GDI NRW

Geodateninfrastruktur Nordrhein-Westfalen

Testbed II

Web Security Service

Februar – Dezember 2002

Dokumentation
Version 1.0

Teilnehmer

AED Graphics

con terra

FhG ISST

GIA

GIUB

ibR

IfGI

interactive instruments

lat/lon

Bearbeitungshinweise

Redaktion

Jan Drewnak
Institut für Geoinformatik
Robbert-Koch-Str. 26-28
D-48149 Münster

Tel.: 0251 / 83 33966
E-Mail: drewnak@ifgi.uni-muenster.de

Letzte Änderungen

8.8.2002	Initialisierung des Dokumentes
20.12.2002	- Session XML eingeführt - Einfügen der DTDs/Schemas und entsprechender Beispiele

Inhaltsverzeichnis

1 Über dieses Dokument

Die Initiative GDI NRW ist eine Initiative des Landes NRW zur Entwicklung der nationalen Geodateninfrastruktur.

Zielsetzung und Inhalte der Initiative werden im *Referenzmodell GDI NRW* beschrieben. Interessierte und aktive Teilnehmer sind im Rahmen von Special Interest Groups (SIGs) an der Entwicklung des Referenzmodells beteiligt.

Die im Titel benannten Teilnehmer (alle aktiv in SIGs beteiligt) richten ein gemeinsames Testbed ein, das zur Prüfung der bestehenden Konzepte und zur Gewinnung weiterer Spezifikationen für das Referenzmodell genutzt werden soll.

Im Topdokument *GDI NRW Testbed II* ist der fachliche, technische und organisatorische Rahmen des Testbeds beschrieben.

Das vorliegende Dokument bezieht sich auf die generellen Spezifikationen der OGC zum Basic Service Model und stützt sich in weiten Teilen zum auf die *Security Assertion Markup Language* (SAML) der *Organization for the Advancement of Structured Information Standards (OASIS)* und trifft auf dieser Basis zusätzliche fachliche und technische Festlegungen für den Bereich des GDI NRW Testbed II.

Das Dokument verbleibt im Zeitraum der Spezifikations- und Implementierungsphase im Kreis der an diesem Testbed aktiv beteiligten Institutionen.

Mit Beendigung des GDI Testbed II wird das vorliegende Dokument veröffentlicht und allen Interessierten, die aktiv an dem Aufbau einer (nationalen) GDI mitwirken, zur Verfügung gestellt.

Diese Draft Specification klammert die beiden Kapitel „Zielsetzung“ und „Fachlicher Rahmen“ aus.

2 Bezugnahme auf vorhandene Spezifikationen

Die folgende Tabelle listet alle für diese Spezifikation relevanten existierenden (Prä-)Standards. Die in der Tabelle genannten Versionsnummern und -bezeichnungen dieser (Prä-)Standards gelten für jede weitere Nennung dieser Standards im weiteren Dokument.

Spezifikationstitel	**Kurzbeschreibung, Version und Quelle**
OGC Basic Service Model (BSM) (Version 0.0.8)	Grundlage der GDI-Testbed II Service Architektur (gemeinsam mit ISO 19119).
Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)	Committee Specification 01, 31 May 2002
Authentication Service	Version 0.1.0. Bestandteil des Authentifizierungs- und Autorisierungssystems (AA-System) zu Zugriffkontrolle innerhalb der GDI NRW.

3 Technischer Rahmen

Das vorliegende Dokument spezifiziert das Verhalten eines Dienstes (sog. Security Service), der den Zugriff auf OGC Web Services (OWS) nur für identifizierte Nutzer zulässt.

3.1 Architektur

Ein Security Service dient zur Absicherung jeweils eines OWS. Dabei muss sichergestellt sein, dass auf den abzusichernden OWS *nur* der Security Service zugreifen kann.

Der Security Service eröffnet bei Vorlage gültiger Authentifizierungsinformationen durch den AA-Client eine Session. Die dabei erzeugte Session ID dient bei folgenden Service Requests zur eindeutigen Zuordnung des Requests zu einem identifizierten Nutzer.

Ein Security Service lehnt einen Service Request ab oder leitet ihn an einen OWS weiter und agiert so als Service Client. Die Response eines nicht abgelehnten Requests wird vom Security Service an den Client weitergeleitet (vgl. Abbildung 1).

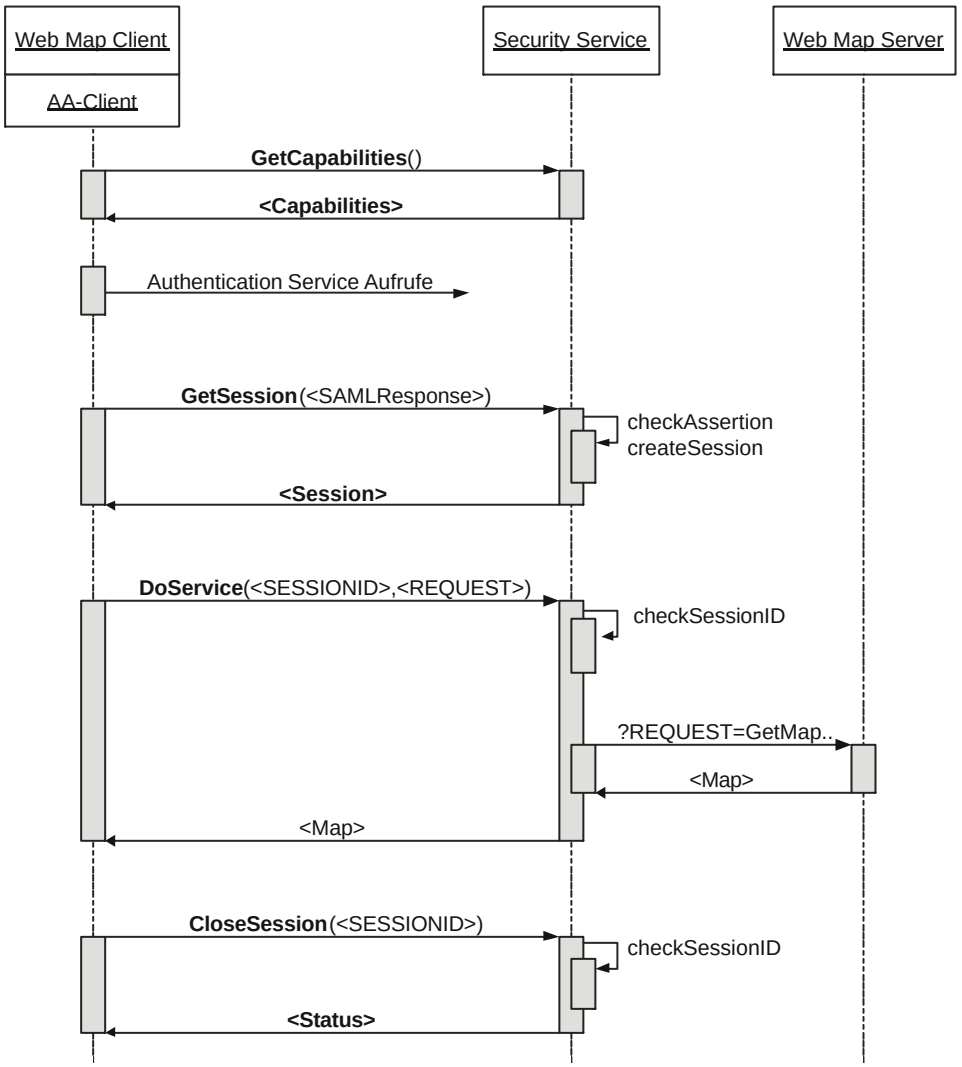

Abbildung 1: Beispiel einer Sequenz von Service Requests an den Security Service

Der Security Service definiert vier Operationen:

GetCapabilities (required): Auslesen der Dienstmetadaten.

GetSession (required): Erzeugen einer Session und Senden der Session ID an den Client. Zur Erzeugung einer Session ist ein gültiges SAML-konformes Authentifizierungs-Token notwendig.

CloseSession (required): Schließen einer Session, d.h. Entfernen aller zur Session gehörigen Informationen.

DoService (required): Ausführen eines OGC Web Service Request. Der Request wird bei gültiger Session ID an den abgesicherten GI Service weitergeleitet, die Response an den Client.

SAML

Die Durchführung der Authentifizierung (z.B. Überprüfen von Kennung und Passwort) von Clients (Benutzern) ist *nicht* Teil dieser Spezifikation. Dies ist die Aufgabe des Authentication Service. Für den Austausch von Authentifizierungsinformationen zwischen Authentication Service und dem Security Service wird die Security Assertion Markup Language (SAML) genutzt.

3.2 Spezifikation der Schnittstellen

3.2.1 Basic Service Elements

An dieser Stelle gelten die Spezifikationen gemäß Basic Service Model, Kapitel 5.

3.2.2 Security Service Operations

3.2.2.1 GetCapabilities (required)

Tabelle 1: Parameter einer GetCapabilities-Request URL

Request Parameter	Required/ Optional	Description
VERSION=version	O	Request Version
SERVICE=Security	R	Service Type
REQUEST=GetCapabilities	R	Request Name

Request Parameters

VERSION

Der VERSION-Parameter und seine Verwendung sind in Abschnitt 3.2.1 genauer beschrieben.

SERVICE

Dieser Parameter gibt an, welcher Dienst einer Dienstinstanz aufgerufen werden soll. Beim Aufruf eines Security Service soll der Wert „Security“ verwendet werden.

REQUEST

Die generelle Verwendung des Request-Parameter ist in Abschnitt 3.2.1 genauer beschrieben. Um die GetCapabilities-Operation aufzurufen soll der Wert „GetCapabilities“ verwendet werden.

GetCapabilities Response

Der Security Service antwortet mit einem gegenüber der in Abschnitt A.3 des Anhangs angegebenen DTD validen Capabilities Dokument oder einer Service Exception bei ungültigem Request. Es gelten

weiterhin die in Abschnitt 3.2.1 gemachten Aussagen bzgl. der GetCapabilities Response. Die Response soll den MIME Type `application/vnd.gdinrw.secure_xml` besitzen, wenn kein Fehler auftritt.

General Service Metadata (<service>)

Das <Service>-Element der GetCapabilites Response liefert allgemeine Metadaten zum Security Service.

<SecuredServiceType>

Mit dem obligatorischen <SecuredServiceType>-Element wird angegeben, welchen Typ von OWS durch diesen Security Service abgesichert wird. Erlaubte Werte sind die mit dem SERVICE-Parameter des GetCapabilities Request eines OWS angegeben Service-Typen, z.B. „WMS“, „WFS“, „WCS“ usw.

<AcceptedAuthenticationService>

Das Capabilities-Dokument gibt mit diesem Element an, welche Authentication Services von diesem Security Service akzeptiert werden. Er enthält eine Liste von <AuthNService>-Elementen

<AuthNService>

Das <AuthNService>-Element beschreibt einen vom Security Service akzeptierten Authentication Service. Der Inhalt des <Name>-Elements sollte dem im <Name>-Element der GetCapabilities Response eines Authentication Service angegebenen Namen entsprechen.

Das <OnlineRessource>-Element gibt die URL des Authentication Service an, während mit beliebig vielen <Version>- und <AuthenticationMethod>-Elementen angegeben werden kann, welche Voraussetzungen der AuthenticationService bzgl. Version und Authentifizierungsverfahren erfüllen muss.

<Session>

Das Attribut “Duration” dieses Elements gibt die Dauer eines Session mit diesem Service in Sekunden an.

3.2.2.2 GetSession (required)

General

Mit GetSession identifiziert sich der Client einmalig beim Security Service. Indem der Client eine SAML Response mit Authenticarion Assertion präsentiert, eröffnet der Security Service eine Session, die ein wiederholtes senden der SAMLResponse durch den Client erübrigt. Die in der GetSession-Response (Session XML) enthaltene Session ID sollte bei DoService-Requests mitgeschickt werden. GetSession wird durch HTTP POST aufgerufen.

GetSession Overview

Tabelle 2: Parameter der GetSession-Request URL

Request Parameter	Required/ Optional	Description
VERSION=version	R	Request Version
REQUEST=GetSession	R	Request Name
SAMLResponse=response	R	SAML Response mit Authentication Assertion

Request Parameters

VERSION

Der VERSION-Parameter und seine Verwendung sind in Abschnitt 3.2.1 genauer beschrieben.

REQUEST

Dieser Parameter soll den Wert „GetSession“ besitzen.

SAMLResponse

Dieser Parameter soll eine Base64-codierte SAML Response gemäß Browser POST Profile enthalten, die genauer in [2] und [1] beschrieben ist. Sie besteht aus einer Liste von Assertions, u.a. der Authentication Assertion mit den Informationen über die vorangegangene Authentifizierung (z.B. der ID des Nutzers).

GetSession Response

Die GetSession Response soll gegenüber dem in Abschnitt A.1 des Anhangs angegebenen Schema valide sein. Die Response soll den MIME Type `application/vnd.gdinrw.session_xml` besitzen, wenn kein Fehler auftritt. Ein ungültiger Request, insbesondere bei ungültiger SAML-Response, führt zu einer Service Exception.

Das <Session>-Element besitzt die Attribute id und expirationDate. Ersteres ist die im weiteren Verlauf der Kommunikation mit dem Security Service zu verwendende Session ID. Letzteres gibt den Zeitpunkt an, zu dem die Session ungültig wird. Die Zeit ist wie in Abschnitt 3.2.1 beschrieben formatiert und nutzt die Zeit des Security Service als Referenz. Das <Issuer>-Element macht Angaben zum Ersteller der Session, um eine clientseitige Verwaltung des Session-Dokuments zu erleichtern. Mit dem <Status>-Element wird der Zustand der Session angegeben. Eine neu erstellte Session besitzt den Wert „opened“.

3.2.2.3 CloseSession (Required)

General

Mit dem CloseSession Request wird eine Session durch den Client beendet.

CloseSession Overview

Tabelle 3: Parameter einer CloseSession-Request Url

Request Parameter	Required/ Optional	Description
VERSION=version	R	Request Version
REQUEST=CloseSession	R	Request Name
SESSIONID=id	R	Identifikator einer Session

Request Parameters

VERSION

Der VERSION-Parameter und seine Verwendung sind in Abschnitt 3.2.1 genauer beschrieben.

REQUEST

Dieser Parameter muss den Wert „CloseSession“ besitzen.

SESSIONID

Der Session-ID Parameter gibt an, welche Session beendet werden soll.

CloseSession Response

Die GetSession Response soll gegenüber dem in Abschnitt A.1 des Anhangs angegebenen Schema valide sein. Die Response soll den MIME Type `application/vnd.gdinrw.session_xml` besitzen. Ein ungültiger Request, insbesondere bei ungültiger Session ID, führt zu einer Service Exception.

Im Gegensatz zum GetSession Request hat das <Status>-Element den Wert „closed“

3.2.2.4 DoService (required)

General

Der DoService-Request wird von einem AA-Client an den Security Service geschickt. Er enthält als zentrale Elemente den Request der unter dem Security Service Protokoll liegenden Protokoll-Schicht (z.B. WMS oder WPOS) sowie eine gültige Session ID.

Der DoService Request wird durch HTTP POST oder HTTP GET aufgerufen.

DoService Overview

Tabelle 4: Parameter einer DoService -Request URL

Request Parameter	Required/ Optional	Description
VERSION=version	R	Request Version
REQUEST=DoService	R	Request Name
SERVICEREQUEST=request	R	Query String eines Service Request
SESSIONID=id	O	Identifikator einer Session

Request Parameters

VERSION

Der VERSION-Parameter und seine Verwendung sind in Abschnitt 3.2.1 genauer beschrieben.

REQUEST

Dieser Parameter muss den Wert „DoService“ besitzen.

SERVICEREQUEST

Der ServiceRequest-Parameter enthält den Query String eines OGC Web Service Request, der an dem vom Security Service abgesicherten GI Service weitergeleitet werden soll. Bsp.: `SERVICE=WMS&REQUEST=GetCapabilities`

SESSIONID

Der SessionID-Parameter ist eine Session ID, die durch einen vorausgehenden GetSession-Request vom Client mitgeschickt wird. Der Security Service muss prüfen, ob es sich um eine gültige Session ID handelt. Gültig bedeutet hier: Es existiert eine zur Session ID gehörige Session die von diesem Service erzeugt wurde und noch nicht abgelaufen oder beendet worden ist. Trifft dies nicht zu, muss der Security Service den Request mit einer Service Exception beantworten und darf den Service Request nicht durchführen.

DoService Response

Das Format der Antwort des Security Service variiert je nach dem, welcher geschützte Service angesprochen wurde. Ein ungültiger Request im Sinne der hier spezifizierten Operation, insbesondere bei ungültiger Session ID, führt zu einer Service Exception.

Anhang

A XML-Schema Definitionen / Document Type Definitions

A.1 AA Session XML Schema

Dieser Abschnitt enthält eine Schema-Definition für ein Session-Dokument. Instanzen des Dokuments werden bei GetSession-Anfragen erzeugt. Das Dokument ist als AA-session.xsd verfügbar.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://gdi-nrw.uni-muenster.de/aa-service"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:session="http://gdi-nrw.uni-muenster.de/aa-
service" elementFormDefault="qualified">
   <xsd:element name="Session">
      <xsd:complexType>
         <xsd:sequence>
            <xsd:element name="Issuer">
               <xsd:complexType>
                  <xsd:sequence>
                     <xsd:element name="Name" type="xsd:string"/>
                     <xsd:element name="URL" type="xsd:string"/>
                  </xsd:sequence>
               </xsd:complexType>
            </xsd:element>
            <xsd:element name="Status">
               <xsd:simpleType>
                  <xsd:restriction base="xsd:string">
                     <xsd:enumeration value="opened"/>
                     <xsd:enumeration value="closed"/>
                  </xsd:restriction>
               </xsd:simpleType>
            </xsd:element>
         </xsd:sequence>
         <xsd:attribute name="id" type="xsd:string" use="required"/>
         <xsd:attribute name="expirationDate" type="xsd:string"/>
      </xsd:complexType>
   </xsd:element>
</xsd:schema>
```

A.2 AA Session XML Beispiel

```
<?xml version="1.0" encoding="UTF-8"?>
<session:Session
       xmlns:session="http://gdi-nrw.uni-muenster.de/aa-service"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="“http://gdi-nrw.uni-muenster.de/aa-service“
       id="634hj-0987gf-64ggh6-re12d2"
       expirationDate="2002-12-22T08:30:45.284">
       <session:Issuer>
              <session:Name>IfGI SWMS</session:Name>
              <session:URL>http://rizzo.uni-muenster.de/SWMS</session:URL>
       </session:Issuer>
       <session:Status>opened</session:Status>
</session:Session>
```

A.3 Security Service Capabilities DTD

```
<!ELEMENT GDINRW_SecurityService_Capabilities (Service, Capability)>
<!ATTLIST GDINRW_SecurityService_Capabilities
   version CDATA #FIXED "0.1.0"
   updateSequence CDATA #IMPLIED>
<!-- Elements used in multiple places. -->
<!-- The Name is typically for machine-to-machine communication. -->
<!ELEMENT Name (#PCDATA)>
<!-- The Title is for informative display to a human. -->
<!ELEMENT Title (#PCDATA)>
<!-- The abstract is a longer narrative description of an object. -->
```

```
<!ELEMENT Abstract (#PCDATA)>
<!-- An OnlineResource is typically an HTTP URL. The URL is placed in the
xlink:href attribute. The xmlns:xlink attribute is a required XML namespace
declaration. -->
<!ELEMENT OnlineResource EMPTY>
<!ATTLIST OnlineResource
   xmlns:xlink CDATA #FIXED "http://www.w3.org/1999/xlink"
   xlink:type CDATA #FIXED "simple"
   xlink:href CDATA #REQUIRED
>
<!-- A container for listing an available format's MIME type. -->
<!ELEMENT Format (#PCDATA)>
<!-- A container for listing accepted Versions for Authentication Services. -->
<!ELEMENT Version  (#PCDATA)>
<!-- A container for listing accepted Authentication Methods -->
<!ELEMENT AuthenticationMethod EMPTY>
<!ATTLIST AuthenticationMethod
   Method (urn:oasis:names:tc:SAML:1.0:am:password | urn:unknown)
   "urn:oasis:names:tc:SAML:1.0:am:password">
<!-- Information about accepted Authentication Services. -->
<!ELEMENT AuthNService (Name, OnlineResource, Version?, AuthenticationMethod?)> <!-- General
service metadata. -->
<!ELEMENT Service (Name, Title, Abstract?, KeywordList?, OnlineResource, ContactInformation?,
Fees?, AccessConstraints?)>
<!-- List of keywords or keyword phrases to help catalog searching. -->
<!ELEMENT KeywordList (Keyword*)>
<!-- A single keyword or phrase. -->
<!ELEMENT Keyword (#PCDATA)>
<!-- Information about a contact person for the service. -->
<!ELEMENT ContactInformation (ContactPersonPrimary?, ContactPosition?, ContactAddress?,
ContactVoiceTelephone?, ContactFacsimileTelephone?, ContactElectronicMailAddress?)>
<!--The primary contact person.-->
<!ELEMENT ContactPersonPrimary (ContactPerson, ContactOrganization)>
<!--The person to contact.-->
<!ELEMENT ContactPerson (#PCDATA)>
<!--The organization supplying the service.-->
<!ELEMENT ContactOrganization (#PCDATA)>
<!--The position title for the contact person.-->
<!ELEMENT ContactPosition (#PCDATA)>
<!--The address for the contact supplying the service.-->
<!ELEMENT ContactAddress (AddressType, Address, City, StateOrProvince, PostCode, Country)>
<!--The type of address.-->
<!ELEMENT AddressType (#PCDATA)>
<!--The street address.-->
<!ELEMENT Address (#PCDATA)>
<!--The address city.-->
<!ELEMENT City (#PCDATA)>
<!--The state or province.-->
<!ELEMENT StateOrProvince (#PCDATA)>
<!--The zip or postal code.-->
<!ELEMENT PostCode (#PCDATA)>
<!--The address country.-->
<!ELEMENT Country (#PCDATA)>
<!--Contact telephone number.-->
<!ELEMENT ContactVoiceTelephone (#PCDATA)>
<!--The contact fax number.-->
<!ELEMENT ContactFacsimileTelephone (#PCDATA)>
<!--The e-mail address for the contact.-->
<!ELEMENT ContactElectronicMailAddress (#PCDATA)>
<!-- Elements indicating what fees or access constraints are imposed. -->
<!ELEMENT Fees (#PCDATA)>
<!ELEMENT AccessConstraints (#PCDATA)>
<!-- A Capability lists available request types, how exceptions
may be reported, and whether any vendor-specific capabilities are defined. -->
<!ELEMENT Capability (Request, Exception, VendorSpecificCapabilities?, SecuredServiceType,
AcceptedAuthenticationService?, Session)>
<!-- Available AuthNService Operations are listed in a Request element. -->
<!ELEMENT Request (GetCapabilities, GetSession, DoService, CloseSession)>
<!-- For each operation offered by the server, list the available output
formats and the online resource. -->
<!ELEMENT GetCapabilities (Format+, DCPType+)>
<!ELEMENT GetSession (Format+, DCPType+)>
<!ELEMENT DoService (Format+, DCPType+)>
<!ELEMENT CloseSession (Format+, DCPType+)>
<!-- Available Distributed Computing Platforms (DCPs) are
listed here. At present, only HTTP is defined. -->
```

```
<!ELEMENT DCPType (HTTP)>
<!-- Available HTTP request methods. One or both may be supported. -->
<!ELEMENT HTTP (Get | Post)+>
<!-- URL prefix for each HTTP request method. -->
<!ELEMENT Get (OnlineResource)>
<!ELEMENT Post (OnlineResource)>
<!-- An Exception element indicates which error-reporting formats are supported. -->
<!ELEMENT Exception (Format+)>
<!--This element contains the service type being secured, e.g. WMS, WFS, WCS etc.-->
<!ELEMENT SecuredServiceType (#PCDATA)>
<!--This element contains all Authentication Services accepted by this Security Service-->
<!ELEMENT AcceptedAuthenticationService (AuthNService?)>
<!--The Session element indicates the duration of a session offered by this service-->
<!ELEMENT Session EMPTY>
<!ATTLIST Session
   Duration CDATA #REQUIRED>
```

A.4 Security Service Capabilities Beispiel

```
<?xml version="1.0" encoding="UTF-8"?>
<GDINRW_SecurityService_Capabilities version="0.1.0" updateSequence="0">
   <Service>
      <Name>GDINRW:SecurityService</Name>
      <Title>IfGI Security Service</Title>
      <Abstract>Security Service Prototype for the GDI NRW</Abstract>
      <KeywordList>
         <Keyword>Security Service</Keyword>
         <Keyword>IfGI</Keyword>
      </KeywordList>
      <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink" xlink:type="simple"
         xlink:href="http://ifgi.uni-muenster.de"/>
      <ContactInformation>
         <ContactPersonPrimary>
            <ContactPerson>Jan Drewnakt</ContactPerson>
            <ContactOrganization>IfGI</ContactOrganization>
         </ContactPersonPrimary>
         <ContactPosition>Developer</ContactPosition>
         <ContactAddress>
            <AddressType>postal</AddressType>
            <Address>Robert-Koch-Strasse 26-28</Address>
            <City>Muenster</City>
            <StateOrProvince>NRW</StateOrProvince>
            <PostCode>48149</PostCode>
            <Country>Germany</Country>
         </ContactAddress>
         <ContactVoiceTelephone>+49 (0)251 - 83-33966</ContactVoiceTelephone>
         <ContactFacsimileTelephone>+49 (0)251 - 83-39763</ContactFacsimileTelephone>
         <ContactElectronicMailAddress>
            drewnak@ifgi.uni-muenster.de</ContactElectronicMailAddress>
      </ContactInformation>
      <Fees>none</Fees>
      <AccessConstraints>none</AccessConstraints>
   </Service>
   <Capability>
      <Request>
         <GetCapabilities>
            <Format>application/vnd.gdinrw.secure_xml</Format>
            <DCPType>
               <HTTP>
                  <Get>
                     <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
                        xlink:type="simple"
                        xlink:href="http://rizzo.uni-muenster.de:8080/SecurityService"/>
                  </Get>
                  <Post>
                     <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
                        xlink:type="simple"
                        xlink:href="http://rizzo.uni-muenster.de:8080/SecurityService"/>
                  </Post>
               </HTTP>
            </DCPType>
         </GetCapabilities>
         <GetSession>
            <Format>application/vnd.gdinrw.session_xml</Format>
            <DCPType>
```

```
               <HTTP>
                  <Post>
                     <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
                        xlink:type="simple"
                        xlink:href="application/vnd.gdinrw.session_xml"/>
                  </Post>
               </HTTP>
            </DCPType>
         </GetSession>
         <DoService>
            <Format>application/vnd.gdinrw.unknown</Format>
            <DCPType>
               <HTTP>
                  <Post>
                     <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
                        xlink:type="simple"
                        xlink:href="http://rizzo.uni-muenster.de:8080/SecurityService"/>
                  </Post>
               </HTTP>
            </DCPType>
         </DoService>
         <CloseSession>
            <Format>application/vnd.gdinrw.session_xml</Format>
            <DCPType>
               <HTTP>
                  <Get>
                     <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
                        xlink:type="simple"
                        xlink:href="http://rizzo.uni-muenster.de:8080/SecurityService"/>
                  </Get>
               </HTTP>
            </DCPType>
         </CloseSession>
      </Request>
      <Exception>
         <Format>application/vnd.ogc.se_xml</Format>
      </Exception>
      <SecuredServiceType>WMS</SecuredServiceType>
      <AcceptedAuthenticationService>
         <AuthNService>
            <Name>GDINRW:AuthenticationService001</Name>
            <OnlineResource xmlns:xlink="http://www.w3.org/1999/xlink"
               xlink:type="simple" xlink:href="http://helium.do.isst.fhg.de:8080
               /aaa/servlet/AuthenticationAuthority"/>
            <Version>0.1.0</Version>
            <AuthenticationMethod Method="urn:oasis:names:tc:SAML:1.0:am:password"/>
         </AuthNService>
      </AcceptedAuthenticationService>
      <Session Duration="600"/>
   </Capability>
</GDINRW_SecurityService_Capabilities>
```

A.5 Service Exception DTD

Die hier angeführte DTD entspricht der im BSM definierten DTD, die online unter <http://www.digitalearth.gov/wmt/xml/exception_1_1_0.dtd> verfügbar ist. In diesem Abschnitt werden des weiteren Exception Codes definiert, die in einer Exception verwendet werden sollten.

```
<!ELEMENT ServiceExceptionReport (ServiceException*)>
<!ATTLIST ServiceExceptionReport version CDATA #FIXED "1.1.0">
<!ELEMENT ServiceException (#PCDATA)>
<!ATTLIST ServiceException code CDATA #IMPLIED>
```

Tabelle 5: Service Exception Codes

Exception Code	Bedeutung
InvalidSAMLResponse	Die per GetSession Request gesendete SAMLResponse ist ungültig.
InvalidSessionID	Eine per CloseSession oder DoService Request gesendete Session ID ist ungültig, d.h. es existiert keine zugehörige Session.

A.6 Service Exception Beispiel

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ServiceExceptionReport SYSTEM
"http://www.digitalearth.gov/wmt/xml/exception_1_1_0.dtd">
<ServiceExceptionReport version="1.1.0">
   <ServiceException code="InvalidSessionID">
      Session ID ungültig. Session nicht vorhanden.
   </ServiceException>
</ServiceExceptionReport>
```

A.7 SAML Response Beispiel

Das hier aufgeführte Beispiel zeigt eine (nicht Base64-kodierte, unsignierte) SAML Response mit Authentication Assertion, wie sie das SAML Browser POST Profile spezifiziert.

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol" InResponseTo="321781385"
IssueInstant="2002-09-12T10:44:56Z" MajorVersion="1" MinorVersion="0"
Recipient=" rizzo.uni-muenster.de:8080/SecurityService "
ResponseID="2a69a794-107b-4c88-b26a-3d42410851f8">
   <Status>
      <StatusCode Value="samlp:Success"/>
   </Status>
   <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
   AssertionID="0ecf2abb-b437-492c-914f-3bddf1dd6207" IssueInstant="2002-09-12T10:45:01Z"
   Issuer="Jans Org" MajorVersion="1" MinorVersion="0">
      <Conditions NotBefore="2002-09-12T10:44:56Z" NotOnOrAfter="2002-09-12T10:50:56Z"/>
      <AuthenticationStatement AuthenticationInstant="2002-09-12T10:44:54Z"
      AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
         <Subject>
            <NameIdentifier Format="email" NameQualifier="drewnak@ifgi.uni-muenster.de">
            Jan Drewnak</NameIdentifier>
            <SubjectConfirmation>
               <ConfirmationMethod></ConfirmationMethod>
               <SubjectConfirmationData></SubjectConfirmationData>
            </SubjectConfirmation>
         </Subject>
         <SubjectLocality DNSAddress="ifgi-usb4.uni-muenster.de" IPAddress="128.176.146.135"/>
      </AuthenticationStatement>
   </Assertion>
</Response>
```

Referenzen

[1] OASIS (2002): Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML). <http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf>

[2] OASIS (2002) Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML). <http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf>

[3] GDI NRW (2002): Testbed II. Authentication Service