

Sichere GDI in der Praxis – ein Erfahrungsbericht

AK WebGIS 2007, 13. Juni 2007, Hannover

Einführung

- **Konzepte, verfügbare Freie Software**
- ▶ **Beispiel GDI-NI**
 - **Ausgangssituation, Aufgabenstellung**
 - **Server-Seite**
 - **Klienten-Seite**
 - **Verfügbare Software**

▶ **Philosophie:**

- ▶ Zukunftsweisende EDV-Konzepte herstellerunabhängig und auf Basis von Freier Software entwickeln und umsetzen

▶ **Kernkompetenzen:**

- ▶ IT-Dienstleistungen zu strategischer Beratung, Projekt-Management & Umsetzung sowie Geographische Informationssysteme (GIS)

▶ **Engagement:**

- ▶ Linux-Verband und im IuK Netzwerk Osnabrück
- ▶ FSF Europa
- ▶ Gründer der führenden Übersicht für Freie Software im GIS-Bereich (www.freegis.org).

- ▶ **Anbietersicht: Absicherung gegen**
 - ▶ **abhören**
 - ▶ **unbefugte Nutzung**
 - Abruf
 - Bearbeitung
- ▶ **Anwendersicht: Absicherung gegen**
 - ▶ Mißbrauch des eigenen Nutzerkontos
 - ▶ Unterschieben falscher Daten
 - ▶ Einschränkung der digitalen Selbstbestimmung

▶ **Grundlage: Nutzerkonten**

- ▶ sonst keine vernünftige Zuordnung von Rechten
- ▶ bedeutet: individuelle Authentifizierung notwendig
- ▶ Alternativen: z.B. IP-basierte Freigaben (kaum praktikabel)

▶ **Verschlüsselte Verbindungen (SSL, TLS, bedingt: VPN)**

- ▶ Absicherung gegen abhören, Mißbrauch des Kontos

▶ **Authentifizierungs-Mechanismen:**

- ▶ Name/Passwort, Biometrisch (lieber nicht)
- ▶ Variante: Gegen andere Dienste authentifizieren (z.B. LDAP)
- ▶ Erweiterung: Tickets (Benutzerkonten als Anbieter nicht selbst pflegen, Rollen werden sehr wichtig)

- ▶ **Es gibt noch keine vereinbarten OGC Standards**
- ▶ **WAS/WSS: Web Authentication/Security Service**
 - ▶ Ticket-System
- ▶ **GeoXACML/SAML**
 - ▶ aktuell in Diskussion bei OGC
- ▶ **SSL: Secure Socket Layer**
 - ▶ abgesicherter Tunnel
- ▶ **Proxy (Stellvertreter)**
 - ▶ Filter

- ▶ **Verschlüsselung (SSL):**
 - ▶ Web-Server (z.B. Apache)
 - ▶ PKI-Management (z.B. OpenSSL+OpenLDAP)
- ▶ **Serverseitige Authentifizierung und Autorisierung:**
 - ▶ deegree
 - ▶ 52N
 - ▶ Mapbender
- ▶ **Klient-seitig:**
 - ▶ InteProxy
 - ▶ 52N

- ▶ **deegree „iGeoSecurity“**
 - ▶ deegree OWS-Proxy
 - ▶ deegree U3R (+ Web-Admin-GUI)
 - ▶ deegree WAS, WSS
 - ▶ deegree WAC (Intranet Proxy)
 - ▶ Verschiedene Anmelde-mechanismen
 - ▶ Java, GNU LGPL
 - ▶ Vorteile: sehr flexibel, mächtig
 - ▶ Nachteile: großer Brocken, komplex

▶ 52N „Security Modules“

▶ Java, GNU GPL

▶ 52N WAS, 52N WSS

▶ 52N WSC (Web Security Client)

▶ Nachteile

- Hauptsächlich Authentifizierung. Autorisierungen nur über Adapter, WSS: flache Autorisierung
- WSC: Lizenzunklarheiten

- ▶ **Mapbender „OWS-Security Proxy“**
 - ▶ php, GNU GPL
 - ▶ OWSproxy: Autorisierungsmodul
 - ▶ Web-GUI für Autorisierungs-Administration ist Teil der Portal-Administration von Mapbender
 - ▶ integrierte Lösung für Mapbender Portal
 - ▶ Nachteile:
 - eigenes Ticketsystem erfunden, Browser notwendig (kein DesktopGIS)
 - nur in Verbindung mit Mapbender nutzbar
 - nur WMS (weitere Dienste in RC-Stadium)

▶ GDI-NI im Betrieb bei LGN

- ▶ Hauptsächlich WMS-Dienste; geplant: WFS, Kataloge
- ▶ Teilweise zusammengefasst über Geodatenportal (NiedersachsenViewer[Plus], GeoTask); die Viewer basieren auf WMS.
- ▶ Weitere, direkte WMS-Dienste; beliebige WMS-Klienten
- ▶ Eigene Daten sowie WMS/WFS von anderen Behörden
- ▶ Bisher keine Absicherungen nach außen (WMS URLs leicht zu erraten)
- ▶ Landes-Behörden intern: VPN

▶ Anforderungen

- ▶ Absicherung Kommunikation Klienten – Server (SSL)
- ▶ Authentifizierung (wer)
- ▶ Autorisierung (was)
- ▶ Abrechnungsmechanismus (wieviel)
- ▶ Herstellerunabhängig (Freie Software, „Open Source“)
- ▶ Minimalinvasiv für Server und Klienten-Programme
- ▶ Plattformunabhängig (Windows, Linux, ...)
- ▶ Inbetriebnahme Sommer 2007

▶ Vorüberlegungen:

- ▶ Allgemeine Verfügbarkeit von Absicherung/Authentisierung bei Desktop-Klienten ist auf viele Jahre nicht absehbar.
- ▶ Komplexe Authentisierung (WAS/WSS/...): Aufwändig (teuer), konkrete Standardisierung ungewiss

▶ Pragmatischer Ansatz: ein Kompromiss

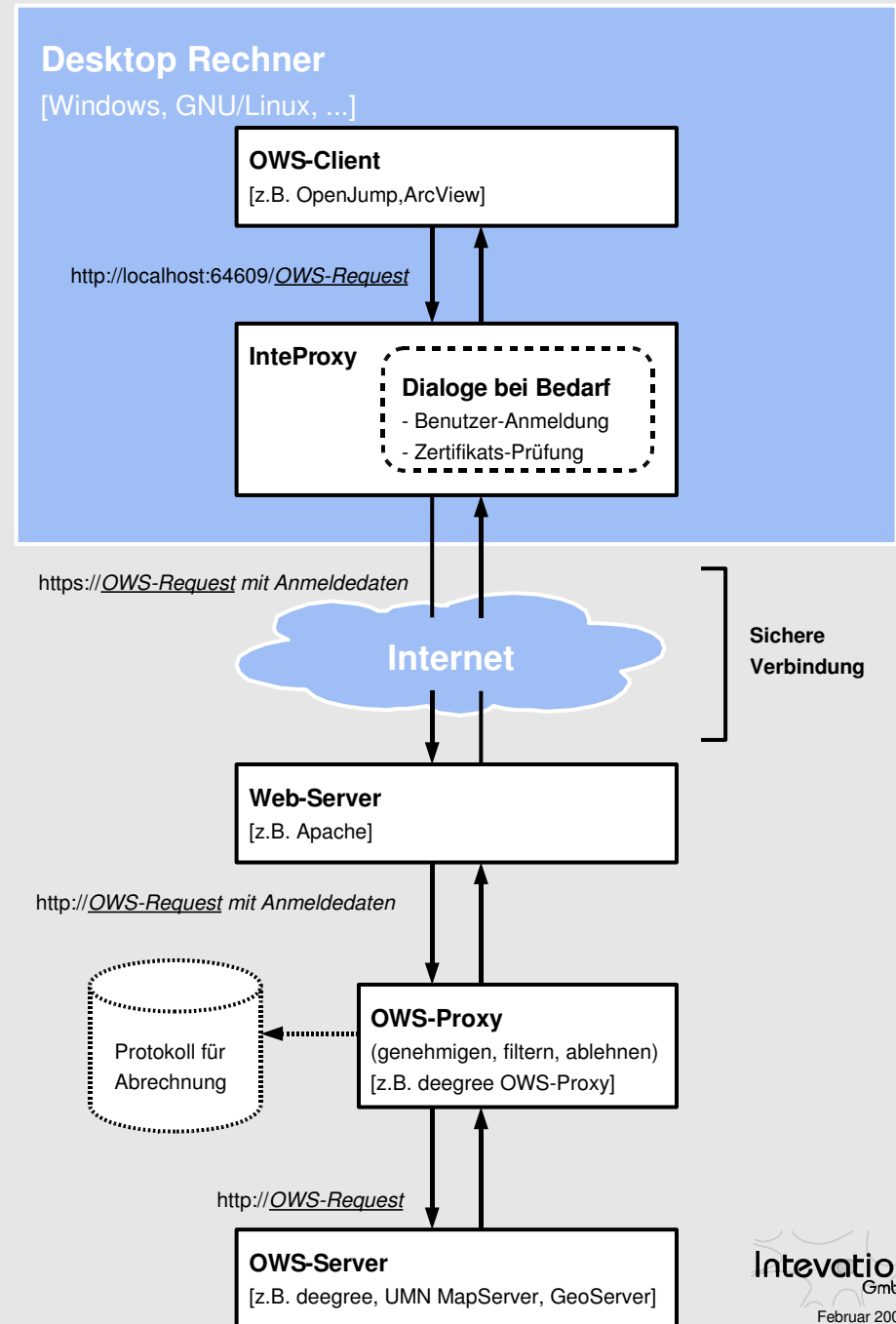
- ▶ Flexible Sonderlösung für Desktops
- ▶ Server: Einfache, aber unmittelbar verfügbare Technologie, leicht anpassbar für zukünftige Standards

- ▶ **Desktop Klienten: beliebige (OpenJump, ArcView, ...)**
- ▶ **Problem: kein SSL, keine Authentifizierung**
- ▶ **Notwendig: Desktop-Proxy**
- ▶ **Denkbare Varianten:**
 - ▶ Zwangs-Proxy
 - ▶ Regulärer Proxy (lokal oder Intranet)
 - ▶ Bedarfs-Proxy (nur für OWS-Anfragen genutzt)
- ▶ **Lösung: InteProxy - ist ein regulärer Proxy, optional auch Bedarfs-Proxy einsetzbar**

- ▶ Einfaches Installationspaket für Windows XP
- ▶ Desktop Hintergrundprozess
`http://localhost:64609/OWS-Request`
- ▶ Aufbau SSL-Verbindung
- ▶ Nutzeridentifikation (cached)
- ▶ URL/Request Rewrite
- ▶ für verschiedene OWS-Proxies konfigurierbar



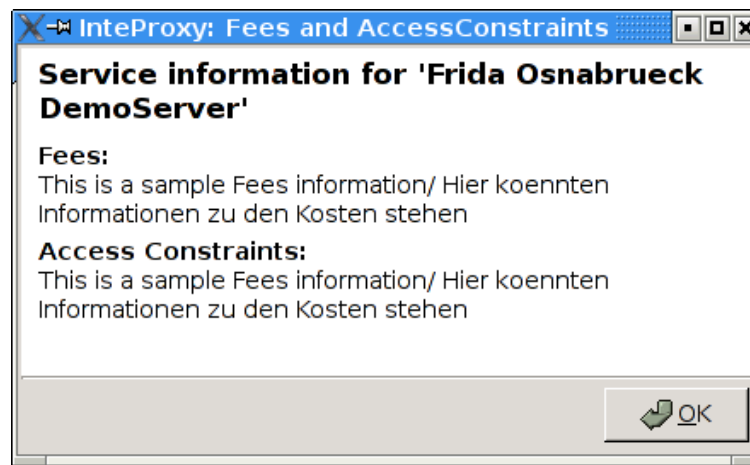
<http://inteproxy.wald.intevation.org>



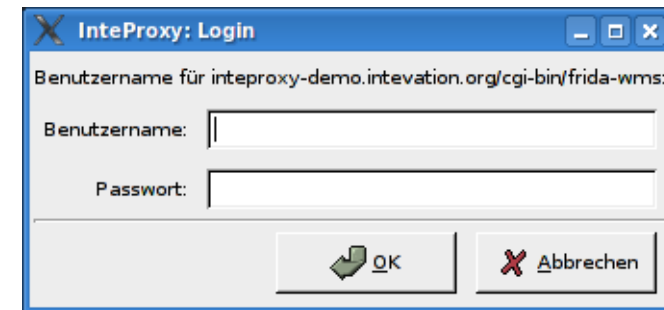
► Das Gesicht von InteProxy



Startbildschirm



Fees-Dialog

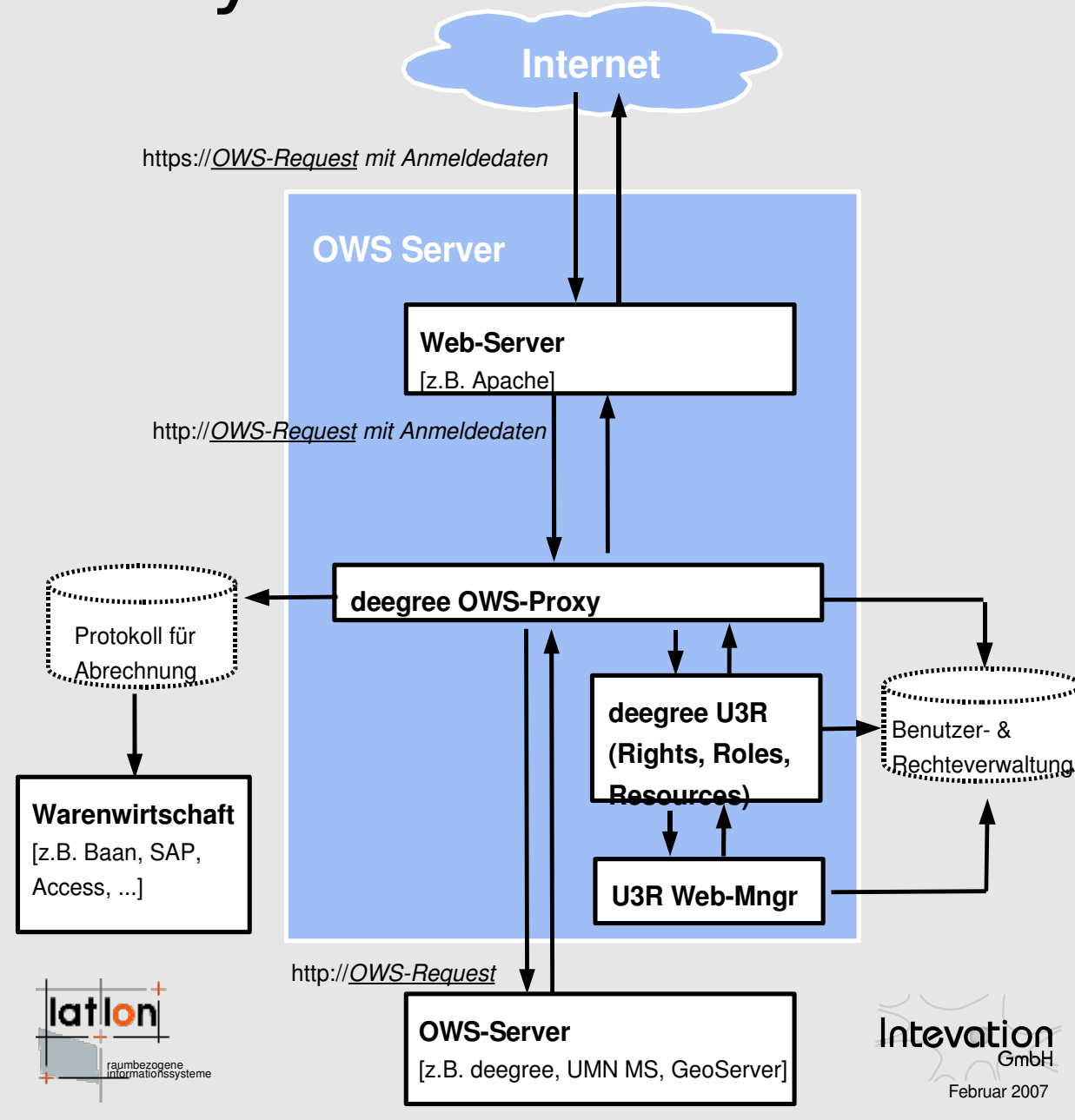


Passwort-Dialog

- ▶ **Info-Dialog „Fees & accessConstraints“ [Done]**
- ▶ **InteProxy optional als regulärer Proxy [Done]**
- ▶ **InteProxy als Tray-Icon [Done]**
- ▶ **SSL Zertifikats-Management (Vertrauens-Aussprache)**
- ▶ **Umfangreiche GUI**
 - ▶ Dynamischer Anmeldedialog für verschiedene Typen von OWS-Proxies
 - ▶ Konfiguration
 - ▶ Management für Nutzerkonten und Zertifikate

- ▶ **GeoTask hat eigene Benutzerverwaltung**
 - ▶ nicht ausreichend für benötigte Autorisierungen
 - ▶ Proprietär, keine Standard-Schnittstelle
- ▶ **Notwendig: beides, eigene Nutzer- und Rechteverwaltung**
- ▶ **Gewünscht: sehr feinkörnige Rechtevergabe (Polygone, getFeatureInfo, ...)**
- ▶ **Weitere Herausforderungen**
 - ▶ GeoPortal kein reines OWS, Änderungen von Layernamen ...
- ▶ **Lösung: iGeoSecurity Module deegree OWS-Proxy und U3R**

- ▶ Apache mit SSL (CA)
- ▶ deegree OWS-Proxy
- ▶ deegree U3R
- ▶ Modellierung: Rollen, Gruppen



- ▶ **deegree U3R GUI: Management-Erleichterungen**
- ▶ **deegree OWS-Proxy: Ankopplung Abrechnungs-Modul**

Weitere Herausforderungen:

- ▶ **Kaskadierung von jeweils gesicherten OGC-Diensten**
- ▶ **... die Praxis hält noch einige bereit**

- ▶ [**gdi@lgn.niedersachsen.de**](mailto:gdi@lgn.niedersachsen.de) (Thorsten Jakob)
- ▶ [**www.geodaten.niedersachsen.de**](http://www.geodaten.niedersachsen.de)

- ▶ [**Stephan.Holl@intevation.de**](mailto:Stephan.Holl@intevation.de)
- ▶ [**www.intevation.de/geospatial/**](http://www.intevation.de/geospatial/)

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?