

## **Zugriffskontrolle in Geodateninfrastrukturen: Web Authentication Service (WAS) und Web Security Service (WSS)**

Jan Drewnak<sup>1</sup>, Rüdiger Gartmann<sup>2</sup>

<sup>1</sup>Institut für Geoinformatik  
Universität Münster  
drewnak@ifgi.uni-muenster.de

<sup>2</sup>Fraunhofer-Institut für Software- und Systemtechnik  
Dortmund  
gartmann@do.isst.fhg.de

### **ZUSAMMENFASSUNG**

Im Rahmen des Testbed II der Initiative Geodateninfrastruktur Nordrhein-Westfalen (GDI NRW) wurden vom Fraunhofer-Institut für Software- und Systemtechnik (ISST) und vom Institut für Geoinformatik der Universität Münster (IfGI) mit dem Web Authentication Service (WAS) und dem Web Security Service (WSS) zwei Spezifikationen entwickelt und prototypisch umgesetzt, die es erlauben, den Zugriff auf OGC Web Services zu kontrollieren. Die beiden interoperablen Sicherheitsdienste, die auf der Security Assertion Markup Language (SAML) des OASIS Konsortiums und dem Basic Services Model des OpenGIS Consortiums basieren, ermöglichen die Authentifizierung und Autorisierung von Clients sowie den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen unterschiedlichen OGC Web Services.

### **EINLEITUNG**

Weltweit schreitet die Entwicklung von Geodateninfrastrukturen voran. Im Rahmen dieser Infrastrukturen stellen Anbieter ihre Geoinformationen über standardisierte Web Services zur Verfügung. Hierdurch soll eine breitere Nutzung dieser Ressourcen durch einen vereinfachten Zugang sowie eine effizientere Nutzung durch vielfältige Integrationsmöglichkeiten unterschiedlicher Datenbestände erzielt werden. Durch die Standardisierungsbemühungen des OpenGIS Consortiums (OGC) stehen bereits eine Reihe von Geoinformationsdiensten (GI-Dienste) für die Nutzung über das Internet zur Verfügung.

Allerdings sind diese Geoinformationen zum Teil wertvoll und nicht öffentlich, wie etwa personenbezogene oder militärische Daten. Diese Daten sind zum Teil nur bestimmten Benutzergruppen zugänglich, zudem sollen sie in der Regel kommerziell genutzt, also verkauft werden. Nachdem mit dem

Web Pricing and Ordering Service (WPOS) (Wagner und Gartmann 2002) bereits eine Lösung zur Abwicklung von kommerziellen Transaktionen mit Geodaten in den Standardisierungsprozess des OGC eingereicht wurde, besteht der nächste Schritt darin, den Zugriff auf Geodatenbestände nur berechtigten Personen, also Personen, die dafür gezahlt haben oder die eine anderweitige Berechtigung besitzen, zu gestatten. Eine wichtige Forderung in diesem Zusammenhang ist, die Vorteile von Geodateninfrastrukturen damit nicht aufzugeben. Im Einzelnen bedeutet dies, dass diese Dienste für berechnigte Benutzer nach wie vor über das Internet zugreifbar bleiben und dass weiterhin Standardsoftware einsetzbar sein soll, die die vom OGC spezifizierten Schnittstellen unterstützt und nicht mit zusätzlichen Sicherheitsfunktionen erweitert werden muss. Bislang gibt es für diese Problemstellung seitens des OGC noch keine Lösung.

Im Rahmen des Testbed II der Geodateninfrastruktur Nordrhein-Westfalen (GDI NRW) wurde ein Ansatz entwickelt, um diesen Anforderungen gerecht zu werden. Der hier vorgestellte Web Authentication Service (WAS) (Drewnak, Gartmann et al. 2003) sowie der Web Security Service (WSS) (Drewnak 2003) sind das vorläufige Ergebnis dieser Arbeiten. Beide Dienste sind auf der Grundlage des Basic Services Model des OGC (OpenGIS Consortium 2001) spezifiziert worden und garantieren dadurch ein notwendiges Maß an Interoperabilität mit den OGC Web Services wie z.B. Web Map Service oder Web Feature Service.

#### **SZENARIO**

Ziel der Schaffung einer Geodateninfrastruktur ist unter anderem, den Markt für Geoinformationen zu aktivieren und die Nutzung z. B. behördlicher oder privater Geodaten zu optimieren (Kuhn, Basedow et al. 2001). Werden diese Daten über OGC Web Services im Internet angeboten, besteht das Problem, dass sie grundsätzlich für jedermann zugänglich sind. Exemplarisch wird folgendes charakteristisches Szenario skizziert, in dem Dienste innerhalb einer GDI angeboten werden:

Ein Web Map Server in der Höheren Forstbehörde ermöglicht die Visualisierung der Forsteinrichtungskarte, deren Daten über einen Web Feature Server (WFS) bezogen werden. Die Geometrien und Sachinformationen der Forsteinrichtung können über den WFS von Bearbeitern in den einzelnen Forstämtern mit einem Client editiert werden. Gleichzeitig stehen die Forsteinrichtungsdaten über den WFS weiteren Behörden zur Verfügung, die die Daten allerdings nicht ändern dürfen.

Das Szenario macht deutlich, dass es möglich sein sollte, die Nutzung bestimmter GI-Dienste oder einiger Funktionen von GI-Diensten auf einzelne Nutzergruppen zu beschränken. Dazu muss a) bekannt sein, *wer* auf einen GI-Dienst zugreifen will (Authentifizierung) und b) ermittelt werden, *ob* der identifizierte Client bzw. Nutzer berechtigt ist, auf die Ressource zuzugreifen (Autorisierung).

## KONZEPTE

### Authentifizierung und Autorisierung

Zu den wesentlichen Aufgaben, die ein Zugriffskontrollsystem leisten muss, gehören Authentifizierung und Autorisierung. Durch die Authentifizierung wird die Identität eines Clients überprüft. Der Client muss dazu z.B. eine bestimmte Kennung/Passwort-Kombination angeben, ein signiertes Zertifikat oder andere vom Authentifizierungsverfahren abhängige Authentifizierungsinformationen (*credentials*) vorweisen. Auf der Basis einer erfolgreichen Authentifizierung kann eine Autorisierung durchgeführt werden, um zu überprüfen, welche Rechte der identifizierte Client gegenüber einer Ressource besitzt (*policy decision*) und ob die Rechte für die gestellte Anfrage ausreichen (*policy enforcement*).

Da Authentifizierung und Autorisierung die beiden elementaren Aufgaben des hier vorgestellten Zugriffskontrollsystems sind, wird im Folgenden vom „AA-System“ gesprochen.

### Standards und Protokolle

Ebenso wie für die OGC-basierten GI-Dienste gehört die Interoperabilität zu den wichtigsten Forderungen an die „AA-Dienste“ WAS und WSS. Einzelne Dienste-Anbieter könnten zwar proprietäre Sicherheitssysteme installieren, es kommt aber darauf an, die Interoperabilität, die zur Kooperation zwischen den Diensten notwendig ist, nicht durch einzelne nicht-interoperable Sicherheitssysteme zu vernichten. Das bedeutet, dass die Kommunikation mit den AA-Diensten anhand standardisierter Schnittstellen und Nachrichten vorgenommen werden muss und die Dienste in der Lage sein müssen, ihre eigenen Fähigkeiten zu beschreiben. Die Spezifikationen von WAS und WSS basieren deshalb im Wesentlichen auf der Security Assertion Markup Language (SAML) zum Austausch von Sicherheitsinformationen (OASIS 2002) und dem Basic Services Model (BSM) des OGC (OpenGIS Consortium 2001).

### Basic Services Model

WAS und WSS richten sich nach dem Basic Services Model, das als Framework für alle OGC Web Services (OWS) dient, und können gemäß Service Taxonomie (ISO/TC 211 & OGC 2002) der Gruppe der „System Management Services“ zugeordnet werden.

Zu den Vorgaben des BSM, die in den Spezifikationen der AA-Dienste umgesetzt werden, gehören:

- Implementieren der GetCapabilities-Schnittstelle und damit die Möglichkeit zur Beschreibung der eigenen Fähigkeiten,
- Verwendung des HTTP-Protokolls und damit des Internets als Distributed Computing Platform, und
- Konformität mit den „Basic Service Elements“, u.a. Request-, Response- und Exception-Format, Versionsaushandlung usw.

### SAML

Die Security Assertion Markup Language (SAML) des OASIS Konsortiums definiert ein XML-basiertes Austauschformat u. a. für Authentifizierungsinformationen. Dieses wird von WAS und WSS genutzt, um Informationen über die erfolgte Authentifizierung eines Clients auszutauschen.

Den Kern der SAML Spezifikationen bilden die Assertions. Eine Assertion ist eine Angabe über zu einem Client gehörende Fakten (Statements). Neben den *Authentication Statements* über stattgefundenene Authentifizierungen definiert SAML *Attribute Statements* über Eigenschaften eines Clients und *Authorization Decision Statements* über Zugriffsrechte des Subjekts.

Authentication Assertions, d. h. Assertions, die nur aus Authentication Statements bestehen, enthalten Informationen wie verwendete Authentifizierungsmethode, Ausstellungszeitpunkt, Gültigkeitsdauer, ID des authentifizierten Nutzers, URL der Ressource, für die die Assertion bestimmt ist etc. Die Authentication Assertion kann damit vom Client dem geschützten Dienst vorgelegt werden und als „Zertifikat“ für eine erfolgreiche Authentifizierung dienen.

## ARCHITEKTUR UND SPEZIFIKATIONEN

### Überblick

Das hier beschriebene Zugriffskontrollsystem spezifiziert derzeit zwei Diensttypen. Der Web Authentication Service (WAS) authentifiziert

Clients/Nutzer und stellt SAML-konforme Authentication Assertions aus. Der Web Security Service (WSS) stellt ein "Gateway" für zugriffsbeschränkte OGC Web Services dar, indem er die Authentication Assertion auswertet und die Requests autorisierter Clients an den geschützten Dienst weiterleitet.

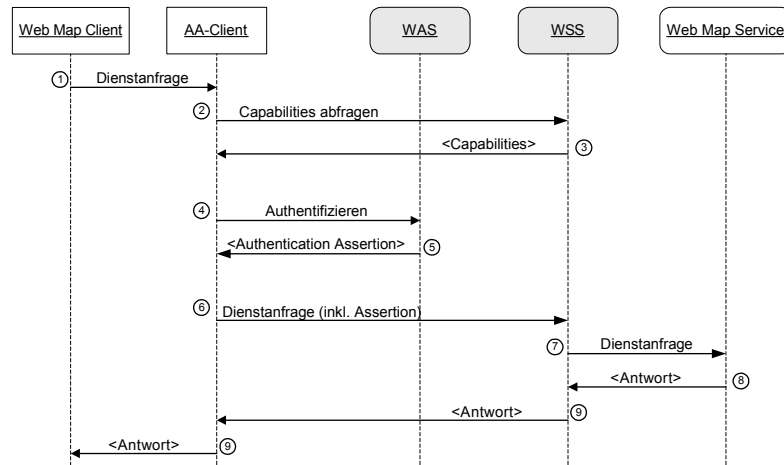


Abb. 1: Vereinfachtes Beispiel einer Dienstnutzung

Abb. 1 zeigt in einem Sequenzdiagramm beispielhaft die Interaktion der Komponenten des Zugriffskontrollsystems in einer GI-Dienste-basierten Umgebung. Der WSS sichert in diesem Beispiel Web Map Service ab, auf den der Nutzer über einen Web Map Client zugreift, der um AA-spezifische Funktionen erweitert worden ist (sog. AA-Client). Anhand dieses Beispiels sollen die Schritte, die für das Abrufen einer Karte vom geschützten Web Map Service notwendig sind, erläutert werden.

1. Der Nutzer setzt einen Request an den geschützten Web Map Service ab. Dieser wird vom AA-Client entgegengenommen.
2. Der AA-Client fragt die Capabilities des WSS ab.
3. Der WSS schickt das Capabilities-Dokument an den Client zurück. Die Capabilities enthalten unter anderem die URL eines akzeptierten WAS und die Anforderung, dass ein passwortbasiertes Authentifizierungsverfahren gewählt werden soll.

4. Anhand der Informationen aus Schritt 2 und der Authentifizierungsinformationen, die der AA-Client vom Nutzer erhält, führt der AA-Client eine Authentifizierung beim WAS durch.
5. Bei erfolgreicher Authentifizierung wird eine Authentication Assertion zurückgesendet.
6. Der AA-Client sendet die Dienstanfrage des Web Map Client (z.B. GetMap) sowie die Assertion an den WSS.
7. Der WSS überprüft die Assertion und extrahiert die darin enthaltenen Nutzerdaten. Dann wird überprüft, ob der Nutzer berechtigt ist, die Anfrage zu stellen (Autorisierung). Ist dies der Fall, wird die Anfrage an den Web Map Service weitergeleitet.
8. Der Web Map Server beantwortet wie üblich die Anfrage, z.B. mit einem Kartenausschnitt als PNG-Datei.
9. Der WSS leitet die Datei weiter an den AA-Client und dieser weiter an den Web Map Client.

### **Protokollschachtelung**

Die vom OGC spezifizierten Web Services beziehen sich auf reine GI-Dienste. Mit diesen Diensten ist es möglich, komplexe Geodateninfrastrukturen aufzubauen, die es erlauben, verteilte Geoinformationen über Internetprotokolle zu integrieren und zu nutzen. Zusatzdienste wie Authentifizierung oder Verkaufstransaktionen sind in diesen Diensten nicht berücksichtigt. Bei der Entwicklung von Zusatzdiensten ist es daher anzustreben, diese so zu spezifizieren, dass deren Nutzung keine Auswirkung hinsichtlich der Implementierung der bereits vorhandenen Infrastrukturen hat. Vorhandene GI-Dienste Clients sollen also ungestört mit ihren GI-Diensten kommunizieren, unabhängig davon, ob diese Interaktion durch einen Zusatzdienst wie den WAS oder WSS unterstützt wird. Die Nutzung solcher Zusatzdienste soll somit für die GI-Dienste völlig transparent geschehen.

Um dieses Ziel zu erreichen, müssen das GI-Dienste Protokoll und das AA-Dienste-Protokoll auf unterschiedlichen logischen Schichten realisiert werden. Das Verfahren wird bereits vom Web Pricing and Ordering Service genutzt (Wagner 2002) und wird in Abb. 2 veranschaulicht.

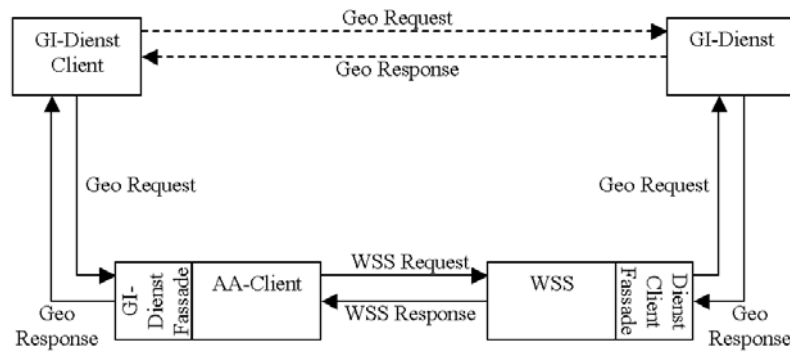


Abb. 2: Prinzip der Protokollschichtung

In der Abb. 2 wird auf die Darstellung der Kommunikation mit dem WAS zur Einholung des Zertifikats verzichtet, da dies für die Beschreibung des Protokollschichtungsansatzes nicht von Relevanz ist. Die gestrichelten Pfeile stellen die Kommunikation ohne Zugriffsschutz dar. In diesem Fall sendet der GI-Dienst Client einen Request an den GI-Dienst und bekommt die entsprechende Response.

Die durchgezogenen Pfeile veranschaulichen das Verfahren bei Benutzung des Zugriffsschutzes. Der GI-Dienst Client erzeugt den gleichen Request als würde er direkt den GI-Dienst ansprechen. Statt des direkten Aufrufs wird dieser Request aber an den AA-Client umgeleitet. Dieser AA-Client bietet die gleichen Operation an wie der GI-Dienst, er besitzt also sozusagen eine GI-Dienst Fassade. Das bedeutet, er nimmt jeden Request entgegen, führt die Authentifizierung durch und leitet den Request zusammen mit den Authentifizierungsinformationen an den WSS weiter, der den eigentlichen GI-Dienst kapselt. Hierzu transformiert er den Geo Request nun in das WSS Protokoll. Dieses Protokoll muss die benötigten Funktionalitäten des gekapselten Dienstes, hier also des WSS, aufnehmen sowie den eigentlichen Geo Request mittransportieren. In diesem Fall geschieht dies dadurch, dass dem Geo Request ein Zertifikat hinzugefügt wird. Der WSS prüft das Zertifikat, extrahiert den ursprünglichen Geo Request und sendet ihn an den GI-Dienst. Dabei agiert der WSS als GI-Dienst Client, er besitzt sozusagen eine GI-Dienst Client Fassade und ist für den GI-Dienst nicht von anderen GI-Dienst Clients unterscheidbar. Der GI-Dienst produziert die Response auf den an ihn gerichteten Request und leitet diese durch den WSS und den AA-Client wieder an den GI-Dienst Client zurück.

Auf diese Weise können beliebige Zusatzdienste in bestehende Geodateninfrastrukturen eingebettet werden. Unabhängig von der Art des Zusatz-

dienstes ist für dieses Schachtelungsverfahren die Fassadentechnik sowie der Transport des Geoprotokolls im Protokoll des Zusatzdienstes kennzeichnend. Dieses Verfahren kann auch mehrfach angewandt werden, etwa indem ein WPOS Protokoll noch in das WSS Protokoll hineingeschachtelt wird. In diesem Fall müsste der WPO Client eine WSS Fassade und der WPOS eine Fassade des WAA Clients besitzen. In das WPOS Protokoll müsste dabei das WSS Protokoll aufgenommen werden.

### **Web Authentication Service (WAS)**

Die Authentifizierung von Nutzern wird im AA-System vom WAS durchgeführt. Hierzu muss der Nutzer bei diesem Dienst registriert sein. Eine Authentisierung erfolgt, wenn der Nutzer durch einen speziellen AA-Client dem WAS mitteilt, welche Ressource, also welchen GI-Dienst, er nutzen will. Zudem muss er sich gegenüber dem WAS authentifizieren. Dies kann grundsätzlich durch verschiedene Verfahren geschehen, beispielsweise durch Verwendung von Passwörtern, durch Kryptographiekarten oder mit Hilfe von biometrischen Verfahren. Eine Festlegung auf ein bestimmtes Verfahren ist nicht Bestandteil der WAS Spezifikation und soll flexibel gehalten werden. Der WAS prüft nun die Identität des Nutzers. Fällt die Prüfung positiv aus, so erstellt der WAS eine digital signierte, SAML-konforme Authentication Assertion, die den Nutzer berechtigt, auf den gewünschten GI-Dienst zuzugreifen.

Im Gegensatz zu einer direkten Authentifizierung des Nutzers durch den GI-Dienst selbst, besitzt diese Lösung den Vorteil, dass der Nutzer dem GI-Dienst nicht bekannt sein muss, sondern nur dem WAS, der als Authentifizierungsdienst für eine Gruppe von Diensten innerhalb einer GDI dienen kann. Dieses Verfahren entlastet so den Nutzer davon, bei allen zu benutzenden Diensten separate Accounts anzulegen und möglicherweise sogar noch unterschiedliche Authentifizierungsverfahren nutzen zu müssen. Auf der anderen Seite entfällt für die GI-Dienste der Aufwand, eine eigene Benutzer- und Rechteverwaltung zu unterhalten.

Der WAS besitzt gemäß Spezifikation vier Operationen, die im Folgenden kurz erläutert werden:

- **GetCapabilities:** Mit den im BSM beschriebenen Parametern, liefert der Aufruf dieser Operation Metadaten über den konkreten WAS. Neben den allen OWS gemeinsamen Metadaten (Name, Kontaktinformationen etc.), gibt der WAS im CapabilitiesXML-Dokument insbesondere an, welche Authentifizierungsverfahren er unterstützt. Anhand dieser Information kann z. B. ein AA-Client eine an das Authentifizierungsverfahren angepasste Benutzerschnittstelle anbieten und so

auf die Auswahl eines bestimmten WAS durch einen Nutzer reagieren.

- **getSession**: Sowohl in die WAS- wie auch in die WSS-Spezifikationen ist ein Session-Konzept integriert, durch das eine wiederholte Übertragung von Credentials, z. B. Kennung und Passwort, vermieden wird. Die Credentials werden dem WAS unter Angabe der gewünschten Authentifizierungsmethode mit dem `getSessionRequest` übergeben. Bei erfolgreicher Authentifizierung enthält die Response ein `SessionXML`-Dokument, das eine Session-ID ausweist.
- **getSAMLResponse**: Über diese Operation gelangt ein AA-Client in den Besitz einer Authentication Assertion. Er muss dazu die URL der Zielressource, der die Authentication Assertion vorgelegt werden soll, sowie eine gültige Session-ID angeben. Die Response enthält eine Authentication Assertion, die für begrenzte Zeit gültig ist.
- **closeSession**: Diese Operation erlaubt es dem Client, eine im Vorfeld beantragte Session zu schließen und die Session-ID zu annullieren, um eventuellen Missbrauch der Session durch Dritte zu verhindern.

Abb. 3 zeigt eine typische Sequenz von Client-Requests an den WAS.

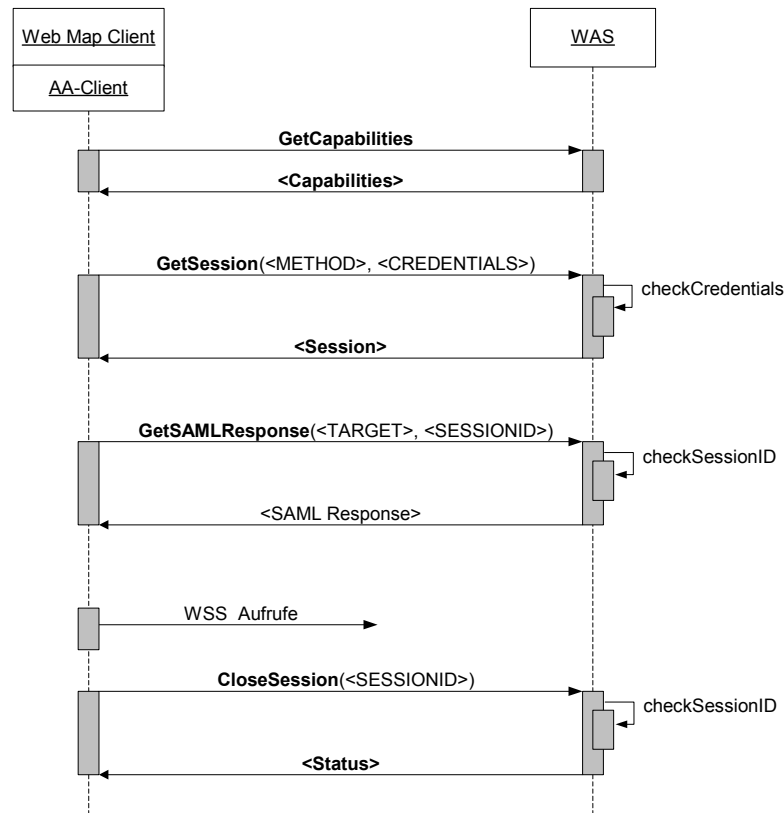


Abb. 3: Sequenz einer Nutzung des Web Authentication Service

### Web Security Service (WSS)

Ein Web Security Service dient im AA-System als "Gateway" für genau einen zugriffsbeschränkten GI-Dienst. Auf den geschützten GI-Dienst darf niemand außer dem WSS zugreifen. Der WSS ist so spezifiziert, dass er ohne Modifikation jeden beliebigen OWS-Typ absichern kann.

Der WSS teilt dem Client mit, von welchen WAS er Zertifikate (= Authentication Assertions) akzeptiert. Er überprüft vorgelegte Zertifikate auf ihre Gültigkeit und leitet berechnete Anfragen an den GI-Dienst weiter. Eine differenzierte Autorisierung findet hier nicht statt. Alle Requests, die von

einem authentifizierten Client kommen, werden als autorisiert betrachtet (vgl. Schlussbemerkung).

Die vier Operationen der WSS-Spezifikation sind:

- **GetCapabilities:** Neben den üblichen OWS-Metadaten, gibt der WSS über die Capabilities bekannt, welcher OWS-Typ abgesichert wird (z. B. WMS), welche WAS er akzeptiert und welche WAS-Versionen und Authentifizierungsmethoden für eine Authentifizierung verwendet werden dürfen.
- **GetSession:** Analog zum WAS integriert der WSS ein Session-Konzept. Ein Client übergibt mit dieser Methode eine gültige Authentication Assertion und erhält eine Session-ID in einem Session XML-Dokument zurück, falls die Authentication Assertion gültig ist.
- **DoService:** Diese Operation wird vom Client verwendet, um einen Request an den abgesicherten OWS zu senden. Zusätzlich zum Request muss eine gültige Session-ID angegeben werden, damit der WSS den Request einem Client zuordnen kann.
- **CloseSession:** Diese Operation ist analog zur CloseSession-Operation der WAS-Spezifikation definiert.

Im Sequenzdiagramm aus Abb. 4 wird beispielhaft die Kommunikation eines Clients mit WSS und abgesichertem Web Map Service dargestellt.

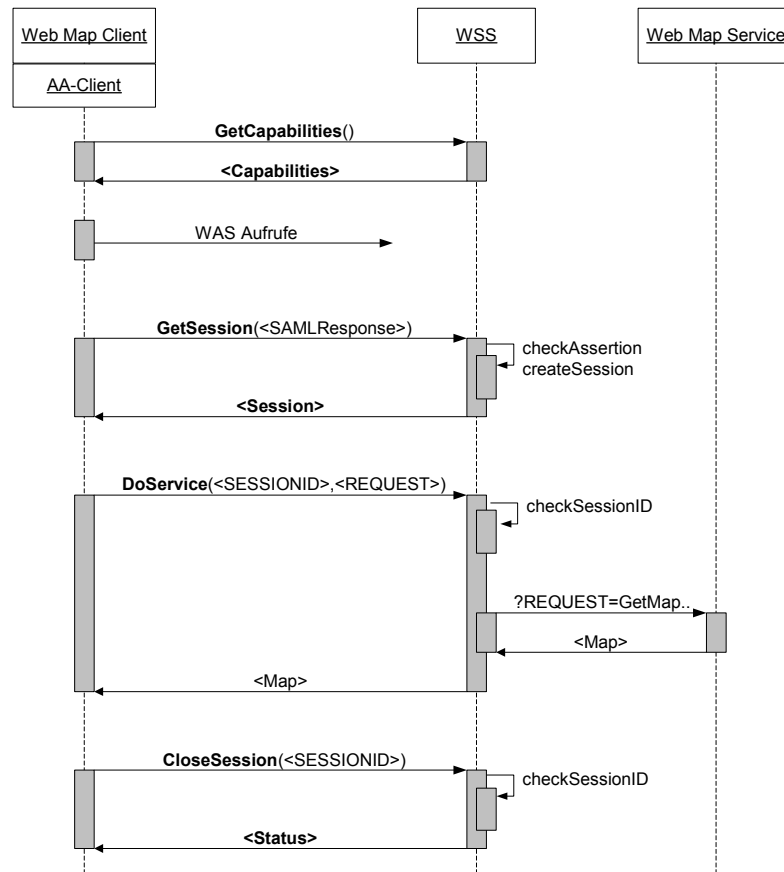


Abb. 4: Beispiel-Sequenz der Nutzung ein Secure Web Map Service

## SICHERHEIT

Die über das Internet transportierten Authentifizierungsinformationen sind vertraulich und müssen deshalb sicher vor dem Zugriff Dritter transportiert werden. Dazu setzen WAS und WSS die Nutzung von SSL (Secure Socket Layer) voraus. SSL stellt ein anerkanntes und verbreitetes Verfahren u.a. im Bereich des E-Commerce dar und bietet auch im Rahmen einer GDI ein ausreichendes Sicherheitsmaß. Um das Maß an Sicherheit weiter zu erhöhen, wurde das Session-Konzept in die Spezifikationen integriert, durch das

ein wiederholtes Übertragen von sensiblen Sicherheitsinformationen (z.B. dem Zertifikat oder Kennung und Passwort) mit jedem Request an den WAS oder WSS vermieden wird.

Zu beachten ist, dass mit der Spezifikation von WAS und WSS kein detailliertes Sicherheitsmodell für den Schutz z. B. vertraulicher Daten umgesetzt wird, sondern eine interoperable Architektur für den Transport von Authentifizierungs- und Autorisierungsinformationen in der Anwendungsschicht des Netzwerkprotokolls. Ausgeklammert wurden Aspekte der Netzwerksicherheit wie Vermeidung von Denial of Service Attacks oder ähnliches in den niedrigeren Abstraktionsschichten des Netzwerkmodells.

#### **SCHLUSSBEMERKUNG**

Die Spezifikationen von WAS und WSS sind im Rahmen des GDI NRW Testbed II im Jahr 2002 vom Fraunhofer-Institut für Software- und Systemtechnik (ISST) und vom Institut für Geoinformatik (IfGI) der Universität Münster prototypisch umgesetzt worden und beweisen die Tauglichkeit des Konzepts im praktischen Einsatz. Zur Demonstration von WAS und WSS wurde ein AA-Client entwickelt, der eine passwortbasierte Authentifizierung ermöglicht und in einen bestehenden Web Map Client integriert wurde. Mit diesem erweiterten Client wird die Nutzung eines geschützten Web Map Service ermöglicht.

Der momentane Stand der Spezifikation und Implementierung des WSS ist bislang noch auf die Authentifizierung beschränkt. Dies ist gleichbedeutend damit, dass ein registrierter Nutzer Dienste ohne weitere Einschränkung nutzen kann, das heißt, ein authentifizierter Benutzer ist gleichzeitig auch für den Dienst autorisiert. Der nächste Schritt ist die Entwicklung eines feineren Autorisierungsmodells, das die Zuordnung von Nutzern zu Nutzergruppen und eine differenzierte Rechtevergabe erlaubt, beispielsweise ausschließlich Leserechte für einen transaktionalen Web Feature Service für einen bestimmten Nutzer. Dabei ist zu beachten, dass in diesem Fall die Autorisierungskomponente nicht unabhängig vom zu nutzenden OWS-Typ ist, da für eine Autorisierung die Requests abhängig vom Dienst-Typ interpretiert werden müssen.

Die als Ergebnis der Testbed II-Aktivitäten entstandenen Spezifikationen werden als offizielle GDI NRW-Dokumente in der Version 1.0 öffentlich publiziert.

**LITERATUR**

- Drewnak, J. (2003): *Testbed II - Web Security Service*, [www.gdi-nrw.org](http://www.gdi-nrw.org).
- Drewnak, J., R. Gartmann, F. Jungermann (2003): *Testbed II - Web Authentication Service*, [www.gdi-nrw.org](http://www.gdi-nrw.org).
- ISO/TC 211 & OGC (2002): *Geographic information Services Draft ISO/DIS 19119*, OpenGIS Service Architecture. Version 4.3. <http://www.opengis.org/techno/abstract/02-112.pdf>.
- Kuhn, W., S. Basedow, C. Brox, C. Riedemann, H. Rossol, K. Senkler, K. Zens (2001): *Referenzmodell 3.0 Geodaten-Infrastruktur Nordrhein-Westfalen*, Düsseldorf.
- 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>.
- OpenGIS Consortium (2001): *Basic Services Model Draft Candidate Implementation specification 0.0.8*, <http://www.opengis.org>.
- Wagner, R. (2002): *Perspektiven mit dem Complex Configuration & Pricing Format (XCPF) und dem kaskadierfähigen Web Pricing & Ordering Service*, (AGIT-Symposium 14, 2002, Salzburg). In: J. Strobl: *Angeordnete Geographische Informationsverarbeitung XIV*, Beiträge zum AGIT-Symposium Salzburg 2002. Heidelberg. Wichmann. S. 573-578.
- Wagner, R., R. Gartmann (2002): *GIS Meets eBusiness. Web Pricing & Ordering Service (WPOS)*, (Geospatial Information & Technology Association (Annual Conference), 2002, Tampa/FL, USA). In: Geospatial Information & Technology Association -GITA-, GITA Annual Conference 25.