

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Übergreifende Spezifikation Tokenbasierte Authentisierung**

Version:	1.2.0
Revision:	716277
Stand:	15.05.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_TBAuth

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

Die Änderungen zur Vorversion beruhen auf P18.1.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	04.08.17		freigegeben	gematik
			Ergänzung ePA-Inhalte	gematik
1.1.0	18.12.18		freigegeben	gematik
1.2.0 CC	01.03.19		zur Abstimmung freigegeben	gematik
			Einarbeitung Eigenkommentare und Änderungsliste P18.1	
1.2.0	15.05.2019		freigegeben	gematik
			Anpassung in TAB_TBAuth_01	

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokumentes .....</b>	<b>5</b>
1.1 Zielsetzung .....	5
1.2 Zielgruppe .....	5
1.3 Geltungsbereich .....	5
1.4 Arbeitsgrundlagen .....	6
1.5 Abgrenzung des Dokuments .....	6
1.6 Methodik .....	6
1.6.1 Anforderungen .....	6
<b>2 Systemüberblick .....</b>	<b>8</b>
2.1 Akteure und Rollen .....	9
2.1.1 Nutzer .....	9
2.1.2 Client .....	9
2.1.3 Dienste .....	9
2.1.4 Identitätsbestätigung .....	9
2.1.5 Identity Provider (IDP) .....	9
2.1.5.1 Lokaler Identity Provider .....	10
2.1.5.2 Providerseitiger Identity Provider .....	10
2.1.6 Basisdienst tokenbasierte Authentisierung (BD-TBAuth) .....	10
2.2 Nachbarsysteme .....	10
2.2.1 Konnektor .....	10
2.2.2 Karten .....	10
2.3 Weiterer Begriff: Security Token Service (STS) .....	11
<b>3 Übergreifende Festlegungen .....</b>	<b>12</b>
3.1 Anforderung von Identitätsbestätigungen .....	12
3.2 Prüfung von Identitätsbestätigungen .....	12
3.3 Annullieren von Identitätsbestätigungen .....	13
3.4 Verwendete Standards .....	14
<b>4 Informationsmodell .....</b>	<b>16</b>
4.1 Namensräume .....	16
4.2 Behauptungen in Identitätsbestätigungen .....	16
4.3 Identitätsbestätigung .....	19
4.4 Antworten mit Identitätsbestätigungen .....	25
<b>5 Anhang A – Verzeichnisse .....</b>	<b>28</b>
5.1 Abkürzungen .....	28
5.2 Glossar .....	28

<b>5.3 Abbildungsverzeichnis.....</b>	<b>29</b>
<b>5.4 Tabellenverzeichnis .....</b>	<b>29</b>
<b>5.5 Referenzierte Dokumente .....</b>	<b>29</b>
5.5.1 Dokumente der gematik.....	29
5.5.2 Weitere Dokumente.....	30
<b>6 Anhang B .....</b>	<b>31</b>
<b>6.1 Beispiel.....</b>	<b>31</b>

---

## **1 Einordnung des Dokumentes**

---

### **1.1 Zielsetzung**

Dieses Dokument enthält Anforderungen an Systeme, die Identitätsbestätigungen (entsprechend der tokenbasierten Authentisierung) verarbeiten, wie z.B. Dienste und Identity Provider (IDPs).

### **1.2 Zielgruppe**

Das Dokument enthält Festlegungen zur Authentisierung, die insbesondere für folgende Akteure relevant sein können:

- Hersteller von Systemen, die Identitätsbestätigungen verarbeiten
- Anbieter und Betreiber von Diensten
- Softwarehersteller von Primärsystemen und lokalen Identity Providern
- Verantwortliche für Zulassung und Test

### **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 Telematikinfrastruktur 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.

### **Schutzrechts-/Patentrechtshinweis**

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik mbH übernimmt insofern keinerlei Gewährleistungen.*

## **1.4 Arbeitsgrundlagen**

Grundlagen für die Ausführung dieses Dokumentes sind insbesondere:

- Konzept Architektur der TI-Plattform [gemKPT\_Arch\_TIP]
- 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**

An der tokenbasierten Authentisierung sind mehrere Systeme beteiligt. Dieses Dokument legt Anforderungen fest, die für mehr als ein System gelten. Zudem beschreibt es die Interaktion der Systeme untereinander. Die in diesem Dokument spezifizierten Anforderungen werden nicht alle notwendigerweise im Rahmen von Zulassungstests geprüft, sondern können, je nach Adressat, auch in Implementierungsleitfäden aufgegriffen werden.

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.

Der Basisdienst tokenbasierte Authentisierung ist Teil des Konnektors. In der Spezifikation Basisdienst tokenbasierte Authentisierung [gemSpec\_Kon\_TBAuth] werden die durch den Basisdienst bereitgestellten (angebotenen) Schnittstellen spezifiziert.

In der Konnektor-Spezifikation [gemSpec\_Kon] sind Leistungsmerkmale des Konnektors beschrieben. So wie Fachmodule des Konnektors in separaten Dokumenten beschrieben werden, wird die tokenbasierte Authentisierung in dem vorliegenden Dokument beschrieben.

Die in diesem Dokument festgelegten Vorgaben zur Struktur von Identitätsbestätigungen, deren Wertebereich und die unterstützten Behauptungen (Claims) sind auch außerhalb des Basisdienstes tokenbasierte Authentisierung in der Telematikinfrastruktur übergreifend verbindlich.

## **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

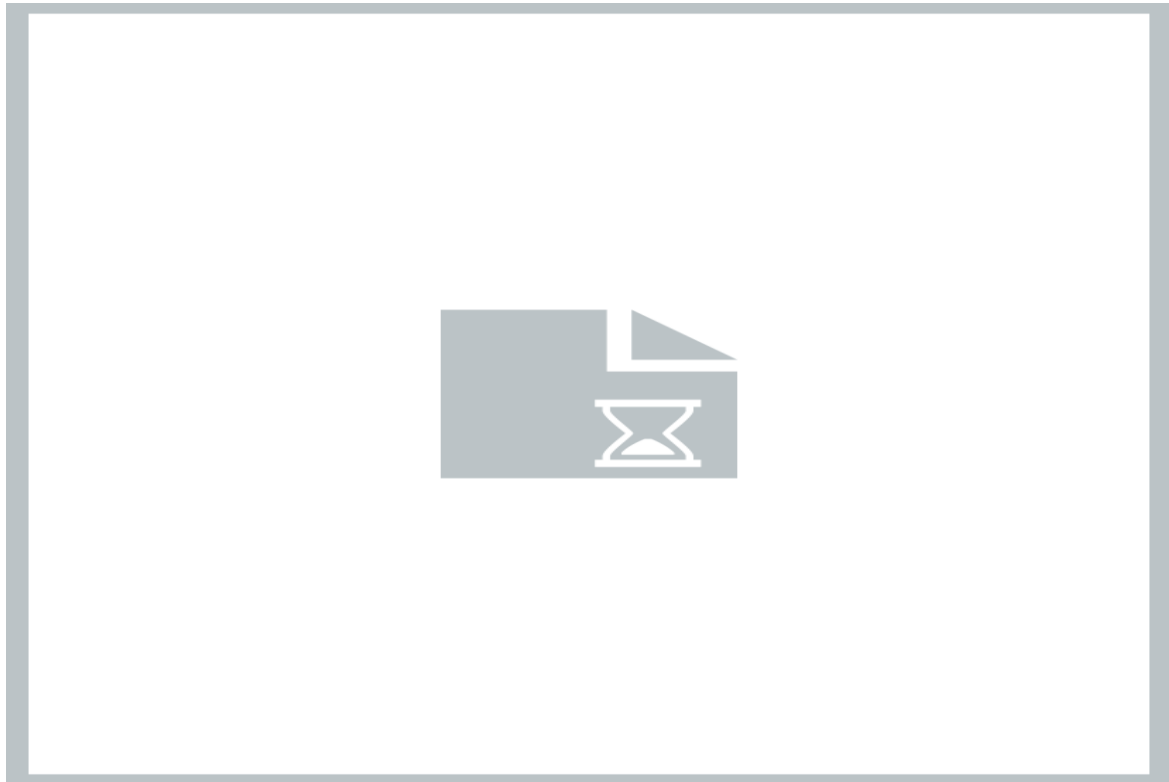
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [<=]  
angeführten Inhalte.

---

## **2 Systemüberblick**

---



**Abbildung 1: Systemzerlegung tokenbasierte Authentisierung**



**Abbildung 2 Systemzuordnung zu Architekturzonen**



## **2.1 Akteure und Rollen**

Viele der in diesem Dokument verwendeten (und in diesem Kapitel erläuterten) Begriffe wurden aus relevanten Webservice-Standards übernommen.

### **2.1.1 Nutzer**

Als Nutzer treten Mitarbeiter von Organisationen auf, die über eine SMC-B verfügen. Die Nutzer der TI (auch: Benutzer) verwenden die tokenbasierte Authentisierung, um sich gegenüber Diensten zu authentisieren. IDPs stellen den Nutzern Identitätsbestätigungen aus. Technisch treten Nutzer mittels ihrer Clients in Aktion.

### **2.1.2 Client**

Clients sind Clientsysteme in der Consumer Zone. Die Nutzer verwenden als Client entweder einen Webbrowser (auch als „passive client“ bezeichnet), der kein SOAP-Protokoll implementiert, oder einen nativen Client (auch als „active client“ bezeichnet), der SOAP und WS\*-Spezifikationen implementiert hat und selbständig Identitätsbestätigungen anfordern und verarbeiten kann.

Bei der Verwendung eines nativen Clients ist dies das System, welches Identitätsbestätigungen anfordert.

### **2.1.3 Dienste**

Bei der Verwendung von Webbrowsern ist der Dienst das System, welches Identitätsbestätigungen anfordert (die Anforderung wird über den Client an einen IDP geleitet). Bei der Verwendung aktiver Clients rufen diese die Security Policy des Diensts zur Auswertung ab. Der Dienst prüft die erhaltenen Identitätsbestätigungen zur Authentifizierung der Nutzer. Über die Autorisierung der eigentlichen fachlichen Transaktion entscheidet der Dienst z.B. anhand von Rollen- und weiterer Identitätsinformationen in der Identitätsbestätigung des aufrufenden Nutzers.

### **2.1.4 Identitätsbestätigung**

Identitätsbestätigungen (auch: Sicherheitstoken, Security Token, SAML-Assertion) sind XML-Daten (konkret: SAML 2.0) die die Identität des Nutzers bestätigen. Sie enthalten Informationen die seine Identität beschreiben (z.B. Name, ID), können auch weitere Informationen wie z.B. Rollen enthalten, und sind von dem herausgebenden Identity Provider (IDP) signiert, um die Authentizität des Ausstellers und die Integrität der Identitätsbestätigung zu gewährleisten.

### **2.1.5 Identity Provider (IDP)**

IDPs kann es in unterschiedlichen Ausprägungen geben, die im Folgenden erläutert werden. Gemeinsam ist ihnen, dass sie Benutzern Identitätsbestätigungen ausstellen.

Es ist grundsätzlich möglich, mehrere IDPs so zu kombinieren, dass sie ein föderiertes Gesamtsystem ergeben. Vorgaben und Festlegungen werden dazu in diesem Dokument nicht getroffen.

### **2.1.5.1 Lokaler Identity Provider**

Der lokale Identity Provider ist ein System in der Consumer Zone. Es verfügt über eine Benutzerdatenbank, authentifiziert Nutzer mittels geeigneter, aber hier nicht näher festgelegter Authentisierungsmittel und stellt ihnen entsprechende Identitätsbestätigungen aus. Diese werden mit dem für tokenbasierte Authentisierung verwendeten Schlüsselmaterial der SM-B signiert. Die in der Identitätsbestätigung enthaltenen Aussagen über den Nutzer (sog. Behauptungen) können durch den lokalen IDP festgelegt werden.

### **2.1.5.2 Providerseitiger Identity Provider**

Ein oder mehrere Identity Provider in der Provider Zone der TI können in folgenden Varianten auftreten, sind jedoch für die Nutzung von TBAuth nicht zwingend erforderlich:

- Sie authentifizieren Nutzer unter Zuhilfenahme beliebiger geeigneter Authentisierungsverfahren selber. Dieser Fall wird in diesem Dokument nicht weiter betrachtet.
- Sie sind einem Dienst zugeordnet und delegieren (indirekt über den Client) die Authentisierung an den lokalen IDP oder an den BD-TBAuth (siehe nächsten Abschnitt). Der providerseitige IDP verwendet die lokal ausgestellte Identitätsbestätigung zur Authentifizierung des Nutzers gegenüber dem zugeordneten Dienst. Dieser Fall wird auch als föderiertes Identitätsmanagement bezeichnet.
- Sie delegieren (indirekt über den Client) die Authentisierung an den lokalen IDP oder an den BD-TBAuth. In diesem Fall nehmen die providerseitigen IDPs die lokal ausgestellte Identitätsbestätigung als Basis und reichern diese durch eigene Attribute an. Die so angereicherten Identitätsbestätigungen werden weitergeleitet und z.B. von einem (nicht näher zugeordneten) Dienst zur Authentifizierung verwendet. Dieser Fall wird in diesem Dokument nicht weiter betrachtet. Dieser Fall wird auch als föderiertes Identitätsmanagement bezeichnet.

### **2.1.6 Basisdienst tokenbasierte Authentisierung (BD-TBAuth)**

Der Basisdienst tokenbasierte Authentisierung (BD TBAuth) ist Bestandteil des Konnektors. Es stellt einen IDP dar, indem es Nutzer authentifiziert und ihnen (bzw. ihren Clients) Identitätsbestätigungen ausstellt. Diese signiert der BD-TBAuth mittels dem für tokenbasierte Authentisierung verwendeten Schlüsselmaterial der SM-B.

## **2.2 Nachbarsysteme**

### **2.2.1 Konnektor**

Der Basisdienst TBAuth ist integraler Bestandteil des Konnektors. Das Nachbarsystem auf der logischen Ebene ist der Anwendungskonnektor als einbettende Komponente.

### **2.2.2 Karten**

Im Kontext von TBAuth wird ausschließlich die Karte SM-B (also SMC-B bzw. HSM-B) verwendet.

## **2.3 Weiterer Begriff: Security Token Service (STS)**

Die häufig im Umfeld von WS-Trust und WS-Security verwendete Bezeichnung Security Token Service (STS) wird in dieser Spezifikation nicht verwendet. Stattdessen wird von Identity Provider gesprochen der die Funktionalität eines STS umfassen kann. Eine entsprechende Festlegung des jeweiligen IDP erfolgt jedoch nicht über diese Begrifflichkeiten, sondern über die Funktionsbeschreibung.

---

## **3 Übergreifende Festlegungen**

---

### **3.1 Anforderung von Identitätsbestätigungen**

#### **GS-A\_5492 - Geltungsbereich von Identitätsbestätigungen**

Systeme, die Identitätsbestätigungen anfordern, **MÜSSEN** deren Geltungsbereich auf den jeweilig zu verwendenden Dienst einschränken.

[<=]

Für unterschiedliche Nutzer und für unterschiedliche Dienste können unterschiedliche Sicherheitsanforderungen gelten.

#### **GS-A\_5493 - Zeitstempel für Identitätsbestätigungen**

Systeme, die Identitätsbestätigungen anfordern, **MÜSSEN** einen aktuellen Zeitstempel sowie einen Verfallszeitpunkt übergeben, der den jeweiligen Sicherheitsanforderungen genügt.

[<=]

### **3.2 Prüfung von Identitätsbestätigungen**

#### **GS-A\_5505 - Vorgaben für Identitätsbestätigungen**

Systeme, die vom Basisdienst TBAuth ausgestellte (Issuer „IDP TI-Plattform“) Identitätsbestätigungen prüfen, **MÜSSEN** sicherstellen, dass diese konform zu den Vorgaben in TAB\_TBAuth\_03 Identitätsbestätigung (SAML 2.0 Assertion), TAB\_TBAuth\_04 RequestSecurityTokenResponse und TAB\_TBAuth\_05 RequestSecurityTokenResponseCollection sind.

[<=]

Wenn Identitätsbestätigungen mit dem für tokenbasierte Authentisierung verwendeten Schlüsselmaterial auf der SM-B signiert und gültig sind, dann kann anhand des Elements `/saml2:Assertion/saml2:Issuer` erkannt werden, ob es vom IDP des Konnektors oder von einem lokalen IDP ausgestellt wurde. Wenn der Issuer „IDP TI-Plattform“ lautet, wurde die Identitätsbestätigung über die Schnittstellen `I_IDP_Auth_Active_Client` oder `I_IDP_Auth_Passive_Client` (durch den Basisdienst TBAuth des Konnektors) ausgestellt. Wenn der Issuer anders lautet und gleichzeitig die Identitätsbestätigung durch einen für tokenbasierte Authentisierung verwendeten Schlüssel der SM-B signiert wurde, wurde die Identitätsbestätigung durch einen lokalen IDP ausgestellt.

Je nach Anwendungsfall können Dienste Identitätsbestätigungen aus dem gesamten TI-Vertrauensraum akzeptieren oder nur von einzelnen IDPs, mit denen sie z.B. ein direktes Vertragsverhältnis unterhalten. Letztere müssten ggf. in dem Dienst als vertrauenswürdig konfiguriert werden. Eine solche Konfiguration bzw. Berechtigung ist nicht Gegenstand der hier beschriebenen Leistung sondern liegt in der Hoheit des Diensts.

#### **GS-A\_5494 - Prüfung des berechtigten IDP/Issuers**

Systeme, die Identitätsbestätigungen prüfen, **MÜSSEN** sicherstellen, dass sie nur Identitätsbestätigungen akzeptieren, die von vorab berechtigten IDP/Issuer ausgestellt wurden.

[<=]

#### **A\_15556 - Identitätsbestätigungen - Prüfung der Signatur**

Systeme, die Identitätsbestätigungen prüfen, MÜSSEN die Gültigkeit der Signatur im Element `/saml2:Assertion/ds:Signature` prüfen. [ $\leq$ ]

#### **A\_15557 - Identitätsbestätigungen - Prüfung des Signaturzertifikates**

Systeme, die Identitätsbestätigungen prüfen, MÜSSEN das zur Signatur verwendete Zertifikat (des Issuers) im Element `/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate` auf Gültigkeit zum aktuellen Zeitpunkt prüfen. Die Prüfung MUSS gemäß TUC\_PKI\_018 [gemSpec\_PKI] im Prüfmodus OCSP erfolgen. [ $\leq$ ]

#### **A\_15637 - Identitätsbestätigungen - Prüfung der zeitlichen Gültigkeit**

Systeme, die Identitätsbestätigungen prüfen, MÜSSEN Identitätsbestätigungen ablehnen, falls der Prüfzeitpunkt nicht im Zeitraum zwischen `/saml2:Assertion/saml2:Conditions/@NotBefore` und `/saml2:Assertion/saml2:Conditions/@NotOnOrAfter` liegt. [ $\leq$ ]

#### **GS-A\_5495 - Geltende Security Policy**

Systeme, die Identitätsbestätigungen prüfen, MÜSSEN folgende Policy durchsetzen:

```
<wsp:Policy wsu:Id="Transport_policy" xmlns:wsp="http://www.w3.org/ns/ws-policy">
  <wsp:ExactlyOne>
    <wsp:All>
      <wsap10:UsingAddressing/>
      <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702">
        <wsp:Policy>
          <sp:TransportToken>
            <wsp:Policy>
              <sp:HttpsToken/>
            </wsp:Policy>
          </sp:TransportToken>
          <sp:AlgorithmSuite>
            <wsp:Policy>
              <sp:Basic256Sha256/>
            </wsp:Policy>
          </sp:AlgorithmSuite>
          <sp:Layout>
            <wsp:Policy>
              <sp:Lax/>
            </wsp:Policy>
          </sp:Layout>
          <sp:IncludeTimestamp/>
        </wsp:Policy>
      </sp:TransportBinding>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
```

[ $\leq$ ]

### **3.3 Annullieren von Identitätsbestätigungen**

Die Reichweite der Annullierung von Identitätsbestätigungen beschränkt sich auf den ausstellenden IDP, wodurch die Erneuerung bestehender Identitätsbestätigungen unterbunden wird. Bestehende Sitzungen und die Verwendung bereits ausgestellter Identitätsbestätigungen gegenüber etwaigen anderen Systemen werden hierdurch nicht berührt. Daher sollen bei einer Annullierung zusätzlich z.B. Kopien der Identitätsbestätigung verworfen werden und Sitzungen geschlossen werden.

**GS-A\_5496 - Unberechtigte Authentisierung nach Annullierung verhindern**

Systeme, die Identitätsbestätigungen mittels der Operation `I_IDP_Auth_Active_Client::cancel_Identity_Assertion` oder `I_IDP_Auth_Passive_Client::signOut` annullieren, MÜSSEN sicherstellen, dass eine erfolgreiche Authentisierung mit der annullierten Identitätsbestätigung nicht mehr möglich ist.

[<=]

### **3.4 Verwendete Standards**

Die Architektur der tokenbasierten Authentisierung orientiert sich an EFA 2.0 und basiert auf dazu kompatiblen Technologien und Standards.

**GS-A\_5497 - Verwendung von WS-Trust 1.3**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, MÜSSEN den Standard [WS-Trust1.3] unterstützen.

[<=]

**GS-A\_5498 - optionale Verwendung von WS-Trust 1.4**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, KÖNNEN den Standard [WS-Trust1.4] unterstützen.

[<=]

**GS-A\_5499 - Konformität zu WS-I Basic Profile 1.2**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, MÜSSEN den Standard [BasicProfile1.2] unterstützen.

Abweichend von R1012 in [BasicProfile1.2] MUSS nur das Character Encoding UTF-8 unterstützt werden.

[<=]

**GS-A\_5500 - Verwendung von WS-Security Policy 1.3 und WS-I Basic Security Profile 1.1**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, MÜSSEN die Standards [WS-SecurityPolicy1.3] und [BasicSecurityProfile1.1] unterstützen.

[<=]

Abweichend von [BasicProfile1.2], [WS-SecurityPolicy1.3] und [BasicSecurityProfile1.1] dürfen ausschließlich die laut [gemSpec\_Krypt] zulässigen Algorithmen, Protokolle und sonstigen Vorgaben unterstützt werden.

**GS-A\_5501 - Verwendung von SAML 2.0**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, MÜSSEN Identitätsbestätigungen im Format SAML 2.0 Assertions [SAML2.0] unterstützen.

[<=]

**GS-A\_5502 - Ausstellung im Format SAML 2.0**

Systeme, die Identitätsbestätigungen ausstellen, MÜSSEN diese im Format SAML 2.0 Assertions [SAML2.0] ausstellen.

[<=]

**GS-A\_5503 - Verwendung von WS-Federation 1.2**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, MÜSSEN den Standard [WS-Federation1.2] unterstützen.

[<=]

**GS-A\_5504 - Geltende Präfixe und Namensräume**

Systeme, die tokenbasierte Authentisierung nutzen oder anbieten, **MÜSSEN** die Präfixe und Namensräume entsprechend TAB\_TBAuth\_01 Präfixe und Namensräume verwenden.  
[<=]

## 4 Informationsmodell

### 4.1 Namensräume

**Tabelle 1: TAB\_TBAuth\_01 Präfixe und Namensräume**

Präfix	Namensraum
ds	http://www.w3.org/2000/09/xmldsig#
ec	http://www.w3.org/2001/10/xml-exc-c14n#
saml2	urn:oasis:names:tc:SAML:2.0:assertion
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
xsi	http://www.w3.org/2001/XMLSchema-instance

### 4.2 Behauptungen in Identitätsbestätigungen

In ihren Behauptungen unterscheiden sich Identitätsbestätigungen für Personen ggü. denen für Institutionen. Für beide Arten von Identitätsbestätigungen wird eine Liste der möglichen Behauptungen dargestellt. Im Basisdienst TBAuth werden nur Identitätsbestätigungen für Institutionen unterstützt.

Der Basisdienst TBAuth entnimmt sämtliche in der ausgestellten Identitätsbestätigung enthaltenen Informationen über den Benutzer (sog. Claims, Behauptungen) aus dem zugrundeliegenden Authentisierungs-Zertifikat C.HCI.OSIG der SM-B. Da einige Attribute optional sind, übernimmt der Basisdienst TBAuth im konkreten Fall möglichst viele der in Tabelle 2: TAB\_TBAuth\_02\_1 Behauptungen für Institutionen aufgeführten Attribute in die Identitätsbestätigung.

Um eine Interoperabilität zu möglichst vielen Drittsystemen zu erreichen, verwendet der Basisdienst TBAuth lediglich die von [IDMI1.0] spezifizierten Behauptungen. Zusätzlich werden die zwei Behauptungen „name“ und „nameidentifizier“ aus [MSClaimTypes] verwendet, da sie für den Informationswert der Identitätsbestätigung wichtig sind.

Folglich sind in den Identitätsbestätigungen insbesondere keine Informationen über Art der Organisation/Einrichtung des Gesundheitswesens enthalten.

Andere IDPs, als der BD-TBAuth, können zusätzliche Behauptungen verwenden, die hier mit ausgewiesen werden.



**Tabelle 2: TAB\_TBAuth\_02\_1 Behauptungen für Institutionen**

Behauptung	Optional?	TBAuth	Attribut im Zertifikat	AttributValue
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	nein	x	commonName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	ja	x	givenName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	ja	x	surname	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress</a>	ja	x	streetAddress	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode</a>	ja	x	postalCode	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality</a>	ja	x	localityName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince</a>	ja	x	stateOrProvinceName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country</a>	nein	x	countryName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>	nein	x	RegistrationNumber (Telematik-ID)	Aus Zertifikat
urn:gematik:subject:organization-id	ja	-	RegistrationNumber (Telematik-ID)	InstanceIdentifier @extension [Telematik-ID] @root 1.2.276.0.76.4.188
urn:gematik:subject:authreference	ja	-	serialNumber	Aus Zertifikat

Für personenbezogene Identitätsbestätigungen gelten nachfolgende Behauptungen.  
Der Basisdienst TBAuth unterstützt diese Identitätsbestätigungen nicht.

**Tabelle 3: TAB\_TBAuth\_02\_2 Behauptungen für Personen**

Behauptung	Optional?	TBAuth	Attribut im Zertifikat	AttributValue
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	nein	-	commonName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	nein	-	givenName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</a>	nein	-	surname	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country</a>	nein	-	countryName	Aus Zertifikat
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>	nein	-	unveränderlicher Anteil der KVNR oder Registrationnummer (Telematik-ID)	Aus Zertifikat
urn:gematik:subject:subject-id	ja	-	unveränderlicher Anteil der KVNR  oder  Registrationnummer (Telematik-ID)	InstanceIdentifier @extension [KVNR] @root 1.2.276.0.76.4.8  oder InstanceIdentifier @extension [Telematik-ID] @root 1.2.276.0.76.4.188
urn:gematik:subject:authreference	ja	-	serialNumber	Aus Zertifikat

## 4.3 Identitätsbestätigung

**Tabelle 4: TAB\_TBAuth\_03 Identitätsbestätigung (SAML 2.0 Assertion)**

<b>Name des Rückgabewerts</b>	<b>Verpflichtung</b>	<b>zusätzliche Konsistenzregel</b>
/saml2:Assertion	erforderlich	
/saml2:Assertion /@ID	erforderlich	
/saml2:Assertion /@IssueInstant	erforderlich	
/saml2:Assertion /@Version	erforderlich	Der Wert des Parameters MUSS wie folgt sein: 2.0
/saml2:Assertion /@xsi:type	erforderlich	Der Wert des Parameters MUSS wie folgt sein: saml2:AssertionType
/saml2:Assertion /saml2:Issuer	erforderlich	
/saml2:Assertion /ds:Signature	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:CanonicalizationMethod	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:CanonicalizationMethod /@Algorithm	erforderlich	Der Wert des Parameters MUSS wie folgt sein:  <a href="http://www.w3.org/2001/10/xml-exc-c14n#">http://www.w3.org/2001/10/xml-exc-c14n#</a>

Name des Rückgabewerts	Verpflichtung	zusätzliche Konsistenzregel
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:SignatureMethod	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:SignatureMethod /@Algorithm	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /@URI	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:Transforms	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:Transforms /ds:Transform	erforderlich	

Name des Rückgabewerts	Verpflichtung	zusätzliche Konsistenzregel
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:Transforms /ds:Transform /@Algorithm	erforderlich	Der Wert des Parameters MUSS wie folgt sein:  <a href="http://www.w3.org/2000/09/xmldsig#enveloped-signature">http://www.w3.org/2000/09/xmldsig#enveloped-signature</a>
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:Transforms /ds:Transform /@Algorithm	erforderlich	Der Wert des Parameters MUSS wie folgt sein:  <a href="http://www.w3.org/2001/10/xml-exc-c14n#">http://www.w3.org/2001/10/xml-exc-c14n#</a>
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:Transforms /ds:Transform /@Algorithm='http://www.w3.org/2001/10/xml-exc-c14n#'  /ec:InclusiveNamespaces /@PrefixList	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:DigestMethod	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:DigestMethod /@Algorithm	erforderlich	

Name des Rückgabewerts	Verpflichtung	zusätzliche Konsistenzregel
/saml2:Assertion /ds:Signature /ds:SignedInfo /ds:Reference /ds:DigestValue	erforderlich	
/saml2:Assertion /ds:Signature /ds:SignatureValue	erforderlich	
/saml2:Assertion /ds:Signature /ds:KeyInfo	erforderlich	
/saml2:Assertion /ds:Signature /ds:KeyInfo /ds:X509Data	erforderlich	
/saml2:Assertion /ds:Signature /ds:KeyInfo /ds:X509Data /ds:X509Certificate	erforderlich	
/saml2:Assertion /saml2:Subject	erforderlich	
/saml2:Assertion /saml2:Subject /saml2:NameID	erforderlich	
/saml2:Assertion /saml2:Subject /saml2:NameID /@Format	erforderlich	Der Wert des Parameters MUSS wie folgt sein:  urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation	erforderlich	

<b>Name des Rückgabewerts</b>	<b>Verpflichtung</b>	<b>zusätzliche Konsistenzregel</b>
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation ation /@Method	erforderlich	Der Wert des Parameters <b>MUSS</b> wie folgt sein:  urn:oasis:names:tc:SAML: 2.0:cm:hol der-of-key oder  urn:oasis:names:tc:SAML: 2.0:cm:be arer
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation ation	nur bei urn:oasis:names:tc:SAML: 2.0:cm:hol der-of-key <b>erforderlich</b>	
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation ation  /saml2:SubjectConfirmationData	nur bei urn:oasis:names:tc:SAML: 2.0:cm:hol der-of-key <b>erforderlich</b>	
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation ation  /saml2:SubjectConfirmationData /@xsi:type	nur bei urn:oasis:names:tc:SAML: 2.0:cm:hol der-of-key <b>erforderlich</b>	Der Wert des Parameters <b>MUSS</b> wie folgt sein:  saml2:KeyInfoConfirmationData DataType
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation ation  /saml2:SubjectConfirmationData /ds:KeyInfo	nur bei urn:oasis:names:tc:SAML: 2.0:cm:hol der-of-key <b>erforderlich</b>	

Name des Rückgabewerts	Verpflichtung	zusätzliche Konsistenzregel
/saml2:Assertion /saml2:Subject  /saml2:SubjectConfirmation  /saml2:SubjectConfirmationData /ds:KeyInfo /ds:KeyValue	nur bei urn:oasis:names:tc:SAML:2.0:cm:holder-of-key erforderlich	
/saml2:Assertion /saml2:Conditions	erforderlich	
/saml2:Assertion /saml2:Conditions /@NotBefore	erforderlich	
/saml2:Assertion /saml2:Conditions /@NotOnOrAfter	erforderlich	
/saml2:Assertion /saml2:Conditions  /saml2:AudienceRestriction	erforderlich	
/saml2:Assertion /saml2:Conditions  /saml2:AudienceRestriction /saml2:Audience	erforderlich	Dieser Parameter MUSS die URI des Dienstes enthalten, für den die Identitätsbestätigung gültig ist. Dieser Parameter KANN mehrmals enthalten sein.
/saml2:Assertion /saml2:AuthnStatement	erforderlich	
/saml2:Assertion /saml2:AuthnStatement /@AuthnInstant	erforderlich	Dieser Parameter MUSS den Zeitpunkt der Erstellung der Identitätsbestätigung enthalten.



<b>Name des Rückgabewerts</b>	<b>Verpflichtung</b>	<b>zusätzliche Konsistenzregel</b>
/saml2:Assertion /saml2:AuthnStatement /saml2:AuthnContext	erforderlich	
/saml2:Assertion /saml2:AuthnStatement /saml2:AuthnContext  /saml2:AuthnContextClassRef	erforderlich	Der Wert des Parameters MUSS wie folgt sein:  urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard oder  urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI oder  urn:oasis:names:tc:SAML:2.0:ac:classes:X509
/saml2:Assertion  /saml2:AttributeStatement	erforderlich	Dieser Parameter MUSS die in "TAB_TBAuth_02_1 Behauptungen für Institutionen" oder "TAB_TBAuth_02_2 Behauptungen für Personen" definierten Behauptungen enthalten, sofern sie aus dem zugrundeliegenden Zertifikat entnommen werden können.

## 4.4 Antworten mit Identitätsbestätigungen

In diesem Abschnitt sind Antworten definiert, wie sie von I\_IDP\_Auth\_Active\_Client und I\_IDP\_Auth\_Passive\_Client umgesetzt werden.

**Tabelle 5: TAB\_TBAuth\_04 RequestSecurityTokenResponse**

<b>Name des Rückgabewerts</b>	<b>Verpflichtung</b>	<b>zusätzliche Konsistenzregel</b>
/wst:RequestSecurityTokenResponse	erforderlich	
/wst:RequestSecurityTokenResponse /wst:TokenType	erforderlich	Der Wert des Parameters MUSS wie folgt sein: <a href="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</a>
/wst:RequestSecurityTokenResponse /wst:RequestedSecurityToken	erforderlich	
/wst:RequestSecurityTokenResponse /wst:RequestedSecurityToken /saml2:Assertion	erforderlich	Dieser Parameter MUSS die in Tabelle 3: TAB_TBAuth_03 Identitätsbestätigung definierte Identitätsbestätigung enthalten
/wst:RequestSecurityTokenResponse /wst:Lifetime	erforderlich	Alle Systeme, die Identitätsbestätigungen prüfen, MÜSSEN Identitätsbestätigungen ablehnen, falls deren Erstellungsdatum unterschritten oder deren Ablaufzeitpunkt überschritten ist.
/wst:RequestSecurityTokenResponse /wst:Lifetime /wsu:Created	erforderlich	
/wst:RequestSecurityTokenResponse /wst:Lifetime /wsu:Expires	erforderlich	

**Tabelle 6: TAB\_TBAuth\_05 RequestSecurityTokenResponseCollection**

<b>Name des Rückgabewerts</b>	<b>Verpflichtung</b>	<b>zusätzliche Konsistenzregel</b>
/wst:RequestSecurityTokenResponseCollection	erforderlich	Dieser Parameter MUSS ein einziges RequestSecurityTokenResponse-Element enthalten.
/wst:RequestSecurityTokenResponseCollection /wst:RequestSecurityTokenResponse	erforderlich	Dieser Parameter MUSS die in Tabelle 4: TAB_TBAuth_04 RequestSecurityTokenResponse definierte Identitätsbestätigung enthalten

Entsprechend WS-Trust lautet bei Active Requestor Profile für zurückgegebene RequestSecurityTokenResponseCollection die Action <http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal>.

---

## 5 Anhang A – Verzeichnisse

---

### 5.1 Abkürzungen

Kürzel	Erläuterung
BD	Basisdienst
BD-TBAuth	Basisdienst tokenbasierte Authentisierung
IDP	Identity Provider (eine Teilkomponente eines IAM)
SAML	Security Assertion Markup Language
STS	Security Token Service
WS	Webservice

### 5.2 Glossar

Das Glossar erläutert Begriffe dieser Spezifikation, welche nicht in [gemKPT\_Arch\_TIP] oder [gemGlossar] erläutert sind.

Begriff	Erläuterung
HSM-B	Hardware Security Module Typ B
Identity Provider (IDP)	Die Begriffe Security Token Service und Identity Provider werden synonym verstanden. Der besseren Verständlichkeit wegen wird auf den Begriff Security Token Service weitestgehend verzichtet sondern stattdessen einheitlich Identity Provider verwendet.
Security Token Service (STS)	Die Begriffe Security Token Service und Identity Provider werden synonym verstanden. Der besseren Verständlichkeit wegen wird auf den Begriff Security Token Service weitestgehend verzichtet, sondern stattdessen einheitlich Identity Provider verwendet.
SM-B	Oberbegriff für SMC-B und HSM-B

## 5.3 Abbildungsverzeichnis

Abbildung 1: Systemzerlegung tokenbasierte Authentisierung .....	8
Abbildung 2 Systemzuordnung zu Architekturzonen .....	8

## 5.4 Tabellenverzeichnis

Tabelle 1: TAB_TBAuth_01 Präfixe und Namensräume .....	16
Tabelle 2: TAB_TBAuth_02_1 Behauptungen für Institutionen .....	17
Tabelle 3: TAB_TBAuth_02_2 Behauptungen für Personen .....	18
Tabelle 4: TAB_TBAuth_03 Identitätsbestätigung (SAML 2.0 Assertion) .....	19
Tabelle 5: TAB_TBAuth_04 RequestSecurityTokenResponse .....	26
Tabelle 6: TAB_TBAuth_05 RequestSecurityTokenResponseCollection .....	27

## 5.5 Referenzierte Dokumente

### 5.5.1 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 jeweils gültige Versionsnummer ist in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

<b>[Quelle]</b>	<b>Herausgeber: Titel</b>
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzeption Architektur TI der Plattform
[gemSpec_Kon_TBAuth]	Spezifikation I Konnektor Basisdienst tokenbasierte Authentisierung
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

[Quelle]	Herausgeber: Titel
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI

## 5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BasicProfile1.2]	WS-I Basic Profile Version 1.2 <a href="http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html">http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html</a>
[BasicSecurityProfile1.1]	OASIS Basic Security Profile Version 1.1 <a href="https://docs.oasis-open.org/ws-brsp/BasicSecurityProfile/v1.1/BasicSecurityProfile-v1.1.html">https://docs.oasis-open.org/ws-brsp/BasicSecurityProfile/v1.1/BasicSecurityProfile-v1.1.html</a>
[IDMI1.0]	Identity Metasystem Interoperability Version 1.0 <a href="https://docs.oasis-open.org/imi/identity/v1.0/identity.html">https://docs.oasis-open.org/imi/identity/v1.0/identity.html</a>
[MSClaimTypes]	Microsoft ClaimTypes Members <a href="https://msdn.microsoft.com/en-us/library/microsoft.identitymodel.claims.claimtypes_members.aspx">https://msdn.microsoft.com/en-us/library/microsoft.identitymodel.claims.claimtypes_members.aspx</a>
[SAML2.0]	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 <a href="http://docs.oasis-open.org/security/saml/v2.0/">http://docs.oasis-open.org/security/saml/v2.0/</a>
[WS-Federation1.2]	OASIS Web Services Federation Language (WS-Federation) Version 1.2 <a href="https://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html">https://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html</a>
[WS-SecurityPolicy1.3]	OASIS WS-SecurityPolicy 1.3 <a href="https://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html">https://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/errata01/ws-securitypolicy-1.3-errata01-complete.html</a>
[WS-Trust1.3]	WS-Trust 1.3 <a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf">http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf</a>
[WS-Trust1.4]	WS-Trust 1.4 <a href="http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf">http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf</a>

## 6 Anhang B

### 6.1 Beispiel

Im folgenden Beispiel wird WS-Trust 1.4 verwendet, welches abwärtskompatibel zu WS-Trust 1.3 ist.

#### Beispiel

```
<ns2:RequestSecurityTokenResponseCollection 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:RequestSecurityTokenResponse>  
    <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="_bee0a6d5-e96b-40e0-b8bc-  
59d923741920" IssueInstant="2016-08-29T07:20:33.195Z" 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="#_bee0a6d5-e96b-40e0-b8bc-59d923741920">  
              <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>1NQzrWgBjGRQbkry0BXUyupHmUefvxazw5Iws5zB  
kRDs=</ds:DigestValue>  
          </ds:Reference>  
        </ds:SignedInfo>  
      </ns2:RequestedSecurityToken>  
    </ns2:RequestSecurityTokenResponse>  
  </ns2:RequestSecurityTokenResponseCollection>
```

```
<ds:SignatureValue>DAXFFk/Z97rMniFVBhK0VagwQLy992Eh4e+9tqsgs4zb
5B4YqNlnCvXHTHm0DoH25Wi3RNwkJh4Ehqt3QHkjt3Z8PgUDLRKtkXSaGwffc9QSp8SM/uXjwQl0gSS+wxj
+K7LUSJYlorthboN3lJv9hjqpJiNLhKxb7IzNMufKocEWWb9E42/dE8MFDuGqwbyE88DieFTo3BQGkwGOlQ
X07JHQZZKH6pHskzyCg6HOvrBZqIpuryFP935Dh2c9MlMlXcelbqxmc+dxr+ho/hnHWFPIuM5/0rXQ6ZwoH
82GT6+/eVV4HPNL8jSSyAir48V/EsZOLdOiaCiPl1FW9fGMiw==</ds:SignatureValue>

<ds:KeyInfo>

<ds:X509Data>

<ds:X509Certificate>MIIFEzCCA/ugAwIBAgIHA8zEnhRtVTANBgk
qhkiG9w0BAQsFADCBMTELMAkGA1UEBhMCREUxHzAd
BgNVBAoMFmdlbWw0aWsgR2liSCBOT1QtVkFMSUQxSDBGBgNVBAsMP0luc3RpdHV0aW9uIGRlcyBH
ZXNlbnRoZWl0c3dlc2Vucy1DQSBkZXIvGvGvZWlhdGlrZW5mcmFzdHJ1a3RlcjEfmB0GA1UEAwW
R0VNLlNNQ0ItQ0E3IFRFRU1QtT05MWTAEfW0xNTA2MzAwMDAwMDBaFw0yMDA2MzAwMDAwMDBAIH
MQswCQYDVQQGEWJERTEYMBYGA1UECAwPQmVpc3BpZWxzZD0+/vWR0MRgwFgYDVQQHDA9CZWlzcGll
bHN077+9ZHQxDjAMBgNVBBEMBTaxMjM0MRswGQYDVQQJDBJHZN1bnRoZWl0c2dhc3NlIDMxDzAN
BgNVBAUTBjEwMDAwMTFGMEQGA1UEAw9S3JhbmthbmhhdXMgQmVpc3BpZWxzZD0+/vWR0LUtsaW5p
ayBm77+9ciBLYXJkaW9sb2dpZVRFRU1QtT05MWTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAL/uetzxukiQQ4yd9gVyK5ZTgCrxxAH5ZlPoJcKOKo+oKZ5i/NpgjkXCBQl25gXuQJACkEjN
pa3E2JqOXLgwsLTZXVShc8v1b49DcbNPSDsWtN7NwF7RemmnP9aKunqehFNUicRABfGa0j4LAs
8eV3bqRg9y/+Cx6Y9GFr5ODfxLYs73HE7T1k7s9L7ufJtSfpm0FqZY5dkZk3a9jxbSJ3ovDBaL30
h3uKxTvBMU+przKZC/xf84KjJxm1+PGD7I5/NTCCX5w8uxKW/tNqQTFkhsArP4XdSIKiiyGXrAM
YBoa/oOlH/pF3LepfgHPXLfid5uOdT5+hpsou/UkvBUCAwEAAaOCAS4wggEgMB0GA1UdDgQWBQp
9vXBG9pPNsqBE1LNDe26RYztJzATBgNVHSUEDDAKBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMDoG
BSskCAMDBDEwLzAtMCswKTAhMA0MC0tyYW5rZW5oYXVzMAkGBYqCFAFABMDUTCzUtMkllLTmxNDE1
MB8GA1UdIwQYMBAAFDw5CIxOUpeco4wu+AhSBLSD2rnMCwGA1UdIAQlMCMwCgYIKoIUAwEgSMw
CQYHKoIUAwEgETAKBgqgghQATASBKjAOBgNVHQ8BAf8EBAMCBAAwSwYIKwYBBQUHAQEEPzA9MDsG
CCsGAQUFBzABhi9odHRwOi8vb2NzcC5wa2kudGVSZWlhdGlrLXRlc3Q6ODA4MC9DTU9DU1AvT0NT
UDANBgkqhkiG9w0BAQsFAAOCAQEAC9tRPAgRoamvei0eX5IiHmj/mt4zX9kvhNRe3HMBUYMnvV10
J4h7EaT8/PeXBCTBAuthri4xfqD+WDQhEayWYfsKL5GTfuzQXExgt0r5aZdH6V8kChXJ7JldKNiS7QH
rtlZOhY7qPLPdDyQs99Uy79h7Y+MsZh1sI/lwCSQ/Tl5uVgJTM8q+0xi49VHVzebsGHLRdWVAZA
W7DibaeP30G7r36nBfc5LBjM9MghL88Wgi/JPd4l09gQWfxRV0yiUlp9LQ+yU1AM13BesZ3Niu3q
vrHiTD0Y0QrOR2/AM4ETNPaoKc/ClzkyBZhng/B3cWdTncVuFWINmEDLGNmycyN0Pw==</ds:X509Certif
icate>

</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=#0c084865696e72696368,2.5.4.4=#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+Pj5yoYml1uayO2UUpCq69pZ
xWbhCco6Q7X4YaRQ+Zc3DGqKUU8U891/qt2hVe9yAjTe9btPKdC8gyidZi+/0Y+h19KGRA8GGrCbSQa8gMk
/9FJqJF42CqSZAAOAb2Z/sAZOe4bCiO1D1i2KAC+/cHUEy+RyX61ud7833GAdG0JxjcVTHg+kIDTASC16r5
KATsErPHmgjmFEamnCBRN9WTDymQxSGotQYFbdSgGTrPeoElI6McXOZN0VoqDQ+7G2OhGLxqyyA3gpT+j
s0j6j3jILdxTWGMBCEEKgg3kfoP2OqOwD0EIFQVnD2SamJham5O45n4tbrGPxw==</ds:Modulus>
      <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
  </ds:KeyValue>
</ds:KeyInfo>
</saml2:SubjectConfirmationData>
</saml2:SubjectConfirmation>
</saml2:Subject>
  <saml2:Conditions NotBefore="2016-08-29T07:20:33.341Z"
NotOnOrAfter="2016-08-29T07:50:33.341Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>urn:telematik:gesundheitsdatendienst:www:In
stanz23</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2016-08-29T07:20:33.290Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:
classes:SmartcardPKI</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    ...
  </saml2:AttributeStatement>
</saml2:Assertion>
</ns2:RequestedSecurityToken>
  <ns2:RequestedAttachedReference>
    <ns4:SecurityTokenReference xmlns:wssell="http://docs.oasis-
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
wssell: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">_bee0a6d5-e96b-40e0-b8bc-
59d923741920</ns4:KeyIdentifier>
    </ns4:SecurityTokenReference>
  </ns2:RequestedAttachedReference>
  <ns2:RequestedUnattachedReference>
```

```
<ns4:SecurityTokenReference xmlns:wss1="http://docs.oasis-  
open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"  
wss1: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">_bee0a6d5-e96b-40e0-b8bc-  
59d923741920</ns4:KeyIdentifier>  
</ns4:SecurityTokenReference>  
</ns2:RequestedUnattachedReference>  
<ns2:Lifetime>  
  <ns3:Created>2016-08-29T07:20:33.341Z</ns3:Created>  
  <ns3:Expires>2016-08-29T07:50:33.341Z</ns3:Expires>  
</ns2:Lifetime>  
</ns2:RequestSecurityTokenResponse>  
</ns2:RequestSecurityTokenResponseCollection>
```