Modul 6: Voraussetzungen einer GDI
Vertiefende Dokumente I Stand: 24.01.2012

Sicherheit in einer GDI

Beim Thema Sicherheit müssen natürlich zunächst übliche IT-Sicherheitsmaßnahmen (redundante Server mit Lastverteilung, Virenscanner, Firewalls, Demilitarized Zones - DMZ, etc.) beachtet werden, auf welche an dieser Stelle allerdings nicht weiter eingegangen werden soll.

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

Der typische Fall ist ein einzelner lesender Zugriff auf Geodaten eines Servers durch den Nutzer, sei es zur bloßen Darstellung auf dem Bildschirm (z.B. die Nutzung des Hessenviewers zur Visualisierung dienstebasierter Geodaten) oder sei es zum lokalen Abspeichern oder Ausdrucken (z.B. das Abspeichern von Geodaten zur Weiterverwendung im GML-Format auf Grundlage eines Web Feature Services). 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. Teilweise sind Anwendungen aber auch so gestaltet, dass eine Datenerfassung oder -Aktualisierung über Netz-Schnittstellen durchführbar ist - beispielsweise ist hier ein Transaktionen unterstützender Web Feature Service (WFS-T) zu nennen. 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, zum Beispiel durch eine automatische Konsistenz- oder Plausibilitätsprüfungen. 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.

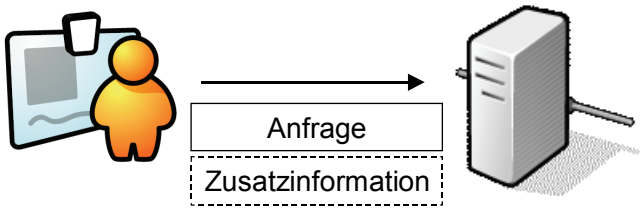
Nachdem der Nutzer die Daten erhalten hat, stellt sich die Frage, was er mit den Daten machen darf. Dies ist der Bereich der Digitalen Rechteverwaltung (DRM). Der erste Teilaspekt ist die Formulierung von Nutzungsrechten und die Mitteilung an den Nutzer. Der zweite, schwierigere Teilaspekt ist die Überwachung 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 gegebenenfalls rückverfolgen zu können oder arbeiten mit Verschlüsselung und software-überwachter Nutzung, die aber die Unterstützung der GIS-Hersteller für derartige Verfahren voraussetzt, was wiederum dem Interoperabilitäts-Gedanken entgegensteht.

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.

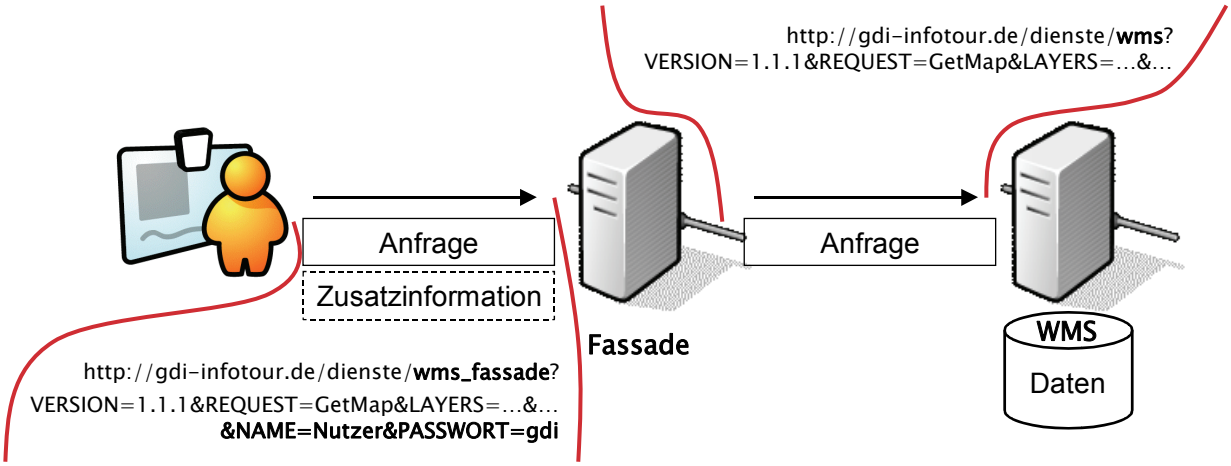
Technische Lösungen für Sicherheitsmaßnahmen

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 Passwort 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.

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.



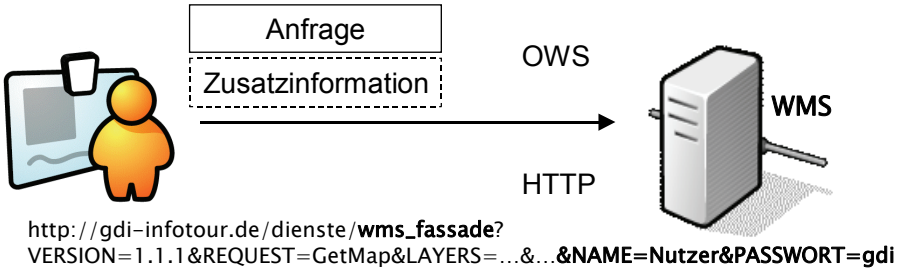
Ein solcher Architekturansatz wird in der Softwareentwicklung als "Fassade" bezeichnet. Der entscheidende Vorteil bei Verwendung einer Fassade ist, dass diese die definierten Schnittstellen des dahinter liegenden Services nicht verändert, und daher die vorhandene Systemlandschaft nur minimal angepasst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

Betrachtet man diese Lösung beispielhaft an einem geschützten Zugriff auf einen WMS, so würde unter anderem der gewöhnliche GetMap-Request direkt an die URL der Fassade gesendet werden. Die üblichen Parameter aus der OGC-Spezifikation, also VERSION, REQUEST, SERVICE, LAYERS, STYLES etc. werden dann um weitere dienstespezifische Parameter, wie beispielsweise NAME und PASSWORT zur Authentfizierung erweitert. Diese zusätzlichen Parameter gehören nicht zur Standard-Schnittstelle und müssen dem Nutzer natürlich bekannt sein. Die Fassade filtert anschließend diese Zusatzparameter und leitet die Anfrage bei erfolgreicher Authentifizierung an den WMS-Server weiter, wobei dieser nur noch die standardisierten WMS-GetMap-Parameter beinhaltet.

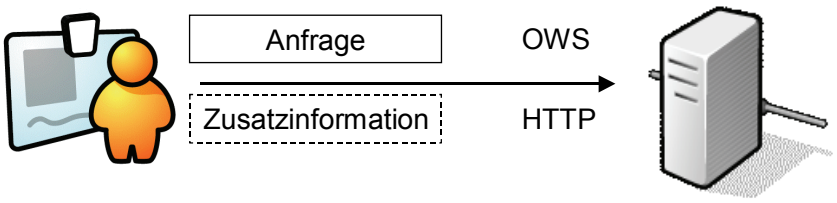
Bleibt noch die Frage inwiefern die Interoperabilität durch einen solchen Lösungsansatz beeinträchtigt wird. Grundsätzlich ist es möglich auch auf diese Weise geschützte Dienste in jeden beliebigen Viewer oder in jedes beliebige Geoinformationssystem anzubinden. Will man zum Beispiel einen Dienst im Hessenviewer anbinden, gibt man in der Regel die URL bis zum Fragezeichen an. Die dazugehörigen Parameter werden vom Viewer automatisch ermittelt und angefügt (was dem Nutzer allerdings verborgen bleibt). Zusätzliche Parameter, wie zum Beispiel ein Passwort, müsste man allerdings direkt hinter dem Fragezeichen mit angeben. Der Viewer setzt dann die standardisierten WMS-Parameter wiederum hinten dran. Auf diese Art und Weise ist also auch die Interoperabilität gewährleistet, wird aber natürlich insofern bewusst eingeschränkt, dass der Nutzer zwingend Kenntnis über die Zusatz-Parameter und deren Werte haben muss. Auch ein direktes Aufrufen des Dienstes im Hessenviewer aus dem Geodatenkatalog Hessen ist hier nicht möglich, da zwingend eine entsprechende Eingabe durch den Nutzer erfolgen muss. Außerdem kann es hier unter

Umständen zu Schwierigkeiten bei der Verkettung von Diensten kommen, da andere Dienste diese speziellen (proprietären) Parameter natürlich nicht kennen.

Eine elegantere Lösung wäre es, wenn auch solche sicherheitsrelevanten Parameter durch das OGC soweit möglich standardisiert werden würden, man den Request also mit zusätzlichen Parametern direkt an den WMS senden könnte.



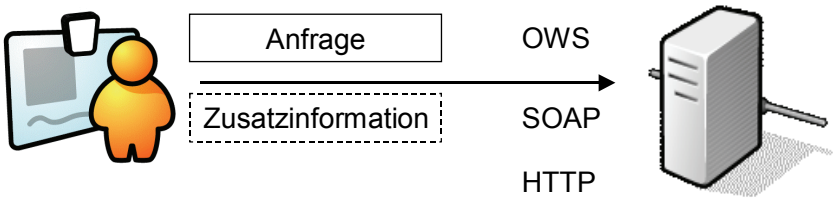
Eine weitere Methode setzt bei tieferen Protokollschichten an. Der WMS und andere OGC-Standards basieren auf einem darunter liegenden Transportprotokoll: HTTP. Dieses Transportprotokoll sieht bereits standardisierte Mechanismen für die Authentifizierung eines Benutzers vor, beispielsweise die „basic authentication“, bei der es sich um die aus dem Internet bekannte Abfrage nach einem Benutzernamen und dem Passwort handelt. Ist diese erfolgreich, kann der Nutzer auf den Webserver und somit auch auf den darauf laufenden Dienst zugreifen. Allerdings ist es mit dieser Lösung im Gegensatz zu der erstgenannten nicht möglich, lediglich Zugriff auf bestimmte Daten zu gewährleisten (also beispielsweise den Zugriff per WMS nur für einen Teil der Geodaten durch räumliche oder objektabhängige Einschränkungen benutzerabhängig zu beeinflussen).



Verknüpft man HTTP mit dem Verschlüsselungsprotokoll 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 Online-Banking bereits gebräuchlich.

Ein weiterer, allerdings derzeit noch nicht in Frage kommender, Ansatz ist das SOAP-Protokoll. Dieser Standard wird derzeit allerdings nicht von OGC Web Services unterstützt. Um SOAP in Zukunft zu unterstützen gibt es derzeit beim OGC einen WMS Change Request zum Thema „Support for WSDL & SOAP“. Ab welcher WMS-Version die SOAP-Unterstützung vorgesehen wird, ist jedoch noch offen.

SOAP erlaubt die Übertragung von Sicherheits-Zusatzinformation in vielfältiger Weise für die unterschiedlichsten Anforderungen, wie Verschlüsselung oder Signierung zur Integritäts-sicherung und Sicherung der Vertraulichkeit.



Zusammenfassend ist zu sagen, dass das Thema Sicherheit im IT-Bereich und speziell bei Geodateninfrastrukturen sehr komplex ist. Alle Möglichkeiten haben ihre Vor- und Nachteile. Während beispielsweise eine Fassade speziell auf die Bedürfnisse innerhalb einer GDI angepasst werden kann, handelt es sich bei der basic authentication für HTTP und insbesondere mit dem OASIS-WS-Security-Standard (WS-S) für SOAP bereits um stabile und erprobte Standards. Es muss also individuell entschieden werden, welche technischen Maßnahmen man ergreifen möchte.

Weiterführende Informationen sind auch dem Kapitel 9 zum Architekturkonzept der GDI-DE (Version 2.0) zu entnehmen. Hier werden einerseits grundsätzliche Begriffe erläutert und andererseits weitere Sicherheits-Standards erwähnt.