

Sichere GDI in der Praxis – ein Erfahrungsbericht

Deegree-Day 2007, 12. Juni 2007, Bonn

Einführung

- **Konzepte, verfügbare Freie Software**

▶ **BeispielGDINI**

- **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, Projektmanagement & Umsetzung sowie Geographische Informationssysteme (GIS)

▶ Engagements:

- ▶ Linux-Verband und in UK 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
 - ▶ Unterschreiben 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

▶ Authentifizierungsmechanismen:

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

- ▶ **Es gibt noch keine vereinbarten OGC Standards**
- ▶ **WAS / SS: 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

▶ **Klientseitig:**

- ▶ InteProxy

- ▶ 52N

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

▶ 52N „Security Modules“

▶ Java, GNU GPL

▶ 52N W AS, 52N W SS

▶ 52N W SC (Web Security Client)

▶ Nachteile

- Hauptsächlich Authentifizierung. Autorisierungen nur über Adapter, W SS: flache Autorisierung
- W SC: Lizenzunklarheiten

- ▶ **Mapbender „OW S-Security Proxy“**
 - ▶ php, GNU GPL
 - ▶ OW Sprox: 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:

- ▶ Allgemein eine 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 umsetzbar verfügbare Technologie, leicht anpassbar für zukünftige Standards

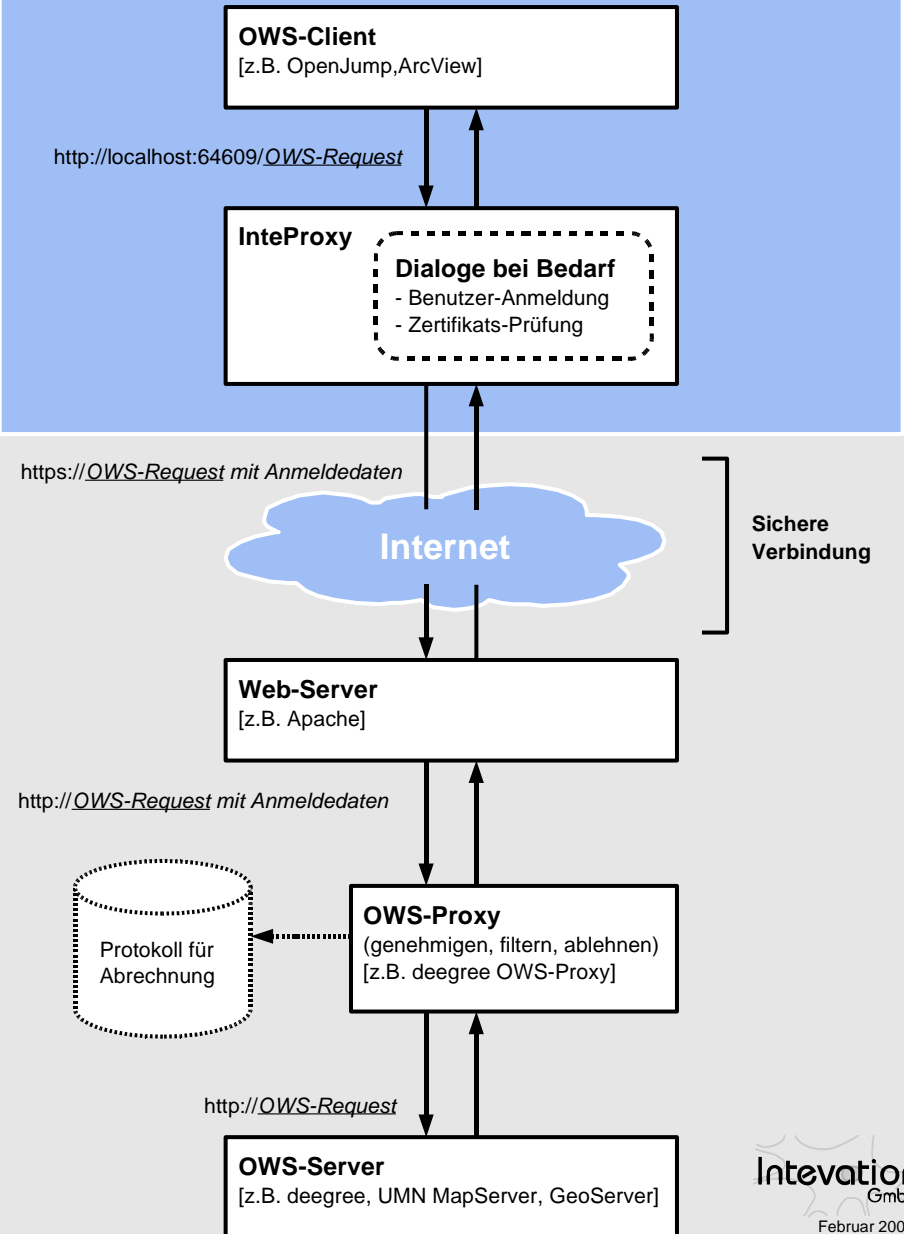
- ▶ **Desktop Klienten: beliebige (OpenJump, ArcView, ...)**
- ▶ **Problem: kein SSL, keine Authentifizierung**
- ▶ **Notwendig: Desktop-Proxy**
- ▶ **Denkbare Varianten:**
 - ▶ Zwangs-Proxy
 - ▶ Regulärer Proxy (bka oder Intranet)
 - ▶ Bedarfs-Proxy (nur für OWS-Anfragen genutzt)
- ▶ **Lösung: InteProxy – 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/RequestRewrite
- ▶ für verschiedene OWS-Proxies konfigurierbar



Desktop Rechner

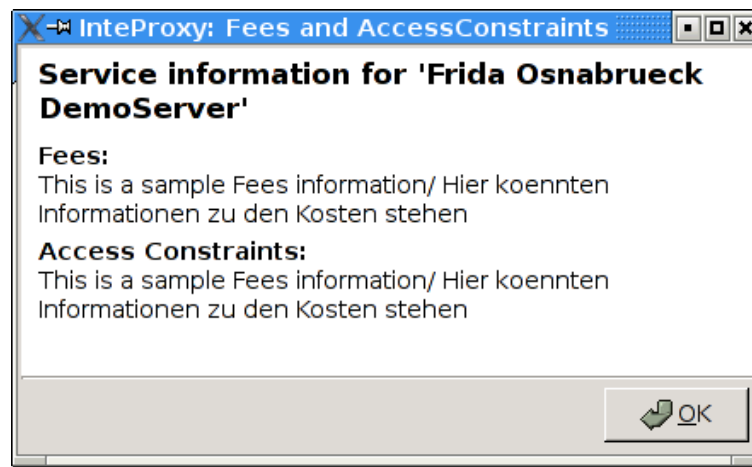
[Windows, GNU/Linux, ...]



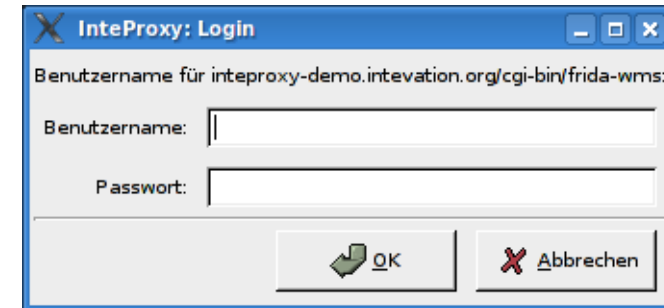
► Das Gesicht von InteProxy



Startbildschirm



Fees-Diäbg

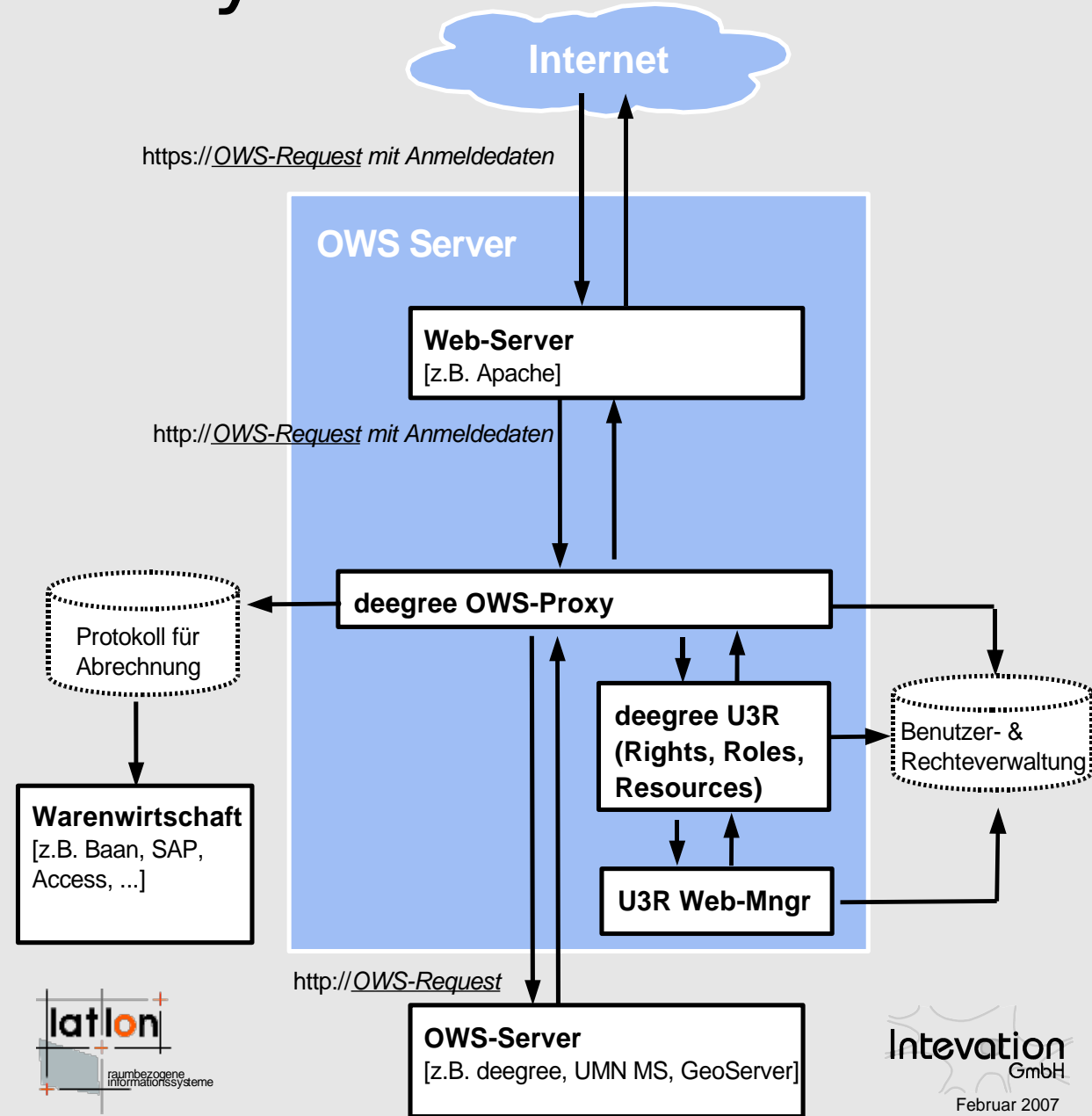


Passwort-Diäbg

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

- ▶ **GeoTask hateigene Benutzerverwaltung**
 - ▶ nichtausreichend fürbenötigte 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: GeoSecurity Module deegree OWS-Proxy und U3R**

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



- ▶ **deegree U3R GUI: Managem ent-Erleichterungen**
- ▶ **deegree OW S-Proxy: Ankopp lung Abrechnungs-Modul**

W eitere Herausforderungen:

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

- ▶ gdi@lgn.niedersachsen.de (Thorsten Jakob)
- ▶ www.geodaten.niedersachsen.de

- ▶ Stephan.Holl@intevation.de
- ▶ www.intevation.de/geospatial/

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?