gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Konnektor Basisdienst tokenbasierte Authentisierung

Version:	1.2.0
Revision:	19021
Stand:	14.05.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_Kon_TBAuth

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zur Vorversion beruhen auf P15.4.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Initialversion Online-Rollout Stufe 2.1	gematik
1.0.0	02.08.17		freigegeben	gematik
	05.12.17		Einarbeitung P15.1	gematik
1.1.0	18.12.17		freigegeben	gematik
			Einarbeitung P15.4	gematik
1.2.0	14.05.18		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Dieses Dokument enthält die Anforderungen an den Basisdienst tokenbasierte Authentisierung (BD-TBAuth), welches einen Teil des Produkttyps Konnektor darstellt. Der BD-TBAuth ist eine „Komfortfunktion“ im Rahmen der Authentisierung lokaler Benutzer. Dazu stellt er Identitätsbestätigungen aus, die mit der SM-B signiert werden. Dadurch müssen die Bestätigungen nicht vom Clientsystem selbst erzeugt werden. Der Konnektor gewährleistet dabei aber nicht, dass die behauptete Identität in der Identitätsbestätigung korrekt ist, bietet also keine zusätzliche Sicherheit an. Die Bestätigungen können für die Authentisierung gegenüber Gesundheitsdatendiensten in der TI genutzt werden.

1.2 Zielgruppe

Das Dokument richtet sich an Konnektorhersteller sowie Hersteller und Anbieter von Produkttypen und anderen Systemen, die mit dem BD-TBAuth (als Teil des Konnektors) interagieren. Letzteres betrifft sowohl Systemhersteller, die eine direkte Schnittstelle zum BD-TBAuth anbieten (z. B. Primärsysteme, Client, lokaler IDP), als auch Systemhersteller, die indirekt mit dem BD-TBAuth interagieren (z. B. Dienste).

1.3 Geltungsbereich

Dieses Dokument enthält normative Anforderungen und Festlegungen, die von Herstellern und Betreibern von Komponenten und Diensten im Rahmen der Projekte der Neuausrichtung zur Einführung der elektronischen Gesundheitskarte und der Telematik Infrastruktur des Deutschen Gesundheitswesens zu beachten sind.

Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung im Zulassungs- und Bestätigungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Arbeitsgrundlagen

Grundlagen für die Ausführung dieses Dokumentes sind insbesondere:

- Übergreifende Spezifikation tokenbasierte Authentisierung [gemSpec_TBAuth]
- Konzept Architektur der TI-Plattform [gemKPT_Arch_TIP]
- Konnektor-Spezifikation [gemSpec_Kon]
- OASIS WS-SecurityPolicy Spezifikation [WS-SecurityPolicy1.3]
- OASIS WS-Trust Spezifikation [WS-Trust1.3] [WS-Trust1.4]
- OASIS WS-Federation [WS-Federation1.2]

1.5 Abgrenzung des Dokuments

Spezifiziert werden in dem Dokument die vom Basisdienst tokenbasierte Authentisierung bereitgestellten (angebotenen) Schnittstellen.

Festlegungen, die nicht ausschließlich für den Basisdienst, sondern auch für andere Systeme gelten, werden in [gemSpec_TBAuth] getroffen. Dies umfasst insbesondere den Systemüberblick und Informationsmodelle.

Die Außenschnittstellen des Basisdienstes tokenbasierte Authentisierung sind in [gemKPT_Arch_TIP] beschrieben, welches die fachlichen Anforderungen an die Plattform auf Systemebene umsetzt. Für das Verständnis dieser Spezifikation wird die Kenntnis von [gemKPT_Arch_TIP] vorausgesetzt.

Angrenzende Systeme, z. B. Dienste, Clients, in der dezentralen Umgebung der TI betriebene IDPs (sog. lokale IDPs) und IDPs, die in der Provider-Zone der TI betrieben werden, werden nicht durch die gematik zugelassen und auch nicht in diesem Dokument beschrieben.

1.6 Methodik

1.6.1 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=**]**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

1.6.2 Dokumentenstruktur

Anders als andere Plattformfunktionen des Konnektors, werden die TBAuth-Funktionen des Konnektors nicht in [gemSpec_Kon] sondern im vorliegenden Dokument beschrieben. Diese Untergliederung in mehrere Dokumente erlaubt eine stärkere Strukturierung der Inhalte und einfachere Handhabung der Dokumente.

1.6.3 Detaillierungstiefe

Diese Spezifikation beschreibt detailliert die Außenschnittstellen sowie relevante interne Funktionalitäten. Auf eine Beschreibung zusätzlicher interner sowie implementierungsabhängiger Details wird verzichtet.

2 Systemüberblick

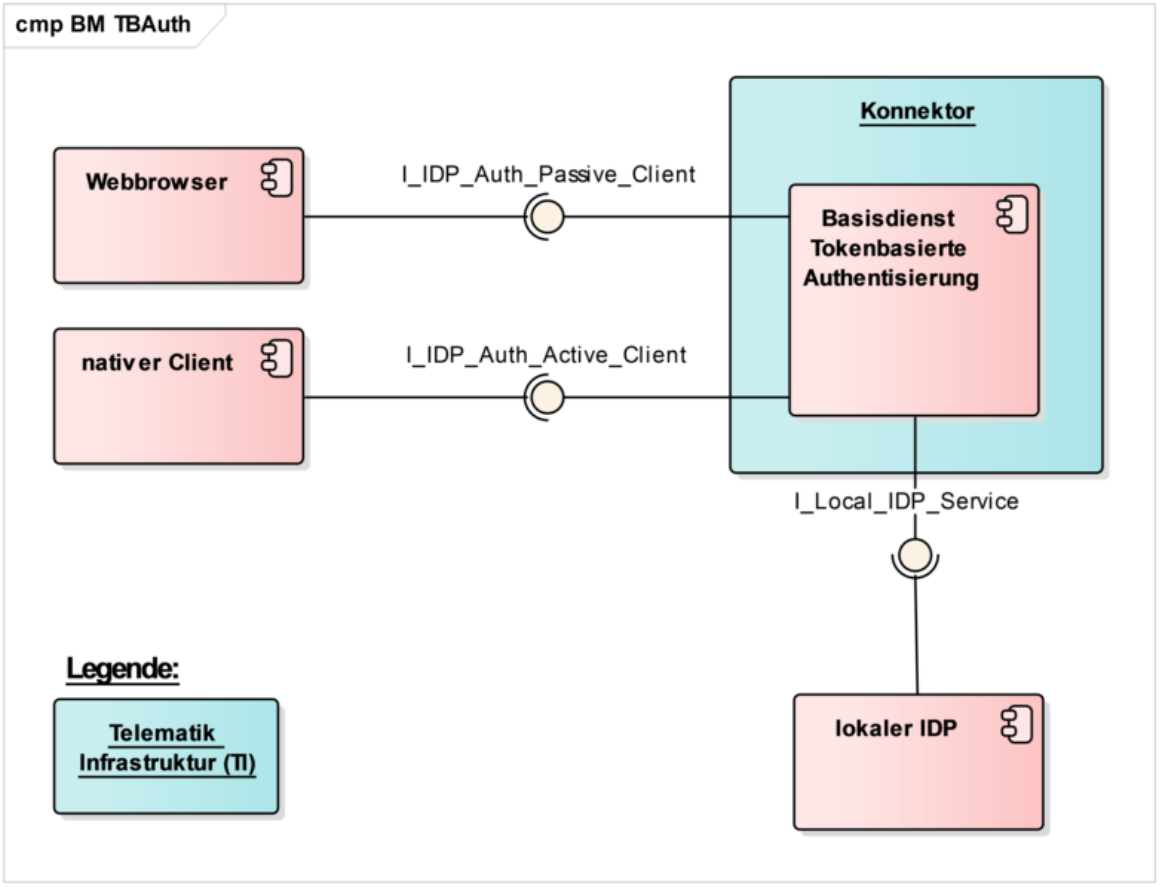

Abbildung 1: Systemzerlegung tokenbasierte Authentisierung

Akteure, Rollen und Nachbarsysteme sind in [gemSpec_TBAuth#2] erläutert.

3 Übergreifende Festlegungen

3.1 Verwendete Identität der SM-B

Um die Authentifizierung und Autorisierung durchzuführen, müssen prüfende Dienste in der Lage sein, eindeutig zu erkennen, von welcher Institution eine Identitätsbestätigung ausgestellt wurde.

TIP1-A_6791 - Verwendung von ID.HCI.OSIG
Der Basisdienst TBAuth MUSS zur Signatur von Identitätsbestätigungen an I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service das Schlüsselmaterial ID.HCI.OSIG der jeweiligen SM-B verwenden.
[<=]

Der Konnektor prüft die Gültigkeit der SM-B regelmäßig und stellt somit sicher, dass die verwendete SM-B gültig ist.

3.2 Allgemein

TIP1-A_6798 - Mandantenkontext verwenden
Der Basisdienst TBAuth MUSS ausschließlich SM-Bs und Kartenterminals verwenden, die dem jeweiligen Mandanten zugeordnet sind.
[<=]

Konfigurationsdaten werden über die Managementschnittstelle des Konnektors verwaltet.

TIP1-A_6799 - Konfigurationsdaten wirksam machen
Der Basisdienst TBAuth MUSS Konfigurationsdaten direkt nach Eingabe wirksam machen.
[<=]

3.3 Statusrückmeldung und Fehlerbehandlung

Für das Fehlermanagement gelten neben den hier aufgeführten spezifischen Anforderungen für den Basisdienst TBAuth die Anforderungen aus Kapitel 3 der übergreifenden Spezifikation [gemSpec_OM].

Da die Schnittstelle I_IDP_Auth_Passive_Client keine SOAP-Schnittstelle ist, gelten hierfür die Vorgaben aus [WS-Federation1.2] (siehe Kapitel 4.2).

TIP1-A_6883 - Rückgabedetails bei Fehlern
Der Basisdienst TBAuth DARF beim Auftreten von Fehlern NICHT Implementierungsdetails wie z. B. die Fehlerkette (Trace) an den Aufrufer zurückgeben.
[<=]

3.4 Protokollierung

Die Protokollierung des Basisdienstes stützt sich auf das in [gemSpec_KON#4.1.10] definierte Funktionsmerkmal „Protokollierungsdienst“ des Konnektors. Zur Administration und Einsichtnahme in das Protokoll stellt der Konnektor dem Administrator eine Managementschnittstelle (s. [gemSpec_Kon#4.1.10.6]) zur Verfügung.

Laut [gemSpec_Kon#TIP1-A_4710] werden keine medizinischen und (außer bei Sicherheitsvorfällen) keine personenbezogenen Daten protokolliert.

TIP1-A_6804 - Protokollierung von Aufrufen
Der Basisdienst TBAuth MUSS jeden Aufruf der vom Basisdienst angebotenen Operationen im Systemprotokoll des Konnektors protokollieren: Datum mit Uhrzeit, Schnittstelle und Operation, Vorgangsnummer, Ergebnis (Erfolg oder Fehlermeldung) und ggf. erfolgter PIN-Eingabe (Rückgabewert/Fehlercode).
[<=**]**

TIP1-A_6793 - Protokollierung mit Vorgangsnummer
Der Basisdienst TBAuth MUSS beim Aufruf einer Schnittstelle eine pseudozufällige Vorgangsnummer vergeben und diese bei allen Protokollierungsvorgängen protokollieren.
[<=**]**

TIP1-A_6805 - Protokollierung allgemeiner Fehler
Der Basisdienst TBAuth MUSS alle auftretenden nicht-sicherheitsrelevanten Fehler (eventType Op) inkl. Der Aufrufparameter im Systemprotokoll des Konnektors protokollieren.
[<=**]**

Dem Administrator soll ermöglicht werden, aufgetretene Fehler jeglicher Art näher zu analysieren und erforderliche Maßnahmen zur Behebung abzuleiten.

TIP1-A_6806 - Ergänzende Information zur Protokollierung von Fehlern
Der Basisdienst TBAuth MUSS bei der Protokollierung von Fehlern den Umfang der protokollierten Informationen entsprechend der „severity“ angemessen ausgestalten und z.B. bei Severity „Error“ und „Fatal“ die Fehlerkette (Trace) protokollieren.
[<=**]**

TIP1-A_6807 - Protokollierung sicherheitsrelevanter Fehler
Der Basisdienst TBAuth MUSS alle sicherheitsrelevanten Fehler (eventType Sec), inklusive aller Aufrufparameter, im Sicherheitsprotokoll des Konnektors protokollieren.
[<=**]**

3.5 Versionierung

Der Basisdienst TBAuth ist integraler Bestandteil des Konnektors und Teil von dessen Firmware-Version. Bezüglich der Selbstauskunft gelten die Festlegungen in [gemSpec_Kon#TIP1-A_4812].

3.6 Verwendete WS-Standards

Die Architektur des BD-TBAuth orientiert sich an der Elektronischen Fallakte (EFA) [EFA2.0] und basiert auf dazu kompatiblen Technologien und Standards. Trotzdem ist diese Schnittstelle nicht auf vollständige Kompatibilität zu EFA ausgelegt.

TIP1-A_6808 - Verwendung von WS-Trust 1.3
Der Basisdienst TBAuth MUSS für die Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service den Funktionsumfang eines Security Token Service (STS) gemäß WS-Trust 1.3 [WS-Trust1.3] implementieren.
[<=]

TIP1-A_6809 - optionale Verwendung von WS-Trust 1.4
Der Basisdienst TBAuth KANN für die Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service den Funktionsumfang eines Security Token Service (STS) gemäß WS-Trust 1.4 [WS-Trust1.4] implementieren.
[<=]

TIP1-A_6810 - Konformität zu WS-I Basic Profile 1.2
Der Basisdienst TBAuth MUSS an den Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service die für die Clientsystemschnittstelle definierten Web-Services konform zu [BasicProfile1.2] anbieten. Abweichend von R1012 in [BasicProfile1.2] MUSS der Basisdienst TBAuth nur das Character Encoding UTF-8 unterstützen. Andere Kodierungen MUSS der Basisdienst mit einem Fehler beantworten.
[<=]

TIP1-A_6811 - Verwendung von WS-Security Policy 1.3 und WS-I Basic Security Profile 1.1
Der Basisdienst TBAuth MUSS an den Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service den Standard [WS-SecurityPolicy1.3] verwenden und konform zu [BasicSecurityProfile1.1] arbeiten.
[<=]

TIP1-A_6792 - Konformität zu [gemSpec_Krypt]
Der Basisdienst TBAuth MUSS abweichend von [BasicProfile1.2], [WS-SecurityPolicy1.3] und [BasicSecurityProfile1.1] ausschließlich die laut [gemSpec_Krypt] zulässigen Algorithmen, Protokolle und sonstigen Vorgaben unterstützen.
[<=]

TIP1-A_6812 - Verwendung von WS-Federation 1.2
Der Basisdienst TBAuth MUSS die Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service entsprechend [WS-Federation1.2] implementieren.
[<=]

TIP1-A_6813 - Verwendung von Webservice-Fehlern
Der Basisdienst TBAuth MUSS an den Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service die in den verwendeten Webservice-Spezifikationen definierten Fehler und Fehlercodes verwenden.
[<=]

Die Fehlerbehandlung in [WS-Trust1.3#Kapitel11] und identisch [WS-Trust1.4#Kapitel11] legen den zu verwendenden SOAP-Fault-Mechanismus fest. Unter SOAP 1.1 wird ein Fehler über die Parameter faultcode und faultstring an den Aufrufer zurückgegeben. Es

sind die [WS-Trust1.3#Kapitel11] bzw. [WS-Trust1.4#Kapitel11] per faultcode und faultstring angegebenen Fehler zu verwenden.

In sämtlichen Fehlernachrichten wird ein SOAPAction-Header verwendet. Das zu verwendende SOAPAction-Element für die WS-Trust Fehler gibt Tabelle TAB_BD_TBAuth_13 an.

Tabelle 1 TAB_BD_TBAuth_13 WS-Trust Fehler

Error that occurred (faultstring)	Fault code (faultcode)	Fault Action URI (SOAPAction)
The request was invalid or malformed	wst:InvalidRequest	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/InvalidRequest
Authentication failed	wst:FailedAuthentication	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/FailedAuthentication
The specified request failed	wst:RequestFailed	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/RequestFailed
Security token has been revoked	wst:InvalidSecurityToken	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/InvalidSecurityToken
Insufficient Digest Elements	wst:AuthenticationBadElements	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/AuthenticationBadElements
The specified RequestSecurityToken is not understood	wst:BadRequest	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/BadRequest
The request data is out-of-date	wst:ExpiredData	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/ExpiredData
The requested time range is invalid or unsupported	wst:InvalidTimeRange	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/InvalidTimeRange
The request scope is invalid or unsupported	wst:InvalidScope	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/InvalidScope
A renewable security token has expired	wst:RenewNeeded	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/RenewNeeded
The requested renewal failed	wst:UnableToRenew	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Fault/UnableToRenew

Es ist im Sinne der Anforderung [TIP1-A_6883] das optionale Fault detail Element aus SOAP 1.1 in der Fehlernachricht nicht zu verwenden.

Zusätzlich zu den in [WS-Trust1.3#Kapitel11] bzw. [WS-Trust1.4#Kapitel11] definierten Fehlern werden ausschließlich die folgenden TI-spezifischen Fehler verwendet.

TIP1-A_6815 - TI-spezifische Fehler
Der Basisdienst TBAuth MUSS an den Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service die Fehler aus TAB_BD_TBAuth_02 TI-spezifische Fehler entsprechend [WS-Federation1.2] und [gemSpec_Kon] verwenden.

Tabelle 2: TAB_BD_TBAuth_02 TI-spezifische Fehler

Fehlercode	ErrorType	Severity	Fehlertext (faultstring)

6	Technical	Fatal	Protokollfehler
101	Security	Fatal	Kartenfehler
4004	Technical	Error	Ungültige Mandanten-ID
4005	Technical	Error	Ungültige Clientsystem-ID
4006	Technical	Error	Ungültige Arbeitsplatz-ID
4008	Technical	Error	Karte nicht als gesteckt identifiziert
4010	Security	Error	Clientsystem ist dem Mandanten nicht zugeordnet
4011	Security	Error	Arbeitsplatz ist dem Mandanten nicht zugeordnet
4013	Security	Error	SM-B_Verwaltet ist dem Mandanten nicht zugeordnet
4014	Security	Error	Für den Mandanten ist der Arbeitsplatz nicht dem Clientsystem zugeordnet
4045	Technical	Error	Fehler beim Zugriff auf die Karte
4058	Security	Error	Aufruf nicht zulässig

faultcode und soapaction werden wie folgt aus dem Fehlercode abgeleitet:

- faultcode="gem:"+Fehlercode (z.B. gem:6)
- soapaction=http://ws.gematik.de/conn/tbauth/fault/+Fehlercode (z.B. http://ws.gematik.de/conn/tbauth/fault/6)

[<=]

TI-spezifische Fehler sind immer einer Fehlerklasse zugeordnet, so dass festgelegt ist, welche dieser Fehler sicherheitsrelevant sind (ErrorType=Security).

TIP1-A_6814 - Sicherheitsrelevante Webservice-Fehler
Der Basisdienst TBAuth MUSS an den Schnittstellen I_IDP_Auth_Active_Client, I_IDP_Auth_Passive_Client und I_Local_IDP_Service die folgenden Fehler als sicherheitsrelevante Fehler (eventType Sec) behandeln:

- wst:FailedAuthentication (z. B. falsche PIN-Eingabe)

- wst:InvalidSecurityToken (z. B. bei RenewTarget)
- wst:InvalidTimeRange (z. B. aufgrund bei /wst:Lifetime/wsu:Expires)

[<=**]**

4 Funktionsmerkmale

Folgend sind die Funktionsmerkmale des Basisdienstes TBAuth, seine Schnittstellen und Operationen definiert. Für jede Operation werden das an der Schnittstelle sichtbare und damit testbare Verhalten und die Berechtigungen normativ spezifiziert.

4.1 Schnittstelle I_IDP_Auth_Active_Client

Die Schnittstelle I_IDP_Auth_Active_Client stellt authentifizierten Aufrufern, mit nativen Clients in der dezentralen Umgebung der TI, Nutzeridentitätsbestätigungen gemäß [SAML2.0] aus und signiert diese mit der für tokenbasierte Authentisierung verwendeten Schlüssel auf der SM-B.

4.1.1 WSDL und Security Policy

TIP1-A_6816 - WSDL für I_IDP_Auth_Active_Client
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Active_Client gemäß IdpServiceActiveRequestor.wsdl (siehe Anhang B) umsetzen.
[<=]

TIP1-A_6817 - Gültige Anfragen an I_IDP_Auth_Active_Client
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client ausschließlich Anfragen (Requests) akzeptieren, die der geltenden Schnittstellendefinition (WSDL) entsprechen. Aufrufe mit ungültigen Anfragen MÜSSEN mit einem SOAP-Fault abgebrochen werden.
[<=]

4.1.2 SOAP-Envelope

TIP1-A_6818 - I_IDP_Auth_Active_Client: SOAP-Envelope der Aufrufe
Der Basisdienst TBAuth MUSS Aufrufe der Schnittstelle I_IDP_Auth_Active_Client ablehnen, wenn sie nicht dem folgenden SOAP-Envelope entsprechen, wobei „…“ Platzhalter sind. Falls kein Body verwendet wird MUSS der Basisdienst TBAuth anstelle von <soap:Body>…</soap:Body> auch <soap:Body/> akzeptieren.

```
<soap:Envelope xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/”>
    <soap:Header>
        <Action xmlns=”http://www.w3.org/2005/08/addressing”>…</Action>
        <MessageID xmlns=“http://www.w3.org/2005/08/addressing“>…</MessageID>
        <To xmlns=”http://www.w3.org/2005/08/addressing”>…</To>
        <ReplyTo xmlns=”http://www.w3.org/2005/08/addressing”>
            <Address>…</Address>
        </ReplyTo>
        …
    </soap:Header>
    <soap:Body>
        …
    </soap:Body>
</soap:Envelope>
```

[<=]

TIP1-A_6819 - I_IDP_Auth_Active_Client: SOAP-Envelope der Antworten
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Active_Client so umsetzen, dass alle Antworten dem folgenden SOAP-Envelope entsprechen, wobei „…“ Platzhalter sind.

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/addressing">…</Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">…</MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">…</To>
        <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">…</RelatesTo>
        …
    </soap:Header>
    <soap:Body>
        …
    </soap:Body>
</soap:Envelope>
```

[<=]

TIP1-A_6876 - I_IDP_Auth_Active_Client: Alternative Schreibweise bei leerem Element <soap:Body>
Falls kein Body verwendet wird, KANN der Basisdienst TBAuth in der Antwort der Schnittstelle I_IDP_Auth_Active_Client anstelle von <soap:Body>…</soap:Body> auch <soap:Body/> verwenden.
[<=]

4.1.3 Security Header

Da die Authentifizierung der Nutzer über die Mandanten-, Arbeitsplatz und Client-System-IDs umgesetzt wird, ist eine Signatur des Security Headers nicht erforderlich.

TIP1-A_6820 - I_IDP_Auth_Active_Client: Security Header entsprechend WS-Policy
Der Basisdienst TBAuth MUSS sicherstellen, dass an der Schnittstelle I_IDP_Auth_Active_Client der Security Header des Aufrufs den Vorgaben der WS-Policy des jeweilig adressierten Service Endpunkts entspricht.
[<=]

TIP1-A_6821 - Security-Header von I_IDP_Auth_Active_Client
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Active_Client so umsetzen, dass alle akzeptierten Aufrufe und alle Antworten den Security-Header entsprechend TAB_BD_TBAuth_03 Security-Header von I_IDP_Auth_Active_Client verwenden, wobei die Präfixe und Namensräume entsprechend TAB_BD_TBAuth_13 Präfixe und Namensräume gelten.

Tabelle 3: TAB_BD_TBAuth_03 Security-Header von I_IDP_Auth_Active_Client

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wsse:Security /wsu:Timestamp	erforderlich	Zur Sicherstellung einer zeitlichen Konsistenz übergibt der Aufrufer seine aktuelle Zeit. Die in diesem Parameter übergebene Zeit DARF NICHT mehr als eine Minute von der Zeit des Konnektors abweichen.
/wsse:Security /wsu:Timestamp	erforderlich	

/wsu:Created		
/wsse:Security /wsu:Timestamp /wsu:Expires	optional	Falls der Parameter nicht vorhanden ist MUSS eine Verfallsdauer von 3 Minuten angenommen werden. Die Verarbeitung der Nachricht MUSS mit einem Fehler abgebrochen werden, falls der Verfallszeitpunkt überschritten ist.

[<=]

Beispiel

Mit Auslassungspunkten „…“ ausgewiesene Textstellen sind gekürzt.

```
<wsse:Security xmlns:wsse=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd”
xmlns:wsu=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd” soap:mustUnderstand=”1”>
    <wsu:Timestamp wsu:Id=“TS-e3fe5d9a-7940-4e95-9e5b-e550d3bbee01“>
        <wsu:Created>…</wsu:Created>
        <wsu:Expires>…</wsu:Expires>
    </wsu:Timestamp>
</wsse:Security>
```

4.1.4 Operation get_Metadata

Über diese Operation get_Metadata werden die Schnittstelle und Operationen publik gemacht, die durch aktive Clients verwendet werden können.

TIP1-A_6822 - Namensdienst SRV-Records für I_IDP_Auth_Active_Client::get_Metadata
Der Konnektor MUSS entsprechend [WS-Federation1.2] den Endpunkt über den die Operation I_IDP_Auth_Active_Client::get_Metadata aufrufbar ist im Namensdienst mittels SRV-Records veröffentlichen.
[<=]

TIP1-A_6823 - WS-Adressing für I_IDP_Auth_Active_Client::get_Metadata
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation get_Metadata gemäß dem Standard WS-Addressing [WS-Addressing1.0] anbieten.

[<=]

TIP1-A_6824 - WS-Metadata Exchange für I_IDP_Auth_Active_Client::get_Metadata
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client Anfragen an die Operation get_Metadata mit Metadaten entsprechend [WS-MetadataExchange1.1] beantworten und dabei WSDL, WS-Policy und Referenzen auf verwendete XML Schemata zurückgeben.
[<=]

TIP1-A_6825 - Aufruf von I_IDP_Auth_Active_Client::get_Metadata
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation get_Metadata entsprechend „Get“ nach [WS-Transfer2006] an der Adresse

/sts/transport/mex anbieten.
[<=]

Beispiel:

Mit Auslassungspunkten „…“ ausgewiesene Textstellen sind gekürzt.

```
<soap:Envelope xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/”>
    <soap:Header>
        <Action
xmlns=”http://www.w3.org/2005/08/addressing”>http://schemas.xmlsoap.org/ws/2004/
09/transfer/Get</Action>
        <MessageID xmlns=“http://www.w3.org/2005/08/addressing“>…</MessageID>
        <To
xmlns=”http://www.w3.org/2005/08/addressing”>https://konnektor.konlan/sts/transp
ort/mex</To>
        <ReplyTo xmlns=”http://www.w3.org/2005/08/addressing”>
            <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
        </ReplyTo>
    </soap:Header>
    <soap:Body/>
</soap:Envelope>
```

TIP1-A_6826 - Antworten von I_IDP_Auth_Active_Client::get_Metadata
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation get_Metadata mit folgender Antwort entsprechend “GetResponse” nach [WS-Transfer2006] anbieten und dabei die geltende WSDL zurückliefern.
[<=]

Beispiel:

Mit Auslassungspunkten „…“ ausgewiesene Textstellen sind gekürzt.

```
<soap:Envelope xmlns:soap=”http://schemas.xmlsoap.org/soap/envelope/”>
    <soap:Header>
        <Action
xmlns=”http://www.w3.org/2005/08/addressing”>http://schemas.xmlsoap.org/ws/2004/
09/transfer/GetResponse</Action>
        <MessageID xmlns=“http://www.w3.org/2005/08/addressing“>…</MessageID>
        <To
xmlns=”http://www.w3.org/2005/08/addressing”>http://www.w3.org/2005/08/addressin
g/anonymous</To>
        <RelatesTo xmlns=”http://www.w3.org/2005/08/addressing”>…</RelatesTo>
    </soap:Header>
    <soap:Body>
        <Metadata xmlns=”http://schemas.xmlsoap.org/ws/2004/09/mex”>
            <MetadataSection Dialect=”http://schemas.xmlsoap.org/wsdl/”
Identifier=”http://docs.oasis-open.org/ws-sx/ws-trust/200512/”>
                …
        </Metadata>
    </soap:Body>
</soap:Envelope>
```

4.1.5 Operation issue_Identity_Assertion

TIP1-A_6827 - issue_Identity_Assertion mit WS-Trust und WS-Federation
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation issue_Identity_Assertion entsprechend der Operation „Issue“ und „RequestSecurityToken“ nach WS-Trust und [WS-Federation1.2] für Active Requestor Profile implementieren.

[<=]

TIP1-A_6828 - Behauptungen der Identitätsbestätigung – I_IDP_Auth_Active_Client
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Active_Client::issue_Identity_Assertion, Identitätsbestätigungen entsprechend den in [gemSpec_TBAuth] *TAB_TBAuth_02 Behauptungen des Basisdienstes TBAuth* aufgeführten Behauptungen ausstellen und diese aus den jeweiligen Attributen des verwendeten Zertifikats befüllen. Als optional gekennzeichnete Behauptungen MÜSSEN verwendet werden, sofern das Attribut des jeweiligen Zertifikats vorhanden ist.
[<=]

TIP1-A_6829 - Issuer „IDP TI-Plattform“ – I_IDP_Auth_Active_Client
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Active_Client::issue_Identity_Assertion in Identitätsbestätigungen den Issuer „IDP TI-Plattform“ eintragen.

[<=]

4.1.5.1 Aufrufparameter issue_Identity_Assertion

TIP1-A_6830 - Aufrufparameter von issue_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation issue_Identity_Assertion mit den Aufrufparametern aus TAB_BD_TBAuth_04 Aufrufparameter von issue_Identity_Assertion anbieten, wobei die Präfixe und Namensräume entsprechend TAB_BD_TBAuth_13 Präfixe und Namensräume gelten.

Tabelle 4: TAB_BD_TBAuth_04 Aufrufparameter von issue_Identity_Assertion

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wst:RequestSecurityToken	erforderlich	
/wst:RequestSecurityToken /wsp:AppliesTo	erforderlich	Referenz auf den zu verwendenden Dienst, um den Geltungsbereich der Identitätsbestätigung zu beschränken. Dieser Parameter MUSS ein Element <saml2:Audience> aus der AudienceRestriction [gemSpec_TBAuth] enthalten .
/wst:RequestSecurityToken /wst:Lifetime	erforderlich	
/wst:RequestSecurityToken /wst:Lifetime /wsu:Created	erforderlich	Der BD-TBAuth MUSS Anfragen abbrechen falls der Erstellungszeitpunkt mehr als eine Minute von der eigenen Systemzeit abweicht.

/wst:RequestSecurityToken /wst:Lifetime /wsu:Expires	optional	Der BD-TBAuth MUSS Identitätsbestätigungen mit der in diesem Aufrufparameter angegebenen Lebensdauer ausstellen. Falls der Parameter nicht vorhanden ist MUSS der BD-TBAuth die Identitätsbestätigung mit einer Gültigkeitsdauer von drei Stunden ausstellen. Der BD-TBAuth DARF NICHT Identitätsbestätigungen ausstellen die länger als 24 Stunden gültig sind.
/wst:RequestSecurityToken /wst:SecondaryParameters	optional	Der BD-TBAuth MUSS innerhalb von SecondaryParameters ausschließlich die hier spezifizierten Aufrufparameter akzeptieren und MUSS diese so, wie jeweils hier spezifiziert, behandeln. Aus Kompatibilitätsgründen SOLLEN ausschließlich als optional spezifizierte Aufrufparameter innerhalb von SecondaryParameters verwendet werden.
/wst:RequestSecurityToken /wst:TokenType	optional	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0 Falls der Parameter nicht übergeben wird, so MUSS dieser Wert als Standardwert verwendet werden.
/wst:RequestSecurityToken /wst:KeyType	optional	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey Falls der Parameter nicht übergeben wird, so MUSS dieser Wert als Standardwert verwendet werden.
/wst:RequestSecurityToken /wst:RequestType	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
/wst:RequestSecurityToken /wst:UseKey	erforderlich	Die Gültigkeit des übergebenen Zertifikats oder Schlüssels DARF NICHT überprüft werden, da es sich um einen selbst-signierten Holder-of-Key-Schlüssel (HoK-Schlüssel) handelt. Dieser MUSS einen Algorithmus verwenden, der laut gemSpec_Krypt zulässig ist.
/wst:RequestSecurityToken /wst:UseKey /ds:KeyInfo	erforderlich	
/wst:RequestSecurityToken /wst:UseKey /ds:KeyInfo /ds:KeyValue	erforderlich	
/wst:RequestSecurityToken /wst:Renewing	optional	Falls der Parameter nicht vorhanden ist, MUSS der BD-TBAuth eine erneuerbare

		Identitätsbestätigung ausstellen.
/wst:RequestSecurityToken /wst:Renewing /@Allow	optional	
/wst:RequestSecurityToken /gem:mandantId	erforderlich	Der zu verwendende Mandant.
/wst:RequestSecurityToken /gem:clientSystemId	erforderlich	Das zu verwendende Client System.
/wst:RequestSecurityToken /gem:workplaceId	erforderlich	Der zu verwendende Arbeitsplatz des Benutzers.
/wst:RequestSecurityToken /gem:iccsn	optional	Die Seriennummer der zu verwendenden Karte, mit der die Identitätsbestätigung signiert werden soll.

[<=]

Beispiel:

```
<wst:RequestSecurityToken xmlns:wst=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”>
    <wsp:AppliesTo><saml2:Audience>urn:telematik:gesundheitsdatendienst:www:Instanz23</saml2:Audience> </wsp:AppliesTo>
    <wst:Lifetime>
        <wsu:Created>2016-08-29T07:20:33.341Z</wsu:Created>
        <wsu:Expires>2016-08-29T07:50:33.341Z</wsu:Expires>
    </wst:Lifetime>
        <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
        <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/PublicKey</wst:KeyType>
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
    <wst:UseKey>
        <ds:KeyInfo xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
            <ds:KeyValue>
                <ds:RSAKeyValue>
                    <ds:Modulus>oh83Kp6+Pj5yoYml1uayO2UupCq69pZxWbhCco6Q7X4YaRQ+Zc3DGqKUU8U89
1/qt2hVe9yAjTe9btPKdC8gyidZi+/0Y+h19KGRA8GgrCbSQa8gMk/9FJqJF42CqSZAAOAb2Z/sAZOe4bCiO1D1i2KAC+
/cHUEy+RyX61ud7833GadG0JxjcVTHg+kIDTASC16r5KATsErPHmgjmFEamnCBRN9WTDymQxSGotQYFbdSgGTKtrPeoEl
I6McXOZN0VoqDQ+7G2OhGLxqyyA3gpT+js0j6j3jILdxTWGMBCeeKgq3kfoP2OqOwD0EIFQVnD2SamJham5O45n4tbr
GPxw==</ds:Modulus>
                    <ds:Exponent>AQAB</ds:Exponent>
                </ds:RSAKeyValue>
            </ds:KeyValue>
        </ds:KeyInfo>
```

```
    </wst:UseKey>
    <wst:Renewing/>
    <gem:workplaceId>a1</gem:workplaceId>
    <gem:mandantId>m1</gem:mandantId>
    <gem:clientSystemId>cs1</gem:clientSystemtId>
    <gem:iccsn>12345678912345678</gem:iccsn>
</wst:RequestSecurityToken>
```

4.1.5.2 Rückgabewerte issue_Identity_Assertion

TIP1-A_6831 - Rückgabewerte von issue_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation issue_Identity_Assertion mit dem Rückgabewert “Request Security Token Response” (RSTR) nach WS-Trust und mit den Rückgabewerten aus [gemSpec_TBAuth] *TAB_TBAuth_05 RequestSecurityTokenResponseCollection* anbieten.
[<=]

4.1.6 Operation renew_Identity_Assertion

Diese Operation ermöglicht das Erneuern einer vorhandenen Identitätsbestätigung basierend auf WS-Trust, SAML 2.0 Assertions, und WS Federation für Active Requestor Profile. Die erneuerte Identitätsbestätigung wird grundsätzlich nicht verändert, sondern unterscheidet sich zur ursprünglichen Identitätsbestätigung im Wesentlichen durch eine aktualisierte Gültigkeitsdauer und eine aktualisierte Signatur.

TIP1-A_6832 - renew_Identity_Assertion mit WS-Trust und WS-Federation
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation renew_Identity_Assertion entsprechend der Operation „Renew“ und „RequestSecurityToken“ nach WS-Trust und [WS-Federation1.2] für Active Requestor Profile implementieren.

[<=]

TIP1-A_6833 - renew_Identity_Assertion: Prüfung der Erneuerung
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client bei der Operation renew_Identity_Assertion sicherstellen, dass es die zu erneuernde Identitätsbestätigung zuvor selber über die Schnittstellen I_IDP_Auth_Active_Client oder I_IDP_Auth_Passive_Client ausgestellt hat und diese noch nicht abgelaufen ist oder annulliert wurde.
[<=]

TIP1-A_6884 - renew_Identity_Assertion: Herausgabe mit gleichem Schlüssel
Der Basisdienst TBAuth MUSS sicherstellen, dass es erneuerte Identitätsbestätigungen mit dem gleichen Schlüssel wie die ursprüngliche Identitätsbestätigung signiert.
[<=]

Aufrufe der Operation renew_Identity_Assertion kann der BD-TBAuth anhand der Signatur des Aufrufs und anhand der Parameter /wst:RequestSecurityToken /gem:workplaceId und /wst:RequestSecurityToken /gem:mandantId dem Benutzer zuordnen.

TIP1-A_6834 - renew_Identity_Assertion Erneuerung nur für Benutzer
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client bei der Operation renew_Identity_Assertion sicherstellen, dass Anfragen vom Benutzer der zu

erneuernden Identitätsbestätigung stammen.
[<=]

TIP1-A_6835 - Beschränkung der Erneuerbarkeit
Der Basisdienst TBAuth DARF NICHT an der Schnittstelle I_IDP_Auth_Active_Client bei der Operation renew_Identity_Assertion, Identitätsbestätigungen über die konfigurierte maximale Dauer (über die Identitätsbestätigungen hinweg erneuert werden dürfen) hinaus erneuern. Diese Dauer beginnt zum Erstellungszeitpunkt der ersten Identitätsbestätigung und bezieht sich auf das Gültigkeitsende der Identitätsbestätigung bzw. seiner erneuerten Nachfolger.
[<=]

TIP1-A_6836 - Konfiguration maximale Erneuerbarkeit
Der Basisdienst TBAuth MUSS es dem Administrator über die Managementschnittstelle des Konnektors ermöglichen, die maximale Dauer über die Identitätsbestätigungen hinweg erneuert werden dürfen, zu verwalten. Diese Dauer MUSS standardmäßig auf 24 Stunden gesetzt sein.
[<=]

4.1.6.1 Aufrufparameter renew_Identity_Assertion

TIP1-A_6837 - Aufrufparameter renew_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation renew_Identity_Assertion mit den Aufrufparametern aus TAB_BD_TBAuth_05 Aufrufparameter der Operation renew_Identity_Assertion anbieten, wobei die Präfixe und Namensräume entsprechend TAB_BD_TBAuth_13 Präfixe und Namensräume gelten.

Tabelle 5: TAB_BD_TBAuth_05 Aufrufparameter der Operation renew_Identity_Assertion

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wst:RequestSecurityToken	erforderlich	
/wst:RequestSecurityToken /wst:Lifetime	optional	
/wst:RequestSecurityToken /wst:Lifetime /wsu:Created	optional	Der BD-TBAuth MUSS Anfragen abbrechen, falls der Erstellungszeitpunkt mehr als eine Minute von der eigenen Systemzeit abweicht.
/wst:RequestSecurityToken /wst:Lifetime /wsu:Expires	optional	Der BD-TBAuth MUSS Identitätsbestätigungen mit der in diesem Aufrufparameter angegebenen Lebensdauer ausstellen. Falls der Parameter nicht vorhanden ist, MUSS der BD-TBAuth die Identitätsbestätigung mit einer Gültigkeitsdauer von drei Stunden ausstellen.
/wst:RequestSecurityToken /wst:TokenType	optional	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
/wst:RequestSecurityToken /wst:RequestType	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/ws-sx/ws-

		trust/200512/Renew
/wst:RequestSecurityToken /wst:RenewTarget	erforderlich	Der Wert des Aufrufparameters MUSS die zu erneuernde Identitätsbestätigung aus [gemSpec_TBAuth] *TAB_TBAuth_03 Identitätsbestätigung (SAML 2.0 Assertion)* enthalten.
/wst:RequestSecurityToken /wst:Renewing	optional	
/wst:RequestSecurityToken /wst:Renewing /@Allow	optional	
/wst:RequestSecurityToken /gem:mandantId	erforderlich	Der zu verwendende Mandant.
/wst:RequestSecurityToken /gem:clientSystemId	erforderlich	Das zu verwendende Client System.
/wst:RequestSecurityToken /gem:workplaceId	erforderlich	Der zu verwendende Arbeitsplatz des Benutzers.

[<=]

Beispiel:

```
<wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Renew</wst:RequestType>
    <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
    <wst:Lifetime xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <wsu:Created>2016-10-12T17:27:02.768Z</wsu:Created>
        <wsu:Expires>2016-10-12T17:32:02.768Z</wsu:Expires>
    </wst:Lifetime>
    <wst:RenewTarget>
        <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_aa3a0632-aff2-4b3b-9d4e-2a3ede2b6410" IssueInstant="2016-10-12T17:26:22.933Z" Version="2.0" xsi:type="saml2:AssertionType">
            <saml2:Issuer>1-1a25sd-d529</saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <ds:Reference URI="#_aa3a0632-aff2-4b3b-9d4e-2a3ede2b6410">
                        <ds:Transforms>
```

```
                              <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                              <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                    <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                              </ds:Transform>
                           </ds:Transforms>
                           <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                           <ds:DigestValue>Yqu92UhpYiLIvb5EqxLPqnzS6FGU07ejILo4ED6q
rts=</ds:DigestValue>
                        </ds:Reference>
                     </ds:SignedInfo>
                     <ds:SignatureValue>KFD7r91D6JXUQbW2IjjhfX0ziAmxjoUa/v6cnCyF0Io19
IedbFUdd8sJDcOT0fEFbD
TmaRvsly+NH/22StRI1zx0WmtFQPLl4YhRyQ9PQtm1zC87F/jJksl2DW4iabHwEdsld8SxyV49MTHt7X
sZ0GuKSsA5G7xSbazUzqp
GkOBLW6fhKNIc/i+vXP5edEtPrs3t1scxG/7HpfbISUV5dFojHKft1Vs20eN812gMpFpw1hiBuNBSh5r
4VG1l+yEmott0V7L+LvgS
u+GGA9eIDvHWmU0xAlNgea57XZYGqSghGppGJUzRT/P1pY5kIjVE13ePb9WQrgkKwXG8mNiXXg==</ds
:SignatureValue>
                     <ds:KeyInfo>
                        <ds:X509Data>
                           <ds:X509Certificate>MIIFEzCCA/ugAwIBAgIHA8zEnhRtVTANBgkq
hkiG9w0BAQsFADCBmTELMA
kGA1UEBhMCREUxHzAd
BgNVBAoMFmdlbWF0aWsgR21iSCBOT1QtVkFMSUQxSDBGBgNVBAsMP0luc3RpdHV0aW9uIGRlcyBH
ZXN1bmRoZWl0c3dlc2Vucy1DQSBkZXIgVGVsZW1hdGlraW5mcmFzdHJ1a3R1cjEfMB0GA1UEAwwW
R0VNLlNNQ0ItQ0E3IFRFU1QtT05MWTAeFw0xNTA2MzAwMDAwMDBaFw0yMDA2MzAwMDAwMDBaMIHH
MQswCQYDVQQGEwJERTEYMBYGA1UECAwPQmVpc3BpZWxzdO+/vWR0MRgwFgYDVQQHDA9CZWlz
MQswCQYDVQQGEwJERTEYMBYGA1UECAwPQmVpc3BpZWxzdO+cGll
bHN077+9ZHQxDjAMBgNVBBEMBTAxMjM0MRswGQYDVQQJDBJHZXN1bmRoZWl0c2dhc3NlIDMx
bHN077+DzAN
BgNVBAUTBjEwMDAwMTFGMEQGA1UEAww9S3Jhbmtlbmhhd XMgQmVpc3BpZWxzdO+/vWR0Luts
BgNVBAUTBjEwMDAwMTFGMEQGA1UEAww9S3Jhbmtlbmhhd XMgQmVpc3BpZWxzdO+aW5p
ayBm77+9ciBLYXJkaW9sb2dpZVRFU1QtT05MWTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
ayBm77+AqoC
ggEBAL/uetzxukiQQ4yd9gVyK5ZtgCrxzAH5ZlPoJcKOKo+oKZ5i/NpgjkXCBQl25gXuQJACkEjN
pa3E2JqOXLgwsLTZXVShc8v1b49DcbNPSDswWTnE7NwF7RemmnP9aKunqehFNUicRABfGa0j4Las
8eV3bqRg9y/+Cx6Y9GFr5OdfxLYs73HE7T1k7s9L7ufJtSfpm0FqZY5dkZk3a9jxbSJ3ovDBaL30
h3uKxTvBMU+przKZC/xf84Kjjxm1+PGD7I5/NTcCCX5w8uxKW/tNqQTFkhsArP4XdSIKiiyG
h3uKxTvBMU+XrAM
Yboa/oOlH/pF3LepfgHPXLfid5uOdT5+hpsoU/UkvBUCAwEAAaOCAS4wggEqMB0GA1UdDgQWBBQp
9vXBG9pPNsqBE1LNDe26RYztJzATBgNVHSUEDDAKBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMDoG
BSskCAMDBDEwLzAtMCswKTAnMA0MC0tyYW5rZW5oYXVzMAkGByqCFABMBDUTCzUtMklLLTMxNDE1
MB8GA1UdIwQYMBaAFDw5CixOUpeco4wu+AhSBLSZD2rnMCwGA1UdIAQlMCMwCgYIKoIUAEwE
MB8GA1UdIwQYMBaAFDw5CixOUpeco4wu+gSMw
CQYHKoIUAEwETAKBggqghQATASBKjAOBgNVHQ8Baf8EBAMCBaAwSwYIKwYBBQUHAQEEPzA9MDsG
CCsGAQUFBzABhi9odHRwOi8vb2NzcC5wa2kudGVsZW1hdGlrLXRlc3Q6ODA4MC9DTU9DU1AvT0NT
UDANBgkqhkiG9w0BAQsFAAOCAQEAC9tRPAgRoamvei0eX5IiHmj/mt4zX9kvhNRe3HMBUYMnvV10
J4h7EaT8/PeXBCtbari4xfqD+WDQhEayWYfsKL5GTFuzQXExgt0r5aZdH6V8kChXJ7JldKNiS7QH
rt1ZohY7qPLpDdYqQS99Uy79h7Y+MsZh1sI/1wCSQ/Tl5uVgjTM8q+0xI49VHVzebsGHLRdW
rt1ZohY7qPLpDdYqQS99Uy79h7Y+VAZa
W7DibaeP30G7r36nBfc5LBJm9MghL88Wgi/JPd4l09gQWfxRV0yiUlp9LQ+yUlAM13BesZ3Niu3q
vrHiTD0Y0QrOR2/AM4ETNPa0Kc/ClzkyBZhng/B3cwdTNcVuFWINmEDLGNmycyN0Pw==</ds:X509Cer
tificate>
                        </ds:X509Data>
```

```
                </ds:KeyInfo>
            </ds:Signature>
            <saml2:Subject>
                <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName"
NameQualifier="http://cxf.apache.org/sts">2.5.4.5=#130c313233343536373839303133,
2.5.4.42=#0c0848
65696e72696368,2.5.4.4=#0c03466974,CN=Dr. med. Heinrich Fit\, Facharzt für
Physikalische Therapie,C=DE</saml2:NameID>
                <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                    <saml2:SubjectConfirmationData
xsi:type="saml2:KeyInfoConfirmationDataType">
                        <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:KeyValue>
                                <ds:RSAKeyValue>
                                    <ds:Modulus>oh83Kp6+Pj5yoYml1uayO2UupCq69pZx
WbhCco6Q7X4YaRQ+Zc
3DGqKUU8U891/qt2hVe9yAjTe9btPKdC8gyidZi+/0Y+h19KGRA8GgrCbSQa8gMk/9FJqJF42CqSZAAO
Ab2Z/sAZOe4bCiO1D1
i2KAC+/cHUEy+RyX61ud7833GadG0JxjcVTHg+kIDTASC16r5KATsErPHmgjmFEamnCBRN9WTDymQxSG
otQYFbdSgGTKtrPeoEl
I6McXOZN0VoqDQ+7G2OhGLxqyyA3gpT+js0j6j3jILdxTWGMBCeeKgq3kfoP2OqOwD0EIFQVnD2SamJh
am5O45n4tbrGPx
w==</ds:Modulus>
                                    <ds:Exponent>AQAB</ds:Exponent>
                                </ds:RSAKeyValue>
                            </ds:KeyValue>
                        </ds:KeyInfo>
                    </saml2:SubjectConfirmationData>
                </saml2:SubjectConfirmation>
            </saml2:Subject>
            <saml2:Conditions NotBefore="2016-10-12T17:26:22.933Z"
NotOnOrAfter="2016-10-12T17:56:22.933Z"/>
            <saml2:AuthnStatement AuthnInstant="2016-10-12T17:26:22.933Z">
                <saml2:AuthnContext>
                    <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:c
lasses:SmartcardPKI
</saml2:AuthnContextClassRef>
                </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
                    <saml2:AttributeValue>Heinz Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
```

```
                    <saml2:AttributeValue>Heinz</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
                    <saml2:AttributeValue>Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">
                    <saml2:AttributeValue>Deutschland</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
                    <saml2:AttributeValue>test@example.com</saml2:AttributeValue
>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">
                    <saml2:AttributeValue>1-1a25sd-d529</saml2:AttributeValue>
                </saml2:Attribute>
            </saml2:AttributeStatement>
        </saml2:Assertion>
    </wst:RenewTarget>
    <wst:Renewing Allow=”true”/>
</wst:RequestSecurityToken>
```

4.1.6.2 Rückgabewerte renew_Identity_Assertion

TIP1-A_6838 - Rückgabewerte von renew_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation renew_Identity_Assertion mit dem Rückgabewert “Request Security Token Response” (RSTR) nach WS-Trust und mit den Rückgabewerten aus [gemSpec_TBAuth] *TAB_TBAuth_04 RequestSecurityTokenResponse* anbieten.
[<=]

Beispiel:

```
<ns2:RequestSecurityTokenResponse xmlns=”http://docs.oasis-open.org/ws-sx/ws-
trust/200802” xmlns:ns2=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”
xmlns:ns3=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd” xmlns:ns4=”http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-wssecurity-secext-1.0.xsd” xmlns:ns5=”http://www.w3.org/2005/08/addressing”>
    <ns2:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0</ns2:TokenType>
    <ns2:RequestedSecurityToken>
        <saml2:Assertion xmlns:saml2=”urn:oasis:names:tc:SAML:2.0:assertion”
xmlns:xsd=”http://www.w3.org/2001/XMLSchema”
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” ID=”_a714bd3a-4c94-40fb-
87fb-3db5964c1623” IssueInstant=”2016-10-12T17:26:23.397Z” Version=”2.0”
xsi:type=”saml2:AssertionType”>
            <saml2:Issuer>1-1a25sd-d529</saml2:Issuer>
            <ds:Signature xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
```

```
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <ds:Reference URI="#_a714bd3a-4c94-40fb-87fb-3db5964c1623">
                        <ds:Transforms>
                            <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            <ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>xLswm3sg5aSXxwiL+CMQkgrGnkoO9x1PMz+eSnSj
lB8=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>NFNQkpgfBRxToA1QCb02K/4AwRTH9Kgdy0vb1d1qVBSyp
oRuWTenVmQ/+O9e+tsCMb
8cH4U6A6Qv7fwWkB21xrrQ4x/4uAFH3DP5/wMuqp3CyD6+rdiDcnz85Hw1a2G4R6vcfm/mZvUniCSkT7
p/+7AvgZwnAqyCVakVH24
VaMutl1lCm17f8wVEaUVW1dO/Cz7sciGBxlxZmAG+E/CIY7oEr2maHJc+/H4OFHjJxO6zauzNtGwmEUf
qMda7SPf55O52jlhbX2ES
GyEBQS2P6SJEMyVHLrwkFPeyE07bSk57WkM5++y8uqpl4RrXa4LyffnD9z6l0i0zvzYgCCjkJA==</ds
:SignatureValue>
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>MIIFEzCCA/ugAwIBAgIHA8zEnhRtVTANBgkq
hkiG9w0BAQsFADCBmTELMA
kGA1UEBhMCREUxHzAd
BgNVBAoMFmdlbWF0aWsgR21iSCBOT1QtVkFMSUQxSDBGBgNVBAsMP0luc3RpdHV0aW9uIGRlcyBH
ZXN1bmRoZWl0c3dlc2Vucy1DQSBkZXIgVGVsZW1hdGlraW5mcmFzdHJ1a3R1cjEfMB0GA1UEAwwW
R0VNLlNNQ0ItQ0E3IFRFU1QtT05MWTAeFw0xNTA2MzAwMDAwMDBaFw0yMDA2MzAwMDAwMDBaMIHH
MQswCQYDVQQGEwJERTEYMBYGA1UECAwPQmVpc3BpZWxzdO+/vWR0MRgwFgYDVQQHDA9CZWlz
MQswCQYDVQQGEwJERTEYMBYGA1UECAwPQmVpc3BpZWxzdO+cGll
bHN077+9ZHQxDjAMBgNVBBEMBTAxMjM0MRswGQYDVQQJDBJHZXN1bmRoZWl0c2dhc3NlIDMx
bHN077+DzAN
BgNVBAUTBjEwMDAwMTFGMEQGA1UEAww9S3Jhbmtlbmhhd XMgQmVpc3BpZWxzdO+/vWR0Luts
BgNVBAUTBjEwMDAwMTFGMEQGA1UEAww9S3Jhbmtlbmhhd XMgQmVpc3BpZWxzdO+aW5p
ayBm77+9ciBLYXJkaW9sb2dpZVRFU1QtT05MWTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
ayBm77+AqoC
ggEBAL/uetzxukiQQ4yd9gVyK5ZtgCrxzAH5ZlPoJcKOKo+oKZ5i/NpgjkXCBQl25gXuQJACkEjN
pa3E2JqOXLgwsLTZXVShc8v1b49DcbNPSDswWTnE7NwF7RemmnP9aKunqehFNUicRABfGa0j4Las
8eV3bqRg9y/+Cx6Y9GFr5OdfxLYs73HE7T1k7s9L7ufJtSfpm0FqZY5dkZk3a9jxbSJ3ovDBaL30
h3uKxTvBMU+przKZC/xf84Kjjxm1+PGD7I5/NTcCCX5w8uxKW/tNqQTFkhsArP4XdSIKiiyG
h3uKxTvBMU+XrAM
Yboa/oOlH/pF3LepfgHPXLfid5uOdT5+hpsoU/UkvBUCAwEAAaOCAS4wggEqMB0GA1UdDgQWBBQp
9vXBG9pPNsqBE1LNDe26RYztJzATBgNVHSUEDDAKBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMDoG
BSskCAMDBDEwLzAtMCswKTAnMA0MC0tyYW5rZW5oYXVzMAkGByqCFABMBDUTCzUtMklLLTMxNDE1
MB8GA1UdIwQYMBaAFDw5CixOUpeco4wu+AhSBLSZD2rnMCwGA1UdIAQlMCMwCgYIKoIUAEwE
MB8GA1UdIwQYMBaAFDw5CixOUpeco4wu+gSMw
CQYHKoIUAEwETTAKBggqghQATASBKjAOBgNVHQ8Baf8EBAMCBaAwSwYIKwYBBQUHAQEEPzA9MDsG
```

```
CCsGAQUFBzABhi9odHRwOi8vb2NzcC5wa2kudGVsZW1hdGlrLXRlc3Q6ODA4MC9DTU9DU1AvT0NT
UDANBgkqhkiG9w0BAQsFAAOCAQEAC9tRPAgRoamvei0eX5IiHmj/mt4zX9kvhNRe3HMBUYMnvV10
J4h7EaT8/PeXBCtbari4xfqD+WDQhEayWYfsKL5GTFuzQXExgt0r5aZdH6V8kChXJ7JldKNiS7QH
rt1ZohY7qPLpDdYqQS99Uy79h7Y+MsZh1sI/1wCSQ/Tl5uVgjTM8q+0xI49VHVzebsGHLRdW
rt1ZohY7qPLpDdYqQS99Uy79h7Y+VAZa
W7DibaeP30G7r36nBfc5LBJm9MghL88Wgi/JPd4l09gQWfxRV0yiUlp9LQ+yUlAM13BesZ3Niu3q
vrHiTD0Y0QrOR2/AM4ETNPa0Kc/ClzkyBZhng/B3cwdTNcVuFWINmEDLGNmycyN0Pw==</ds:X509Cer
tificate>

                    </ds:X509Data>

                </ds:KeyInfo>

            </ds:Signature>

            <saml2:Subject>

                <saml2:NameID Format=”urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName”
NameQualifier=”http://cxf.apache.org/sts”>2.5.4.5=#130c313233343536373839303133,
2.5.4.42=#0c084865696e
72696368,2.5.4.4=#0c03466974,CN=Dr. med. Heinrich Fit\, Facharzt für
Physikalische Therapie,C=DE</saml2:NameID>

                <saml2:SubjectConfirmation
Method=”urn:oasis:names:tc:SAML:2.0:cm:holder-of-key”>

                    <saml2:SubjectConfirmationData
xsi:type=”saml2:KeyInfoConfirmationDataType”>

                        <ds:KeyInfo
xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>

                            <ds:KeyValue>

                                <ds:RSAKeyValue>

                                    <ds:Modulus>oh83Kp6+Pj5yoYml1uayO2UupCq69pZx
WbhCco6Q7X4YaRQ+Zc3DGq
KUU8U891/qt2hVe9yAjTe9btPKdC8gyidZi+/0Y+h19KGRA8GgrCbSQa8gMk/9FJqJF42CqSZAAOAb2Z
/sAZOe4bCiO1D1i2KAC+/c
HUEy+RyX61ud7833GadG0JxjcVTHg+kIDTASC16r5KATsErPHmgjmFEamnCBRN9WTDymQxSGotQYFbdS
gGTKtrPeoElI6McXOZN0Vo
qDQ+7G2OhGLxqyyA3gpT+js0j6j3jILdxTWGMBCeeKgq3kfoP2OqOwD0EIFQVnD2SamJham5O45n4tbr
GPxw==</ds:Modulus>

                                    <ds:Exponent>AQAB</ds:Exponent>

                                </ds:RSAKeyValue>

                            </ds:KeyValue>

                        </ds:KeyInfo>

                    </saml2:SubjectConfirmationData>

                </saml2:SubjectConfirmation>

            </saml2:Subject>

            <saml2:Conditions NotBefore=”2016-10-12T17:27:02.768Z”
NotOnOrAfter=”2016-10-12T17:32:02.768Z”/>

            <saml2:AuthnStatement AuthnInstant=”2016-10-12T17:26:22.933Z”>

                <saml2:AuthnContext>

                    <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:c
lasses:SmartcardPKI<
/saml2:AuthnContextClassRef>

                </saml2:AuthnContext>

            </saml2:AuthnStatement>

            <saml2:AttributeStatement>
```

```
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
                    <saml2:AttributeValue>Heinz Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
                    <saml2:AttributeValue>Heinz</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
                    <saml2:AttributeValue>Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">
                    <saml2:AttributeValue>Deutschland</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
                    <saml2:AttributeValue>test@example.com</saml2:AttributeValue
>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">
                    <saml2:AttributeValue>1-1a25sd-d529</saml2:AttributeValue>
                </saml2:Attribute>
            </saml2:AttributeStatement>
        </saml2:Assertion>
    </ns2:RequestedSecurityToken>
    <ns2:RequestedAttachedReference>
        <ns4:SecurityTokenReference xmlns:wsse11=”http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd”
wsse11:TokenType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0”>
            <ns4:KeyIdentifier ValueType=”http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.1#SAMLID”>_a714bd3a-4c94-40fb-87fb-
3db5964c1623</ns4:KeyIdentifier>
        </ns4:SecurityTokenReference>
    </ns2:RequestedAttachedReference>
    <ns2:RequestedUnattachedReference>
        <ns4:SecurityTokenReference xmlns:wsse11=”http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd”
wsse11:TokenType=”http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0”>
            <ns4:KeyIdentifier ValueType=”http://docs.oasis-open.org/wss/oasis-
wss-saml-token-profile-1.1#SAMLID”>_a714bd3a-4c94-40fb-87fb-
3db5964c1623</ns4:KeyIdentifier>
        </ns4:SecurityTokenReference>
    </ns2:RequestedUnattachedReference>
```

```
    <ns2:Lifetime>
        <ns3:Created>2016-10-12T17:27:02.768Z</ns3:Created>
        <ns3:Expires>2016-10-12T17:32:02.768Z</ns3:Expires>
    </ns2:Lifetime>
</ns2:RequestSecurityTokenResponse>
```

4.1.7 Operation cancel_Identity_Assertion

Die Operation erlaubt das Annullieren bestehender Identitätsbestätigungen. Die Reichweite der Annullierung beschränkt sich jedoch auf den Konnektor, wodurch die Erneuerung bestehender Identitätsbestätigungen unterbunden wird. Bestehende Sitzungen und die Verwendung bereits ausgestellter Identitätsbestätigungen gegenüber etwaigen anderen Systemen werden hierdurch nicht berührt.

TIP1-A_6839 - cancel_Identity_Assertion mit WS-Trust und WS-Federation
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation cancel_Identity_Assertion entsprechend der Operation „Cancel“ und „RequestSecurityToken“ nach WS-Trust und [WS-Federation1.2] für Active Requestor Profile implementieren.
[<=]

TIP1-A_6886 - cancel_Identity_Assertion akzeptiert nur eigene Identitätsbestätigungen
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Active_Client::cancel_Identity_Assertion nur Identitätsbestätigungen akzeptieren, die es zuvor über I_IDP_Auth_Active_Client oder I_IDP_Auth_Passive_Client ausgestellt hat.
[<=]

TIP1-A_6840 - cancel_Identity_Assertion: Annullierung verhindert Erneuerung
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client sicherstellen, dass es mittels der Operation cancel_Identity_Assertion annullierte Identitätsbestätigungen zukünftig nicht mehr erneuert.
[<=]

Aufrufe der Operation renew_Identity_Assertion kann der BD-TBAuth anhand der Signatur des Aufrufs und anhand der Parameter /wst:RequestSecurityToken /gem:workplaceId und /wst:RequestSecurityToken /gem:mandantId dem Benutzer zuordnen.

TIP1-A_6841 - cancel_Identity_Assertion Annullierung nur für Benutzer
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client bei der Operation cancel_Identity_Assertion sicherstellen, dass Anfragen vom Benutzer der zu annullierenden Identitätsbestätigung stammen.
[<=]

4.1.7.1 Aufrufparameter cancel_Identity_Assertion

TIP1-A_6842 - Aufrufparameter cancel_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation cancel_Identity_Assertion mit den Aufrufparametern aus TAB_BD_TBAuth_06 Aufrufparameter der Operation cancel_Identity_Assertion anbieten.

Tabelle 6: TAB_BD_TBAuth_06 Aufrufparameter der Operation cancel_Identity_Assertion

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wst:RequestSecurityToken	erforderlich	
/wst:RequestSecurityToken /wst:RequestType	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Cancel
/wst:RequestSecurityToken /wst:CancelTarget	erforderlich	Der Wert des Aufrufparameters MUSS die zu annullierende Identitätsbestätigung aus [gemSpec_TBAuth] *TAB_TBAuth_03 Identitätsbestätigung (SAML 2.0 Assertion)* enthalten.

[<=]

Beispiel:

```
<wst:RequestSecurityToken xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Cancel</wst:RequestType>
    <wst:CancelTarget>
        <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_e5dcb3a4-64be-4255-8d25-18fe477ff2ad" IssueInstant="2016-10-21T13:36:55.544Z" Version="2.0" xsi:type="saml2:AssertionType">
            <saml2:Issuer>1-1a25sd-d529</saml2:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                    <ds:Reference URI="#_e5dcb3a4-64be-4255-8d25-18fe477ff2ad">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                        <ds:DigestValue>gipJOTYEnBwZMptZL7EzhQV47Y/ucoI0r6tC/sqQIgQ=</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
```

```
                <ds:SignatureValue>p9FO92d48/5thTpEpAl3ALF1ltukpbR6TM+qqprzoqqUK
Rf6Cmbt9MApIcULG4PfIA7
gYsjxyOVUrGYT+YepBji/M5TPjLMCqykuEBlrLuH5meSH1BtTLVBfrDDSs5lPT9F/qYCkpp48VukVlI3
t7V+6QfTKA0wJqORwgjpES
k+8lCoa93Ty1u7FBl7sSF5bZe3N0yNWSWgrNWyTfF7B8VAMSyGDa2PQ1nZgv7b1HV+texouluiKfmexo
koVDftYzXNpvxsppqv6keh
seybtVpvi1djb1CFG1ZjKkObGmlRU6RMNuIPbZqq9PF1SUFdPo1FjpAidDvmAFbfget6Ezw==</ds:Si
gnatureValue>

                <ds:KeyInfo>

                    <ds:X509Data>

                        <ds:X509Certificate>MIIFEzCCA/ugAwIBAgIHA8zEnhRtVTANBgkq
hkiG9w0BAQsFADCBmTELMAk
GA1UEBhMCREUxHzAd
    BgNVBAoMFmdlbWF0aWsgR21iSCBOT1QtVkFMSUQxSDBGBgNVBAsMP0luc3RpdHV0aW9uIGRlcyBH
    ZXN1bmRoZWl0c3dlc2Vucy1DQSBkZXIgVGVsZW1hdGlraW5mcmFzdHJ1a3R1cjEfMB0GA1UEAwwW
    R0VNLlNNQ0ItQ0E3IFRFU1QtT05MWTAeFw0xNTA2MzAwMDAwMDBaFw0yMDA2MzAwMDAwMDBaMIHH
    MQswCQYDVQQGEwJERTEYMBYGA1UECAwPQmVpc3BpZWxzdO+/vWR0MRgwFgYDVQQHDA9CZWlzcGll
    bHN077+9ZHQxDjAMBgNVBBEMBTAxMjM0MRswGQYDVQQJDBJHZXN1bmRoZWl0c2dhc3NlIDMxDzAN
    BgNVBAUTBjEwMDAwMTFGMEQGA1UEAww9S3Jhbmtlbmhhd XMgQmVpc3BpZWxzdO+/vWR0LutsaW5p
    ayBm77+9ciBLYXJkaW9sb2dpZVRFU1QtT05MWTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
    ggEBAL/uetzxukiQQ4yd9gVyK5ZtgCrxzAH5ZlPoJcKOKo+oKZ5i/NpgjkXCBQl25gXuQJACkEjN
    pa3E2JqOXLgwsLTZXVShc8v1b49DcbNPSDswWTnE7NwF7RemmnP9aKunqehFNUicRABfGa0j4Las
    8eV3bqRg9y/+Cx6Y9GFr5OdfxLYs73HE7T1k7s9L7ufJtSfpm0FqZY5dkZk3a9jxbSJ3ovDBaL30
    h3uKxTvBMU+przKZC/xf84Kjjxm1+PGD7I5/NTcCCX5w8uxKW/tNqQTFkhsArP4XdSIKiiyGXrAM
    Yboa/oOlH/pF3LepfgHPXLfid5uOdT5+hpsoU/UkvBUCAwEAAaOCAS4wggEqMB0GA1UdDgQWBBQp
    9vXBG9pPNsqBE1LNDe26RYztJzATBgNVHSUEDDAKBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMDoG
    BSskCAMDBDEwLzAtMCswKTAnMA0MC0tyYW5rZW5oYXVzMAkGByqCFABMBDUTCzUtMklLLTMxNDE1
    MB8GA1UdIwQYMBaAFDw5CixOUpeco4wu+AhSBLSZD2rnMCwGA1UdIAQlMCMwCgYIKoIUAEwEgSMw
    CQYHKoIUAEwETTAKBggqghQATASBKjAOBgNVHQ8Baf8EBAMCBaAwSwYIKwYBBQUHAQEEPzA9MDsG
    CCsGAQUFBzABhi9odHRwOi8vb2NzcC5wa2kudGVsZW1hdGlrLXRlc3Q6ODA4MC9DTU9DU1AvT0NT
    UDANBgkqhkiG9w0BAQsFAAOCAQEAC9tRPAgRoamvei0eX5IiHmj/mt4zX9kvhNRe3HMBUYMnvV10
    J4h7EaT8/PeXBCtbari4xfqD+WDQhEayWYfsKL5GTFuzQXExgt0r5aZdH6V8kChXJ7JldKNiS7QH
    rt1ZohY7qPLpDdYqQS99Uy79h7Y+MsZh1sI/1wCSQ/Tl5uVgjTM8q+0xI49VHVzebsGHLRdWVAZa
    W7DibaeP30G7r36nBfc5LBJm9MghL88Wgi/JPd4l09gQWfxRV0yiUlp9LQ+yUlAM13BesZ3Niu3q
    vrHiTD0Y0QrOR2/AM4ETNPa0Kc/ClzkyBZhng/B3cwdTNcVuFWINmEDLGNmycyN0Pw==</ds:X50
9Certificate>

                    </ds:X509Data>

                </ds:KeyInfo>

            </ds:Signature>

            <saml2:Subject>

                <saml2:NameID Format=”urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName”
NameQualifier=”http://cxf.apache.org/sts”>2.5.4.5=#130c3132333435363738393031333,
2.5.4.42=#0c08486
5696e72696368,2.5.4.4=#0c03466974,CN=Dr. med. Heinrich Fit\, Facharzt f³r
Physikalische Therapie,C=DE</saml2:NameID>

                <saml2:SubjectConfirmation
Method=”urn:oasis:names:tc:SAML:2.0:cm:holder-of-key”>
```

```
                    <saml2:SubjectConfirmationData
xsi:type=”saml2:KeyInfoConfirmationDataType”>
                        <ds:KeyInfo
xmlns:ds=”http://www.w3.org/2000/09/xmldsig#”>
                            <ds:KeyValue>
                                <ds:RSAKeyValue>
                                    <ds:Modulus>oh83Kp6+Pj5yoYml1uayO2UupCq69pZx
WbhCco6Q7X4YaRQ+Zc
3DGqKUU8U891/qt2hVe9yAjTe9btPKdC8gyidZi+/0Y+h19KGRA8GgrCbSQa8gMk/9FJqJF42CqSZAAO
Ab2Z/sAZOe4bCiO1D1
i2KAC+/cHUEy+RyX61ud7833GadG0JxjcVTHg+kIDTASC16r5KATsErPHmgjmFEamnCBRN9WTDymQxSG
otQYFbdSgGTKtrPeoE
lI6McXOZN0VoqDQ+7G2OhGLxqyyA3gpT+js0j6j3jILdxTWGMBCeeKgq3kfoP2OqOwD0EIFQVnD2SamJ
ham5O45n4tbrGPxw==
</ds:Modulus>
                                    <ds:Exponent>AQAB</ds:Exponent>
                                </ds:RSAKeyValue>
                            </ds:KeyValue>
                        </ds:KeyInfo>
                    </saml2:SubjectConfirmationData>
                </saml2:SubjectConfirmation>
            </saml2:Subject>
            <saml2:Conditions NotBefore=”2016-10-21T13:36:55.544Z”
NotOnOrAfter=”2016-10-21T14:06:55.544Z”/>
            <saml2:AuthnStatement AuthnInstant=”2016-10-21T13:36:55.544Z”>
                <saml2:AuthnContext>
                    <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:c
lasses:SmartcardPKI
</saml2:AuthnContextClassRef>
                </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
                    <saml2:AttributeValue>Heinz Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
                    <saml2:AttributeValue>Heinz</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
                    <saml2:AttributeValue>Müller</saml2:AttributeValue>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">
                    <saml2:AttributeValue>Deutschland</saml2:AttributeValue>
                </saml2:Attribute>
```

```
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
                    <saml2:AttributeValue>test@example.com</saml2:AttributeValue
>
                </saml2:Attribute>
                <saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">
                    <saml2:AttributeValue>1-1a25sd-d529</saml2:AttributeValue>
                </saml2:Attribute>
            </saml2:AttributeStatement>
        </saml2:Assertion>
    </wst:CancelTarget>
</wst:RequestSecurityToken>
```

4.1.7.2 Rückgabewerte cancel_Identity_Assertion

TIP1-A_6843 - Rückgabewerte von cancel_Identity_Assertion
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Active_Client die Operation cancel_Identity_Assertion mit den Rückgabewerten aus TAB_BD_TBAuth_07 Rückgabewerte der Operation cancel_Identity_Assertion anbieten.

Tabelle 7: TAB_BD_TBAuth_07 Rückgabewerte der Operation cancel_Identity_Assertion

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wst:RequestSecurityTokenResponse	erforderlich	
/wst:RequestSecurityTokenResponse /wst:RequestTokenCancelled	erforderlich	Der Wert des Aufrufparameters MUSS leer sein.

[<=]

Beispiel:

```
<wst:RequestSecurityTokenResponse>
    <wst:RequestedTokenCancelled/>
</wst:RequestSecurityTokenResponse>
```

4.2 Schnittstelle I_IDP_Auth_Passive_Client

Die Schnittstelle I_IDP_Auth_Passive_Client realisiert Operationen für Webbrowser zur Erzeugung und Annullierung von Identitätsbestätigungen.

TIP1-A_6844 - I_IDP_Auth_Passive_Client mit WS-Federation 1.2 Passive Requestor Profile
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client entsprechend [WS-Federation1.2] Passive Requestor Profile implementieren.
[<=]

TIP1-A_6887 - I_IDP_Auth_Passive_Client über HTTP GET und POST

Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client über HTTP GET und POST anbieten.
[<=]

TIP1-A_6845 - I_IDP_Auth_Passive_Client benutzt gängige Web-Technologien
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Passive_Client gegenüber dem Nutzer ausschließlich gängige Web-Technologien wie z. B. HTML5, Cookies und JavaScript einsetzen, die mit den Webbrowsern Mozilla Firefox, Apple Safari und Microsoft Internet Explorer in der zum Zeitpunkt der Durchführung der Zulassungstests aktuellen Version ohne Anpassungen funktionieren.
[<=]

TIP1-A_5646 - I_IDP_Auth_Passive_Client ohne aktive Inhalte
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client so anbieten, dass sie auch ohne aktive Inhalte (z. B. JavaScript) nutzbar ist.
[<=]

TIP1-A_6738 - I_IDP_Auth_Passive_Client minimale Nutzerinteraktion
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client so anbieten, dass sie mit minimaler Nutzerinteraktion verwendbar ist. Hierzu dürfen aktive Inhalte (z. B. JavaScript) verwendet werden.
[<=]

TIP1-A_6846 - Adresse von I_IDP_Auth_Passive_Client
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client an der Lokation „/idp“ anbieten.
[<=]

TIP1-A_6847 - Timeout von I_IDP_Auth_Passive_Client
Der Basisdienst TBAuth MUSS die Schnittstelle I_IDP_Auth_Passive_Client so umsetzen, dass die PIN-Eingabe bis zu dem in CARD_TIMEOUT_CARD konfigurierten Wert dauern kann, ohne dass ein Timeout des Clients auftritt.
[<=]

4.2.1 Operation signIn

TIP1-A_6849 - Mandantenkontext im Cookie
Der Basisdienst TBAuth MUSS beim Aufruf der Operation signIn und wenn ein persistentes Cookie vorhanden ist, die zu verwendenden Werte clientSystemId, workplaceId, mandantId und Iccsn aus dem persistenten Cookie des Browsers auslesen und als Voreinstellung verwenden.
[<=]

TIP1-A_6850 - voreingestellten Mandantenkontext ändern
Der Basisdienst TBAuth MUSS bei erfolgreichem Auslesen der Voreinstellungen aus dem persistenten Cookies dem Benutzer ermöglichen, die Voreinstellungen zu ändern. Die geänderten Einstellungen MÜSSEN im persistenten Cookie gespeichert werden.
[<=]

TIP1-A_6851 - Auswahl des Mandanten und der Karten
Der Basisdienst TBAuth MUSS beim Aufruf der Operation signIn und wenn es die Voreinstellungen nicht aus einem persistenten Cookie des Benutzers auslesen kann, den Benutzer die zu verwendenden Werte im Webbrowser auswählen lassen.
[<=]

Es soll ermöglicht werden, dass entsprechende persistente Cookies auf Arbeitsplatzsystemen möglichst einfach vorinstalliert werden können, wofür auch die

Entwicklung entsprechender Software-Tools hilfreich sein kann. Daher sollen die im persistenten Cookie hinterlegten Daten durch Dritte, z. B. Leistungserbringerinstitutionen, Administratoren und Softwarehersteller, verändert werden können.

TIP1-A_6852 - Dokumentation des Cookies
Der Basisdienst TBAuth MUSS die Syntax und Semantik des persistenten Cookies für Dritte einsehbar dokumentieren.
[<=]

TIP1-A_6853 - Änderbarkeit des Cookies
Der Basisdienst TBAuth MUSS die persistenten Cookies derart gestalten, dass diese durch Dritte manuell geändert werden können. Das heißt, Dritte dürfen nicht durch Sicherungsmechanismen am persistenten Cookie behindert werden.
[<=]

TIP1-A_6854 - Sicherheit des Cookies
Der Basisdienst TBAuth MUSS in den persistenten Cookies die Attribute Secure, Domain und Path setzen, wobei das Attribut Domain auf die Werte konnektor.konlan oder konlan eingeschränkt wird und der Path auf den Wert /idp gesetzt wird.
[<=]

TIP1-A_6888 - HttpOnly des Cookies
Der Basisdienst TBAuth MUSS in den persistenten Cookies das Attribut HttpOnly setzen, sofern nicht JavaScript verwendet wird, welches mit diesem Attribut nicht funktioniert.
[<=]

TIP1-A_6855 - Umleitung auf Endpunkte ist möglich
Der Basisdienst TBAuth KANN beim Aufruf der Operation signIn den Webbrowser des Benutzers auf eigene Endpunkte des Basisdienstes umleiten.
[<=]

TIP1-A_6856 - Behauptungen der Identitätsbestätigung – I_IDP_Auth_Passive_Client
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Passive_Client:signIn, Identitätsbestätigungen entsprechend den in [gemSpec_TBAuth] *TAB_TBAuth_02 Behauptungen des* Basisdienstes*TBAuth* aufgeführten Behauptungen ausstellen und diese aus den jeweiligen Attributen der verwendeten Zertifikate befüllen. Als optional gekennzeichnete Behauptungen MÜSSEN verwendet werden, sofern das Attribut des jeweiligen Zertifikats vorhanden ist.
[<=]

TIP1-A_6995 - signIn: Gültigkeit der bestätigten Identität
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Passive_Client::signIn sicherstellen, dass die bestätigte Identität gültig ist und deren Gültigkeit innerhalb der letzten 24 Stunden erfolgreich geprüft wurde.
[<=]

TIP1-A_6857 - Issuer „IDP TI-Plattform“ – I_IDP_Auth_Passive_Client
Der Basisdienst TBAuth MUSS an der Operation I_IDP_Auth_Passive_Client:signIn in Identitätsbestätigungen den Issuer „IDP TI-Plattform“ eintragen.
[<=]

TIP1-A_6858 - Aufrufparameter signIn
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Passive_Client die Operation signIn entsprechend [WS-Federation1.2] mit den Aufrufparametern aus TAB_BD_TBAuth_08 Aufrufparameter der Operation signIn anbieten.

Tabelle 8: TAB_BD_TBAuth_08 Aufrufparameter der Operation signIn

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
`wa`	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: `wsignin1.0`
`wct`	erforderlich	Der BD-TBAuth MUSS Anfragen abbrechen falls der Erstellungszeitpunkt mehr als eine Minute von der eigenen Systemzeit abweicht.
`wfresh`	optional	Das BM Der BD-TBAuth MUSS Identitätsbestätigungen mit der in diesem Aufrufparameter angegebenen Lebensdauer ausstellen. Falls der Parameter 0 beträgt oder nicht vorhanden ist, MUSS das BM der BD-TBAuth die Identitätsbestätigung mit einer Gültigkeitsdauer von drei Stunden ausstellen. Das BM Der BD-TBAuth DARF NICHT Identitätsbestätigungen ausstellen die länger als 24 Stunden gültig sind.
`wtrealm`	erforderlich	Referenz auf den zu verwendenden Dienst, auf den der Geltungsbereich der Identitätsbestätigung beschränkt wird. Dieser Parameter MUSS den Festlegungen von AudienceRestriction in [gemSpec_TBAuth] entsprechen.
`wreply`	erforderlich	Der BD-TBAuth MUSS den Benutzer nach Abschluss der Operation auf diese URL leiten.
`wctx`	optional	Der BD-TBAuth MUSS die übergebene Kontextinformation in die Antwort übernehmen.

[<=]

TIP1-A_6859 - Rückgabewerte von signIn
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Passive_Client die Operation signIn entsprechend [WS-Federation1.2] mit den Rückgabewerten aus TAB_BD_TBAuth_10 Rückgabewerte der Operation signIn anbieten.

Tabelle 9: TAB_BD_TBAuth_10 Rückgabewerte der Operation signIn

Name des Rückgabewerts	Verpflichtung	zusätzliche Konsistenzregel
`wa`	erforderlich	Der Wert des Parameters MUSS wie folgt sein: `wsignin1.0`
`wresult`	erforderlich	Der Parameter MUSS ein “Request Security Token Response” (RSTR) nach WS-Trust mit den Rückgabewerten aus [gemSpec_TBAuth] *TAB_TBAuth_05*

		RequestSecurityTokenResponseCollection enthalten.
`wctx`	optional	Der BD-TBAuth MUSS die übergebene Kontextinformation in die Antwort übernehmen.
`wtrealm`	erforderlich	Referenz auf den zu verwendenden Dienst, auf den der Geltungsbereich der Identitätsbestätigung beschränkt wird.

[<=]

Für ein Beispiel siehe Anhang C1.

4.2.2 Operation signOut

Diese Operation ermöglicht das Abmelden basierend auf [WS-Federation1.2] für Passive Requestor Profile. Mit Aufruf dieser Operation loggen sich Nutzer beim Basisdienst TBAuth aus und die Sitzung sowie der ggf. zugehörige Session-Cookie im Browser werden gelöscht.

Da über I_IDP_Auth_Passive_Client ausgestellte Identitätsbestätigungen grundsätzlich auch über I_IDP_Auth_Active_Client::renew_Identity_Assertion erneuert werden können, ist diese Operation signOut auch für I_IDP_Auth_Passive_Client nötig.

TIP1-A_6860 - Aufrufparameter signOut
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Passive_Client die Operation signOut entsprechend [WS-Federation1.2] mit den Aufrufparametern aus TAB_BD_TBAuth_11 Aufrufparameter der Operation signOut anbieten.

Tabelle 10: TAB_BD_TBAuth_11 Aufrufparameter der Operation signOut

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
`wa`	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: `wsignout1.0`
`wreply`	optional	Der BD-TBAuth MUSS den Benutzer nach Abschluss der Operation auf diese URL leiten. Falls dieser Parameter nicht übergeben wird, MUSS der BD-TBAuth dem Benutzer die erfolgreiche Annullierung anzeigen.

[<=]

Sitzungsinformationen könnten die Identitätsbestätigung oder eine Referenz auf diese enthalten, sind aber letzten Endes implementierungsabhängig. Je nach Implementierung des Basisdienstes, könnte dieser Sitzungsinformationen temporär speichern oder auch in einem Session-Cookie im Webbrowser des Nutzers ablegen.

TIP1-A_6862 - Annullierung durch signOut
Der Basisdienst TBAuth MUSS an der Schnittstelle I_IDP_Auth_Passive_Client bei Aufruf der Operation signOut die zugehörige Identitätsbestätigung annullieren, indem es ggf. zugehörige Sitzungs-Cookies im Webbrowser des Benutzers löscht, ggf. temporär gespeicherte Sitzungsinformationen innerhalb des Basisdienstes löscht und für diesen

Nutzer zuvor über I_IDP_Auth_Passive_Client ausgestellte Identitätsbestätigungen (über I_IDP_Auth_Active_Client::renew_Identity_Assertion) nicht mehr erneuert.
[<=]

Nach der Bestätigung durch den Benutzer kann die eigentliche Annullierung mittels der Operation signoutCleanup [WS-Federation1.2] ausgeführt werden. Um zu verhindern, dass sich Nutzer unabsichtlich abmelden – sei es aufgrund eines technischen Fehlers oder als Opfer eines boshaften Angriffs – wird die Operation signoutCleanup nicht separat (ohne Bestätigung) angeboten

Für ein Beispiel siehe Anhang C2.

4.3 Schnittstelle I_Local_IDP_Service

Der Basisdienst TBAuth bietet diese Schnittstelle, zur Ausstellung von Identitätsbestätigungen, für lokale IDPs in der Leistungserbringerumgebung an. Als Aufrufparameter wird eine durch den lokalen IDP erstellte und signierte Identitätsbestätigung übergeben. Der BD-TBAuth übernimmt die Inhalte dieser übergebenen Identitätsbestätigung unverändert und signiert diese mit der für tokenbasierte Authentisierung verwendeten Identität. Die neu signierte Identitätsbestätigung wird als Ergebnis der Operation zurück geliefert.

Als Herausgeber der Identitätsbestätigung wird ein vom Aufrufer vorgegebener Wert verwendet. Der BD-TBAuth stellt jedoch sicher, dass dieses von dem Wert „IDP TI-Plattform“ abweicht. Dadurch können Systeme, die die Identitätsbestätigung prüfen, erkennen, dass die Inhalte der Identitätsbestätigung nicht vom BD-TBAuth, sondern von einem lokalen IDP stammen.

TIP1-A_6864 - WSDL für I_Local_IDP_Service
Der Basisdienst TBAuth MUSS die Schnittstelle I_Local_IDP_Service entsprechend LocalIdpService.wsdl (siehe Anhang B) umsetzen.
[<=]

TIP1-A_6865 - Gültige Anfragen an I_Local_IDP_Service
Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service ausschließlich Anfragen (Requests) akzeptieren, die der geltenden Schnittstellendefinition (WSDL) entsprechen. Aufrufe mit ungültigen Anfragen MÜSSEN mit einem SOAP-Fault abgebrochen werden.
[<=]

4.3.1 SOAP-Envelope

Um Standard-konform zu sein wird die zu signierende Identitätsbestätigung nicht als Teil des RST sondern im Security-Header des SOAP-Envelopes übergeben.

TIP1-A_6866 - I_Local_IDP_Service: SOAP-Envelope der Aufrufe
Der Basisdienst TBAuth MUSS Aufrufe der Schnittstelle I_Local_IDP_Service ablehnen, wenn sie nicht dem folgenden SOAP-Envelope entsprechen, wobei „…“ Platzhalter sind.

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/addressing"> http://docs.oasis-
open.org/ws-sx/ws-trust/200512/RST/Issue</Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">…</MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">…</To>
        <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
            <Address>…</Address>
```

```
        </ReplyTo>
        <wsse:Security soap:mustUnderstand="1">
            <saml2:Assertion>…</saml2:Assertion>
        </wsse:Security>
    </soap:Header>
    <soap:Body>
        …
    </soap:Body>
</soap:Envelope>
```

[<=]

TIP1-A_6867 - I_Local_IDP_Service: SOAP-Envelope der Antworten
Der Basisdienst TBAuth MUSS die Schnittstelle I_Local_IDP_Service so umsetzen, dass alle Antworten dem folgenden SOAP-Envelope entsprechen, wobei „…“ Platzhalter sind.

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <Action xmlns="http://www.w3.org/2005/08/addressing">…</Action>
        <MessageID xmlns="http://www.w3.org/2005/08/addressing">…</MessageID>
        <To xmlns="http://www.w3.org/2005/08/addressing">…</To>
        <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">…</RelatesTo>
        …
    </soap:Header>
    <soap:Body>
        …
    </soap:Body>
</soap:Envelope>
```

[<=]

TIP1-A_6877 - I_Local_IDP_Service: Alternative Schreibweise bei leeren Element <soap:Body>
Falls kein Body verwendet wird KANN der Basisdienst TBAuth in der Antwort der Schnittstelle I_Local_IDP_Service anstelle von <soap:Body>…</soap:Body> auch <soap:Body/> verwenden.
[<=]

4.3.2 Sicherheit

TIP1-A_6868 - I_Local_IDP_Service Security Header entsprechend WS-Policy
Der Basisdienst TBAuth MUSS sicherstellen, dass an der Schnittstelle I_Local_IDP_Service der Security Header des Aufrufs den Vorgaben der WS-Policy des jeweilig adressierten Service Endpunkts entspricht.
[<=]

TIP1-A_6869 - Autorisierung lokaler IDPs an I_Local_IDP_Service
Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service sicherstellen, dass es Identitätsbestätigung nur dann ausstellt, wenn der Aufruf durch einen lokalen IDP signiert wurde.
[<=]

TIP1-A_6870 - Konfiguration lokaler IDPs
Der Basisdienst TBAuth MUSS es dem Administrator über die Managementschnittstelle des Konnektors ermöglichen lokale IDPs zu konfigurieren und Ihnen Zertifikate auszustellen.
[<=]

TIP1-A_6871 - Behauptungen der Identitätsbestätigung – I_Local_IDP_Service

Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service alle Werte aus der übergebenen Identitätsbestätigung in die auszustellende Identitätsbestätigung übernehmen, außer die Signatur und damit zusammenhängende Felder und Werte.
[<=]

TIP1-A_6872 - Issuer der Identitätsbestätigung
Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service sicherstellen, dass die übergebene Identitätsbestätigung kein Element <Issuer> mit dem Wert „IDP TI-Plattform“ enthält (unabhängig von Groß- und Kleinschreibung) und andernfalls mit einem Fehler abbrechen.
[<=]

4.3.3 Operation sign_Token

TIP1-A_6873 - sign_Token mit WS-Trust und WS-Federation
Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service die Operation sign_Token entsprechend der Operation „Issue“ und „RequestSecurityToken“ nach WS-Trust und [WS-Federation1.2] für Active Requestor Profile implementieren.
[<=]

4.3.3.1 Aufrufparameter sign_Token

Um standardkonform zu sein, wird die zu signierende Identitätsbestätigung nicht als Teil des RST, sondern im Security-Header des SOAP-Envelopes übergeben.

TIP1-A_6874 - Aufrufparameter von sign_Token
Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service die Operation sign_Token mit den Aufrufparametern aus TAB_BD_TBAuth_12 Aufrufparameter von sign_Token anbieten.

Tabelle 11: TAB_BD_TBAuth_12 Aufrufparameter von sign_Token

Name des Aufrufparameters	Verpflichtung	zusätzliche Konsistenzregel
/wst:RequestSecurityToken	erforderlich	
/wst:RequestSecurityToken /wst:RequestType	erforderlich	Der Wert des Aufrufparameters MUSS wie folgt sein: http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
/wst:RequestSecurityToken /gem:mandantId	erforderlich	Auf Basis dessen ermittelt das TBAuth die zugeordneten SM-B (eine oder mehrere).
/wst:RequestSecurityToken /gem:clientSystemId	erforderlich	Das zu verwendende Client System.
/wst:RequestSecurityToken /gem:iccsn	optional	Die Seriennummer der Karte mit der die Identitätsbestätigung signiert werden soll.

[<=]

Beispiel:

Mit Auslassungspunkten (…) ausgewiesene Textstellen sind gekürzt.

```
<wst:RequestSecurityToken xmlns:wst=”http://docs.oasis-open.org/ws-sx/ws-trust/200512”>
```

```
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
    <gem:mandantId>…</gem:mandantId>
    <gem:clientSystemId>…</gem:clientSystemId>
    <gem:iccsn>123456789123456789</gem:iccsn>
</wst:RequestSecurityToken>
```

4.3.3.2 Rückgabewerte von sign_Token

TIP1-A_6875 - Rückgabewerte von sign_Token

Der Basisdienst TBAuth MUSS an der Schnittstelle I_Local_IDP_Service die Operation sign_Token mit dem Rückgabewert “Request Security Token Response” (RSTR) nach WS-Trust anbieten.

[<=]

5 Informationsmodell

Die relevanten Informationsmodelle sind in [gemSpec_TBAuth] spezifiziert.

5.1 Namensräume

Tabelle 12: TAB_BD_TBAuth_13 Präfixe und Namensräume

Präfix	Namensraum
gem	http://ws.gematik.de/conn/tbauth/201612
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
BD	Basisdienst
EFA	elektronische Fallakte
HSM-B	Variante der SMC-B, die durch eine schnellere Performance gekennzeichnet ist
IDP	Identity Provider (eine Teilkomponente eines IAM)
SAML	Security Assertion Markup Language
SM-B	Oberbegriff für SMC-B und HSM-B
STS	Security Token Service
WS	Webservice

6.2 Glossar

Das Glossar erläutert Begriffe dieser Spezifikation, welche nicht in [gemKPT_Arch_TIP], [gemSpec_TBAuth] oder [gemGlossar] erläutert sind.

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematik Infrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer ist in der aktuellen von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzeption Architektur der TI-Plattform
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_TBAuth]	Spezifikation tokenbasierte Authentisierung

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BasicProfile1.2]	WS-I Basic Profile Version 1.2 http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html
[BasicSecurityProfile1.1]	OASIS Basic Security Profile Version 1.1 https://docs.oasis-open.org/ws-brsp/BasicSecurityProfile/v1.1/BasicSecurityProfile-v1.1.html
[EFA2.0]	EFA Spezifikation v2.0, http://wiki.hl7.de/index.php?title=cdaefa:EFA_Spezifikation_v2.0
[SAML2.0]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/

[WS-Addressing1.0]	Web Services Addressing 1.0 – Core, W3C Recommendation 9 May 2006. http://www.w3.org/TR/ws-addr-core/
[WS-Federation1.2]	OASIS Web Services Federation Language (WS-Federation) Version 1.2 https://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html
[WS-MetadataExchange1.1]	Web Services Metadata Exchange (WS-MetadataExchange) 1.1 http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf
[WS-SecurityPolicy1.3]	OASIS WS-SecurityPolicy 1.3 https://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html
[WS-Transfer2006]	Web Services Transfer (WS-Transfer) 27 September 2006 https://www.w3.org/Submission/2006/SUBM-WS-Transfer-20060927/
[WS-Trust1.3]	WS-Trust 1.3 http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf
[WS-Trust1.4]	WS-Trust 1.4 http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf

7 Anhang B – Verwendete Schnittstellenversionen

Tabelle 13 : TAB_BD_TBAuth_16 Schnittstellenversionen

Pro Dienst mit Operationen an der Außenschnittstelle: WSDLs des Konnektors und ggf. verwendete XSDs aus dem Namensraum der gematik http://ws.gematik.de		
Lokaler IDP Service		
	WSDL Name	LocalIdpService.wsdl
	WSDL-Version	1.0.0
	TargetNamespace	http://ws.gematik.de/conn/tbauth/LocalIdpService/v1.0
	verwendete XSDs	keine
IDP Service für Active Client		
	WSDL Name	IdpServiceActiveRequestor.wsdl
	WSDL-Version	1.0.0
	TargetNamespace	http://ws.gematik.de/conn/tbauth/IdpServiceActiveRequestor/v1.0
	verwendete XSDs	keine

8 Anhang C

8.1 C1 – Beispiel I_IDP_Auth_Passive_Client::signIn

Dieser Ablauf ist beispielhaft und kann im Detail von der Spezifikation abweichen (z.B. Präfixe). Zudem stellt dieses Beispiel eine mögliche Umsetzungsvariante dar, die sich außerhalb des Spezifikationsbereichs befindet. Konkrete Implementierungen können z.B. mehrere Request-Response-Sequenzen verwenden, wohingegen hier lediglich der initiale Request und die finale Response dargestellt sind.

In der Antwort wird HTML verwendet, um den Webbrowser mittels HTTP POST auf einen anderen Endpunkt umzuleiten.

Mit Auslassungspunkten „…“ ausgewiesene Textstellen sind gekürzt.

1) Initialer Request

```
GET https://konnektor.konlan/idp?wa=wsignin1.0
&wreply=https%3A%2F%2Fwww.gesundheitsdatendienst.telematik/&wtrealm=urn:telemati
k:gesundheitsdatendienst:www:Instanz23&wct
x=32b4bca8-f80e-4a1d-950d-0b88e54cc508
```

```
Parameter:
wa: “wsignin1.0”
wtrealm: “urn:telematik:gesundheitsdatendienst:www:Instanz23”
wreply: “https://www.gesundheitsdatendienst.telematik/”
wctx: „32b4bca8-f80e-4a1d-950d-0b88e54cc508“
```

2) Response mit Identitätsbestätigung

```
HTTP/1.1 200 OK
```

```
Set-Cookie:
JSESSIONID=C06EC2B344F516B512E917390DCBF820
Domain=konnektor.konlan
Path=/idp
Secure
HttpOnly
```

```
Content:
<!DOCTYPE html PUBLIC “-//W3C//DTD HTML 4.01 Transitional//EN”
“http://www.w3.org/TR/html4/loose.dtd”>
<html>
    <head>
        <title>IDP SignIn Response Form</title>
    </head>
    <body>
```

```
        <form id="signinresponseform" name="signinresponseform"
action="https://www.gesundheitsdatendienst.telematik/" method="POST">
            <input type="hidden" name="wa" value="wsignin1.0" />
            <br />
            <input type="hidden" name="wresult"
value="&lt;RequestSecurityTokenResponseCollection xmlns=&quot;http://docs.oasis-
open.org/ws-sx/ws-trust/200512&quot; xmlns:ns2=&quot;http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd&quot;
xmlns:ns3=&quot;http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd&quot;
xmlns:ns4=&quot;http://www.w3.org/2005/08/addressing&quot;
xmlns:ns5=&quot;http://docs.oasis-open.org/ws-sx/ws-
trust/200802&quot;&gt;&lt;RequestSecurityTokenResponse&gt;&lt;TokenType&gt;http:
//docs.oasis-open.org/wss/oasis-wss-saml-token-profile-
1.1#SAMLV2.0&lt;/TokenType&gt;…/>
            <br />
            <input type="hidden" name="wctx" value="32b4bca8-f80e-4a1d-950d-
0b88e54cc508" />
            <br />
            <input type="hidden" name="wtrealm"
value="urn:telematik:gesundheitsdatendienst:www:Instanz23" />
            <br />
            <noscript>
                <p>Script is disabled. Click Submit to continue.</p>
                <input type="submit" name="_eventId_submit" value="Submit" />
                <br />
            </noscript>
        </form>
        <script
language="javascript">window.setTimeout('document.forms[0].submit()',0);</script
>
    </body>
</html>
```

8.2 C2 – Beispiel I_IDP_Auth_Passive_Client::signOut

1) Request signOut

```
GET https://konnektor.konlan/idp?wa=wsignout1.0


Cookies:
JSESSIONID=292C6AE65855DAFA6853DFB660374A2E
FEDIZ_HOME_REALM="urn:telematik:gesundheitsdatendienst:www:Instanz23"


Parameter:
wa:"wsignout1.0"
```

2) Response signOut

```
HTTP/1.1 200 OK
```

```
<!DOCTYPE html PUBLIC “-//W3C//DTD HTML 4.01 Transitional//EN”
“http://www.w3.org/TR/html4/loose.dtd”>
<html>
    <head>
        <title>IDP SignOut Confirmation Response Page</title>
    </head>
    <body>
        <h1>Logout from the following Applications?</h1>
        <div>Fedizhelloworld<br/>
        </div>
        <br/>
        <br/>
        <form id=”signoutconfirmationresponseform”
name=”signoutconfirmationresponseform” action=”/fediz-
idp/federation?wa=wsignout1.0” method=”POST”>
            <input type=”hidden” name=”wa” value=”wsignout1.0” />
            <input type=”hidden” id=”execution” name=”execution” value=”e4s1” />
            <input type=”submit” name=”_eventId_submit” value=”Logout” />
        </form>
    </body>
</html>
```

3) Request signOut

```
POST https://konnektor.konlan/idp?wa=wsignout1.0

Cookie:
JSESSIONID=292C6AE65855DAFA6853DFB660374A2E
FEDIZ_HOME_REALM=”urn:telematik:gesundheitsdatendienst:www:Instanz23”

Content:
wa=wsignout1.0
execution=e4s1
_eventId_submit=Logout
```

4) Response signOut

```
HTTP/1.1 200 OK

Set-Cookie:
JSESSIONID=DD2396E6AFC47E6A9A7874DDDD356147
FEDIZ_HOME_REALM=””

Content:
```

```
<!DOCTYPE html PUBLIC “-//W3C//DTD HTML 4.01 Transitional//EN”
“http://www.w3.org/TR/html4/loose.dtd”>
<html>
    <head>
        <title>IDP SignOut Response Page</title>
    </head>
    <body>
        <h1>CXF Fediz IDP successful logout.</h1><p>Fedizhelloworld<img
src=”https://www.gesundheitsdatendienst.telematik/fedservlet?wa=wsignoutcleanup1
.0”/>
            <br/>
        </p>
    </body>
</html>
```

5) Request signoutCleanup

```
GET
https://www.gesundheitsdatendienst.telematik/fedservlet?wa=wsignoutcleanup1.0


Cookie:
JSESSIONID= 1D0E8AD4CC4B8D7D8DD7A5996496945E


Parameter:
wa:wsignoutcleanup1.0
```

6) Response signoutCleanup

```
HTTP/1.1 200 OK


Set-Cookie:
JSESSIONID=DD2396E6AFC47E6A9A7874DDDD356147
FEDIZ_HOME_REALM=””


Content:
<!DOCTYPE html PUBLIC “-//W3C//DTD HTML 4.01 Transitional//EN”
“http://www.w3.org/TR/html4/loose.dtd”>
<html>
    <head>
        <title>IDP SignOut Confirmed</title>
    </head>
    <body>
        <h1>IDP SignOut Confirmed</h1>
```

```
    </body>
</html>
```