der Bundeswehr Universität München

GeoXACML und SAML

Ubiquitous Protected Geographic Information

Dr. Andreas Matheus
Universität der Bundeswehr München
Andreas.Matheus@unibw.de

Was erwartet Sie in diesem Vortrag?

- Einleitung
  - OpenGIS Web Services
  - Authentifizierung, Authentisierung und Zugriffskontrolle
- Interoperabilitätsbasierte Anforderungen
- Standards von OASIS
  - Security Assertion Markup Language (SAML)
  - eXtensible Access Control Markup Language (XACML)
- GeoXACML
- Beispielhafte Umsetzung
- Zusammenfassung und Ausblick

GeoXACML und SAML

- GeoXACML
  - Geospatial eXtensible Access Control Markup Language
  - OGC discussion paper 05-036
  - http://portal.opengeospatial.org/files/index.php?artifact_id=10471
- SAML
  - Security Assertion Markup Language
  - Standard von OASIS aktuell in der Version 2
  - http://www.oasis-open.org/specs/index.php#samlv2.0
- Was es ist und wofür man es verwenden kann, erfahren Sie in den nächsten 29 Minuten…

Authentifizierung und Authentisierung

- Authentifizierung
  - … der Vorgang der Überprüfung der behaupteten Identität eines Kommunikationspartners (Entität)
- Authentisierung
  - … ist der Vorgang des Nachweises der eigenen Identität
- Methoden der Authentisierung
  - Was man hat: z.B.: EC- oder Signaturkarte
  - Was man weiß: z.B.: PIN oder Benutzername u. Passwort
  - Was man ist: z.B.: Fingerabdruck oder Gesichtsscan
- Starke Authentisierung nutzt Methodenkombination
  - Z.B.: EC-Karte und PIN oder Signaturkarte mit Passwort

Zugriffskontrolle

- Zugriffsrechte / Autorisierung / Durchsetzung
  - **Z.-Rechte**: Wer darf was (Subjekt, Operation, Ressource)
  - **Autorisierung**: Herbeiführung der Z.-Entscheidung, für einen konkreten Zugriff anhand vorhandener Z.-Rechte
  - **Durchsetzung**: Erlaubt oder unterbindet den Zugriff, basierend auf der Z.-Entscheidung
- Zugriffskontrollstrategien
  - **DAC**: Discretionary AC (Objekteigentümer bestimmt)
  - **MAC**: Mandatory AC (Systemadministrator bestimmt)
    - Lattice-based AC: Mehrere Subjekte und mehreren Objekte
    - Rule-based AC: Bedingungen auf Subjekt – u. Objekteigenschaften

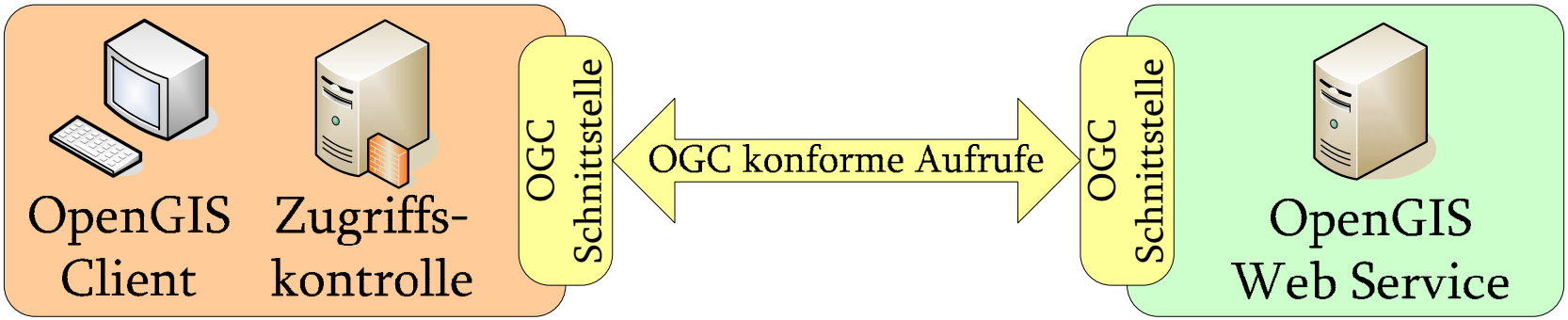
Zugriffskontrolle

- Verschiedene Typen von Kontrolle
  - Kontrolle des Daten, bzw. Informationsflusses
    - Bell – LaPadula Modell: *No read up, no write down*
  - Kontrolle des Zugriffs
    - Capabilities: Rechte für Operationen auf Ressourcen (O, R) die an Subjekte gegeben werden
    - ACL: Rechte für Operationen auf Objekte, die durch Subjekte ausgeführt werden können (S, O) die bei der Ressource sind
- Beispiel Zugriffskontrollmatrix
  - Capabilities für Joe: (WMS-1, execute)
  - ACL für WMS-2: (Bob, execute)

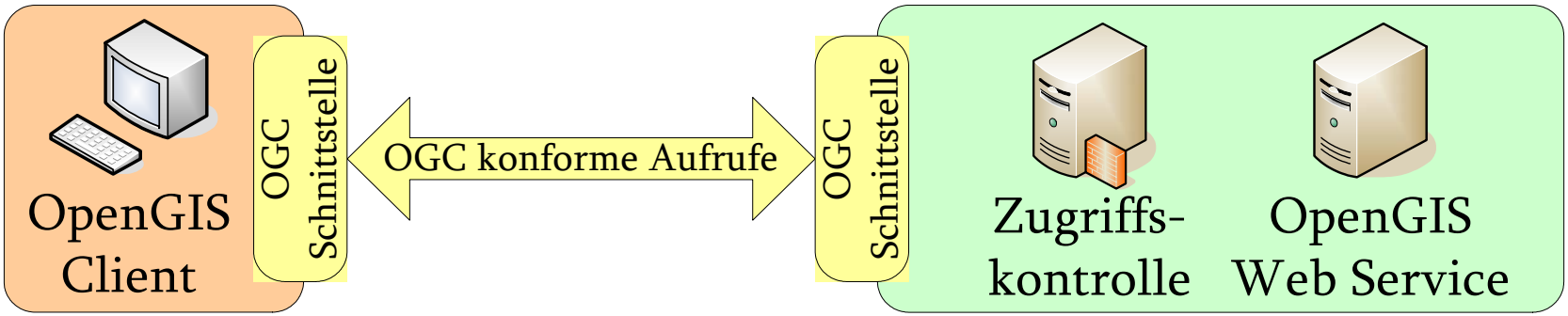
	WMS-1	WMS-2
Joe	execute	
Bob	execute	execute

Umsetzungsarten der Zugriffskontrolle

- Clientseitige Umsetzung (Capabilities)



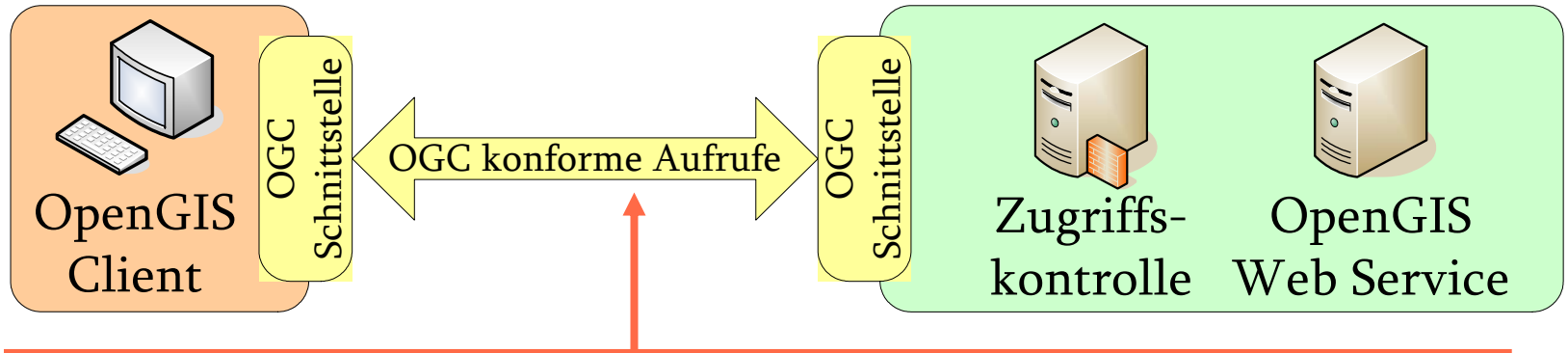
- Serviceseitige Umsetzung (ACL)



OpenGIS Web Service

- Dienst, der Zugriff auf Geoinformationen ermöglicht
- Es gibt verschiedene Typen
  - WMS: Abfrage von Karten und Zusatzinformationen
  - WFS: Abfrage und Veränderung von Features
  - …
- Interoperabilität durch standardisierte Schnittstelle
  - Vordefinierte Parameter (Name, Typ und Bedeutung)
  - HTTP Binding für Get und Post
  - HTTP-SOAP Binding für zukünftige Versionen
- http://myMapServer ? SERVICE=WMS & VERSION= 1.1.0 & REQUEST=GetCapabilities

Interoperabilitätsbasierte Anforderungen bei serviceseitiger Umsetzung



- OGC schnittstellenkonforme Übertragung von Identitätsinformation vom OpenGIS Client zur Zugriffskontrolle (Proxy für OpenGIS Service)
- Erweiterung der OpenGIS Web Service Schnittstelle
  - Sog. Vendor-Specific-Parameter (VSP)
  - http://myMapServer ? SERVICE=WMS & VERSION=1.1.0 & REQUEST=GetMap & USER=AM & PASS=Geheim ☺

Standard von OASIS: SAML

- Security Assertion Markup Language
- XML basiertes Framework zum Austausch von Sicherheitsinformationen durch Zusicherungen
  - Zusicherungen (engl. Assertions)
    - Beschreibung von Formaten für verschiedene Zusicherungen: Authentifizierung, Authentisierung und Autorisierung
  - Protokoll
    - Beschreibung des Austausches von Sicherheitsinformation durch SAML Zusicherungen
  - Binding
    - Beschreibung durch verschiedene Profile, wie SAML in verschiedenen Umgebungen angewendet werden kann

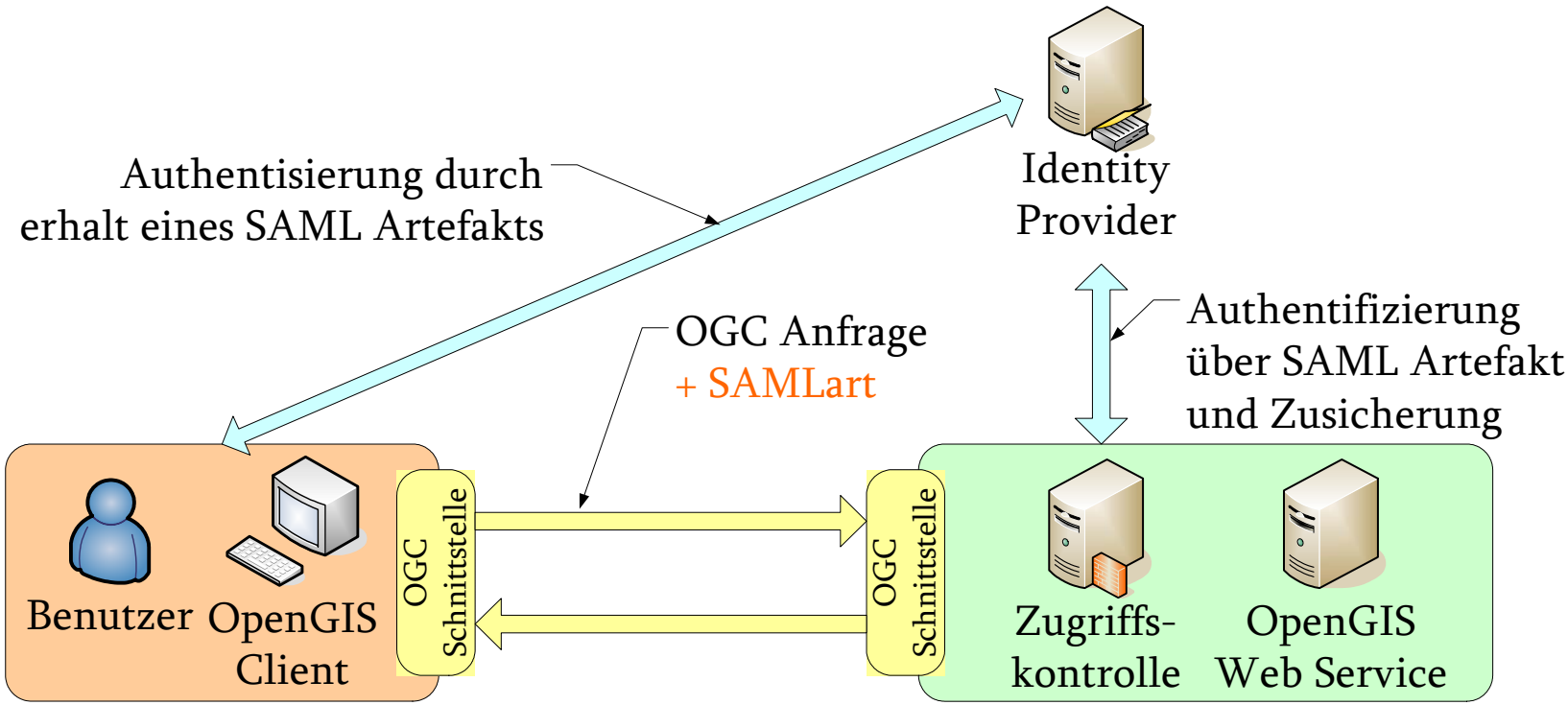
Browser Single Sign On (SSO) Profile

- (Web) Browser Umgebung
  - HTTP zwischen (Web) Client und (WWW) Server
- Austausch von Sicherheitsinformationen basiert auf sog. SAML Artefakten.
- SAML Artefakt (42 Byte lang) ist eine Web-fähige Referenz auf Zusicherungen
  - z.B. 000166a9b8c9e8fac489d8s9384766a9b8c9e8fac43d8fac66a9b89b8c9e8c9e489d8s9384766afac43d

- Nutzung eines sog. Identity-Providers, der die Artefakte ausgibt und Abfragen von Zusicherungen (zum Artefakt) erlaubt

Nutzung von SAML im OGC Kontext

- Erweiterung der OpenGIS Web Service Schnittstelle mit SAMLart als optionaler Parameter



Standard von OASIS: XACML

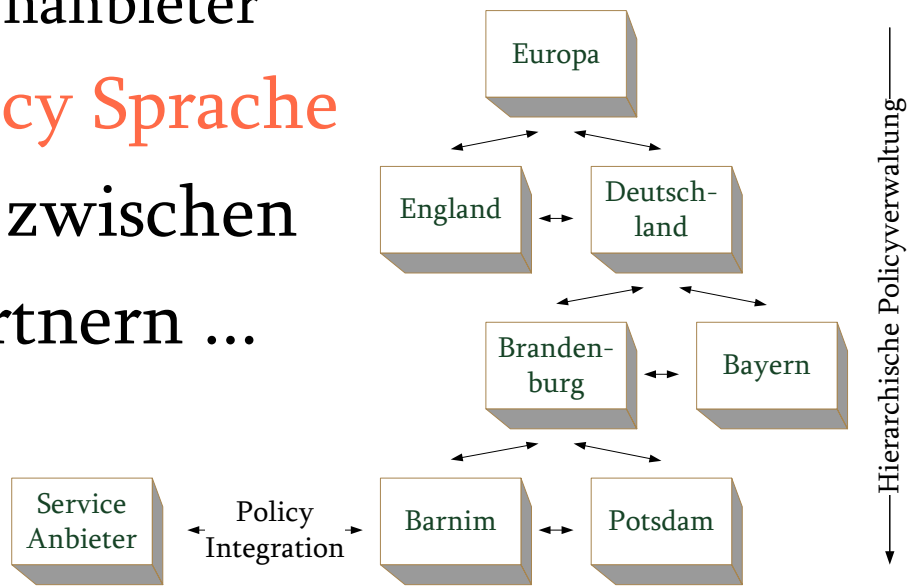
- eXtensible Access Control Markup Language
- Modulare Zugriffskontrolle durch Verwendung einer XML basierten Policy Beschreibungssprache
- Zugriffsrechte können auf Objekte durchgesetzt werden, die in XML beschrieben sind
- Aufbau (Inhalt) des Standards
  - Policy Language: Struktur, Elemente und Funktionen
  - Protokoll: Austausch von Nachrichten zwischen Modulen der Zugriffskontrolle
  - Autorisierung: Zugriffskontrollentscheidung für eine bestimmte Anfrage anhand einer Policy herbeiführen

Warum XACML (im Rahmen einer GDI)?

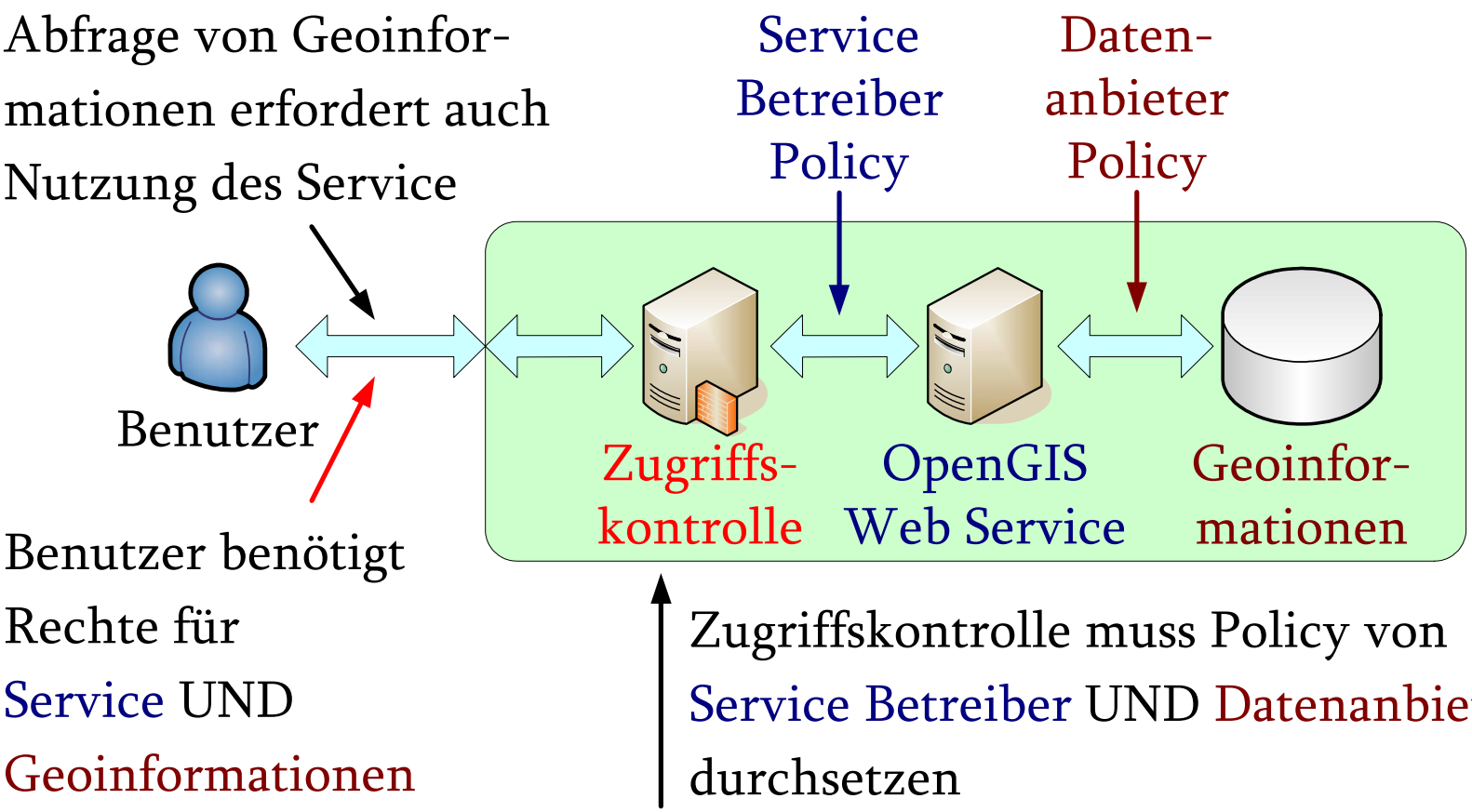
- Unterstützung für hierarchische Rechteverwaltung
  - (Europa) → BR Deutschland → Land → Kommune → …

  und Integration bei verteilter Rechteverwaltung
  - Diensteanbieter ↔ Datenanbieter

  durch gemeinsame Policy Sprache
- Austausch von Policies zwischen Behörden, Geschäftspartnern …



Integration bei verteilter Rechteverwaltung



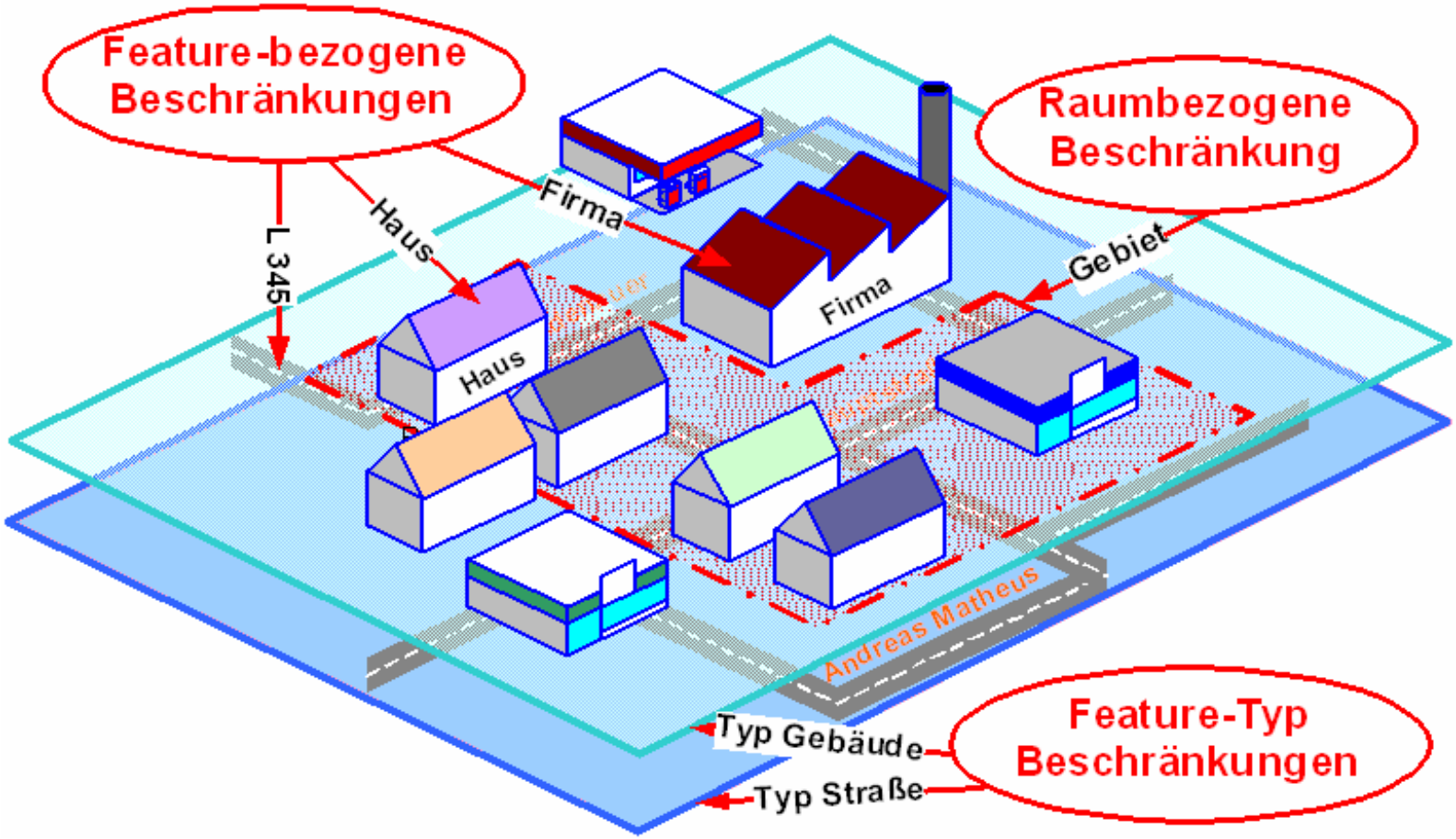
GeoXACML

- Geospatial eXtensible Access Control Markup Language
- Realisierung von geo-spezifischen Anforderungen durch Nutzung der XACML Erweiterungspunkte
  - Spatial Attributes durch Nutzung von GML Geometry

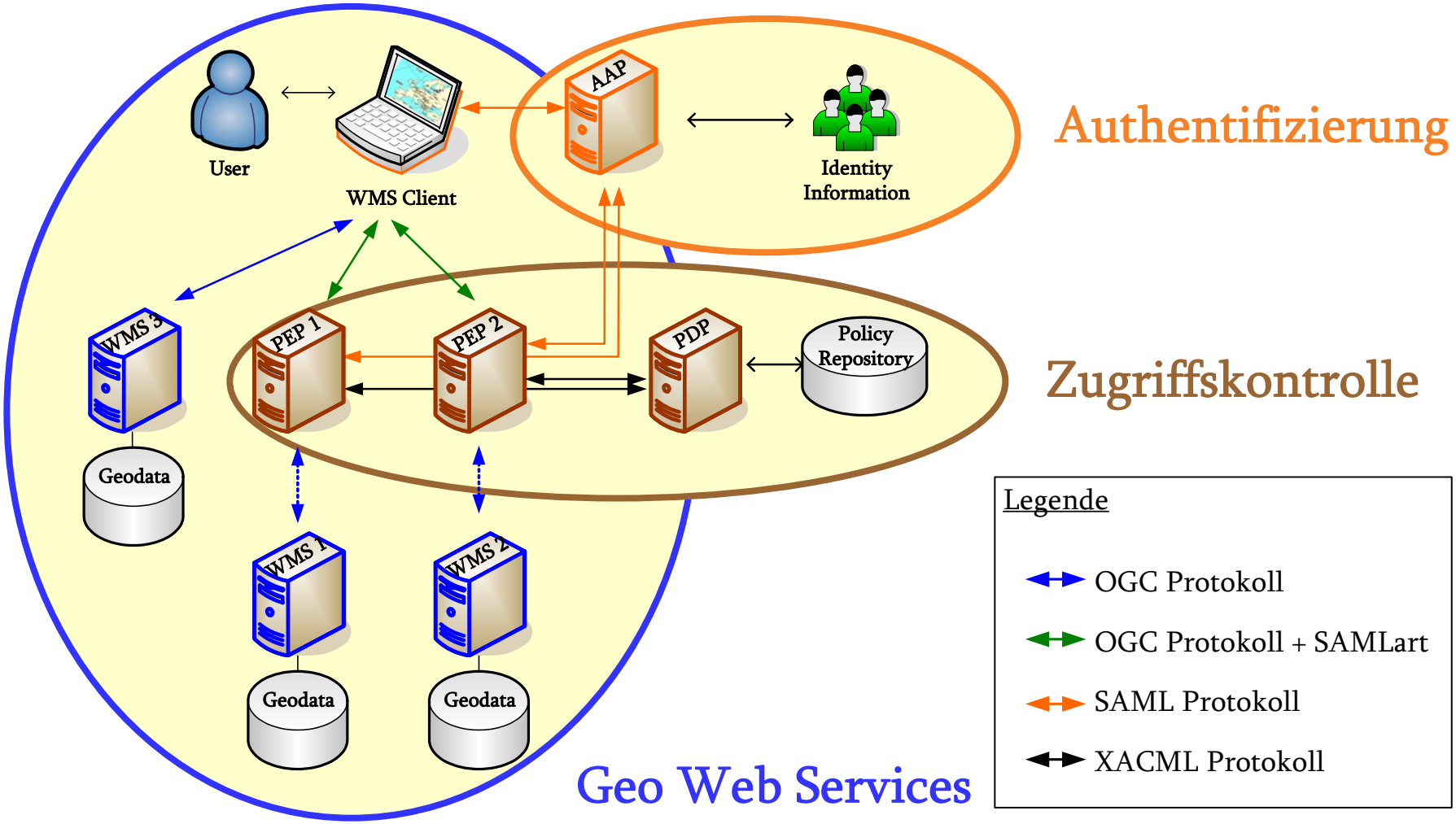
    Point, LineString, LinearRing, Box, Polygon
  - Testfunktionen zur Überprüfung von topologischen Beziehungen zwischen Geometrien

    Disjoint, Touches, Crosses, Within, Overlaps, Intersects, Equals, Contains
- Durchsetzung von Zugriffsrechten auf GML strukturierte Geoinformationen

Feature-spezifische Zugriffsbeschränkungen



SAML + GeoXACML @Work



Zusammenfassung

- Nutzung von SAML und GeoXACML erlaubt eine flexible und modulare Umsetzung von Sicherheitsaspekten für OpenGIS Web Services
- Beispielhafte Nutzung von SAML zur Umsetzung des Disclaimer-Enablements für den DeutschlandViewer

  http://137.193.63.192/dv_develop/
- Beispielhafte Nutzung von SAML und GeoXACML
  - Zugriffsbeschränkung eines WMS (mit SAMLart)
    http://www.geoxacml.org/demo/WMS-Demo-Client.html
  - Lizenzierte Nutzung von WFS-T in OWS-4
    http://iisdemo.informatik.unibw-muenchen.de/ows4/

Auswirkung auf OGC Standardisierung

- Erforderlich für eine interoperable Umsetzung ist Änderung/Erzeugung von OGC Spezifikationen
- Change Request(s) zu OWS Common
  - Aufnahme von SAMLart als optionalen Parameter
  - Deklaration von Fehler Codes
  - Advertisement von Access Constraints in Capabilities Datei
- Change Request(s) zu Catalog oder Metadata WG
  - Auswertung von Zugriffsbeschränkungen bei der Suche
- Standardisierung von GeoXACML

Ausblick

- „Ubiqutious Protected Geographic Information“
- GDI.DE?
- INSPIRE?
- OWS-X?

Die letzte Folie

Dr. Andreas Matheus
Universität der Bundeswehr München
Andreas.Matheus@unibw.de