6. RAHMENPAPIER

GDI – SÜDHESSEN

Sicherheit

VERSION 1.0
25.03.2008

Auftraggeber

HESSEN

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Ansprechpartner (Projektleitung)

Dr.-Ing. Thomas Rossmanith

Amt für Bodenmanagement Heppenheim
Europaplatz 5
64293 Darmstadt

Email: thomas.rossmanith@hvbg.hessen.de
Tel.: 06151 / 50 04 - 303

Dipl.-Ing (FH) Anja Schupp

Hessisches Landesamt für
Bodenmanagement und Geoinformation
Schaperstraße 16
65195 Wiesbaden

Email: anja.schupp@hvbg.hessen.de
Tel.: 0611 / 535 - 54 86

Weitere Informationen zur GDI-Südhessen unter **http://www.gdi-suedhessen.de**.

INHALTSVERZEICHNIS

1. Sicherheit von Web-Services

Wir betrachten anwendungsbezogene Sicherheitsaspekte bei verteilten Geodaten. Dies sind Sicherheitsaspekte bei der Nutzung der Daten oder Dienste über die durch die Anwendung vorgesehenen Schnittstellen. Die Vorgaben für diese Sicherheitsaspekte kommen aus verschiedensten Quellen, seien diese organisatorischer, technischer oder rechtlicher Natur.
Interoperabel sichere Geodateninfrastrukturen lassen sich nur entwickeln, wenn die Maßnahmen zur Durchsetzung dieser Sicherheitsaspekte ihrerseits wieder auf allgemein anerkannten Standards beruhen. Dies können einerseits Erweiterungen der Standards der Geodienste sein, oder andererseits die Verwendung von Standards für die darunter liegenden Protokollschichten. Dadurch erreicht man eine Interoperabilität über den Bereich der Geo Web Services hinaus.

1.1 Einführung

Wie sicher sind Geodaten? Die größtmögliche Sicherheit ergibt sich hier nur, wenn die Daten auf einem unlöschbaren Datenträger in einem Tresor versperrt liegen, und niemand darauf Zugriff hat. Da dies aber dem Sinn von Geodaten widerspricht, die ja gerade durch die Nutzung und Veredelung einen Mehrwert erhalten, ist es notwendig sich Gedanken über die Sicherheit der Daten zu machen, gerade wenn der Zugriff darauf über das Internet – wie in einer GDI der Fall – erfolgen soll.
Was bedeutet dann aber überhaupt "sicher"? Hinter dem Begriff kann sich eine Fülle unterschiedlicher Aspekte verbergen, die durch unterschiedliche Rahmenbedingungen vorgegeben werden können. Nicht selten ergeben sich Missverständnisse, weil nicht klar ist welche Art von Sicherheit gemeint ist.

1.2 Sicherheitsaspekte im Government

Das E-Government-Handbuch des BSI listet im Kapitel II verschiedene Anforderungen an die Sicherheit von E-Government-Anwendungen auf:

- Vertraulichkeit und Integrität
- Verfügbarkeit
- Authentizität
- Revisionsfähigkeit
- Risikoabschätzung durch Vorabkontrolle
- Datenschutzmanagement
- Ausreichende Qualifizierung
- Selbstdatenschutz
- Schriftform-Erfordernis
- Abbildbarkeit (Zuordenbarkeit)

Darüber hinaus spielen im Bereich der Geo Web Services weitere Sicherheitsaspekte eine wichtige Rolle:

- Zugriffskontrolle
- Copyright
- Lizenzierung
- Abrechnung

Maßnahmen zur Sicherung der Verfügbarkeit der Dateien und zum Schutz gegen Viren, Würmer und Hacker sollen hier nicht weiter betrachtet werden, da diese dem Bereich der allgemeinen Datenverarbeitung entspringen und nicht speziell für Geo Web Services sondern auch für Webserver gelten. Stichworte hierzu sind redundante Server mit Lastverteilung, Virenscanner, Firewalls und demilitarisierte Zonen.

Ebenso werden hier Maßnahmen wie Mitarbeiterschulung, Backups und digitale Archive nicht weiter behandelt, da diese ebenfalls der allgemeinen IT und verschiedenen Geschäftsprozessen entspringen und daher nicht spezifisch für Geodaten und –dienste sind.

Es verbleiben anwendungsspezifische Sicherheitsaspekte, also solche, bei denen die Anwender die Daten über die vorgesehenen Schnittstellen und Operationen nutzen, aber ggf. irrtümlich oder mutwillig ihre dabei bestehenden Rechte überschreiten. Dieser Bereich soll im Folgenden etwas näher betrachte werden.

1.3 Anwendungsbezogener Sicherheitsbedarf

Dazu nehmen wir eine weitere Einteilung vor. Der typische Fall ist ein einzelner lesender Zugriff auf Geodaten eines Servers durch den Nutzer, sei es zur bloßen Darstellung auf dem Bildschirm ("Online-Nutzung"), sei es zum lokalen Abspeichern oder Ausdrucken ("download"). Hier gibt es Sicherheitsaspekte, die die Zeit vor dem Zugriff betreffen, solche, die bei dem Zugriff selbst relevant sind, und solche, die erst nach dem Zugriff greifen.

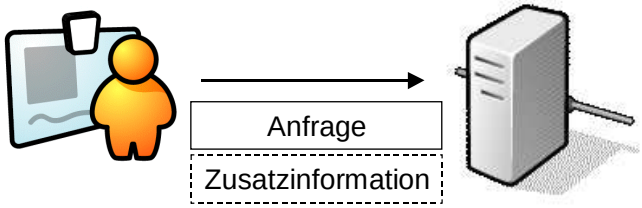
Vor dem Zugriff ist entscheidend, dass die Datenintegrität gewahrt bleibt, so dass der Nutzer beim Zugriff auch die Daten erhält, die er erwartet. In besonderem Fall gilt dies für alle Arten amtlicher Daten. Sofern die Anwendung keine Schnittstellen umfasst, mit denen die Daten geändert werden können, ist die Integrität kein spezielles Problem, es reichen die üblichen Schutzmaßnahmen aus den beiden eingangs angesprochenen Sicherheitsbereichen.

Teilweise sind Anwendungen aber auch so gestaltet, dass eine Datenerfassung oder -Aktualisierung über Netz-Schnittstellen durchführbar ist – speziell seien hier der transactional WFS oder die NAS als ein Derivat davon genannt. In diesem Fall sind gesonderte Maßnahmen erforderlich. Zum Einen muss bei einem ändernden Zugriff sichergestellt werden, dass der Nutzer autorisiert ist, die Änderungen vorzunehmen. Dies ist mit den gleichen Maßnahmen möglich, mit denen Berechtigungen beim lesenden Zugriff geprüft werden. Zum anderen muss die Qualität der Änderung sichergestellt werden, z.B. durch automatische Konsistenz- oder Plausibilitätsprüfungen, durch eine automatische Gegenprüfung vor Freigabe etc. Darüber hinaus muss je nach Anforderungen eventuell eine Archivierung des Ausgangszustandes durchgeführt werden, um eine Historie des Datenbestandes vorhalten zu können.

Im Moment des lesenden Zugriffs muss sicher gestellt werden, dass der Nutzer nur Daten erhält, die er erhalten darf (Autorisierung), dass kein anderer Nutzer die Daten erhält (Zuordenbarkeit) und dass die Daten unverfälscht beim Nutzer ankommen (Integrität). Bei der Autorisierung spielen auch spezifische Aspekte der Geodaten eine Rolle. So kann der Nutzer auf verschiedene Attribute, verschiedene Objektarten, einen Raumbezug oder eine bestimmte Auflösung der Ausgabe festgelegt sein.
Nachdem der Nutzer die Daten erhalten hat, stellt sich die Frage, was er mit den Daten machen darf. Dies ist der Bereich des Digital Rights Managements (DRM). Der erste Teilaspekt ist die Formulierung von Nutzungsrechten und die Mitteilung an den Nutzer. Der zweite, schwierigere Teilaspekt ist die Überwachung dieser Rechte, also den Nutzer technisch so einzuschränken, dass er nur berechtigte Nutzungen der Daten durchführen kann, um so die Urheberrechte des Datenanbieters zu sichern.
Für DRM gibt es eine Reihe existierender Lösungsansätze, die bisher vor allem im Bereich elektronischer Video-, Musik- und Buchmedien Anwendung finden. Das einfachste Verfahren ist es, auf eine technische Überwachung der Rechte zu verzichten und rein juristisch vorzugehen: Vor oder beim Bezug der Daten stimmt der Nutzer zu, die Daten nur in der erlaubten Weise zu verwenden. Weitergehende Ansätze markieren die Daten individuell um eine Verbreitung ggf. rückverfolgen zu können oder arbeiten mit Verschlüsselung und software-überwachter Nutzung, die aber die Unterstützung der GIS-Hersteller für derartige Verfahren voraussetzt.
Eine wichtige Grundlage für viele dieser Sicherheitsmaßnahmen ist es, den zugreifenden Nutzer eindeutig und rechtssicher identifizieren zu können, also eine Authentifizierung durchzuführen. Je nach Anforderung kann es auch ausreichen, dass nicht ein einzelner Benutzer identifiziert wird, sondern dass der Nutzer eine bestimmte Rolle und damit bestimmte Nutzungsrechte für einen Dienst vorweisen kann.

1.4 Technische Lösungen für Sicherheitsmaßnahmen

Die meisten Sicherheitsmaßnahmen lassen sich auf einer einfachen prinzipiellen Basis realisieren: Beim Zugriff überträgt der Nutzer mit seiner Anfrage Zusatzinformationen. Diese werden verwendet, um beim Server Sicherheitsmaßnahmen durchzuführen. Bei der Zusatzinformation kann es sich um unterschiedlichste Angaben handeln, beispielsweise um eine Kombination aus Benutzernamen und Passwort, um einen individuellen kryptografischen Schlüssel, mit dem die Daten verschlüsselt werden sollen, oder um vorgesehene Nutzungsarten, die auf Zulässigkeit geprüft werden sollen.

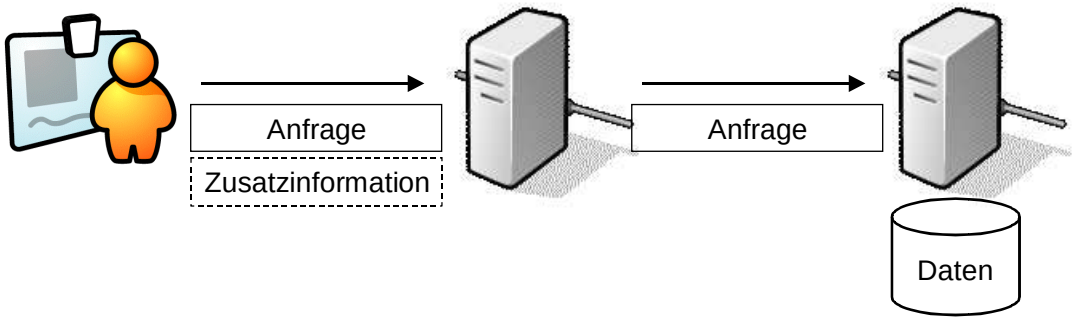


In praktisch allen Fällen enthält die Zusatzinformation zumindest Angaben, die für eine Authentifizierung ausreichen. Dabei kann es sich im einfachsten Fall um eine Kombination aus Name und Pass-

wort handeln, oder beispielsweise um eine elektronische Signatur oder eine kryptografisch geschütze Nutzungsberechtigung. Der Gesetzgeber hat hierbei im Rahmen des Signaturgesetzes und der Signaturverordnung (SigG und SigV) der elektronischen Signatur eine besondere Rechtswirkung zugeordnet, in dem er diese unter bestimmten, strengen Voraussetzungen einer handschriftlichen Unterschrift im Rechtsverkehr gleichgesetzt hat.

Für den Nutzer sollte diese Zusatzinformation mit minimalem Zusatzaufwand verbunden sein. Dies ist möglich, wenn die Client-Software sie weitmöglichst automatisch erstellt. Im Extremfall des „Single-Sign-On“ ist nur eine einmalige Aktion des Nutzers erforderlich, bei allen weiteren Anfragen werden die Sicherheitsmaßnahmen ohne Beteiligung des Nutzers vorgenommen.

Die Auswertung der Zusatzinformation wird in der Regel durchgeführt, bevor die eigentliche Anfrage bearbeitet wird. Aus diesem Grund bietet sich eine einfache Architekturvariante beim Server an: es wird eine separate Software-Komponente "vorgeschaltet". Diese Komponente empfängt alle Anfragen an den Server, extrahiert die Zusatzinformation, führt die Sicherheitsmaßnahmen durch und leitet die Anfragen an den eigentlichen Daten- oder Diensteserver weiter. Auch die Antworten des Servers werden in der Regel über die Sicherheitskomponente geleitet, um z.B. eine Verschlüsselung, Signierung oder eine Kontrolle der übertragenen Ergebnisse durchzuführen.

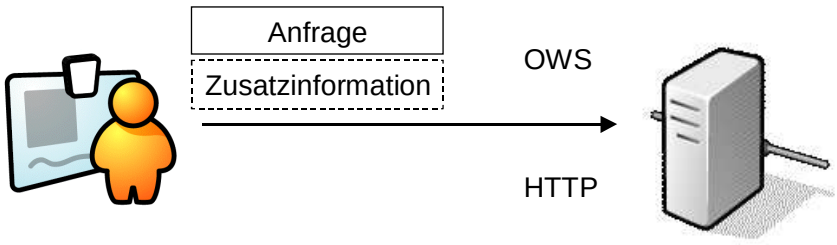


Ein solcher Architekturansatz wird in der Softwareentwicklung als "Fassade" bezeichnet. Der entscheidende Vorteil bei Verwendung einer Fassade ist, dass diese die definierten Schnittstellen des dahinter liegenden Services nicht verändert, und daher die vorhandene Systemlandschaft nur minimal angepasst werden muss.

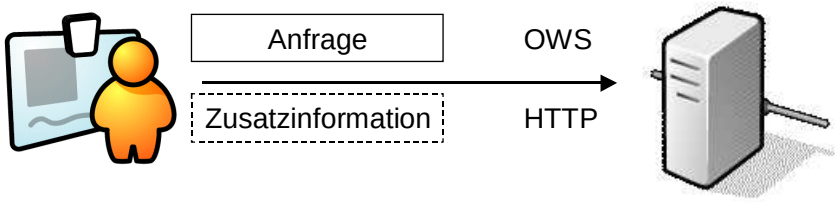
Zwischen Fassade und dem eigentlichen Dienst wird dabei das unveränderte Protokoll für Zugriff und Datenübertragung genutzt. Vor der Fassade muss das Protokoll dagegen modifiziert werden, um die Zusatzinformation für die Sicherheitsmaßnahmen transportieren zu können. Aber auch hier ist es von Vorteil, das Protokoll so wenig wie möglich abzuändern, so dass die Fassade im Idealfall transparent ist. Dadurch wird es möglich, dass auch existierende Clients weiterverwendet werden können, wodurch ein gemischter Zugriff auf gesicherte und ungesicherte Services vereinfacht wird.

1.5 Sicherheit für OGC Web Services

In der Praxis stellt sich damit die technische Frage, wie die notwendige Zusatzinformation im Protokoll untergebracht werden kann, ohne das Protokoll wesentlich zu ändern. Dies ist natürlich abhängig vom bisher verwendeten Protokoll. Es soll dies genauer für die Standard-Zugriffsprotokolle des OGC betrachtet werden, also den Web Map Service WMS, Web Feature Service WFS und ähnliche Standards, die auch als „OGC Web Services“ (OWS) bezeichnet werden.
Eine minimale Erweiterung wäre hier die Verwendung eines zusätzlichen Parameters, der die Zusatzinformation für die Sicherheitsmaßnahmen enthält. Kurzfristig ist die Nutzung eines "vendor-specific" Parameters möglich, der von der Fassade ausgewertet und gemäß dem Standard von allen anderen Servern ignoriert wird. Diese Lösung ist aber auf die spezielle Client/Dienste-Kombination festgelegt, da keine anderen Dienste diesen vendor-specific-parameter auswerten kann. Daher wäre es notwendig, dass für interoperable Lösungen beim OGC ein entsprechender Parameter standardisiert würde.

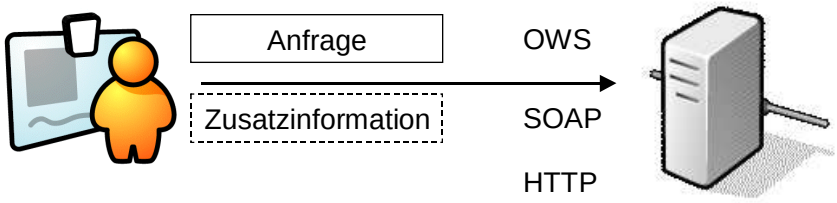


Eine elegantere und effektivere Methode setzt bei tieferen Protokollschichten an. WMS und die verwandten OGC-Standards basieren auf einem darunter liegenden Transportprotokoll. In der Praxis handelt es sich dabei in fast allen Fällen um HTTP, in Zukunft soll hier auch das Web-Service-Protokoll SOAP Verwendung finden.
Diese Transportprotokolle sehen bereits standardisierte Mechanismen für die Authentifizierung eines Benutzers vor. Bei HTTP wäre dies zum Beispiel die „basic authentication“, bei der es sich um die aus dem Internet bekannte Abfrage nach einem Benutzernamen und dem Passwort handelt.



Verknüpft man HTTP mit SSL/TLS, so erhält man zusätzlich die Möglichkeit Zertifikate zur Authentifizierung einzusetzen sowie eine Verschlüsselung des Netzwerkverkehrs auf der Transportebene zur Sicherung der Vertraulichkeit der Daten. Dieser Mechanismus ist vor allem beim Homebanking bereits gebräuchlich.

Das SOAP-Protokoll, auf dem Web Services nach Definition der Informatik basieren, geht hier sehr viel weiter. Es erlaubt die Übertragung von Sicherheits-Zusatzinformation in vielfältiger Weise für die unterschiedlichsten Anforderungen wie Verschlüsselung oder Signierung zur Integritätssicherung und Sicherung der Vertraulichkeit. Jedoch ist die Verwendung dieses Standards erst noch in der Erprobung beim Open Geospatial Consortiums.



Natürlich ist die Erweiterung des Protokolls um den Transport der Zusatzinformation nur ein Teilaspekt. Damit auch die Sicherheitsmaßnahmen interoperabel eingesetzt werden können, muss der Aufbau und die Bedeutung der Zusatzinformation ebenfalls standardisiert werden. Hier zeigt sich ein wesentlicher Vorteil der Unterbringung im Transportprotokoll, sei es HTTP oder SOAP: Mit basic authentication für HTTP und insbesondere mit dem OASIS-WS-Security-Standard für SOAP existieren bereits stabile und erprobte Standards und auch weitverbreitete Softwareumsetzungen dieser Standards.

Bisher außen vor gelassen wurde die Zugriffkontrolle nach der Authentifizierung des Benutzers. Hier werden beim Zugriff bestimmte Zugriffregeln für den Benutzer festgelegt und durchgesetzt. Dies kann ebenfalls beim Fassadenserver erfolgen, bei dem ja bereits die Identitätsinformationen für den Benutzer vorliegen. Für den Bereich der Autorisierung existiert für Web Services auf Basis des Protokolls SOAP der Standard XACML, der für die speziellen Anforderungen der Geodaten zu GeoXACML erweitert und beim OGC eingereicht wurde. Da dieser aber noch nicht zum Standard erhoben wurde, fehlen noch interoperable Lösungen, und Realisierungen von GDI sind derzeit noch auf die proprietären Lösungen der Hersteller angewiesen.

Ein anderes Beispiel für eine Sicherheits-Fassade im Zusammenhang mit OGC-Protokollen ist die Kombination Web Security Service WSS und Web Authentication Services WAS der GDI-NRW. Hierbei handelt es sich um eine nicht-transparente Fassade, die ein eigenes, speziell entworfenes Protokoll zwischen Client und Fassade verwendet, um sowohl Informationen zur Authentifizierung, die Anfragen als auch die Autorisierung zu übernehmen. Aber auch hier gilt, dass diese noch keinen verabschiedeten Standard darstellen.

1.6 Ausblick

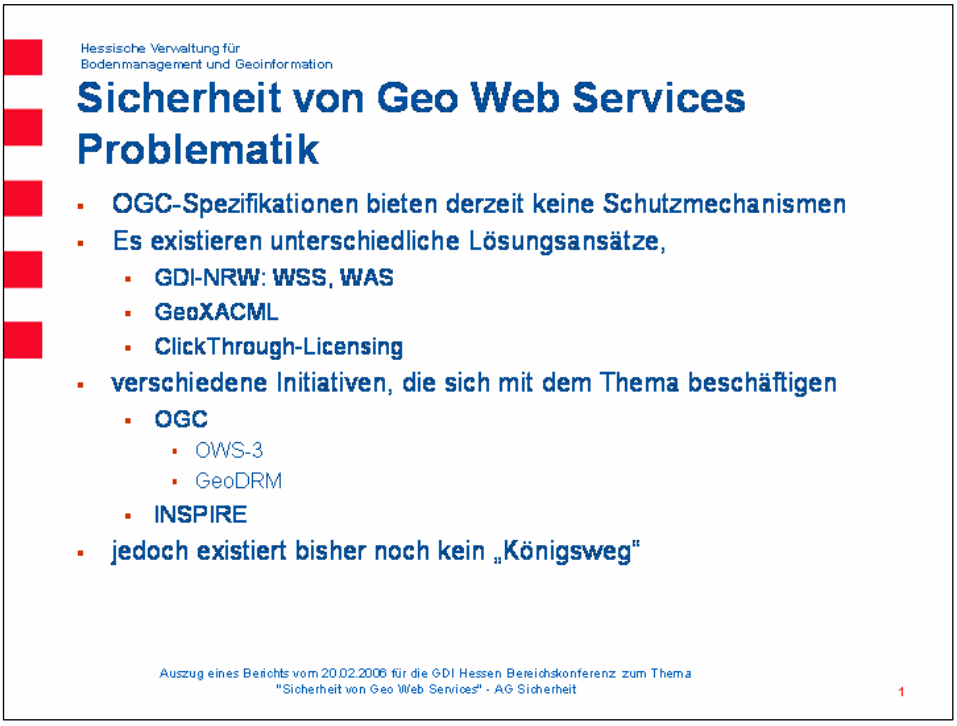
Sicherheitsmaßnahmen für Web-Services im Allgemeinen und für Geo-Web-Services im Besonderen sind ein relevantes, aktuelles, aber auch komplexes Thema. Der überwiegende Anteil der Maßnahmen ist allerdings nicht spezifisch für den Geo-Bereich. Hier bieten sich existierende Lösungen und Standards aus dem IT-Bereich an, die erprobt sind und eine umfassende Interoperabilität gewährleisten.

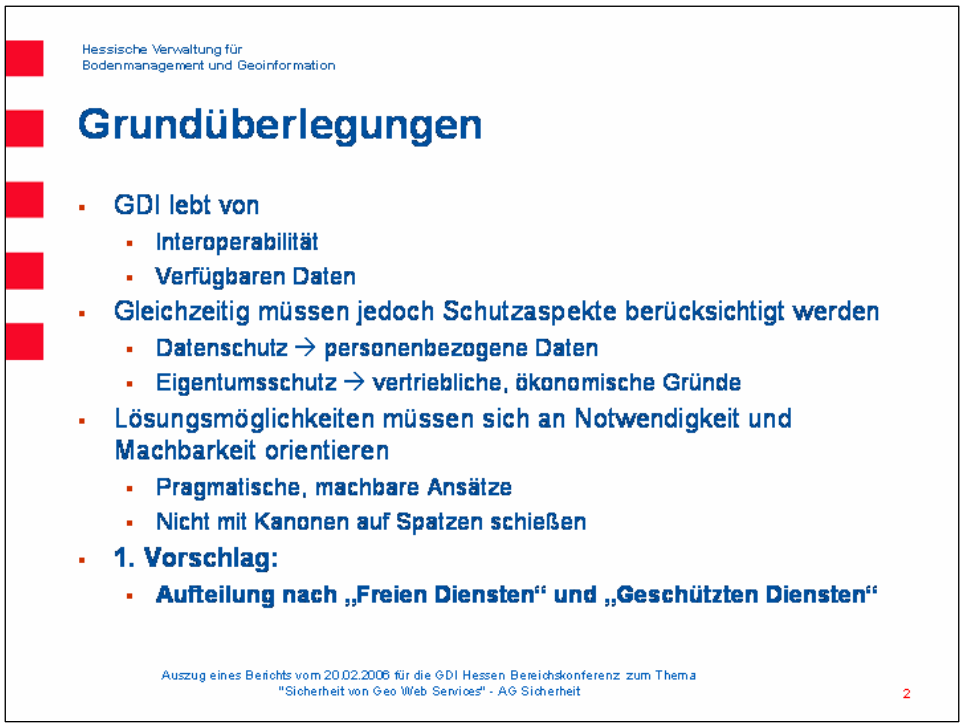
Leider ist zum aktuellen Zeitpunkt eine Zusammenführung der Standards im Geo-Bereich mit allgemeinen Sicherheitsstandards noch in Arbeit. Die steigende Nachfrage auch im Kreis der OGC-Mitglieder lässt hier aber Fortschritte erwarten, wie die Gründung verschiedener Arbeitskreise ja bereits andeutet. Die derzeit einfachste und am schnellsten zu implementierende Lösung besteht im Einbezug der Möglichkeiten, die das Transportprotokoll bietet, ohne existierende OGC-Schnittstellen zu modifizieren. Die bereits bestehenden Bestrebungen, SOAP als Transportprotokoll für OGC-Schnittstellen zu spezifizieren, machen absehbar, dass der OASIS-WS-Security-Standard in Zukunft auch für Geo-Web-Services nutzbar werden wird.

Wer bis dahin kurzfristig sichere Geo-Web-Services implementieren muss, ist auf proprietäre, nicht standardisierte Lösungen angewiesen, die zwar im engen Umfeld der jeweiligen Anwendung alle gewünschten Sicherheitsanforderungen erfüllen können, aber keine Interoperabilität mit anderen geschützten Anwendungen erlauben. Erst mittelfristig werden die Standards im Sicherheitsbereich verfügbar sein, die tragfähig genug für umfassende, breit nutzbare und abgesicherte Geodateninfrastrukturen und kommerzielle Geo-Web-Services sind.

2. Ergebnisse der Arbeitsgruppe Sicherheit

(im Auftrag der Bereichskonferenz GDI Hessen)





Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für Freie Dienste I

1. **Qualitätsverschlechterung**
   - Verringerung der Auflösung, Verwendung entsprechender Symbolisierungen , Kartengeneralisierung
   - Nutzen:
     - Abhebung zu Daten hoher Qualität, eingeschränkte Verwendbarkeit
   - Anforderungen und Auswirkungen
     - Daten in unterschiedlichen Qualitäten vorhalten oder Bereitstellung unterschiedlicher Qualitäten
   - Nachteil:
     - Performanceverlust
2. **Einblendung von Muster-Schriftzügen**
   - Nachteil:
     - Eingeschränkte Lesbarkeit bei Überlagerung → Verwendbarkeit der Dienste daher eingeschränkt
   - Nutzen
     - Abhebung zu Daten hoher Qualität, eingeschränkte Verwendbarkeit
   - Anforderungen
     - Neuer Schriftzug-Layer mit Geodatenlayer ausgeben oder automatischen Ausgabe durch Server

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

3

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für Freie Dienste II

3. **Copyright-Vermerk**
   - Schriftzüge mit i.d.R. transparentem Hintergrund, am Rand eines Kartenausschnitts
   - Nachteil:
     - Überlagerung mehrerer Dienste → eingeschränkte Lesbarkeit des Copyright
     - nureingeschränkten Schutz vor unautorisierter Verwendung → können entfernt bzw. überlagert werden Anforderungen
     - Ausgabe Coppyright-Layer mit Geodatenlayer oder automatische Ausgabe durch Server
4. **Click-Through-License**
   - Im Zusammenhang mit Initiative "OGC Web Services Phase 3" (OWS-3)
   - Keine Veränderung bestehender WMS/WFS-Server und -Dienste, sondern nutzt eine Proxy-Komponente in der DMZ (Demilitarisierte Zone).
   - Lösung zurzeit noch in der Planung bzw. Entwicklung

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

4

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für Freie Dienste III

5. **GetFeatureInfo-Request**
   - optionale Funktion in WMS-Spezifikation
   - Einschränkung bzw. Nichtausgabe von Sachattribute
   - Anforderungen
     - → Konfiguration des Dienstes
6. **Scale hints:**
   - Maßstabsangaben für die Sichtbarkeit einzelner Layer
   - Anforderungen
     - → Konfiguration
7. **Digitales Wasserzeichen**
   - Nutzen:
     - Missbrauch kann nachgewiesen werden
     - Problematik: Es wird nur eine passive Sicherheit gewährleistet
   - Anforderungen/Aufwand
     - Kosten für Erstellung des Wasserzeichens (Lizenzen) und Kosten für Recherche/Nachweis von Wasserzeichen

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 5

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Anforderungen:**
  - Eindeutige Authentifizierung des anfragenden Servers (= Client des WMS-Dienstes)
- **Lösungen**
  - Basistechnologien zur Authentifizierung
    1. IP-Filterung über Webserver
    2. Benutzerkennung und Passwort
       a. Basic Authentication
       b. Variablenübertragung in URL oder http-Body
          - http oder https
    3. Client-Zertifikate
    4. Kaskadierung
  - Kombination von Technologien zur Authentifizierung
    5. Kombination von IP-Filterung und Benutzerkennung/Passwort
    6. Proprietärer Proxy auf WMS-Client-Seite
    7. Lösungsansatz der GDI NRW: WAS und WSS

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 6

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Basistechnologien zur Authentifizierung**
  1. **IP-Filterung über Webserver**
  - **Vorteile**
    - kompatibel zu OGC-Standards
    - Einfache Implementierung
  - **Nachteile**
    - Adress-Translation, DHCP
    - IP-Spoofing
  - **Bewertung:**
    - Technik kostengünstig und OGC-Standard-konform
    - als alleiniges Mittel zur Authentifizierung jedoch nicht geeignet.

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 7

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten/ Basistechnologien I

2. **Benutzerkennung und Passwort**
   - **Übergabe Benutzerkennung und Passwort → Authentifizierung**
   a. **Basic Authentication**
     - Abfrage von User und Passwort durch das http-Protokoll im http-header.
     - Vorteil
       - einfache Umsetzung
     - Nachteil
       - Authentifizierungs-Daten sind unverschlüsselt.
       - Basic-Authentication ist im OGC-WMS-Standard nicht berücksichtigt → keine Unterstützung (Teste)
     - Bewertung
       - als alleiniges Mittel zur Authentifizierung ungeeignet

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 8

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Basistechnologien II → Benutzerkennung und Passwort

b. **Variablenübertragung in URL oder http-Body**
   - **Übergabe von Benutzerkennung und das Passwort als Parameter über die URL**
- **Variante 1: Verwendung von http**
  - **Unverschlüsselte Übertragung von Authentifizierungsinformationen**
  - **Vorteil**
    - OGC-WMS-konform, (Server Specific Parameter)
  - **Nachteil**
    - Die Authentifizierungs-Daten sind unverschlüsselt
  - **Bewertung:**
    - Authentifizierungsinformationen können abgehört werden→ als alleiniges Mittel zur Authentifizierung ungeeignet

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 9

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten/ Basistechnologien III

- **Variablenübertragung in URL oder http-Body**
  - **Variante 2: Einsatz von https**
  - **Authentifizierungsinformationen werden verschlüsselt übertragen.**
  - **Vorteil:**
    - hohes Sicherheitsniveau
  - **Nachteil**
    - https nicht im OGC-WMS-Standard berücksichtigt → keine Unterstützung von WMS-Clients (→ Tests)
  - **Bewertung**
    - Gefahr des Abhörens der Authentifizierungsinformationen ist minimiert.
    - Keine oder nur wenige WMS-Clients könnten den Serverdienst nutzen.

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit 10

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

3. **Client-Zertifikate**
   - **Vorteil**
     - höchste Sicherheitsstufe für die Kommunikation
   - **Nachteile**
     - https ist im OGC-WMS-Standard nicht berücksichtigt (Tests mit Clients)
   - **Bewertung**
     - Keine oder nur wenige WMS-Clients könnten den Serverdienst nutzen

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

11

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Anforderungen:**
  - Eindeutige Authentifizierung des anfragenden Servers (= Client des WMS-Dienstes)
- **Lösungen**
  - Basistechnologien zur Authentifizierung
    1. IP-Filterung über Webserver
    2. Benutzerkennung und Passwort
       a. Basic Authentication
       b. Variablenübertragung in URL oder http-Body
          - http oder https
    3. Client-Zertifikate
    4. Kaskadierung
  - Kombination von Technologien zur Authentifizierung
    5. Kombination von IP-Filterung und Benutzerkennung/Passwort
    6. Proprietärer Proxy auf WMS-Client-Seite
    7. Lösungsansatz der GDI NRW: WAS und WSS

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

12

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Kombination von Technologien zur Authentifizierung**

5. Kombination von IP-Filterung und Benutzerkennung/Passwort
   - Kombination der Basistechnologien „IP-Filterung" und „ Variablenübertragung in URL oder http-Body" → Erhöhung des Sicherheitsniveau
- Folgende Probleme bestehen weiterhin:
   - Ein Restrisiko des Missbrauchs bleibt bestehen.
   - Unverschlüsselt Transport von Nutzerdaten werden → nicht für die Übertragung personenbezogener Daten geeignet

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

13

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Kombination von Technologien zur Authentifizierung**

6. Proprietärer Proxy auf WMS-Client-Seite
   - Zur Authentifizierung Übertragung von Benutzerkennung und Passwort durch Variablenübertragung und https
   - Premiumkunde muss zusätzliches Dienstprogramm (Proprietärer Proxy) installieren:
      - Wandelt Standard-WMS-Anfragen (http) in https-Anfragen umwandelt und leitet diese an den Dienstanbieter weiter

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema "Sicherheit von Geo Web Services" - AG Sicherheit

14

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Lösungsmöglichkeiten für geschützte Dienste

- **Kombination von Technologien zur Authentifizierung**
7. **Lösungsansatz der GDI NRW: WAS und WSS**
   - Ähnlicher Ansatz wie Proprietärer Proxy auf WMS-Client-Seite.
   - Dienste bilden Zwischenschicht zwischen Client und Dienst.
   - WAS als Authentifizierungsservice d,h, bei einer Anfrage an den WMS wird diese auf den WAS umgelenkt und dort eine Prüfung der Autorisierung durchgeführt und anschließend ein „Ticket“ zur Identifikation erstellt. Im weiteren Verlauf wird die Anfrage an den WSS, der als Autorisierungsstelle arbeitet, weitergeleitet. Nach Prüfung durch den WSS wird die Anfrage schließlich an den WMS geleitet.
- **Vorteile**
  - Siehe Lösung 6.
- **Nachteile/Aufwand**
  - Lizenzkosten
  - Noch kein einheitlicher Standard für „Tikets“
  - Lösung ebenfalls noch kein OGC-Standard
  - Komplexe Umsetzung

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema
"Sicherheit von Geo Web Services" - AG Sicherheit

15

Hessische Verwaltung für
Bodenmanagement und Geoinformation

Ausblick

- **Aktivitäten auf unterschiedlichen Ebenen:**
  - OGC
    - Initiative OWS-3
      - Praxisbezogenes Herangehen
    - GeoDRM
      - Erstellung eines Referenzmodells → Vorlage Februar/März
  - INSPIRE
    - Deutsches Netzwerk DT data and service sharing (Wagner)
  - Standardisierungen in GDI-DE
- **FAZIT:**
  - Ein „Königsweg“ existiert noch nicht
  - Allerdings viele Aktivitäten, die in der nächsten Zeit zu Ergebnissen führen werden

Ansprechpartner bei Fragen:
Herr Rabe, Hessisches Landesamt für Bodenmanagement und Geoinformation, Wiesbaden. Email: Hans-Dieter.Rabe@hvbg.hessen.de

Auszug eines Berichts vom 20.02.2006 für die GDI Hessen Bereichskonferenz zum Thema
"Sicherheit von Geo Web Services" - AG Sicherheit

16

3. Weiterführende Literatur

Stand: 07. November 2006

- Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): E-Government-Handbuch, http://www.bsi.bund.de/fachthem/egov/3.htm, Stand 01.01.2006, ISBN 3-89817-180-9
- Bundesamt für Sicherheit in der Informationstechnik BSI (Hrsg.): IT-Grundschutzhandbuch http://www.bsi.bund.de/gshb/deutsch/download/GSHB2004.pdf, Stand 2004
- Franks, J. u.a.: HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, IETF Network Working Group, Juni 1999
- Kooperationsausschuss Automatisierte Datenverarbeitung KoopA ADV (Hrsg.): Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung, http://www.koopa.de/projekte/dokumente/PKI/Krypto-Leitfaden.pdf, Stand Dezember 2002
- Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung KBSt (Hrsg.): Standards und Architekturen für E-Government-Anwendungen Version 2.1, http://www.kbst.bund.de/download/SAGA_2_1.pdf, Stand September 2005
- Mitra, N. (Ed.): SOAP, Version 1.2, W3C Recommendation, 24. Juni 2003
- Nadalin, A., Kaler, C., Hallam-Baker, P., Monzillo, R. (Eds.): Web Services Security: SOAP Message Security 1.0 (WS-Security), OASIS Open, 15. März 2004
- OSCI-Leitstelle (Hrsg.): OSCI-Transport 1.2 – Spezifikation –, http://www.osci.de/materialien/osci_spezifikation_1_2_deutsch.pdf, Stand 06. Juni. 2002
- OSCI-Leitstelle (Hrsg.): OSCI-Transport 1.2 – Entwurfsprinzipien, Sicherheitsziele und –mechanismen –, http://www.osci.de/materialien/osci_entwurfsprinzipien_1_2.pdf, Stand 06. Juni 2002
- Schneier, B.: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt, 1. Auflage, Heidelberg: dpunkt.verlag, 2001 – Übersetzung aus dem Amerikan. – ISBN 3-89864-113-9
- Whiteside, A. (Ed.): OpenGIS Web Service Common Implementation Specification, Version 1.0, Open Geospatial Consortium, Mai 2005