

## C\_11980\_Anlage

Änderung in der gemSpec\_Perf

alt:

### A\_22833 - Performance - Sektoraler Identity Provider in der Föderation - Bearbeitungszeiten unter Last

Der Anbieter des sektoralen Identity Provider MUSS die Bearbeitungszeitvorgaben unter Last aus Tab\_gemSpec\_Perf\_sektoraler\_IDP erfüllen.

Es wird davon ausgegangen, dass der sektorale Identity Provider eingeschwungen ist und z. B. Lokalisierungsanfragen lokal zwischengespeichert sind, sowie Verbindungen nicht neu ausgehandelt werden.

MA ist der Marktanteil des Anbieters gemäß [A\_22225].

Im Fall der Authorization Requests zählt die Zeit von Anfrage des Authenticator-Moduls bis zum Eintreffen der Antwort nicht zur Bearbeitungszeit.

**Tabelle 1: Tab\_gemSpec\_Perf\_sektoraler\_IDP: Bearbeitungszeitvorgaben**

ID	Anwendungsfälle	Lastvorgabe n	Bearbeitungszeitvorgaben
		Spitzenlast [1/sec]	Maximalwert [msec]
IDP.UC_30	Processing of Pushed Authorization Requests	10 + (450 x MA)	800
IDP.UC_31	Processing of Authorization Requests (alle Authentisierungsverfahren)	10 + (450 x MA)	2000
IDP.UC_32, IDP.UC_33 IDP.UC_34	Response of Authorization Requests (mit online Ausweisfunktion) Response of Authorization Requests (mit eGK und PIN) Response of Authorization Requests (alternatives Authentisierungsverfahren)	10 + (450 x MA)	100
IDP.UC_39	Token Requests	10 + (450 x MA)	800

【<=, Anb\_IDP-Sek\_KTR, organ./betriebl. Eignung: Anbietererklärung】

alt:

**A\_22825-01 - Performance - Betriebsdatenlieferung v2 - Spezifika sektoraler IDP - Operation/Duration**

Der Produkttyp MUSS bei Betriebsdatenlieferungen bzgl. der Felder "operation" und "duration\_in\_ms" die Angaben aus der Tabelle

Tab\_gemSpec\_Perf\_Berichtsformat\_sektoraler\_IDP in der Spalte "\$IDP-Operation" und der Spalte "\$Duration" berücksichtigen.

Produkttyp: sektoraler Identity Provider

Schnittstelle: Internet

**Tabelle 2: Tab\_gemSpec\_Perf\_Berichtsformat\_sektoraler\_IDP**

<b>\$IDP-Operation</b>	<b>Operation</b>	<b>\$Duration</b>
IDP.UC_30	Processing of Pushed Authorization Requests	Die Duration beginnt mit der Annahme des Pushed Authorization Request (PAR) vom Authorization-Server des Fachdienstes und endet mit der Übermittlung der "URI-PAR" zum Authorization-Server des Fachdienstes. Zeiten zwischen der optionalen Anfrage "Get Entity Statement RP" des sektoralen IDP an den Fachdienst und der Antwort "Entity Statement" sowie der optionalen Anfrage "Fetch Entity Statement RP" des sektoralen IDP an den Federation Master und Antwort "Entity Statement" sind in der Berechnung für den IDP.UC_30 herauszurechnen.
IDP.UC_31	Processing of Authorization Requests (alle Authentisierungsverfahren)	Die Duration beginnt mit der Annahme des Authorization-Request (URI-PAR) und enden mit dem Absenden der Anfrage zur Authentifizierung.
IDP.UC_32	Response of Authorization Requests (mit online Ausweisfunktion)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).
IDP.UC_33	Response of Authorization Requests (mit eGK und PIN)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).

IDP.UC_34	Response of Authorization Requests (alternatives Authentisierungsverfahren)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).
IDP.UC_39	Token Requests	Die Duration für IDP.UC_39 beginnt mit der Annahme des AUTH_CODE vom Authorization-Server des Fachdienstes und endet mit der Übermittlung des ID_TOKEN (ACCESS_TOKEN) zum Authorization-Server des Fachdienstes.

【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

alt:

#### **A\_22944-02 - Performance - Betriebsdatenlieferung v2 - Spezifika sek IDP - Message**

Der Produkttyp sek IDP MUSS bei Betriebsdatenlieferungen bzgl. des Feldes "message" folgende spezifischen Festlegungen hinsichtlich des Formates und der Inhalte berücksichtigen.

```
{ "cidi": $cidi, "err": $errorcode, "ik": $gemIK }
```

- \$cidi: <Applicationidentifizier> gemäß A\_24582, Datentyp Integer
- \$errorcode: <Fehlercode> gemäß A\_25082, Datentyp Integer
- \$gemIK: <abgestimmtes IK> gemäß A\_25078, Datentyp Integer

*Hinweis: Bei der Erstellung des message-Feldes ist darauf zu achten, dass weder Whitespaces noch Newlines zwischen JSON-Elementen enthalten sind (kein Indenting) und die Vorgaben nach [RFC7493] eingehalten werden.* 【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

alt:

#### **A\_24582 - Präzisierung - Spezifika sek IDP - Message - Nutzung der cidi**

Der Produkttyp sek IDP MUSS bei Betriebsdatenlieferungen genau die Requests in den Betriebsdaten berücksichtigen und den zugehörigen Wert für "cidi" für A\_22944 berichten, bei denen es sich um:

- Anfragen von in der TI-Föderation registrierten Authorization Servern [cidi gemäß A\_24339, Integer] oder
- Anfragen von Signaturdiensten (SigD) [cidi = "111114"] oder
- Anfragen von kassenindividuellen Anwendungen unter Nutzung der GesundheitsID [cidi = "111116"]

handelt. 【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

**Löschen:**

### A\_22048-01 - Performance - Betriebsdatenlieferung v2 - Spezifika IDP-Dienst - Übermittlung bei dislozierten CIs

Der Anbieter KANN die Übermittlung der Betriebsdatenlieferung in Absprache mit dem Gesamtverantwortlichen TI je Standort vollziehen, wobei diese Standorte dann eindeutig identifizierbar sein müssen, sofern das Configuration Item (CI) über mehrere Standorte verteilt ist. [≤, Anb\_IDP-Sek\_KTR, organ./betriebl. Eignung: Anbietererklärung]

#### Löschen (FastTrack):

### A\_22226 - Performance - Sektoraler Identity Provider - Bearbeitungszeit unter Last

Der Anbieter eines sektoralen Identity Provider MUSS die Bearbeitungszeitvorgaben unter Last aus Tab\_gemSpec\_Perf\_Sek\_IDP erfüllen.

Es wird davon ausgegangen, dass der sektorale Identity Provider eingeschwungen ist und z.B. Lokalisierungsanfragen lokal zwischengespeichert sind, sowie Verbindungen nicht neu ausgehandelt werden.

MA ist der Marktanteil des Anbieters gemäß [A\_22225].

Im Fall der Authorization Requests zählt die Zeit von Anfrage des Authenticator-Moduls bis zum Eintreffen der Antwort nicht zur Bearbeitungszeit.

**Tabelle 3: Tab\_gemSpec\_Perf\_sek\_IDP: Bearbeitungszeitvorgaben**

ID	Anwendungsfälle	Lastvorgaben	Bearbeitungszeitvorgaben	
		Spitzenlast [1/sec]	Mittelwert [msec]	99%-Quantil [msec]
IDP.UC_20	Processing of Authorization Request (third-party-based authentication)	10 + (450 x MA)	1500	1964
IDP.UC_21	Token Request (third-party-based authentication)	10 + (450 x MA)	500	664

[≤, , ]

neu:

### A\_22833-01 - Performance - Anbieter Sektoraler Identity Provider Kostenträger - Bearbeitungszeiten unter Last

Der Anbieter Sektoraler Identity Provider Kostenträger MUSS die Bearbeitungszeitvorgaben unter Last aus Tab\_gemSpec\_Perf\_sektoraler\_IDP erfüllen.

Es wird davon ausgegangen, dass der sektorale Identity Provider eingeschwungen ist und z. B. Lokalisierungsanfragen lokal zwischengespeichert sind, sowie Verbindungen nicht neu ausgehandelt werden.

MA ist der Marktanteil des Anbieters gemäß A\_22225.

Im Fall der Authorization Requests zählt die Zeit von der Anfrage des Authenticator-Moduls bis zum Eintreffen der Antwort nicht zur Bearbeitungszeit und muss gemäß A\_22944\* separat als "backendduration" mitgeteilt werden.

**Tabelle 4: Tab\_gemSpec\_Perf\_sektoraler\_IDP: Bearbeitungszeitvorgaben**

ID	Anwendungsfälle	Lastvorgabe	Bearbeitungszeitvorgabe
----	-----------------	-------------	-------------------------

		n	n
		Spitzenlast [1/s]	Maximalwert [ms]
IDP.UC_30	Processing of Pushed Authorization Requests	10 + (450 x MA)	800
IDP.UC_31	Processing of Authorization Requests (alle Authentisierungsverfahren)	10 + (450 x MA)	500
IDP.UC_32, IDP.UC_33 IDP.UC_34	Response of Authorization Requests (mit online Ausweisfunktion) Response of Authorization Requests (mit eGK und PIN) Response of Authorization Requests (alternatives Authentisierungsverfahren)	10 + (450 x MA)	100
IDP.UC_39	Token Requests	10 + (450 x MA)	800

【<=, Anb\_IDP-Sek\_KTR, organ./betriebl. Eignung: Anbietererklärung】

neu:

#### **A\_22825-02 - Performance - Betriebsdatenlieferung v2 - Spezifika Anbieter Sektoraler Identity Provider Kostenträger - Operation/Duration**

Der **sektorale Identity Provider** MUSS bei Betriebsdatenlieferungen bzgl. der Felder "operation" und "duration\_in\_ms" die Angaben aus der Tabelle Tab\_gemSpec\_Perf\_Berichtsformat\_sektoraler\_IDP in der Spalte "\$IDP-Operation" und der Spalte "\$Duration" berücksichtigen.  
Schnittstelle: Internet

**Tabelle 5: Tab\_gemSpec\_Perf\_Berichtsformat\_sektoraler\_IDP**

<b>\$IDP-Operation</b>	<b>Operation</b>	<b>\$Duration</b>
IDP.UC_30	Processing of Pushed Authorization Requests	Die Duration beginnt mit der Annahme des Pushed Authorization Request (PAR) vom Authorization Server des Fachdienstes und endet mit der Übermittlung der "URI-PAR" zum Authorization Server des Fachdienstes. Zeiten zwischen der optionalen Anfrage "Get Entity Statement RP"

		des sektoralen IDP an den Fachdienst und der Antwort "Entity Statement" sowie der optionalen Anfrage "Fetch Entity Statement RP" des sektoralen IDP an den Federation Master und Antwort "Entity Statement" sind in der Berechnung für den IDP.UC_30 nicht enthalten und gemäß A_22944* separat als "backendduration" mitzuteilen.
IDP.UC_31	Processing of Authorization Requests (alle Authentisierungsverfahren)	Die Duration beginnt mit der Annahme des Authorization-Request (URI-PAR) und endet mit dem Absenden der Anfrage zur Authentifizierung.
IDP.UC_32	Response of Authorization Requests (mit online Ausweisfunktion)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).
IDP.UC_33	Response of Authorization Requests (mit eGK und PIN)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).
IDP.UC_34	Response of Authorization Requests (alternatives Authentisierungsverfahren)	Die Duration beginnt mit der Annahme der Antwort auf die Anfrage zur Authentifizierung und endet mit der Übermittlung der Antwort zur redirect_url oder eines Fehlercodes an die Betriebsdatenerfassung (siehe A_22826).
IDP.UC_39	Token Requests	Die Duration für IDP.UC_39 beginnt mit der Annahme des AUTH_CODE vom Authorization Server des Fachdienstes und endet mit der Übermittlung des ID_TOKEN (ACCESS_TOKEN) zum Authorization Server des Fachdienstes.

【<=, IDP-Sek, funkt. Eignung: Test Produkt/FA】

neu: Konkretisierung der Wartezeit (analog zum IDP-Dienst) (Produkt)

#### **A\_26466 - Performance - Sektoraler Identity Provider - Abbruch bei OCSP-Timeout**

Der sektorale Identity Provider MUSS nach einer konfigurierbaren Wartezeit von 5000 ms auf die Antwort des OCSP oder anderen Backendsystemen den Vorgang abbrechen und diesen Abbruch gemäß [gemSpec\_Perf#A\_22015] und [Tab\_gemSpec\_Perf\_Fehlercodes\_IDP-Dienst] mit "OCSP\_ERROR\_NO\_RESPONSE" protokollieren. [≤, IDP-Sek, funkt. Eignung: Test Produkt/FA]

neu: Hintergrundaktivitäten (backendduration) übergreifend einheitlich berücksichtigen (Produkt)

#### **A\_22944-03 - Performance - Betriebsdatenlieferung v2 - Spezifika Sektoraler Identity Provider - Message**

Der sektorale Identity Provider MUSS bei Betriebsdatenlieferungen bzgl. des Feldes "message" folgende spezifischen Festlegungen hinsichtlich des Formates und der Inhalte berücksichtigen.

{ "cidi": \$cidi, "err": \$errorcode, "ik": \$gemIK, "bkdur": \$backendduration }

- \$cidi: <Applicationidentifizier> gemäß A\_24582, Datentyp Integer,
- \$errorcode: <Fehlercode> gemäß A\_25082, Datentyp Integer,
- \$gemIK: <abgestimmtes IK> gemäß A\_25078, Datentyp Integer,
- \$backendduration: Zeit in ms für Abfragen an OCSP oder anderen Backendsystemen, Datentyp Integer.

#### *Hinweis:*

*Der Wert für \$backendduration für Anwendungsfälle ohne Abfragen an OCSP oder anderen Backendsystemen ist NULL oder das Key-Value-Paar ist komplett zu entfernen. Bei der Erstellung des message-Feldes ist darauf zu achten, dass weder Whitespaces noch Newlines zwischen JSON-Elementen enthalten sind (kein Indenting) und die Vorgaben nach [RFC7493] eingehalten werden. [≤, IDP-Sek, funkt. Eignung: Test Produkt/FA]*

Hochkommas entfernt

#### **A\_24582-01 - Performance - Betriebsdatenlieferung v2 - Spezifika Sektoraler Identity Provider - Message - Vorgabe cidi**

Der sektorale Identity Provider MUSS bei Betriebsdatenlieferungen genau die Requests in den Betriebsdaten berücksichtigen und den zugehörigen Wert für "cidi" für A\_22944 berichten, bei denen es sich um:

- Anfragen von in der TI-Föderation registrierten Authorization Servern [cidi gemäß A\_24339, Integer] oder
- Anfragen von Signaturdiensten (SigD) [cidi = 111114, Integer] oder
- Anfragen von kassenindividuellen Anwendungen unter Nutzung der GesundheitsID [cidi = 111116, Integer]

handelt. [≤, IDP-Sek, funkt. Eignung: Test Produkt/FA]

Typ Integer konkretisiert

**A\_24339-01 - Performance - Betriebsdatenlieferung v2 - Spezifika Sektoraler Identity Provider - Aufbereitung Client-ID als cidi**

Der sektorale Identity Provider MUSS einen CRC-32 Hashwert aus der Client-ID (dem iss-claim aus dem Entity Statement des Fachdienstes) erstellen, in einen Integer umwandeln und diesen Wert in den Betriebsdaten im Parameter "cidi" verwenden.

Der Parameter "cidi" ist vom Typ Integer.

Es wird empfohlen, diesen Wert zu speichern (Caching) und nicht jeweils erneut zu berechnen. [≤, IDP-Sek, funkt. Eignung: Herstellererklärung]

Alt:

**A\_22957 - Performance - FedMaster - Verfügbarkeit**

Der Anbieter des Federation Master MUSS sein Produkt so betreiben, dass es zur Hauptzeit und zur Nebenzeit mindestens eine Verfügbarkeit von 98,40 % hat. Genehmigte Wartungsfenster dürfen nur in der Nebenzeit liegen und werden nicht als Ausfallzeit gewertet.

Hauptzeit des Produkttyps ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit.

[≤, Anb\_IDP\_FedMaster, organ./betriebl. Eignung: Betriebshandbuch]

Neu:

**A\_22957-01 - Performance - Anbieter Federation Master - Verfügbarkeit PU**

Der Anbieter Federation Master MUSS folgende Verfügbarkeit in der Produktivumgebung (PU) in den festgelegten Servicezeiten einhalten:

- Hauptzeit: 98,40 %
- Nebenzeit: 98,40 %

[≤, Anb\_IDP\_FedMaster, organ./betriebl. Eignung: Betriebshandbuch]

**A\_27103 - Performance - Anbieter Federation Master - Verfügbarkeit RU + TU**

Der Anbieter Federation Master MUSS folgende Verfügbarkeit in der Test- und Referenzumgebung (RU + TU) in den festgelegten Servicezeiten einhalten:

- Hauptzeit: 90,00 %
- Nebenzeit: 85,00 %

[≤, Anb\_IDP\_FedMaster, organ./betriebl. Eignung: Anbietererklärung]

Zuordnung des Anbieters Federation Master zur AFO A\_23348

Die Service-Zeiten waren bislang innerhalb obiger AFO aufgeführt:

" Hauptzeit des Produkttyps ist Montag bis Sonntag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit."

der Vollständigkeit halber hier explizit erwähnt:

**A\_23348 - Performance - Servicezeiten des Produktes - Hauptzeit - Montag bis Freitag**

Der Produkttyp MUSS folgende Servicezeiten gewährleisten:

- Hauptzeit ist Montag bis Freitag von 6 bis 22 Uhr.
- Bundeseinheitliche Feiertage und alle übrigen Stunden der Woche sind Nebenzeit.

[≤, Intermediär VSDM, KOM-LE FD, UFS, TIM\_FD, VSDD, CMS, TI-M\_FD\_Basis, ZT\_PIP\_PAP, funkt. Eignung: Herstellererklärung]