Geoinformation und Landentwicklung

Kundeninformation

Absicherung Geodatendienste des LGL

Neuerungen bei Authentifizierungsmethoden

Einführung https
= Erhöhte Sicherheit durch Verschlüsselung

September 2017

LGL
www.lgl.bw.de

Baden-Württemberg
LANDESAMT FÜR GEOINFORMATION UND LANDENTWICKLUNG

Absicherung Geodatendienste des LGL

Das Landesamt für Geoinformation und Landentwicklung Baden-Württemberg (LGL) bietet kostenpflichtige oder aufgrund von Datenschutzbestimmungen zugangsbeschränkte Geodatendienste über unterschiedliche Authentifizierungsmethoden an. Authentifizierungsmethoden dienen der konkreten Kommunikation zwischen Benutzer und Geodatendienst, in dem sie sicherstellen, dass nur der Benutzer, der sich über ein nur ihm bekanntes Passwort legitimiert hat, auf die Geodatendienste zugreifen darf. Beispiel für einen Geodatendienst ist ein Web Map Service (WMS).

1 Grundlagen der Authentifizierung

Authentifizierung: Um die Nutzung von Diensten abrechnen zu können, ist es wichtig zu wissen, wer welche Dienste abruft. Daher benötigt jeder Benutzer oder jede Benutzergruppe eine bestimmte Authentifizierung. Die Authentifizierung erfolgt über einen Benutzernamen (Login). Ein nicht kostenpflichtiger Dienst benötigt keine Authentifizierung des Nutzers.

Autorisierung: Der über Authentifizierung (Login) festgestellte Benutzer oder analog eine Benutzergruppe muss sich über ein Passwort ausweisen (autorisieren), dass er auch der berechtigte Benutzer ist. Durch diese Autorisierung erhält er gleichzeitig bestimmte Rechte. Dazu gehören: grundsätzliches Recht zur Nutzung eines bestimmten Dienstes, Rechte zur Nutzung bestimmter Operationen eines Dienstes (z.B. der Operation GetFeatureInfo eines WMS), Rechte zur Nutzung bestimmter Layer bei einer WMS-GetMap-Operation (z.B. eines Layers zur Darstellung von Flurstücksnummern) oder das Recht zur Nutzung eines Layers ohne Wasserzeichen bzw. Copyright.

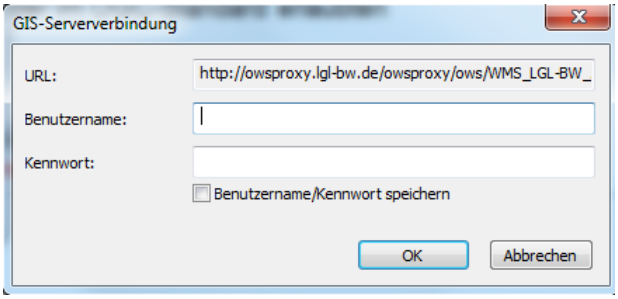
2 Im LGL eingesetzte Authentifizierungsmethoden

Authentifizierung und Autorisierung und damit einhergehend die Zugriffsabsicherung der Geodatendienste erfolgen im LGL über die Absicherungs-Software OWS-Proxy durch Übermittlung von Benutzername und Passwort. Dafür werden zwei verschiedene Methoden angeboten:

- http-Basic-Authentifizierung und
- Verwendung von sogenannten Vendor Specific Parameters (VSP)

2.1 Zugriffsabsicherung über http-Basic-Authentifizierung

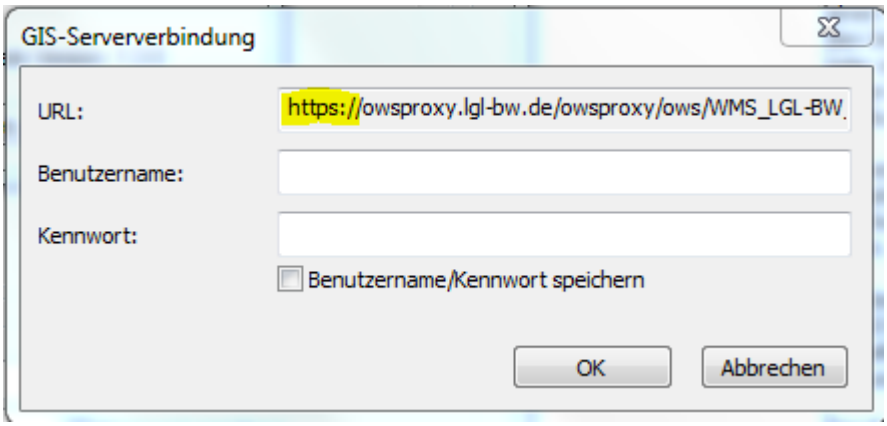
Bei dieser Art der Absicherung erfolgt eine Abfrage auf Benutzername und Passwort. In der Regel wird durch die Anwendung ein Pop-Up-Fenster eingeblendet, über das Benutzername und Passwort angegeben werden kann. Benutzername und Passwort können in viele Anwendungen (intern) hinterlegt werden. Diese Methode sollte zukünftig bevorzugt werden. Sie wird derzeit noch nicht von allen Anwendungen unterstützt.



Bitte prüfen Sie, ob ihre Anwendung die http-Basic-Authentifizierung unterstützt und stellen Sie, wenn möglich, darauf um.

2.2 Zugriffsabsicherung über Vendor Specific Parameters

Dies ist die seither für die WMS des LGL verwendete Methode, um Benutzer und Passwort zu übergeben. Dabei werden beide im Klartext beim Aufruf einer Diensteoperation an den den owsProxy übertragen, wie an folgendem Beispielaufruf deutlich wird (VPS sind farbig hervorgehoben):



http://owsproxy.lgl-bw.de/owsproxy/ows/WMS_LGL-BW_ATKIS_DOP_20_C?user=MaxMustermann&password=20140129Test&request=GetCapabilites...

Der Vorteil hierbei ist, dass derzeit alle bekannten Anwendungen (z.B. Web-Anwendungen wie Geodatenviewer oder GIS-Systeme) diese Methode unterstützen, Nachteil ist, dass sie durch die Klartextübermittlung nur sehr geringe Sicherheit bietet. Bitte setzen Sie diese Methode nur noch ein, falls Ihre Anwendung die http-Basic- Authentifizierung nicht unterstützt!

3 Neuerung bei Authentifizierungsmethoden ab September 2017

Bislang wurden beide Authentifizierungsmethoden parallel verwendet .

Auf eine GetCapabilities-Anfrage erhielt ein Benutzer ein Capabilities-Dokument, das sowohl für VSP als auch für http-Basic-Authentifizierung dieselben Angaben enthielt.

Da in der Vergangenheit nur wenige Anwendungen http-Basic-Authentifizierung unterstützen, war diese Vorgehensweise für die meisten Benutzer die einfachste Handhabung. Eine Anwendung, die http-Basic-Authentifizierung nicht unterstützte, konnte aus den capabilities-Dokument die VSP auslesen und somit dennoch die Geodatendienste nutzen.

Allerdings bedeutet diese Vorgehensweise, dass auch bei http-Basic-Authentifizierung im Capabilities-Dokument Benutzername und Passwort im Klartext aufgeführt sind. Der Sicherheitsgewinn durch die http-Basic-Authentifizierung geht also zumindest bei der Ausführung des GetCapabilities-Request wieder verloren.

Daher werden nun die beiden Authentifizierungsmethoden getrennt.

OWS-Proxy überprüft nun, mit welcher Authentifizierungsmethode die Anfragen gestellt werden. Die Antworten erfolgen dann in entsprechender Form entweder mit Benutzername und Passwort im Klartext bei VSP oder ohne Angabe der Zugangsdaten für http-Basic-Authentifizierung.

Mögliche Auswirkung:

Sollte Ihre Anwendung bisher trotz Verwendung von http-Basic-Authentifizierung bei der Einbindung des Geodatendienstes die weiteren Anfragen mit VSP (eventuell im Hintergrund gestellt haben, kann es sein, dass Ihre Dienste nach der Umstellung nicht mehr funktionieren.

In diesem Fall sollten Sie die Dienste neu mit VSP einbinden – oder eventuell an ein Software-Update denken.

4 Einführung https für Geodatendienste

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert als Mindeststandard für den Austausch von Daten über das Internet eine verschlüsselte Übertragung (https).

„Hypertext Transfer Protocol Secure (**https**, englisch für „sicheres Hypertext-Übertragungsprotokoll“) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen. Es stellt eine *Transportverschlüsselung* dar.“ (wikipedia)

Als Begründung führt das BSI an:

„Das TLS-Protokoll (Transport Layer Security) dient der Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in unsicheren Netzwerken. TLS (Transport Layer Security) ist ein kryptographisches Protokoll zur Etablierung eines sicheren Kanals (verschlüsselt, authentisiert und integritätsgeschützt). Insbesondere ist die TLS-gesicherte Übertragung im Internet (mittels HTTPS) sehr wichtig und weit verbreitet. Heutzutage werden viele Anwendungen wie z. B. Homebanking, E-Commerce, E-Government etc. über das Internet abgewickelt, und gerade bei diesen Anwendungen ist es wichtig, dass die Daten (insbesondere Zugangsdaten, PINs, Passwörter) sicher übertragen werden können. Hier spielt das TLS-Protokoll eine wichtige Rolle. Es dient dazu, einen sicheren Kanal zwischen Sender und Empfänger (z. B. Webbrowser und Webserver) aufzubauen und alle Nutzdaten sicher durch diesen Kanal zu übertragen.“

Quelle und weitere Information:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile&v=3

Dieser Anforderung kommen wir nun auch für Geodatendienste nach, indem wir Geodatendienste im Internet und Intranet zusätzlich über https anbieten.

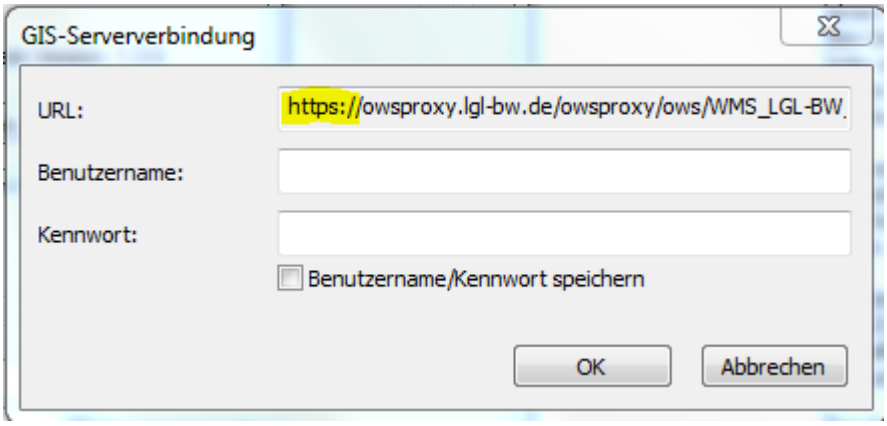
Für Sie als Anwender bedeutet dies, dass Sie – vorausgesetzt Ihre Anwendung bzw. Browser unterstützt bereits https – durch einfaches Ersetzen des http durch https unsere Geodatendienste mit den bisherigen URLs weiterbenutzen können und durch die Verschlüsselung in den Vorteil der erhöhten Sicherheit gelangen.
Username und Passwort werden nun verschlüsselt übertragen und sind daher nicht mehr abgreifbar.
Die Verschlüsselung über https ist unabhängig von der Authentifizierungsmethode.

Probieren Sie es also in Ihrem eigenen Interesse aus und binden Sie Ihre bestehenden Dienste mit https ein.

Beispiel VSP:

```
https://owsproxy.lgl-bw.de/owsproxy/ows/WMS_LGL-BW_ATKIS_DOP_20_C?user=MaxMustermann&password=20140129Test&request=GetCapabilities
```

Beispiel http-Basic-Authentification:



Anwendungen, die über die Einstellungen Ihres Browsers die Internetverbindung für Geodatendienste aufbauen, werden in der Regel ohne Probleme mit https zurechtkommen.

Bei Eigenentwicklungen kann es vorkommen, dass die Geodatendienste nicht funktionieren.

Der Einsatz von https entwickelt sich mehr und mehr zum Standardgebrauch. Moderne Browser werden zukünftig nur noch https anbieten. Etliche Verwaltung akzeptieren aufgrund der BSI-Richtlinie nur noch Webdienste, die mit https übertragen werden.

Auch die Geodatendienste des LGL werden **in Zukunft** aufgrund dieser Anforderungen nur noch über https angeboten werden.

Machen Sie sich daher rechtzeitig mit der https-Thematik vertraut.

Für Rückfragen stehen wir Ihnen gerne über den Benutzerservice zur Verfügung.

Den Benutzerservice des LGL erreichen Sie wie folgt:

Servicezeiten:

Montag bis Donnerstag von 7:30 bis 16:00 Uhr sowie Freitag von 7:30 bis 13:00 Uhr

Kontaktdaten:

Telefon: 07154 / 9598 – 310

Fax: 07154 / 9598 – 883

E-Mail: benutzerservice@lgl.bwl.de

Postanschrift:

Landesamt für Geoinformation und Landentwicklung
Benutzerservice "LGL"
Stuttgarter Str. 161
70806 Kornwestheim