InteProxy – der sichere Proxy für OGC-Dienste

Deegree-Day 2008, 17. Juni 2008, Bonn

- **Einführung: Was ist Absicherung?**
- **Aufbau einer sicheren GDI am Bsp. NDS**
- **Ausblick: Weitere Entwicklungsschritte**
- **(Demonstration)**

Absicherung von Geodiensten: Warum?

- **Anbietersicht: Absicherung gegen**
  - abhören
  - unbefugte Nutzung
    - Abruf
    - Bearbeitung
- **Anwendersicht: Absicherung gegen**
  - Missbrauch des eigenen Nutzerkontos
  - unterschieben falscher Daten
  - Einschränkung der digitalen Selbstbestimmung (kein DRM, TC, sonstige Zwangsvorgaben)

Grundlegende Konzepte

- **Nutzerkonten**
  - sonst keine vernünftige Zuordnung von Rechten
  - bedeutet: Authentifizierung notwendig
  - Alternativen: z. B. IP-basierte Freigaben (selten praktikabel, hoher administrativer Aufwand)
- **Verschlüsselte Verbindungen: SSL, TLS, bedingt VPN**
  - Absicherung gegen abhören
- **Authentifizierung**
  - Name/Passwort, Biometrisch (bitte nicht!)
  - Variante: Gegen andere Dienste authentifizieren, z. B. LDAP
  - Erweiterung: Tickets (Benutzerkonten als Anbieter nicht selbst pflegen, Rollen werden sehr wichtig)

Begriffe und Standards

- **Seit Feb. 2008: GeoXACML Standard bei OGC**
  - Nur ein proprietärer Prototyp, nicht erhältlich
- **WAS/WSS: Web Authentication/Security Service**
  - Ticket-System
- **SSL: Secure Socket Layer**
  - abgesicherter Tunnel ..... und PKI
- **Proxy (Stellvertreter)**
  - Umleiten, filtern

zu viele...

Freie Software Technologien

- **Verschlüsselung (SSL):**
  - Web-Server (z. B. Apache+modssl)
  - PublicKeyInfrastructure(PKI)-Management (z. B. OpenSSL+OpenLDAP)
- **Server-seitige Authentifizierung und Autorisierung für OGC Web Services:**
  - Deegree, Mapbender, 52N
- **Klient-seitig (SSL, Anmeldung):**
  - InteProxy, 52N

GDI-NI: Aufgabenstellung

- **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, ...)

GDI-NI: Umsetzungs-Leitgedanken

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

- **Pragmatischer Ansatz: ein Kompromiss**
  - Flexible Sonderlösung für Desktops
  - Server: Einfache, aber unmittelbar verfügbare Technologie, leicht anpassbar für zukünftige Standards

Klienten-Seite

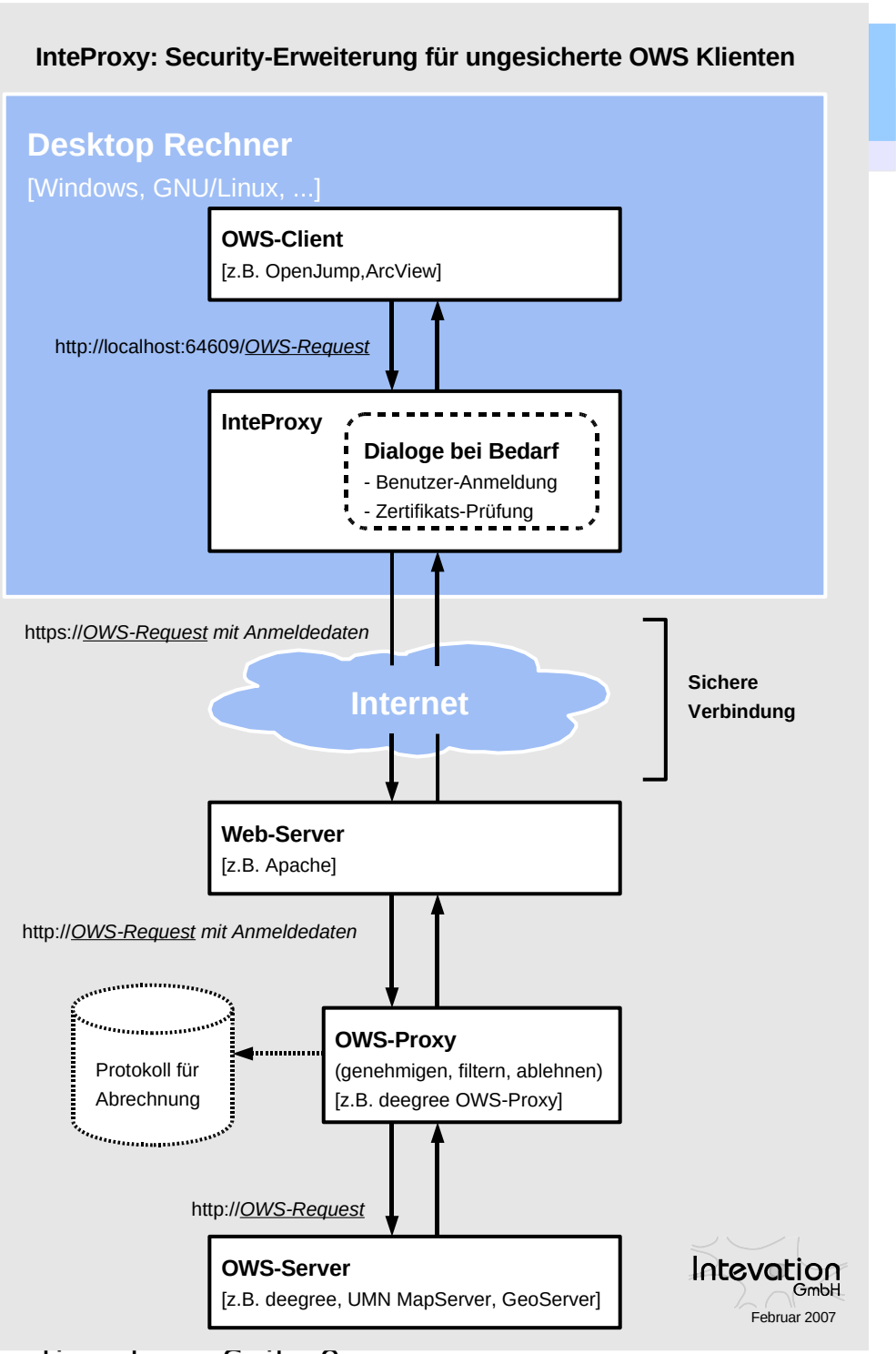
- **Desktop Klienten: beliebige (OpenJump, ArcGIS, ...)**
- **Problem: kein SSL, keine Authentifizierung**
- **Notwendig: Stellvertreter der SSL/Auth. übernimmt**
- **Denkbare Alternativen:**
  - Zwangs-Proxy (tief im System verankert)
  - Regulärer Web-Proxy (lokal oder Intranet)
  - Bedarfs-Proxy (nur für OWS-Anfragen direkt über URL angesprochen)
- **Lösung: InteProxy – ist ein regulärer Web-Proxy, optional auch als Bedarfs-Proxy nutzbar**

InteProxy

- Einfacher Installer für Windows
- (Desktop) Hintergrundprozess
- Aufbau SSL-Verbindung
- Nutzeridentifikation (cached)
- URL/Request/(Response) Rewrite
- für verschiedene OWS-Proxies konfigurierbar, auch HTTP BasicAuth

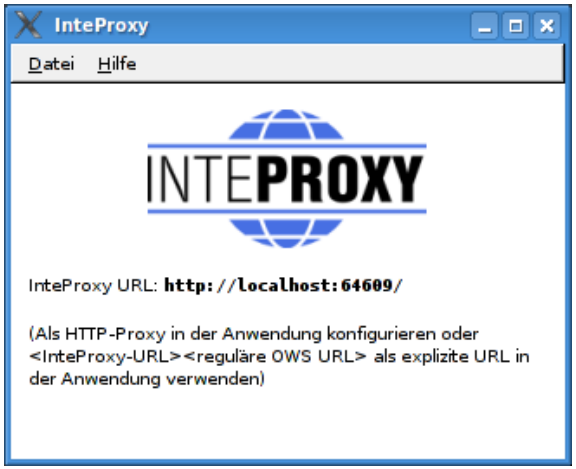
INTEPROXY

http://inteproxy.wald.intevation.org/index-de.html

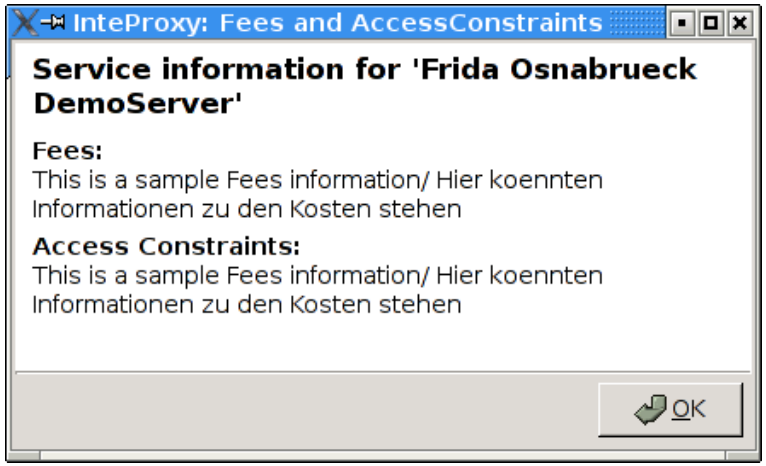


InteProxy-GUI

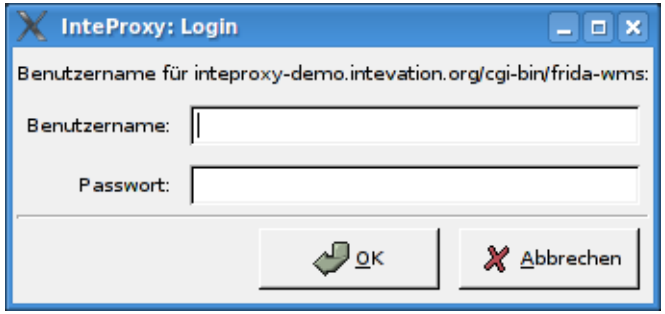
Was man von InteProxy sieht ...



Info-Fenster



Fees-Dialog



Passwort-Dialog

InteProxy Roadmap

Aktuelle Version: 0.3.1

- **SSL Zertifikats-Management (Vertrauens-Aussprache)**
- **Erweiterte graphische Konfiguration**
- **Unterstützung weiterer OWS-Proxy Typen**
- **Server-Modus (Headless)**
- **Spezielle Nutzungsszenarien**
  - Gruppen-Konten, Terminal-Server, ...

... bedürfnisgetriebene Entwicklung!

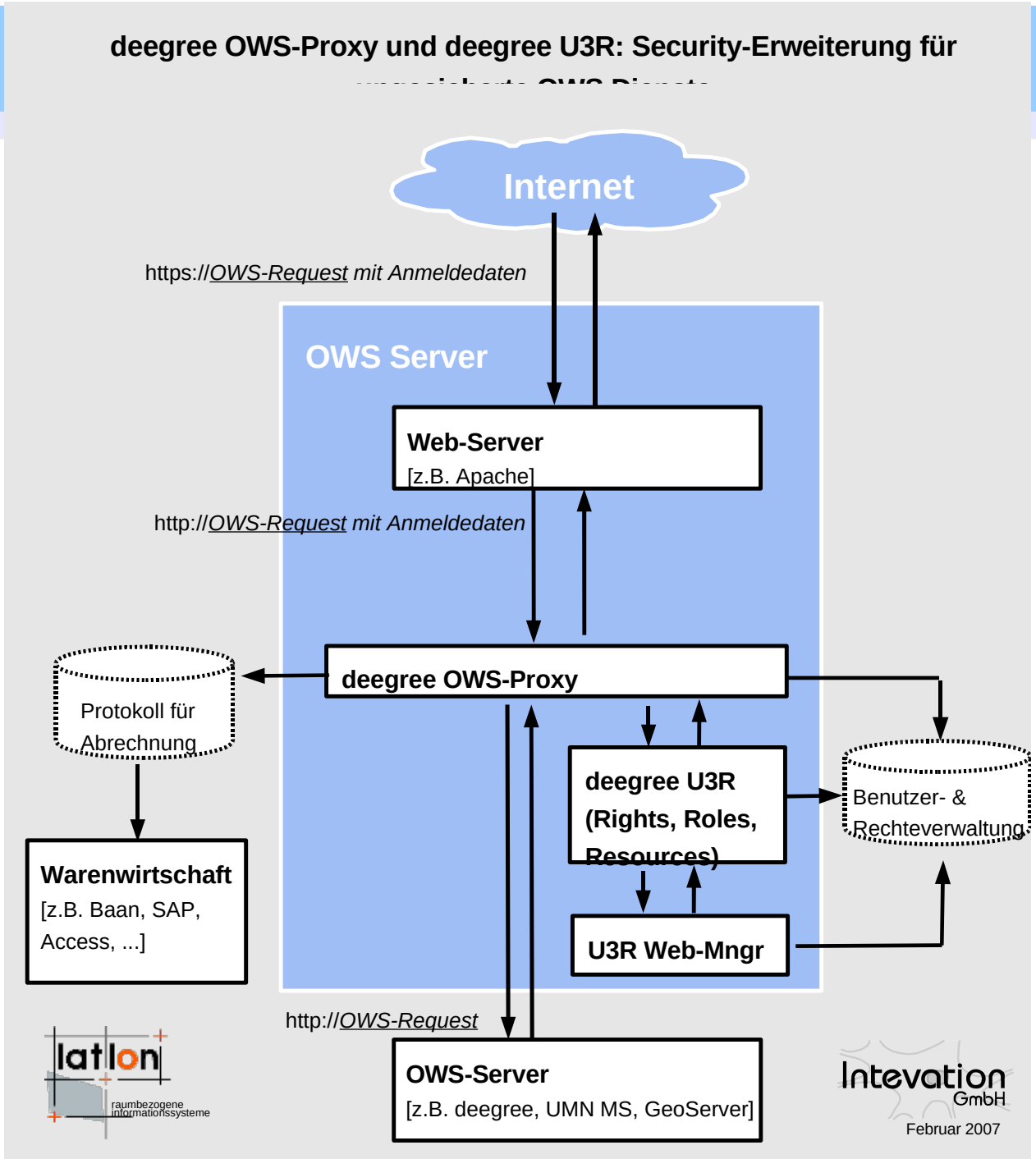
Server-Seite

- **Abzusichernde Dienste**
  - Geodaten-Portal(e)
    - Ohne verallgemeinerbare oder anbindbare Nutzer/Rechte-Verwaltung
  - Direkte WMS (und andere OGC) Dienste
- **Notwendig: Eigene Nutzer- und Rechteverwaltung**
- **Gewünscht: sehr feinkörnige Rechtevergabe (Polygone, GetFeatureInfo, ...)**
- **Weitere Herausforderungen**
  - GeoPortal kein reines OWS, häufige Änderungen bei Layernamen, ...
- **Lösungsbasis: iGeoSecurity Module: deegree OWS-Proxy und U3R**

iGeoSecurity

Inbetriebnahme:

- **Apache mit OpenSSL (CA)**
- **deegree OWS-Proxy**
- **deegree U3R**
- **Modellierung: Rollen, Gruppen**



iGeoSecurity Roadmap

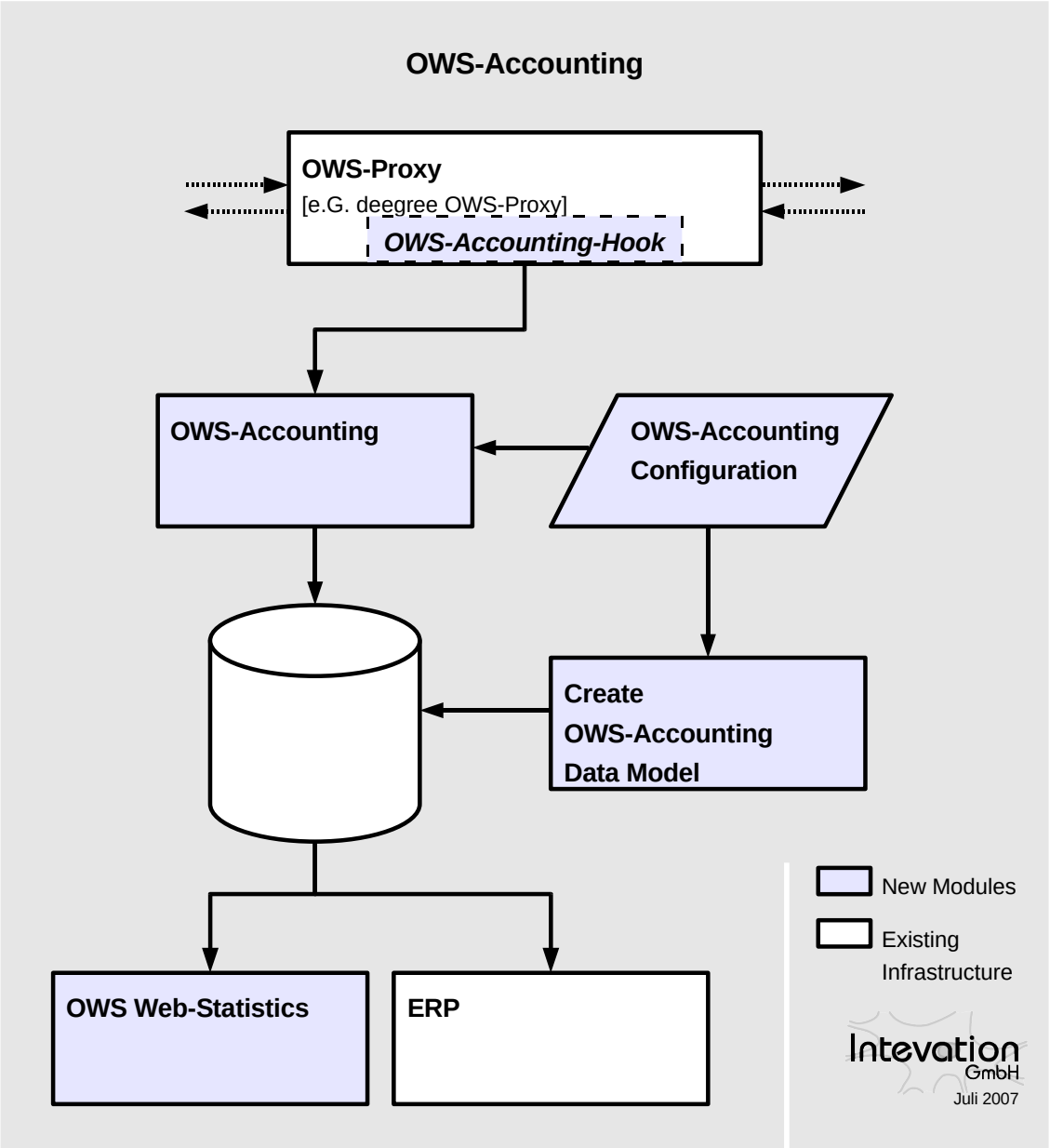
- **deegree U3R GUI: viele Komfort-Erweiterungen denkbar**

Weitere Herausforderungen:

- **Kaskadierung von jeweils gesicherten WMS**
- **... die Praxis hält noch einiges bereit**

OSAAS: Abrechnung und Statistik

- **Neu: „OGC Statistics And Accounting System“**
- **OWSProxy Nutzungsdaten in Warenwirtschaft (Baan, SAP, Access, ...)**
- **Roadmap: Web-Statistics Modul**



https://wald.intevation.org/projects/osaas/

Weitergehende Informationen

- **gdi@lgn.niedersachsen.de (Thorsten Jakob)**
- **www.geodaten.niedersachsen.de**
- **Stephan.Holl@intevation.de**
- **www.intevation.de/geospatial/**

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?