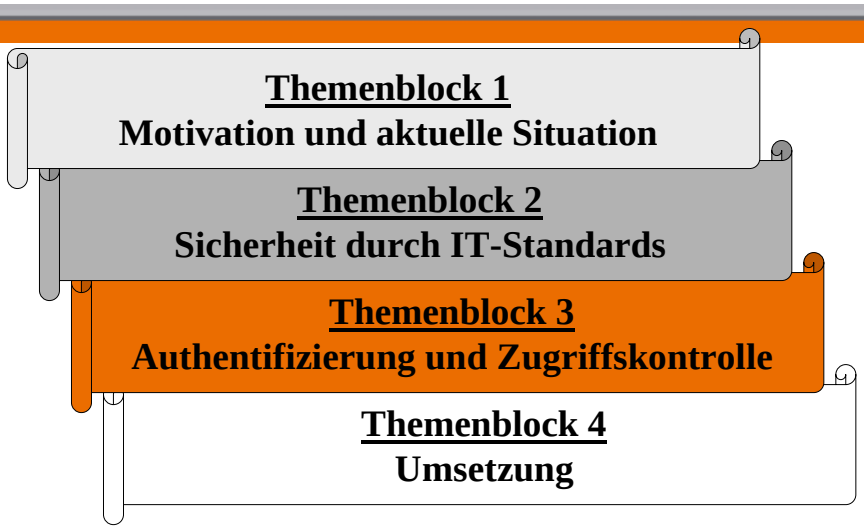
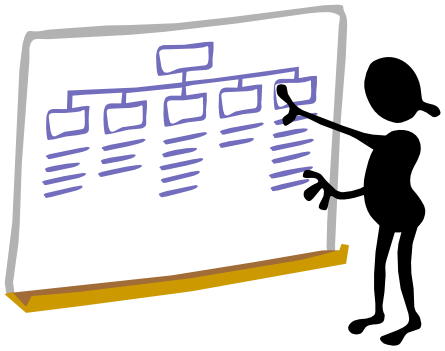
Standardbasierte Sicherheitslösungen für OGC Web Services: Authentifizierug und Zugriffskontrolle

Andreas Matheus
Universität der Bundeswehr München

Was erwartet Sie in diesem Vortrag?

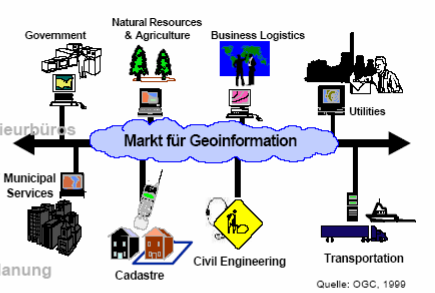


Themenblock 1:
Motivation und aktuelle Situation



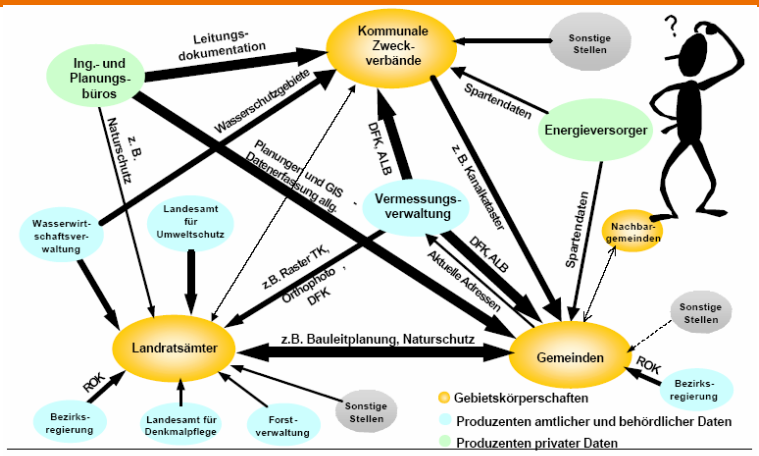
Anwendungsbereiche für GIS und Geodaten

- **Immobilienwirtschaft**
  Bewertung von Immobilien
- **Mobile Data Services**
  Content für Netzprovider
- **Infrastrukturplanung**
  Gebietskörperschaften, EVU`s, Ingenieurbüros
- **Telematik**
  Navigation, Assistance & Emergency
- **Logistik**
  Routen- & Flottenplanung
- **Tourismus**
  Full Travel Services, Virtuelle Reiseplanung
- **Geomarketing**
  Standort- und Gebietsplanung
- **Kommunaler Bereich**
  Kanal, Trinkwasser, Beitragsberechnung, Bodenmanagement
- **Umwelt**
  Landespflege, Naturschutz



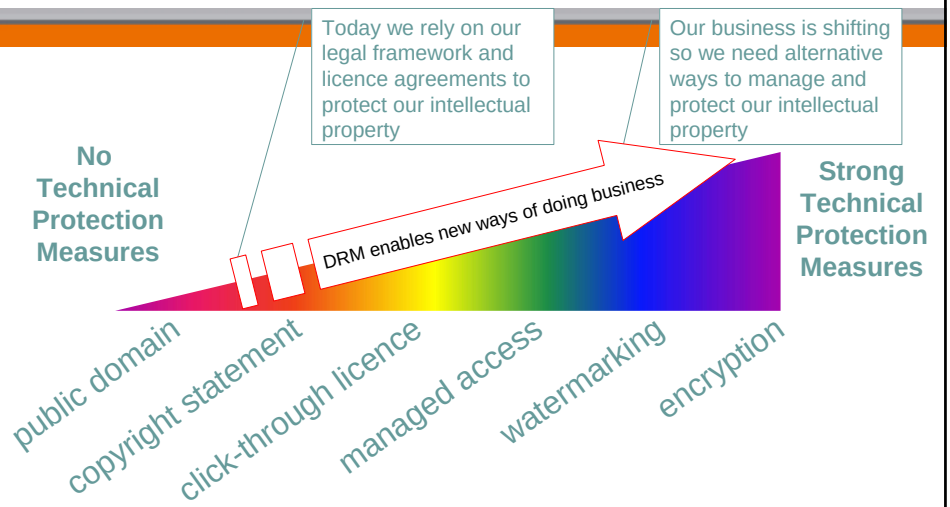
Quelle: Schilcher, M., Deking, I., Donaubauer, A., Hartl, T., Lohse, Ch.: Marktanalyse. Der Geoinformationsmarkt Bayern für Landkreise, kommunale Zweckverbände und Gemeinden. Technische Universität München. München, 2000.

Bedarf für Austausch von Geodaten



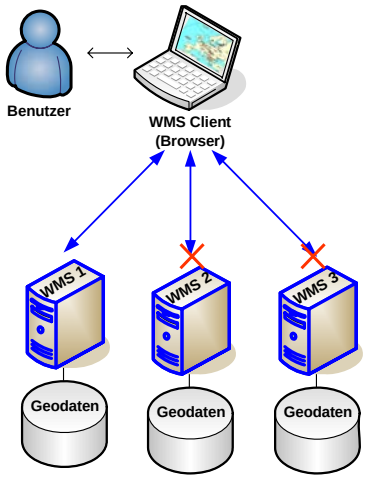
Quelle: Schilcher, M., Deking, I., Donaubauer, A., Hartl, T., Lohse, Ch.: Marktanalyse. Der Geoinformationsmarkt Bayern für Landkreise, kommunale Zweckverbände und Gemeinden. Technische Universität München. München, 2000.

GeoDRM: Measures to protect IP



Quelle: Graham Vowels, Ordnance Survey, Southampton, UK – Chair OGC'S GeoDRM Special Interest Group

OGC Service-basierte Geodatennutzung



- Interaktion Benutzer – Browser-Client – OpenGIS Web Service
- Kombinierte Nutzung verteilter Geodaten ohne Zugriffsschutz
- HTTP-GET basierter Aufruf:

  http://geosrv02.informatik.unibw-muenchen.de/wega-mars/servlets/MarsServlet? VERSION=1.1.0& REQUEST=GetCapabilities& SERVICE=WMS

Welche Anforderungen gibt es?

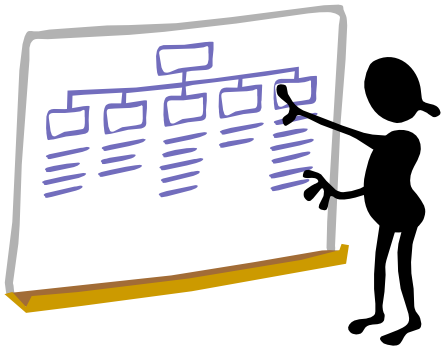
Trust zwischen Kommunikationspartnern
Integrität, Vertraulichkeit, Non-Repudiation, ...

Disclaimer-Enablement

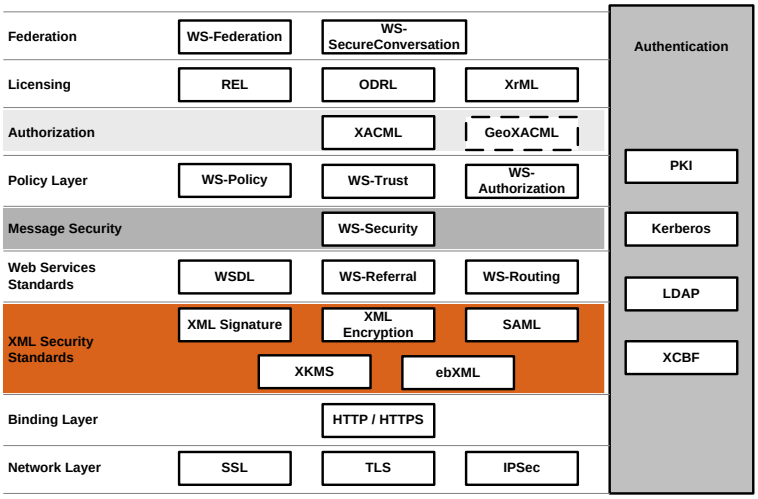
- Flexible Deklaration von Zugriffsrechten
- Raumbezogene Zugriffsrechte

Sichere Authentifizierung
Single-Sign-On
Mehr-Faktor-Authentifizierung

Themenblock 2:
Sicherheit durch IT-Standards



Security Standards ...



Der WS-Security Standard von OASIS

- Web Services Security Standard ermöglicht inter-operablen Austausch von Sicherheitsinformation

  http://www.oasis-open.org/ws-security
- Beschreibt einen Framework für
  - die Strukturierung von Sicherheitsinformation
  - den Austausch von Sicherheitsinformationen
- Definiert Profile für verschiedene Protokolle
  - SOAP Binding über HTTP ← zukünftige OGC Schnittstellen
  - HTTP-GET/POST Binding ← bisherige OGC Schnittstellen

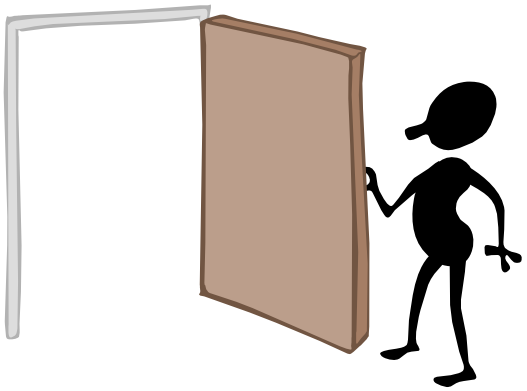
OGC Web Services und SOAP?

OGC® News, July 2006

NEWS FROM THE EDINBURGH MEETING

„Approval of an OGC policy position on SOAP and WSDL. Going forward, all OGC Web Service related specifications will have a mandatory annex defining a SOAP binding and a WSDL expression of that binding“, which is optional to be implemented.

Themenblock 3: Authentifizierung und Zugriffskontrolle



Eine Form von Zugriffskontrolle: Disclaimer-Enablement

- Use Case: Benutzer erhält erst dann Zugriff, wenn er den Nutzungsbedingungen zugestimmt hat
  (a) Bekannter Benutzer
  (b) Anonymer Benutzer
- Anforderung: Nutzung von existierenden Infrastrukturen
- Umsetzung:
  - Sicherheitsrelevante Informationen werden mit dem Service Aufruf mitgeschickt
  - Serviceseitiger Proxy analysiert Aufruf + Zusatzinformation

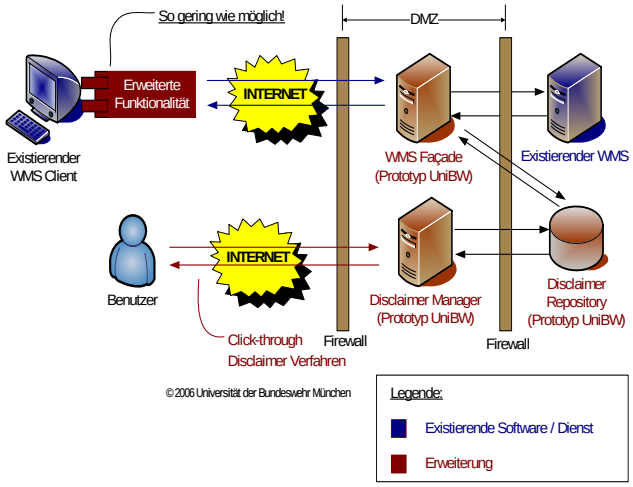
  ⇒ Transportmechanismus erforderlich!

Transportmechanismen für das Übertragen von Sicherheitsinformationen

- HTTP Cookie (Standard vom IETF – RFC 2109)
  - Wird nicht von allen Clients unterstützt
  - Sicherheitsaspekt „Domänengrenze“
- Vendor-Specific-Parameter
  - Müsste von allen OGC standardkonformen Clients unterstützt werden

⇒ Wie kann Interoperabilität bei der zusätzlich übertragenen Information sichergestellt werden?

Einfache Architekturerweiterung zum Disclaimer-Enablement



Was ist SAML?

- **S**ecurity **A**ssertion **M**arkup **L**anguage (SAML)
  - Standard von OASIS
  - Übertragung von sog. Assertions (Zusicherungen)
    - Identitätsinformation - Wer ist wer?
    - Autorisierungsinformation – Wer darf was?
    - Authentifizierungsinformation – Wer hat sich wie angemeldet?
- Unterstützt
  - Single-Sign-On (SSO)
  - SSO-Browser Profile ermöglicht HTTP-GET/POST basierte Übertragung von Identitätsinformation ⇒ SAML Artefakt
- SAML Artefakt = Zeiger auf Identitätsinformation

Was ist das SAML Browser-Profile und wie kann es verwendet werden?

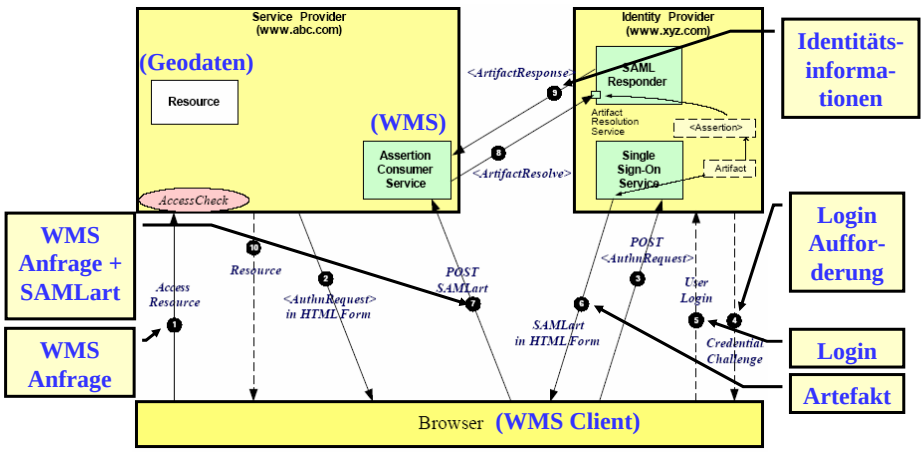


Figure 17: SP initiated: POST->Artifact binding

Was ist XACML / GeoXACML?

- e**X**tensible **A**ccess **C**ontrol **M**arkup **L**anguage (XACML)
  - Standard von OASIS
  - XML-basierte Deklaration von Zugriffsrechten
  - Erweiterbar (zusätzliche Attribute und Funktionen)
  - **Anwendbar auf XML strukturierte Daten**
- **Geo**spatial XACML (GeoXACML)
  - Discussion Paper vom OGC (05-036)
  - Erweitert die XACML um raumbezogene Zugriffsrechte
  - **Anwendbar auf GML strukturierte Geodaten**

Was ist der Unterschied?

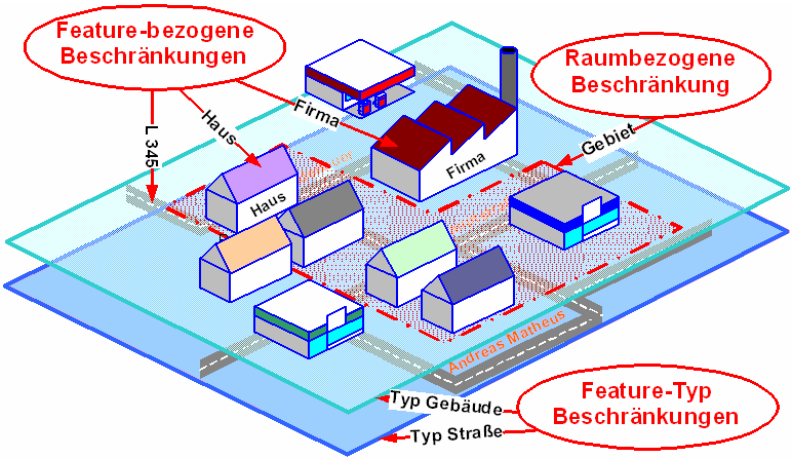
- **XACML**
  - OASIS Standard
- Zugriffsrechte
  - ✓ Umgebungsinformation
  - ✓ Auflösung
  - ✓ Layer, bzw. Feature Typ
  - ✓ Einzelne Features
  - ✗ **Keine** raumbezogenen Zugriffsrechte

- **GeoXACML**
  - Z.Z. OGC Discussion Paper
- Zugriffsrechte
  - ✓ Umgebungsinformation
  - ✓ Auflösung
  - ✓ Layer, bzw. Feature Typ
  - ✓ Einzelne Features
  - ✓ Raumbezogene Zugriffsrechte werden unterstützt

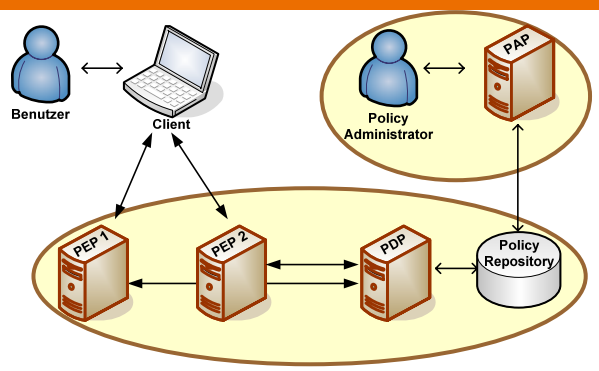
Was sind beispielhafte Zugriffsrechte für einen Web Map Service?

- GetMap-Abfrage im Binärformat
- für die Layer Gebäude und Straße
- ist dem Benutzer mit der Rolle ABC oder dem Namen Mustermann erlaubt, wenn er
- durch die Authentifizierungsmethode Benutzer/Passwort und X.509 Zertifikat identifiziert ist,
- die gewählte Auflösung gröber als 40 Pixel/m2 ist,
- der Ausschnitt innerhalb des (gml:Polygon=…) liegt, der
- Client die IP-Adresse 127.2.1.34 hat
- und der Zugriff von Montag – Freitag, zwischen 9 - 16 Uhr liegt
- FeatureInfo-Abfrage für das
- Layer Bodenrichtwerte ist dann erlaubt, wenn sich das
- Feature innerhalb der Stadtgrenze von München befindet und der
- Benutzer Mitarbeiter der Stadt München ist (z.B. die Rolle Munich hat)

Geodaten-spezifische Zugriffsrechte mit GeoXACML (Visualisierung)



(Geo)XACML-basierte Architektur für eine verteilte Zugriffskontrolle

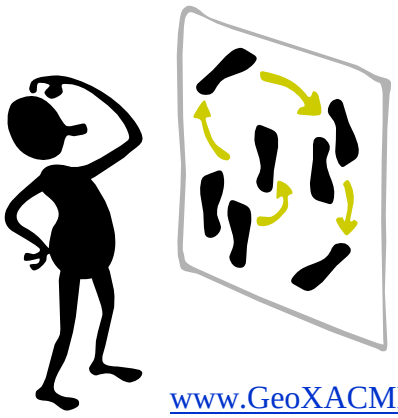


Administration

Zugriffskontrolle

- PAP = Policy Administration Point (Editieren von Rechten)
- PDP = Policy Decision Point (Autorisierungsentscheidung)
- PEP = Policy Enforcement Point (Fassade Geo Web Service)

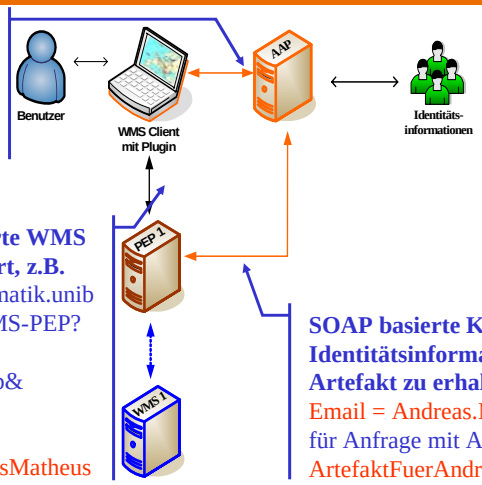
Umsetzung



www.GeoXACML.org/demo

Wie geschieht die Übertragung der Identitätsinformation OGC konform?

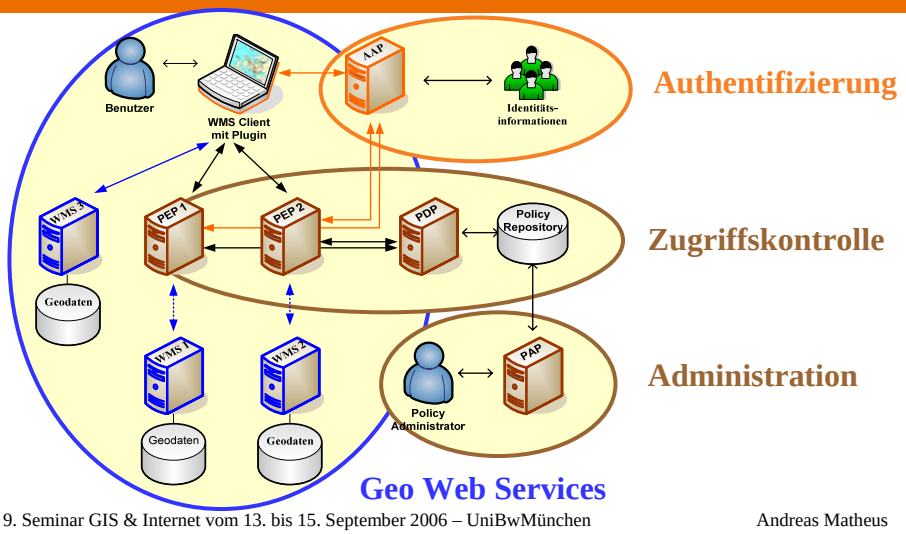
Login via HTTPS
Antwort:
SAML Artefakt,
z.B. ArtefaktFuer
AndreasMatheus



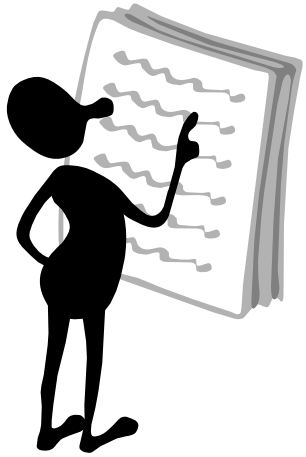
HTTP-GET kodierte WMS Anfrage + SAMLart, z.B.
http://iisdemo.informatik.unibw-muenchen.de/WMS-PEP?
VERSION=1.1.0&
REQUEST=GetMap&
SERVICE=WMS&
SAMLart=
ArtefaktFuerAndreasMatheus

SOAP basierte Kommunikation um Identitätsinformation für SAML Artefakt zu erhalten, z.B.
Email = Andreas.Matheus@unibw.de
für Anfrage mit Artefakt
ArtefaktFuerAndreasMatheus

Wie sieht die erweiterte Infrastruktur aus?



Zusammenfassung



Standards ...

- OGC Spezifikationen adressieren keine Sicherheit
- WS-Security: Standard von OASIS
  - Framework zur Übertragung von Sicherheitsinformation
- SAML: Standard von OASIS
  - Authentifizierung mit Single-Sign-On / Single-Sign-Off
- XACML: Standard von OASIS
  - Zugriffskontrolle für **XML** formatiere Daten
- GeoXACML*: Standard vom OGC?
  - Zugriffskontrolle für **GML** formatierte Geodaten über WFS, aber auch Kartenabfragen mit WMS

*: Standardisierung durch das OGC erwartet

Auswirkungen auf OGC Standards ...

- Für existierende OWS Standards **ohne** SOAP
  - Übertragung von Identitäsinformation gemäß SAML Web Browser SSO Profile (SAML Artefakt)

    => Change Request für OGC Web Services: Optionale Nutzung des Parameters SAMLart
- Für zukünftige OWS Standards **mit** SOAP
  - Übertragung von Identitäsinformation gemäß WS-Security
- Standardisierung von GeoXACML
  - Durchsetzung „feingranularer“ raumbezogener Zugriffsrechte

OGC‘s Security Working Group

The mission is to establish an interoperable security framework for OpenGIS Web Services to enable protected geospatial information processing.

Serve as a forum for the collaboration of developers and users to provide recommendations and guidance how to apply existing security related IT-Standards to accommodate geo-specific security aspects in the “OGC-world”.

Only if otherwise not possible, release own standards.

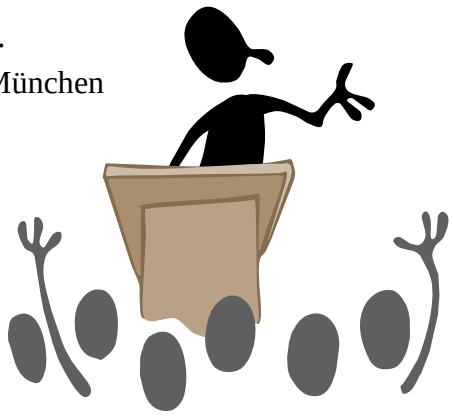
Was sind weitere Ziele / Aktivitäten?

- OGC Standardisierung
  - WS-Security / SAML basierte Authentifizierung
  - GeoXACML basierte Zugriffskontrolle
- Aktuelle Forschungsaktivitäten
  - Bayerischen LVG: „Disclaimer-Enablement“ für WMS
  - OWS-4: Zugriffskontrolle für WFS-T mit GeoXACML
  - OWS-4: IPR zum Thema „Trusted Geo Web Services“
- Zukünftige Forschungsaktivitäten
  mit Ihnen!?

Vielen Dank für Ihre Aufmerksamkeit!

Andreas Matheus, Dr. rer. nat.
Universität der Bundeswehr München

andreas.matheus@unibw.de



Literaturverzeichnis

- OGC
  - http://www.opengeospatial.org/specs/?page=specs
- GeoXACML
  - Demo und OpenSource Software unter www.GeoXACML.org
  - OGC Discussion Paper „GeoXACML, a spatial extension of XACML“ https://portal.opengeospatial.org/files/index.php?artifact_id=10471
  - Persönliche Veröffentlichungen zu GeoXACML auf OASIS Hompage http://lists.oasis-open.org/archives/xacml/200505/msg00028.html
- XACML
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
- WS-Security
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
- SAML
  - http://www.oasis-open.org/specs/index.php#samlv2.0