Norm 410 – Security Token Service

Release und Version

Release 2

Version 2.5.0 (2.4.0) vom 25.04.2013, NAUS-Beschluss vom 14.06.2012

Status

Arbeitsentwurf vom 12.08.2008

Potenzielle Norm vom 28.08.2008

Vorgeschlagene Norm 08.10.2010

RFC Fristende am 12.01.2011

Offizielle Norm unveröffentlicht vom 27.01.2011

Editor

Geschäftsstelle BiPRO e.V.

Autoren

Dr. Dieter Ackermann, VOLKSWOHL BUND (dieter.ackermann@volkswohl-bund.de)

Dr. Günther vom Hofe, Continentale (guenter.vomhofe@continentale.de)

Dr. Thomas Kippenberg, NÜRNBERGER (thomas.kippenberg@nuernberger.de)

Dr. Torsten Schmale, inubit AG (ts@inubit.com)

Sören Chittka, VOLKSWOHL BUND (soeren.chittka@volkswohl-bund.de)

Carsten Baehr, VOLKSWOHL BUND (carsten.baehr@volkswohl-bund.de)

Markus Heussen, Unternehmensberatung (heussen@standardisierung.net)

Fabian Stolz, VOLKSWOHL BUND (fabian.stolz@volkswohl-bund.de)

Gegenstand der Norm

Die vorliegende Norm 410 definiert die Schnittstelle zur Implementierung eines Security-Token-Services (STS).

Voraussetzung

Norm 225 Release 2

Norm 260 Release 2

Norm 270 Release 2

Norm 280 Release 2

Hinweise zum Urheberrecht

Dieses Norm-Dokument, wie auch alle anderen damit im Zusammenhang stehenden Dokumente (z.B. technische Dateien, Datenmodell etc.) von BiPRO unterliegen dem Urheberrecht.

BiPRO-Normen und andere Dokumente stehen während ihrer Entwicklungs- und Qualitätssicherungsphase nur den Mitgliedern des BiPRO e.V. zur Nutzung und Anwendung zur Verfügung. Die Überlassung an diesen geschlossenen Empfängerkreis stellt keine Erstveröffentlichung, zu deren der BiPRO e.V. allein berechtigt ist, dar.

Die BiPRO-Normen werden nach erbrachtem Nachweis der Praxistauglichkeit und mit der Feststellung des Status "Offizielle Norm" (ON) für die allgemeine Veröffentlichung freigegeben (vgl. BiPRO Norm 100: Allgemeine Grundlagen der Normierung) und sodann von BiPRO der Öffentlichkeit als BiPRO-Norm einschließlich der dazugehörigen Dokumente über das vereinsöffentliche Normenportal von BiPRO zur Verfügung gestellt; es gelten die dort veröffentlichten jeweils aktuellen Nutzungsbedingungen www.bipro.net/nutzungsbedingungen.

Inhaltsverzeichnis

Einführung

Verwendete Standards

Grundlage des in dieser Norm spezifizierten Security-Token-Services (STS) sind die folgenden OASIS Spezifikationen.

- **WS-Security** (Version 1.1) Sicherheitsframework für Web Services
- **WS-Trust** (Februar 2005) Definition von Security-Token-Services
- **WS-SecureConversation** (Februar 2005) Abwicklung sicherer Sessions
- **WS-SecurityPolicies** (Juli 2005) Definition der Sicherheitsanforderungen

WS-Trust definiert einen Security-Token-Service und WS-SecureConversation das Verfahren, wie ein Sicherheitskontext-Token (Security Context Token) generiert und genutzt wird. Beide Spezifikationen sind sehr umfassend und wurden explizit als Baustein-System entworfen.

Abgrenzung

Diese Norm enthält lediglich die detaillierte technische Spezifikation der Schnittstelle eines STS im Sinne von BiPRO. Die Verfahren zur Einbindung des STS sind in Norm 260 beschrieben, die Erstellung von Sicherheitspolicies ist ebenfalls Teil der Norm 260.

Spezifikation

Template Definition

Im weiteren Verlauf werden folgende Variablen für Templates verwendet:

Variable	Wert
${X1}	Namespace WS-Trust: http://schemas.xmlsoap.org/ws/2005/02/trust
${X2}	Namespace WS-Policy : http://schemas.xmlsoap.org/ws/2004/09/policy

WSDL-Template für einen Security-Token-Service (STS)

Die verschiedenen Web Service-Funktionen, mit denen die von einem Provider im BiPRO-Umfeld angebotenen Authentifizierungsverfahren realisiert werden, DÜRFEN sich nur auf der untersten Ebene der Schnittstellenbeschreibung unterscheiden, nämlich hinsichtlich der Service-Endpoints. Sie lassen sich darum als Kommunikationsschnittstellen (↔ WSDL-Ports) eines einzigen STS realisieren, dessen WSDL-Beschreibung über drei message-Elemente, ein portType-Element, ein binding-Element und ein service-Element mit mehreren port-Elementen verfügt. Im Folgenden wird ein Template für eine solche WSDL-Beschreibung vorgestellt.

Alternativ DARF jedes Authentifizierungsverfahren in einem eigenen STS realisiert werden. Die WSDL-Beschreibungen dieser Services sind dann weitgehend identisch, da sie sich nur in den – jeweils einzigen – Port-Elementen unterschieden.

Um eine BiPRO-Konformität sicher zu stellen, MUSS die Beschreibung der STS-Schnittstelle unter Verwendung der allgemeinen Muster für WSDL Templates (siehe Norm 225) erfolgen.

wsdl:definitions

Dieses Template definiert den grundlegenden Aufbau der Schnittstellendatei und die relevanten Namensräume (siehe Norm 225).

wsp:Policy

Das Template zu diesem Abschnitt ist in Norm 260 definiert.

wsdl:types

Dieses Template definiert die Objekte und Datentypen, die vom Consumer an den STS oder vom STS an den Consumer übertragen werden können.

Das Template zu diesem Abschnitt wird analog zur Norm 225 gebildet. Entsprechend der verwendeten Spezifikationen werden mehrere externe Schemata importiert.

```
<wsdl:types>
	<xsd:schema version="1.0" xmlns="http://www.w3.org/2001/XMLSchema"
		xmlns:xsd="http://www.w3.org/2001/XMLSchema">
		<xsd:import namespace="${1}"
		schemaLocation="${1}/WS-Trust.xsd" />
	</xsd:schema>
	<xsd:schema version="1.0" xmlns="http://www.w3.org/2001/XMLSchema"
		xmlns:xsd="http://www.w3.org/2001/XMLSchema">
		<xsd:import namespace="${2}"
		schemaLocation="${2}/ws-policy.xsd" />
	</xsd:schema>
</wsdl:types>
```

wsdl:message

Dieses Template definiert die zwischen Consumer und STS zu übertragenden Daten. Hier erfolgt die Verknüpfung der Schnittstellen-Funktionen mit den in den XML-Schemata des Providers und der WS-Trust-Spezifikation definierten Nachrichten bzw. Objekten.

```
<wsdl:message name="RequestSecurityTokenRequest">
	<wsdl:part name="parameters" element="wst:RequestSecurityToken"/>
</wsdl:message>
<wsdl:message name="RequestSecurityTokenResponse">
	<wsdl:part name="parameters" element="wst:RequestSecurityTokenResponse"/>
</wsdl:message>
```

Eine Exception Message wird nicht definiert, da das Fehlerhandling entsprechend Norm 260 über SOAPFaults realisiert ist.

wsdl:portType

Dieses Template definiert die Eingangs-, Ausgangs- und Fehlernachrichten, die im Rahmen der STS-Funktion verwendet werden.

```
<wsdl:portType name="SecurityTokenServicePortType">
	<wsdl:operation name="RequestSecurityToken" parameterOrder="parameters">
		<wsdl:documentation>${3}</wsdl:documentation>
		<wsdl:input message="bipro:RequestSecurityTokenRequest"
			name="RequestSecurityTokenRequest"/>
		<wsdl:output message="bipro:RequestSecurityTokenResponse"
			name="RequestSecurityTokenResponse"/>
	</wsdl:operation>
</wsdl:portType>
```

Variable	Wert
${3}	Dokumentation der STS-Funktion. ACHTUNG: Diese fachliche Erläuterung wird möglicherweise innerhalb eines generischen Clients innerhalb der Benutzeroberfläche visualisiert.

Beispiel

```
<wsdl:portType name="SecurityTokenServicePortType">
	<wsdl:operation name="RequestSecurityToken" parameterOrder="parameters">
		<wsdl:documentation>
			Dieser Service gibt nach erfolgreicher Authentifizierung ein
			Security Token (Security Context Token) zurueck. Die
			Authentifizierung kann dabei entweder mit Benutzername und
			Passwort oder mit einem VDG-Ticket erfolgen.
		</wsdl:documentation>
		<wsdl:input message="bipro:RequestSecurityTokenRequest"
			name="RequestSecurityTokenRequest"/>
		<wsdl:output message="bipro:RequestSecurityTokenResponse"
			name="RequestSecurityTokenResponse"/>
	</wsdl:operation>
</wsdl:portType>
```

wsdl:binding

Dieses Template bestimmt das konkrete Protokoll und die Art der Nachrichtenübertragung innerhalb der einzelnen Funktionen.

```
<wsdl:binding name="SecurityTokenServiceBinding"
	type="bipro:SecurityTokenServicePortType">
	<soapbind:binding style="document"
	transport="http://schemas.xmlsoap.org/soap/http"/>
	<wsp:PolicyReference URI="#${4}" />
	<wsdl:operation name="RequestSecurityToken">
		<soapbind:operation soapAction="urn:RequestSecurityToken"
		style="document"/>
		<wsdl:input name="RequestSecurityTokenRequest">
			<soapbind:body use="literal"/>
		</wsdl:input>
		<wsdl:output name="RequestSecurityTokenResponse">
			<soapbind:body use="literal"/>
		</wsdl:output>
	</wsdl:operation>
</wsdl:binding>
```

Variable	Wert
${X4}	Id der zugehörigen SecurityPolicy

wsdl:service

Dieses Template fasst eine Reihe unterschiedlicher Kommunikationsschnittstellen (Service-Endpoints) in einem Service zusammen. Die Ports sind gewissermaßen Instanzen des PortTypes.

```
<wsdl:service name="SecurityTokenService">
	<wsdl:documentation>${X5}</wsdl:documentation>
	<wsdl:port>${X6}</wsdl:port>
	<wsdl:port>${X6}</wsdl:port>
	<wsdl:port>...</wsdl:port>
</wsdl:service>
```

Variable	Wert
${X5}	Erläuterung der Aufgaben des STS; Fachliche Dokumentation. ACHTUNG: Diese Erläuterung wird möglicherweise von generischen Clients in einer Benutzeroberfläche visualisiert.
${X6}	Template gemäß folgendem Abschnitt „wsdl:port“

wsdl:port

Dieses Template beschreibt eine einzelne Kommunikationsschnittstelle (Service-Endpoint), die zum STS gehört. Jede solche Schnittstelle entspricht einem Authentifizierungsverfahren, das der Provider anbietet.

```
<wsdl:port name="${6}" binding="bipro:SecurityTokenServiceBinding">
	<wsdl:documentation>${X7}</wsdl:documentation>
	<soapbind:address location="${X8}"/>
</wsdl:port>
```

Variable	Wert
${6}	Eindeutige Kennzeichnung des Ports, z. B. `UserPasswordLogin`
${7}	Erläuterung der Aufgabe der Kommunikationsschnittstelle; Fachliche Dokumentation. ACHTUNG: Diese Erläuterung wird möglicherweise von generischen Clients in einer Benutzeroberfläche visualisiert.
${X8}	Internet-Adresse des Web Services, z. B. https://host/path/services/UserPasswordLogin_2.1.0.1.0

Beispiel für ein vollständiges wsdl:service-Element

```
<wsdl:service name="SecurityTokenService_2.1.0.1.0">
	<wsdl:documentation>
		Dieser Service stellt Funktionen fuer die Authentifizierung
		mit Benutzername und Passwort oder mit einem VDG-Ticket zur Verfuegung.
	</wsdl:documentation>
	<wsdl:port name="UserPasswordLogin"
		binding="bipro:SecurityTokenServiceBinding">
		<wsdl:documentation>
```

```
                        Diese Funktion erledigt die Authentifizierung mit
                        Benutzername und Passwort.
                    </wsdl:documentation>
                    <soapbind:address
                    location="https://host/path/services/UserPasswordLogin_2.1.0.1.0"/>
                </wsdl:port>
                <wsdl:port name="VDGTicketLogin"
                    binding="bipro:SecurityTokenServiceBinding">
                    <wsdl:documentation>
                        Diese Funktion erledigt die Authentifizierung mit
                        einem VDG-Ticket.
                    </wsdl:documentation>
                    <wsp:PolicyReference URI="#VDGAuthPolicy"/>
                    <soapbind:address
                    location="https://host/path/services/VDGTicketLogin_2.1.0.1.0"/>
                </wsdl:port>
        </wsdl:service>
```