

Szenario

Ein Benutzer des Stadtbezirkes Perlach kann das Digitale Orthophoto für München sehen. Die Darstellung der Digitalen Stadtgrundkarte ist allerdings auf ein Bebauungsgebiet in Perlach beschränkt, wie es in der folgenden Abbildung gezeigt ist.

Zugriffsbeschränkung



Abbildung 2: Eingeschränkung für die Digitale Stadtgrundkarte im Bereich Perlach

Architektur

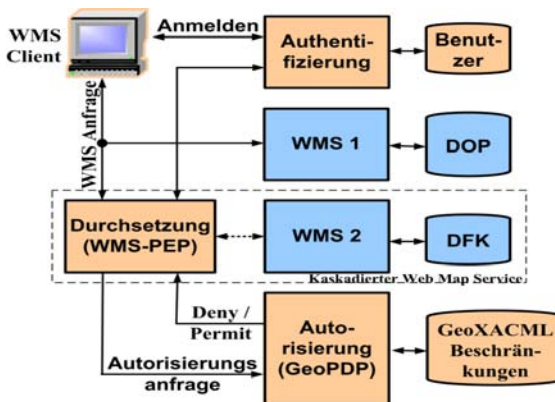


Abbildung 3: GeoXACML basierte Zugriffskontrolle für Web Map Service

Zusammenfassung

GeoXACML unterstützt eine interoperable Deklaration und Durchsetzung von Zugriffsbeschränkungen für geschützte Geodaten, die in einer dienstebasierten GDI verfügbar sind. Eine verteilte Zugriffskontrolle auf der Basis von GeoXACML Beschränkungen kann in eine dienstebasierte GDI durch das Prinzip „Embedding Without Touching“ integriert werden. Dies ermöglicht die Bereitstellung von qualitativ hochwertigen und schützenswerten Geodaten in einer Geodaten Infrastruktur, was möglicherweise neue Geschäftsfelder eröffnet.

Kooperation

Am Institut existiert für die Forschung im Bereich Sicherheit für Geodaten Infrastrukturen eine Kooperation mit dem Runden Tisch GIS e.V. (<http://www.rtg.bv.tum.de>). Speziell für dieses Projekt wird die OGC Testplattform für die Demonstration der Zugriffskontrolle verwendet.

Kontakt

Dr. Andreas Matheus
Universität der Bundeswehr München
Fakultät für Informatik
Institut für Informationstechnische Systeme
Werner-Heisenberg-Weg 39
D-85579 Neubiberg

Tel: +49 89 6004 2745
Fax: +49 89 6004 3898
Mail: andreas.matheus@unibw.de

Zugriffskontrolle für Geo Web Services mit GeoXACML

Interoperable Zugriffskontrolle für die Durchsetzung von feature- und raumbezogenen Beschränkungen in einer Geodaten Infrastruktur

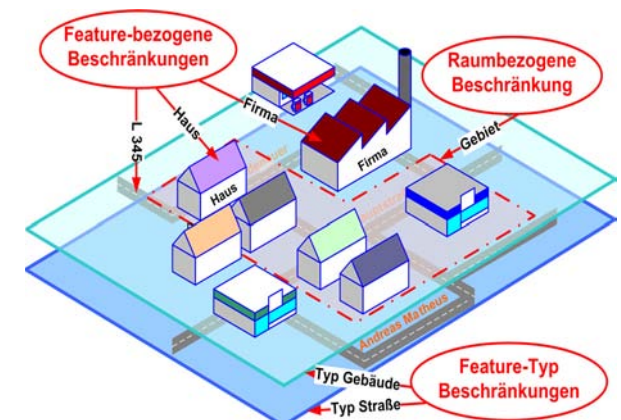


Abbildung 1: Unterstützung für die Durchsetzung von feature- und raumbezogenen Beschränkungen

Motivation

Heutzutage erlaubt eine Geodaten Infrastruktur (GDI) die kombinierte Nutzung von verteilten und heterogenen Geodaten. Eine typische Implementierung einer GDI basiert auf frei zugänglichen, geographischen Diensten; im Englischen als Geo Web Services bezeichnet. Sollen zugriffsgeschützte Geodaten über eine GDI verfügbar sein, so erfordert dies die Einführung einer interoperablen Zugriffskontrolle.

Anforderungen

Der Begriff Geodaten kann als Information über Features charakterisiert werden, die einen Raumbezug haben können. Ein Feature kann über seinen Typ, seine raumbezogenen und nicht raumbezogenen Eigenschaften ausgewählt werden. Daraus ergeben sich die naheliegenden Anforderungen für die Zugriffskontrolle:

- (i) **Feature Typ Beschränkungen** erlauben eine Zugriffskontrolle basierend auf dem Typ des Features: *Zugriff erlaubt für Features des Typs Gebäude.*
- (ii) **Feature Beschränkungen** erlauben eine Zugriffsbeschränkung für individuelle Features: *Zugriff erlaubt für das Gebäude „Der Deutsche Reichstag“.*
- (iii) **Raumbezogene Beschränkungen** erlauben eine Zugriffsbeschränkung basierend auf der Geometrie der Features: *Zugriff erlaubt innerhalb der Berliner Stadtgrenzen.*

- (iv) **Kombination der Beschränkungen (i) - (iii)** erlaubt eine flexible Deklaration für verschiedene Anforderungen: *Zugriff erlaubt für Features des Typs Gebäude, die sich innerhalb der Stadtgrenze von Berlin befinden, außer dem Feature „Der Deutsche Reichstag“.*
- (v) **Durchsetzung der Beschränkungen unabhängig von Diensten** unterstützt ein Zugriffsrechtmanagement für Geodaten, ohne an die Infrastruktur einer GDI gebunden zu sein.

Interoperabilität

Die kombinierte Nutzung von zugriffsgeschützten Geodaten in einer dienstebasierten GDI erfordert Interoperabilität auf drei voneinander unabhängigen Ebenen:

- (i) **Interoperabilität im Datenmodell** erlaubt die eigentliche Kombination von Geodaten. Dies kann u.a. durch Standards, wie der Geography Markup Language vom OGC, umgesetzt werden.
- (ii) **Interoperabilität für den Dienstaufruf** erlaubt die Abfrage von Geodaten in einer dienstebasierten GDI, was z.B. durch die OGC Standards, wie Web Map Service oder Web Feature Service, umgesetzt werden kann.
- (iii) **Interoperabilität bei der Zugriffskontrolle** unterstützt die erforderliche Harmonisierung von Zugriffsrechten auf geschützte und verteilte Geodaten einer GDI. Diese Interoperabilität kann durch den Einsatz von GeoXACML erreicht werden.

GeoXACML

Die Geospatial eXtensible Access Control Markup Language (GeoXACML) definiert eine Erweiterung zum Standard XACML von OASIS. XACML unterstützt die Deklaration und die Durchsetzung von Zugriffsbeschränkungen für XML formatierte Informationen. Für die Durchsetzung von Zugriffsrechten für Features werden die Informationen in GML formatiert. Hierdurch werden die Feature Typ und Feature Beschränkungen bereits durch XACML umgesetzt. Durch die in GeoXACML definierten geometrischen Attribute und die Funktionen zur Überprüfung topologischer Beziehungen, können die Anforderungen für die raumbezogenen Beschränkungen ebenfalls deklariert und durchgesetzt werden. Weitere Informationen finden sie im OGC Discussion Paper Nr. 05-036 unter <http://www.opengeospatial.org/specs/?page=discussion> und auf der GeoXACML Homepage unter <http://www.geoxacml.org>

Demonstration

Für einen existierenden Web Map Service werden GeoXACML basierte Feature Typ und raumbezogene Beschränkungen durchgesetzt. Feature Beschränkungen werden nicht durchgesetzt. Die Demonstration kann durch Laden des Clients über den Link <http://iisdemo.informatik.unibw-muenchen.de/WMSClient/Systems05/> gestartet werden.