
C_12186_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_IDP_Sek.....	3
2.1 Änderung in gemSpec_IDP_FD.....	4
2.2 Änderung in gemSpec_ePA_FdV.....	4
3 Änderungen in Steckbriefen.....	5
3.1 Änderungen in gemProdT_..._PTVx.y.z-n.....	5

1 Änderungsbeschreibung

Derzeit sind wenige allgemeine Anforderungen an ein SSO für ePA-FdV spezifiziert. Implementierungsvarianten sind als Beispiel im Anhang der gemSpec_IDP_Sek dargestellt. Inzwischen wurden Details der Umsetzung abgestimmt, diese Details müssen sich prüfbar Anforderungen widerspiegeln.

2 Änderung in gemSpec_IDP_Sek

Neues Kapitel: 5.2.3 SSO auf Anwendungsebene ePA-FdV

A_27567 - Beschränkung der Fachdienst für ein SSO (befristet)

Der sektorale IDP MUSS sicherstellen, dass ein Single-Sign-On nur für im ePA-FdV gebundene Fachdienste erfolgen kann.

Hinweis 1: Die ClientID (iss) der im ePA-FdV gebundenen Fachdienste können beispielsweise als allow-list im sektoralen IDP hinterlegt sein.

Hinweis 2: Die Anforderung gilt für die zeitlich befristete Übergangslösung. Diese wird von einer ePA-FdV unabhängigen SSO-Lösung nach Abnahme durch das BSI abgelöst.

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

A_27568 - Widerruf und Reaktivierung der SSO-Präferenzen separater Authenticator-APP (befristet)

Ein Hersteller von sektoralen IDP, der ein SSO auf Anwendungsebene implementiert, MUSS sicherstellen, dass ein Nutzer die initial im ePA-FdV erstellte Präferenzen zur SSO-Nutzung ausschließlich über sein Authenticator Modul widerrufen und reaktiviert werden kann.

Hinweis: Die Anforderung gilt für die zeitlich befristete Übergangslösung. Diese wird von einer ePA-FdV unabhängigen SSO-Lösung nach Abnahme durch das BSI abgelöst.

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

A_27570 - Annahme des Parameter Instance-ID im URI-PAR bei separater Authenticator-APP (befristet)

Authenticator-Module von sektoralen IDP für mobile Endgeräte MÜSSEN den Parameter sso_instance_id bei Vorhandensein aus einem URI-PAR Aufruf entgegennehmen und auswerten können. Wird eine sso_instance_id übergeben, so MUSS der Authenticator eine Nutzerauthentifizierung über Single-Sign-On beim sektoralen IDP initiieren.

Hinweis: Die Anforderung gilt für die zeitlich befristete Übergangslösung. Diese wird von einer ePA-FdV unabhängigen SSO-Lösung nach Abnahme durch das BSI abgelöst.

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

2.1 Änderung in gemSpec_IDP_FD

A_27571 - Sicherstellung der Kommunikation zu bekannten Clients

Fachdienste, die eine Nutzerauthentifizierung über SSO auf Anwendungsebene unterstützen, MÜSSEN sicherstellen, dass sie nur mit Clients kommunizieren, die sich über geeignete technische Maßnahmen ("automatic") oder einen vom Fachdienstanbieter zur Verfügung gestellten organisatorischen Prozess ("explicit") bei ihnen registriert haben. [<=, Aktensystem_ePA, Anw_DiGA, PoPP_Modul, SigD, extNutz_GID, IDP-D, digi_ID_OGR, funkt. Eignung: Herstellererklärung, funkt. Eignung: Anbietererklärung]

2.2 Änderung in gemSpec_ePA_FdV

Erweiterung des Kapitel: "6.2.3.1 Authentisieren des Nutzers"

A_27569 - Erzeugung einer Instance-ID durch eine ePA-FdV Instanz bei separater Authenticator-APP (befristet)

Das ePA-FdV MUSS, wenn eine Nutzerauthentifizierung über SSO erfolgen soll, eine Instance-ID erzeugen und diese beim Aufruf der URI-PAR an das Authenticator-Modul als Parameter sso_instance_id übergeben. Die Instance-ID MUSS ein UUID V4 [[RFC9562.html#name-uuid-version-4](https://tools.ietf.org/html/rfc9562#name-uuid-version-4)] generierter Wert und unique für den Anwendungskontext sein. Die Instance-ID MUSS nach Beendigung der App (Beenden des Anwendungskontextes durch Nutzer oder Betriebssystem) ungültig sein.

Hinweis 1: Der Anwendungskontext ist die Laufzeit des ePA-FdV vom Start bis zum Beenden auf dem Gerät des Nutzers.

Hinweis 2: Die Anforderung gilt für die zeitlich befristete Übergangslösung. Diese wird von einer ePA-FdV unabhängigen SSO-Lösung nach Abnahme durch das BSI abgelöst. [<=, ,]

3 Änderungen in Steckbriefen

3.1 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 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	