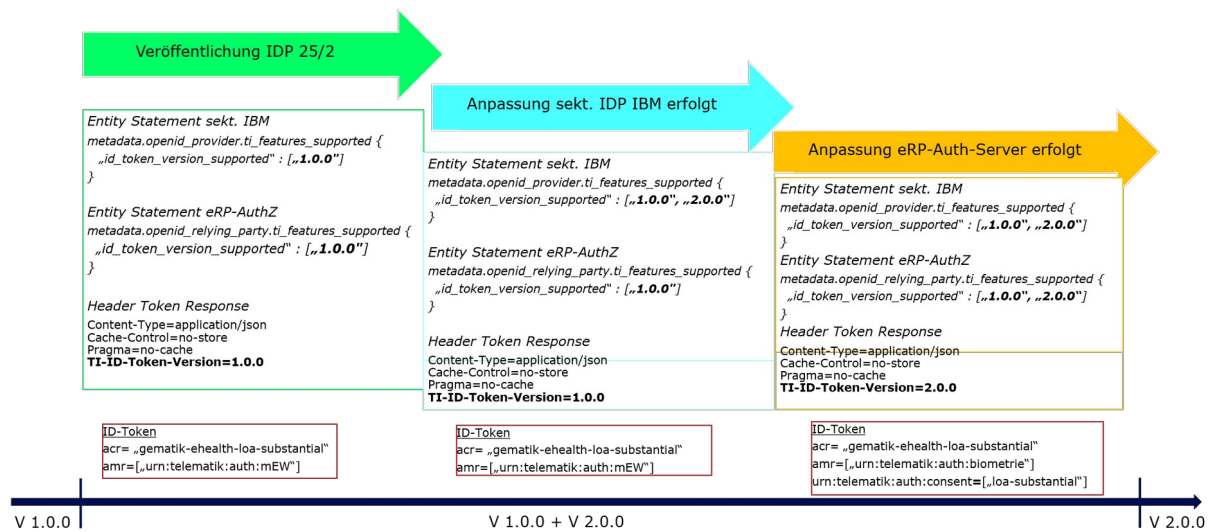
Für die Umsetzung dieses Ansatzes sind folgende Schritte notwendig:

Schritt	Beschreibung	Beteiligte
Spezifikationsanpassung	<ul style="list-style-type: none"> Spezifikation der neuen Anforderungen Markieren der abzulösenden Anforderungen als "Befristet gültig" mit Informationen zu den Alternativen. Die Markierung kann als Hinweistext unter die abzulösende Anforderung und/oder in der Anforderungsbeschreibung erfolgen <p>Beispiel:</p> <p><i>A_23207-02 - (Befristet) Single-Sign-On (SSO) als Authentifizierungsverfahren [≤]</i></p> <p><i>Hinweis: Die Anforderung gilt noch befristet bis zur vollständigen Umsetzung der Anforderungen A_27590, A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation.</i></p> <ul style="list-style-type: none"> Die Festlegung der Syntax für die Eintragungen im Entity Statement erfolgt in der Spezifikation des Entity Statement 	gematik
Signalisierung supporteter Versionen im Entity Statement	<p>Die Teilnehmer der TI-Föderation signalisieren in ihrem Entity Statement, welche Versionen sie unterstützen.</p> <ol style="list-style-type: none"> Nach Spezifikationsveröffentlichung signalisieren sie die Unterstützung der abzulösenden Version <p>Beispiel:</p> <pre>metadata.openid_relying_party.ti_features_supported { „id_token_version_supported“ : ["1.0.0"], }</pre> <ol style="list-style-type: none"> Nach Implementierungsanpassung signalisieren sie die Unterstützung der abzulösenden und der neuen Version <p>Beispiel:</p> <pre>metadata.openid_relying_party.ti_features_supported {</pre>	TI-Teilnehmer

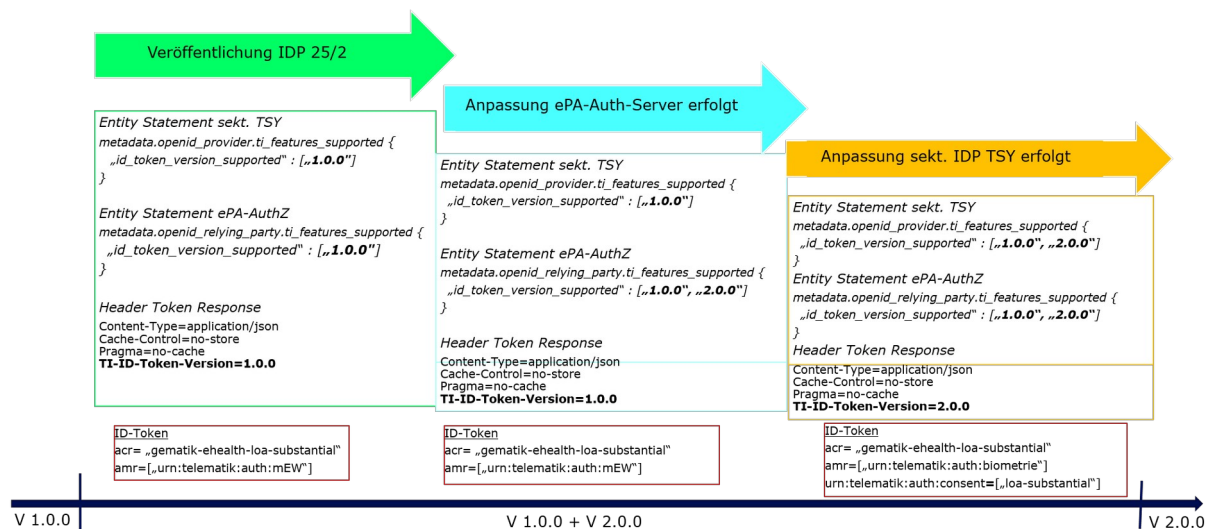
	<pre> „id_token_version_supported“ : [“1.0.0”, “2.0.0”], } </pre> <p>3. Nach Ablauf der Anpassungsfrist signalisieren sie die Unterstützung der neuen Version</p> <p>Beispiel:</p> <pre> metadata.openid_relying_party.ti_features_supported { „id_token_version_supported“ : [“2.0.0”], } </pre>	
Implementierung	<ul style="list-style-type: none"> • Anpassung der Implementierung an die neuen Anforderungen • Aufrechterhaltung der Implementierung an die abgelösten Anforderungen • Signalisierung des Implementierungsfortschritts im Entity Statement • IOP-Tests mit abhängigen TI-Teilnehmern 	TI-Teilnehmer
Bereinigung	<p>Nach Ablauf des Übergangszeitraums (bzw. Abschluss der notwendigen Anpassungen bei den TI-Teilnehmern) muss eine Bereinigung erfolgen.</p> <ul style="list-style-type: none"> • Spezifikationsbereinigung - Der Ausbau der befristet gültigen Anforderungen hat keine Auswirkungen auf die Hersteller und Betreiber • Implementierung - Der Ausbau der abgelösten Version kann unabhängig von anderen TI-Teilnehmern nach Ablösung der befristet gültigen Version individuell durch jeden Teilnehmer erfolgen 	gematik TI-Teilnehmer

Beispiel - nicht abwärtskompatible Änderung des ID-Token

Ein sekt. IDP hat vor einem Fachdienst umgestellt



Ein Fachdienst hat vor einem sekt. IDP umgestellt



3 Änderung in gemSpec_IDP_FD

Ergänzung Hinweis zur beschränkten Gültigkeit der Anforderung A_23202-02

A_23202-02 - Akzeptanz der Einwilligung zur Verwendung von Authentisierungsverfahren "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Die Fachdienste der TI-Föderation MÜSSEN den Zugriff auf Daten mit hohem Schutzbedarf auch bei einer Authentisierung auf dem Niveau gematik-ehealth-loa-substantial gewähren, wenn der Claim amr des ID_TOKEN Elemente mit den Werten urn:telematik:auth:mEW oder urn:telematik:auth:sso enthält und der Nutzer somit der Verwendung dieses Verfahrens für den Zugriff auf Daten mit hohem Schutzbedarf zugestimmt hat.

Hinweis: Die Anforderung ist nur befristet gültig. Nach Absprache mit dem BSI wird sie durch eine Anforderung abgelöst, welche einem Fachdienst sowohl die Information zur durchgeführten Authorization-Method als auch die Information zum Einwilligungsstatus im ID_TOKEN zur Verfügung stellt. [≤, Aktensystem_ePA, Anw_DiGA, TI-M_FD_ePA, SigD, extNutz_GID, IDP-D, PoPP_Service, digi_ID_OGR, Sich.techn. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung, Sich.techn. Eignung: Herstellererklärung]

Hinweis: Die Anforderung gilt noch befristet bis zur vollständigen Umsetzung der Anforderungen A_27590, A_27591, A_27592 und A_27593 durch alle Teilnehmer der TI-Föderation.

Die neue Anforderung A_27593 löst die bestehende A_23202-02 nach einer Übergangszeit ab.

Neu:

A_27593 - Akzeptanz der Einwilligung zur Authentisierung auf "gematik-ehealth-loa-substantial" beim Zugriff auf Daten mit hohem Schutzbedarf

Die Fachdienste der TI-Föderation MÜSSEN den Zugriff auf Daten mit hohem Schutzbedarf auch bei einer Authentisierung auf dem Niveau gematik-ehealth-loa-substantial gewähren, wenn der Claim urn:telematik:auth:consent im ID_TOKEN enthalten ist und dort ein Element loa-substantial signalisiert, dass die Einwilligung des Nutzers in die Absenkung des Vertrauensniveaus damit der Verwendung dieses Verfahrens für den Zugriff auf Daten mit hohem Schutzbedarf zugestimmt hat.

Hinweis: Über den weiteren optionalen Claim urn:telematik:auth:interactive erhält der Fachdienst die Information, ob die Authentisierung mit oder ohne aktive Nutzerinteraktion beim Single-Sign-On durchgeführt wurde. [≤, Aktensystem_ePA, Anw_DiGA, SigD, extNutz_GID, IDP-D, PoPP_Service, digi_ID_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

Neue Anforderung:

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 4 : Durch einen Fachdienst unterstützte TI-Features

claim	Wertebereich	Beschreibung
<code>id_token_version_supported</code>	[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 ein Fachdienst die beiden Versionen: <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.
<code>sso_version_supported</code>	[string], zulässige Werte in Liste: "epafdv_controlled", "idp_controlled"	Das SSO auf ePA-FdV-Anwendungsebene unterscheidet sich von einer Version, in der das ePA-FdV die SSO-Präferenzen kontrolliert. Diese Version wird durch eine Version abgelöst, in welcher die sektoralen IDP die SSO-Präferenzen kontrollieren. Für einen Übergangszeitraum muss ein Fachdienst die beiden Versionen: <ul style="list-style-type: none"> • epafdv_controlled, • idp_controlled, unterstützen.

【<=, Aktensystem_ePA, Anw_DiGA, 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 Response Header unter "TI-ID-Token-Version=1.0.0" bzw. "TI-ID-Token-Version=2.0.0" signalisiert. Das Fehlen dieses Tags im Response Header ist als "TI-ID-Token-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: Ist `sso_version_supported` im Entity Statement einer Relying Party nicht gesetzt, so unterstützt diese nur SSO-Version "epafdv_controlled" gemäß A_23129-04, A_22867-01, A_23207-02 (default).

4 Änderungen in Steckbriefen

4.1 Änderungen in gemProdT_..._PTVx.y.z-n

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. 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)
	[...]	