C_12927_Anlage - IDP-Dienst implementiert HCSL-Client

Inhaltsverzeichnis

1 Änderungsbeschreibung....2

2 Änderung in gemSpec_IDP_Dienst....3

3 Änderungen in Steckbriefen....6

3.1 Änderungen in gemProdT_IDP-Dienst_PTV....6

3.2 Änderungen in gemAnbT_IDP-Dienst_ATV....8

1 Änderungsbeschreibung

In der Prüfkette der Zertifikatsprüfung von Smartcards durch den IDP-Dienst war der Aufruf der OCSP-Responder wiederholt Ursache für Fehler in der Produktivumgebung. Überlastung oder Ausfall der OCSP-Responder führen dazu, dass die Authentifizierung von LEI über SMC-B fehlschlagen und damit der Zugang der LEI zu den TI-Anwendungen verwehrt wird.
HCSL (Hash based Certificate Status List) reduziert die Abhängigkeit der Zertifikatsprüfung von Verfügbarkeit und Stabilität der OCSP-Responder Schnittstelle.

Um HCSL nutzen zu können, muss der IDP-Dienst die Clientschnittstelle gemäß der Spezifikation [gemF_HCSL] implementieren. Dazu werden dem IDP-Dienst alle relevanten Anforderungen der HCSL-Spezifikation (vgl. Abschnitt "5.2 HCSL-Client" [gemF_HCSL]) zugewiesen.

Die Spezifikation gemSpec_IDP_Dienst wird um eine Anforderung erweitert, welche die Implementierung eines HCSL-Client fordert.

2 Änderung in gemSpec_IDP_Dienst

Es wird Kapitel "3.8.1 Erstellung des AUTHORIZATION_CODE" wie folgt angepasst:

Im Fall einer Authentisierung mittels Smartcard sendet der Authorization-Endpunkt eine CHALLENGE an das Authenticator-Modul und prüft anschließend die Signatur der CHALLENGE und das mitgelieferte Zertifikat der Smartcard des Nutzers mittels der TSL der PKI der Telematikinfrastruktur und für die Zertifikatsstausinformationen mittels HCSL [gemF_HCSL] oder OCSP, bevor er die benötigten Attribute ausliest.

Es wird Kapitel "4.3 Schnittstellenbeschreibung des IDP-Dienstes" wie folgt angepasst:

Die erste tokenbezogene Anfrage an den Authorization Server des IDP-Dienstes geht am Authorization-Endpunkt [RFC6749#section-3.1] ein. Das Authenticator-Modul reicht dort am Endpunkt den CONSENT mit der CHALLENGE ein, mit welchem die TOKEN erstellt werden sollen, und erhält den AUTHORIZATION_CODE zurück, falls die Prüfung der signierten CHALLENGE und die Prüfung des übergebenen Smartcard-Zertifikats am TSL-Dienst (und dabei u. a. Verwendung von HCSL oder OCSP) positiv ausfallen.

Es wird Kapitel "5.2.1 Authorization-Endpunkt Eingangsdaten" wie folgt angepasst:

Neue Anforderung A_30517

Neu:

A_30517 - Implementierung eins HCSL-Client

Der Authorization-Endpunkt MUSS einen HCSL-Client gemäß [gemF_HCSL] implementieren. Sollte eine CA der TI-PKI HCSL anbieten (vgl. A_28711-*) so MUSS der Authorization-Endpunkt HCSL für die Zertifikatszustandprüfung für EE-Zertifikate aus solch einer CA verwenden. Er MUSS im Fehlerfall (HCSL) zurückfallen auf die Verwendung von OCSP für die Zertifikatszustandsprüfung.

[<=]

redaktionelle Erweiterung A_20951* und A_20465

Alt:

A_20951-01 -Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN

Der Authorization-Endpunkt MUSS die Signatur des vom Authenticator-Modul übertragenen, signierten CHALLENGE_TOKEN anhand des mitgelieferten Authentifizierungs-Zertifikats überprüfen. Die Überprüfung MUSS neben der Signatur auch das Authentifizierungszertifikat anhand von OCSP umfassen. [<=]

Neu:

A_20951-02 -Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN

Der Authorization-Endpunkt MUSS die Signatur des vom Authenticator-Modul übertragenen, signierten CHALLENGE_TOKEN anhand des mitgelieferten Authentifizierungs-Zertifikats überprüfen. Die Überprüfung MUSS neben der

Signaturprüfung (Zertifikatskette) auch den Zertifikatszustand des Authentifizierungszertifikats ~~anhand von~~mittelsHCSL oder als Fallback OCSP umfassen. [<=]

Alt:

A_20465 - Zertifikatsprüfung gegen OCSP-Responder

Der Authorization-Endpunkt MUSS das Zertifikat des Antragstellers immer gegen den zugehörigen OCSP-Responder innerhalb der TI auf Gültigkeit prüfen. [<=]

Neu:

A_20465-01 - Zertifikatsstatusprüfung gegen HCSL oder OCSP-Responder

Der Authorization-Endpunkt MUSS das Zertifikat des Antragstellers immer gegen den zugehörigen HCSL oder als Fallback OCSP-Responder innerhalb der TI auf Gültigkeit prüfen. [<=]

Es wird Kapitel "6.1 Abkürzungen" wie folgt angepasst:

Kürzel	Erläuterung
...	...
HBA	Heilberufsausweis
HCSL	Hash based Certificate Status List
IDP	Identity Provider
...	...

Es wird Kapitel "6.5.1 Dokumente der gematik" wie folgt angepasst:

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemILF_PS_eRp]	gematik: Spezifikation Implementierungsleitfaden Primärsysteme - E-Rezept
[gemF_HCSL]	gematik:Feature-Spezifikation Hash based Certificate Status List (HCSL)
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider-Frontend
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider-Fachdienst
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

[gemSpec_OID]	gematik: Übergreifende Spezifikation: Festlegung von OIDs
[gemSpec_PKI]	gematik: Übergreifende Spezifikation: PKI
[gemSpec_Perf]	gematik: Übergreifende Spezifikation: Performance und Mengengerüst TI-Plattform

3 Änderungen in Steckbriefen

3.1 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 1: Anforderungen zur sich. techn. Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_30517	Implementierung eins HCSL-Client.	gemSpec_IDP_Dienst
A_29031	HCSL-Client: lokale Aufbereitung/Verfügbarmachung der HCSL-Daten	gemF_HCSL

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20951-01~~	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
A_20951-02	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
~~A_20465~~	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_20465-01	Zertifikatsprüfung gegen OCSP-Responder oder HCSL	gemSpec_IDP_Dienst

Tabelle 3: Anforderungen zur sich. techn. Eignung "Produktgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
~~A_20951-01~~	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
A_20951-02	Validierung der Signatur und des Zertifikats des CHALLENGE_TOKEN	gemSpec_IDP_Dienst
~~A_20465~~	Zertifikatsprüfung gegen OCSP-Responder	gemSpec_IDP_Dienst
A_20465-01	Zertifikatsprüfung gegen OCSP-Responder oder	gemSpec_IDP_Dienst

	HCSL	
A_28957	HCSL-Client: EE-Zertifikatsstatusprüfung auf Basis einer HPL	gemF_HCSL
A_28958	HCSL-Client: EE-Zertifikatsstatusprüfung auf Basis einer HNL	gemF_HCSL
A_28959	HCSL-Client: Bezug von Signaturzertifikaten	gemF_HCSL
A_29029	HCSL-Client: Signaturprüfung bei Neubezug oder Aktualisierung der lokalen HCSL	gemF_HCSL
A_29030	HCSL-Client: zeitliche Prüfung HCSL	gemF_HCSL
A_30387	HCSL-Client: EE-Zertifikatsprüfung, erst Prüfung ob Teil der TI-PKI bevor HCSL-Verwendung	gemF_HCSL

99

100 **Tabelle 4: Anforderungen zur funktionalen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28711	HCSL-Client: Prüfung der HCSL-Verfügbarkeit alle CAs	gemF_HCSL
A_28954	HCSL-Client: regelmäßige Aktualisierung der lokalen HCSL	gemF_HCSL
A_28957	HCSL-Client: EE-Zertifikatsstatusprüfung auf Basis einer HPL	gemF_HCSL
A_28958	HCSL-Client: EE-Zertifikatsstatusprüfung auf Basis einer HNL	gemF_HCSL
A_28959	HCSL-Client: Bezug von Signaturzertifikaten	gemF_HCSL
A_29029	HCSL-Client: Signaturprüfung bei Neubezug oder Aktualisierung der lokalen HCSL	gemF_HCSL
A_29030	HCSL-Client: zeitliche Prüfung HCSL	gemF_HCSL
A_29031	HCSL-Client: lokale Aufbereitung/Verfügbarmachung der HCSL-Daten	gemF_HCSL
A_30287	HCSL-Client: Vorgaben zur den hcsl-config-<aki>.cbor Dateien	gemF_HCSL
A_30288	HCSL-Client: Prüfung der Key-Value-Paare in einer hcsl-config-<aki>.cbor Dateien	gemF_HCSL

A_30330	HCSL-Client: Aktualisierung der HCSL durch Delta-Dateien nach Ausfall im Client	gemF_HCSL
A_30331	HCSL-Client: Verhalten bei nichterfolgreichem Download der Delta-Dateien	gemF_HCSL
A_30387	HCSL-Client: EE-Zertifikatsprüfung, erst Prüfung ob Teil der TI-PKI bevor HCSL-Verwendung	gemF_HCSL

3.2 Änderungen in gemAnbT_IDP-Dienst_ATV

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

Tabelle 5: Anforderungen zur organ./betriebl. Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_30386	HCSL-Client: Alarmbehandlung bei einem Anbieter eines Fachdienstes, dessen Fachdienst HCSL-Client ist	gemF_HCSL

Tabelle 6: Anforderungen zur sich./tech. Eignung "Gutachten (Anbieter)"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_30386	HCSL-Client: Alarmbehandlung bei einem Anbieter eines Fachdienstes, dessen Fachdienst HCSL-Client ist	gemF_HCSL