GDI NRW

Geodateninfrastruktur Nordrhein-Westfalen

Testbed II

Web Authentication & Authorization 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	Felix Jungermann Fraunhofer ISST, Dortmund Emil-Figge-Str. 91 D-44227 Dortmund tel. 0231 / 9 76 77-393 mail jungerma@do.isst.fhg.de
	Rüdiger Gartmann Fraunhofer ISST, Dortmund Emil-Figge-Str. 91 D-44227 Dortmund Tel.: 0231 / 9 76 77-305 Mail: gartmann@do.isst.fhg.de

Letzte Änderungen

4.9.2002	Initialisierung des Dokumentes
6.1.2003	Überarbeitung des Dokumentes
16.1.2003	Ergänzung

Inhaltsverzeichnis

1 ÜBER DIESES DOKUMENT 4

2 ZIELSETZUNGEN 5

3 BEZUGNAHME AUF VORHANDENE SPEZIFIKATIONEN 6

4 FACHLICHER RAHMEN 7

4.1 Gegenstand dieser Spezifikation 7

4.2 Use Cases 7

5 TECHNISCHER RAHMEN 9

5.1 Architektur 9

5.2 Spezifikation der Schnittstellen 9

5.2.1 Basic Service Elements 9
5.2.2 Service Result 9
5.2.3 Service Exceptions 9
5.2.4 Authentication Service Operations 10

6 ANWENDUNGSBEISPIEL 12

7 REFERENZEN 13

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.

2 Zielsetzungen

Das vorliegende Dokument spezifiziert einerseits das Verhalten eines Dienstes, der Nutzer authentifizieren kann und die Informationen über die Authentifizierung als SAML Response an den Nutzer zurückschickt. Dieser Dienst wird im folgenden mit Authentication Service bezeichnet. Die SAML Response kann nachfolgend an Web Services (z.B. Web Security Service Service (WSS) [3]) weitergeleitet werden. Das Dokument spezifiziert Operationen, um die Fähigkeiten des Authentication Services zu erfragen und eine Authentifizierung durchzuführen.

Der hier beschriebene Dienst stellt eine Ausprägung der in der SAML Spezifikation genannten „Authentication Authority“ dar. Da die Authentication Authority keiner Spezifikation bzgl. der Requests unterliegt, ist auch der eigentliche Authentifizierungsprozess (z.B. Übertragung von Kennung und Passwort) nicht standardisiert. Die vorliegende Spezifikation ermöglicht die Entwicklung interoperabler Clients zur Durchführung der Authentifizierung.

Der Authentication Service definiert zur Zeit zwei Operationen:

GetCapabilities (required): Erhalten von Dienst-Metadaten in maschinenlesbarer Form.

Authenticate (required): Senden von ‘credentials’, also von Informationen wie Benutzername und Passwort, die zur Authentisierung verwendet werden können, an den Authentication Service, der bei geglückter Authentifizierung eine SAML Response zurückschickt.

3 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 (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
GDI NRW Testbed II Authentication & Authorization Service	

4 Fachlicher Rahmen

4.1 Gegenstand dieser Spezifikation

Um Zugriffsschutz in verteilten Web Service Umgebungen zu gewährleisten, ist es erforderlich, ein Verfahren zu entwickeln, mit dem sich Clients (Benutzer) gegenüber Diensten authentisieren können. Dies könnte geschehen, indem jeder Client für jeden Dienst ein gesondertes Authentisierungsverfahren nutzt. Viel sinnvoller ist jedoch, ein Verfahren zu wählen, mit dem sich Clients gegenüber vielen Diensten authentisieren können. Im Folgenden wird ein Authentication Service spezifiziert, der die Identität eines Clients bestätigt, indem er ein entsprechendes Zertifikat ausstellt. Dieses Zertifikat kann der Client anschließend benutzen, um einen gesicherten Dienst zu verwenden. Somit entfällt für die verteilten Dienste die Notwendigkeit, die Authentisierung selbst durchzuführen.

In einer Erweiterung kann der Authentication Service auch um eine Autorisierungskomponente erweitert werden. Hierzu müsste für jeden Client geprüft werden, ob er die Berechtigung besitzt, bestimmte Dienste zu nutzen. Die Autorisierung könnte ebenfalls Bestandteil des Zertifikats sein. Die Erweiterung der Funktionalität um die Autorisierung ist nicht Bestandteil dieser Spezifikation. Für die Zukunft ist beabsichtigt, diese Funktionalität zu integrieren.

Zusätzliche Funktionalitäten wie die Registrierung und Verwaltung von Benutzern sind bislang noch nicht spezifiziert, dies wird Inhalt der folgenden Versionen sein.

4.2 Use Cases

Um Geodienste zu nutzen, die nur einem geschlossenen Benutzerkreis zugänglich sind, müssen die Dienste entsprechend geschützt sein. Gleichzeitig wäre es jedoch wünschenswert, dass die Basisdienste, also etwa ein Geocoding Service, nicht um zusätzliche Funktionalitäten erweitert werden müssen, um ein solches Sicherheitsverfahren zu verwenden.

Aus diesem Grund wird hier ein Authentication Client verwendet, der die gleiche Schnittstelle implementiert wie der Geocoding Service. Der Geocoding Client kann also unverändert genutzt werden. Der Authentication Client fragt nun den Authentication Service an, übermittelt seine Authentisierungsinformationen (z.B. Benutzername/Passwort, kryptographischer Schlüssel o.Ä.) und erhält bei erfolgreicher Authentisierung ein Zertifikat (SAML-Response). Im nächsten Schritt ruft der Authentication Client den Web Security Service auf, der den Geocoding Service kapselt. Dieser prüft das Zertifikat und leitet den ursprünglichen Service Request nach erfolgreicher Prüfung an den Geocoding Service weiter. Die Response wird direkt an den Geocoding Client zurückgeleitet.

Das dazugehörige Sequenzdiagramm ist in Abb. 1 dargestellt.

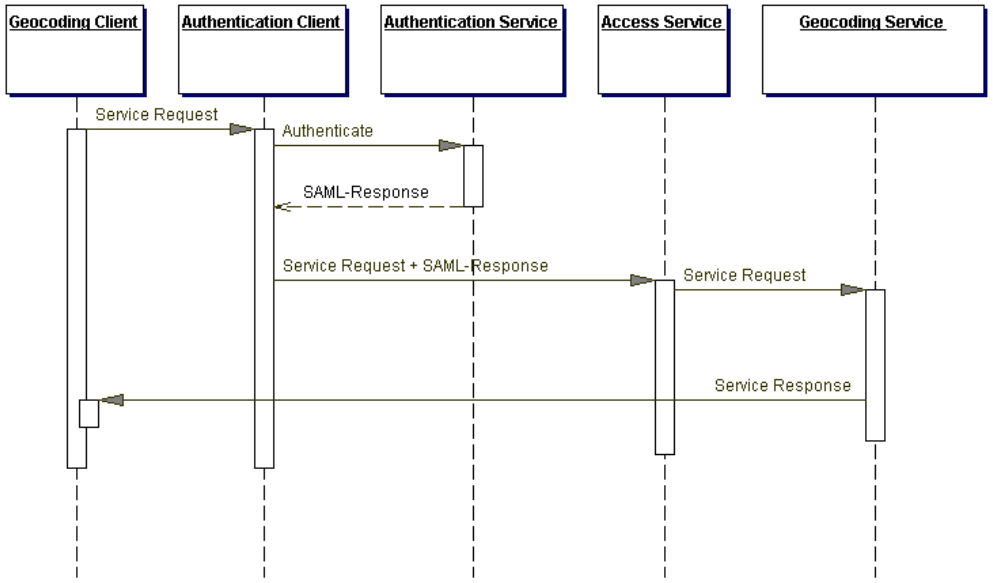

Abbildung 1: Sequenzdiagramm zum Authentisierungsverfahren

5 Technischer Rahmen

5.1 Architektur

Im Rahmen dieser Spezifikation sind neben dem Authentication Service folgenden Komponenten beteiligt:

- *Authentication Client*: Ein Web Client, der in der Lage ist, dem Authentication Service Authentifizierungsinformationen über den zu identifizierenden Nutzer bereitzustellen. Dieser Client ist z.B. ein Web Mapping Client, der Kennung und Passwort eines Nutzers erfragen kann. Zusätzlich ist der Authentication Client in der Lage, nach Benutzung des Authentication Service, anfragen an einen Secure Service zu stellen.
- *Destination Service*: Dienst, der die vom Nutzer gewünschte Business-Funktion ausführt, z.B. ein Secure Service.

Über den Authentication Client authentifiziert sich der Nutzer beim Authentication Service, der daraufhin SAML Authentication Assertion erstellt und in einem SAML Response zurücksendet.

5.2 Spezifikation der Schnittstellen

[Im Falle der vollständigen Übernahme von OGC Spec's, Angabe über etwaige Beschränkungen oder Erweiterungen, sonst komplette Beschreibung der Schnittstellen analog zu OGC-Specs]

5.2.1 Basic Service Elements

5.2.1.1 VERSION

Der VERSION-Parameter spezifiziert die Versionsnummer des Protokolls.

5.2.1.2 REQUEST

Der REQUEST-Parameter gibt an, welche Dienstmethode aufgerufen wird.

5.2.1.3 EXCEPTIONS

Der EXCEPTIONS -Parameter gibt das Format an, in dem Fehler angezeigt werden sollen. Vgl. 5.2.3

Kommentar: Noch offen

5.2.2 Service Result

5.2.3 Service Exceptions

Exceptions noch nicht definiert.

Kommentar: Stimmt das?

5.2.4 Authentication Service Operations

5.2.4.1 GetCapabilities (required)

Tabelle 1: Parameter einer GetCapabilities-Request URL

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

Request Parameters

- **VERSION**
- **SERVICE**
- **REQUEST**

GetCapabilities Response

Die GetCapabilities Response sollte folgende Elemente beinhalten (Reihenfolge z.Z. zufällig):

General Service Metadata

Liefert allgemeine Metadaten zum WAAS Service

Authentication Methods

Liste von Authenifizierungsmethoden, die von dem Service unterstützt werden. Identifier gem. SAML ([2], Sec 7.1). Zur Zeit nur möglich: `urn:oasis:names:tc:SAML:1.0:am:password`.

Output Formats

MIME types.

5.2.4.2 Authenticate (required)

2.4.2.5.1 General

Der Authenticate-Request wird von einem Client (z.B. Web Mapping Client) an den Authentication Service geschickt und enthält alle Informationen, um einen Nutzer zu authentifizieren.

Der Authenticate-Request wird durch HTTP POST aufgerufen.

2.4.2.5.2 Authenticate Overview

Tabelle 2: Parameter einer Authenticate-Request URL

Request Parameter	Required/ Optional	Description
VERSION=version	R	Request Version
REQUEST=Authenticate	R	Request Name
METHOD=method_identifier	R	Identifier der Authentifizierungsmethode
TARGET=target_url	R	Target Service
CREDENTIALS=credential_list	R	Authentifizierungsinformationen

Request Parameters

- **VERSION**

Dieser Parameter sollte den Wert `1.0` besitzen.

- **REQUEST**

Dieser Parameter soll den Wert `Authenticate` besitzen.

- **METHOD**

Dieser Parameter legt fest, mit welcher Methode sich der Client authentifizieren möchte. Identifier gem. SAML ([2], Sec 7.1. Zur Zeit nur möglich: `urn:oasis:names:tc:SAML:1.0:am:password`.

- **TARGET**

Der Target-Parameter enthält die URL des Zieldienstes (z.B. URLs eines WMS oder WPOS). Bsp: `http://geonetz.uni-muenster.de/wms`.

- **CREDENTIALS**

Dieser Paramter besteht aus einer Liste von Authentifizierungsinformationen. Die einzelnen Einträge sind durch Semikolon (und ohne Leerzeichen) getrennt.

Tabelle 3: Credential Lists

Authentication Method	#Credentials	Description	Example
urn:oasis:names:tc:SAML :1.0:am:password	2	Cred1 = Kennung Cred2 = Passwort	drewnak;abcdefg123

2.4.2.5.2 Authenticate Response

Die Authentication Response ist spezifiziert in [1], Sec 4.1.2.5.

6 Anwendungsbeispiel

Da GetCapabilities bei allen Webservices gleich verläuft, wird hier nur Authenticate erläutert.
Ein Authentication Client erfragt Passwort sowie Login des Benutzers und gibt diese als Credential verpackt weiter.

Eine Beispielanfrage wäre also
http://helium.do.isst.fhg.de:8080/aaa/servlet/AuthenticationAuthority?VERSION=1.0.0&REQUEST=Authenticate&METHOD=urn:oasis:names:tc:SAML:1.0:am:password&TARGET=http://geonetz.uni-muenster.de/wms&CREDENTIALS=gartmann;gartmann

Sofern Login und Passwort korrekt waren, gibt der Service eine kodierte Saml-Response zurück.

7 Referenzen

[An diese Stelle werden weitere, für dieses Dokument relevante Spezifikationen. Literaturstellen, etc. referenziert]

[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. Web Security Service (WSS)