
C_11016_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_IDP_Dienst.....	3
3 Änderung in gemSpec_Perf.....	5

1 Änderungsbeschreibung

Der IDP-Dienst hat keine Nutzersessions. Die restlichen Anforderungen, die sich auf Nutzersession beziehen, werden korrigiert.

2 Änderung in gemSpec_IDP_Dienst

A_20521-02 und A_22268 in gemSpec_IDP_Dienst werden geändert

A_20521-02 - Inhalt des CHALLENGE_TOKEN an das Authenticator-Modul

Der IDP-Dienst MUSS die ihm vorliegenden Session-Informationen (z.B. SESSION_ID, CODE_CHALLENGE, SCOPE und alle Informationen über Anwendungsfrontend und Authenticator-Modul) mit seinem privaten Schlüssel PrK_IDP_SIG und der technischen Rolle "oid_idpd" gemäß [gemSpec_OID # Abschnitt 3.5.4] signieren und als JWT ergänzt um die USER_CONSENT-Anfrage an das Authenticator-Modul senden. Als Algorithmus ist dementsprechend "BP256R1" zu wählen. [≤, IDP-D, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

A_20521-03 - Inhalt des CHALLENGE_TOKEN an das Authenticator-Modul

Der IDP-Dienst MUSS die ihm vorliegenden Session-Informationen (z.B. SESSION_ID, CODE_CHALLENGE, SCOPE und alle Informationen über Anwendungsfrontend und Authenticator-Modul) mit seinem privaten Schlüssel PrK_IDP_SIG und der technischen Rolle "oid_idpd" gemäß [gemSpec_OID # Abschnitt 3.5.4] signieren und als JWT ergänzt um die USER_CONSENT-Anfrage an das Authenticator-Modul senden. Als Algorithmus ist dementsprechend "BP256R1" zu wählen. [≤, IDP-D, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA]

A_22268 - Befristet - Prüfung des ID-Token eines sektoralen Identity Provider

Der IDP-Dienst MUSS empfangene ID-Token auf Authentizität gemäß [OpenID.Core#3.1.3.7] prüfen.

Insbesondere MUSS die Signatur mit einem unter jwks_uri referenzierter öffentlichen Schlüssel aus dem Discovery Document des sektoralen Identity Provider prüfbar sein. Dieser ist über die "kid" aus der Signatur des Token auszuwählen.

Des Weiteren MUSS der IDP-Dienst prüfen, ob die im ID-Token enthaltene Nonce dem Wert nonce_idp aus den Sitzungsdaten der Session entspricht. [≤, IDP-D, Sich.techn. Eignung: Produktgutachten]

A_22268-01 - Befristet - Prüfung des ID-Token eines sektoralen Identity Provider

Der IDP-Dienst MUSS empfangene ID-Token auf Authentizität gemäß [OpenID.Core#3.1.3.7] prüfen.

Insbesondere MUSS die Signatur mit einem unter jwks_uri referenzierter öffentlichen Schlüssel aus dem Discovery Document des sektoralen Identity Provider prüfbar sein. Dieser ist über die "kid" aus der Signatur des Token auszuwählen.

Des Weiteren MUSS der IDP-Dienst prüfen, ob die im ID-Token enthaltene Nonce dem Wert nonce_idp aus den Sitzungsdaten der Session entspricht. [≤, IDP-D, Sich.techn. Eignung: Produktgutachten]

Abbildung "Datenfluss-Diagramm IDP-Dienst" in 3.3 wird geändert

Beschreibungstext "... erzeugt der Authorization-Server dieSUBJECT_SESSION ..." in 4.3 wird geändert

5.2 wird geändert

Vorbedingung ist, dass sich das Authenticator-Modul bereits eine SUBJECT_SESSION mit dem Authorization-Server etabliert, sich das Discovery Document heruntergeladen und dieses erfolgreich ausgewertet hat.

3 Änderung in gemSpec_Perf

A_20153 und A_20154 in gemSpec_Perf werden gestrichen.

A_20153 - Performance - IDP-Dienst - Anzahl paralleler Sessions - TI

Der Produkttyp IDP-Dienst MUSS mindestens 95.000 gleichzeitige Sessions für Leistungserbringer unterstützen.

[<=, Anb_IDP-D, organ./betriebl. Eignung: Anbietererklärung]

A_20154 - Performance - IDP-Dienst - Anzahl paralleler Sessions - Internet

Der Produkttyp IDP-Dienst MUSS mindestens 2.400.000 gleichzeitige Sessions für Versicherte unterstützen.

[<=, Anb_IDP-D, organ./betriebl. Eignung: Anbietererklärung]