

Zuverlässiges Deployment von deegree-Komponenten am Beispiel von GISpatcher

27.05.2009, deegree day 2009, Bonn

- Grundlagen für den Betrieb einer sicheren Geodateninfrastruktur (GDI)
- Technische Anforderungen
- Das Projekt GISpatcher
 - Merkmale von GISpatcher
 - Auslieferung und Deployment
 - Wartbarkeit
 - Komponenten
- Fazit

- **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)

- **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

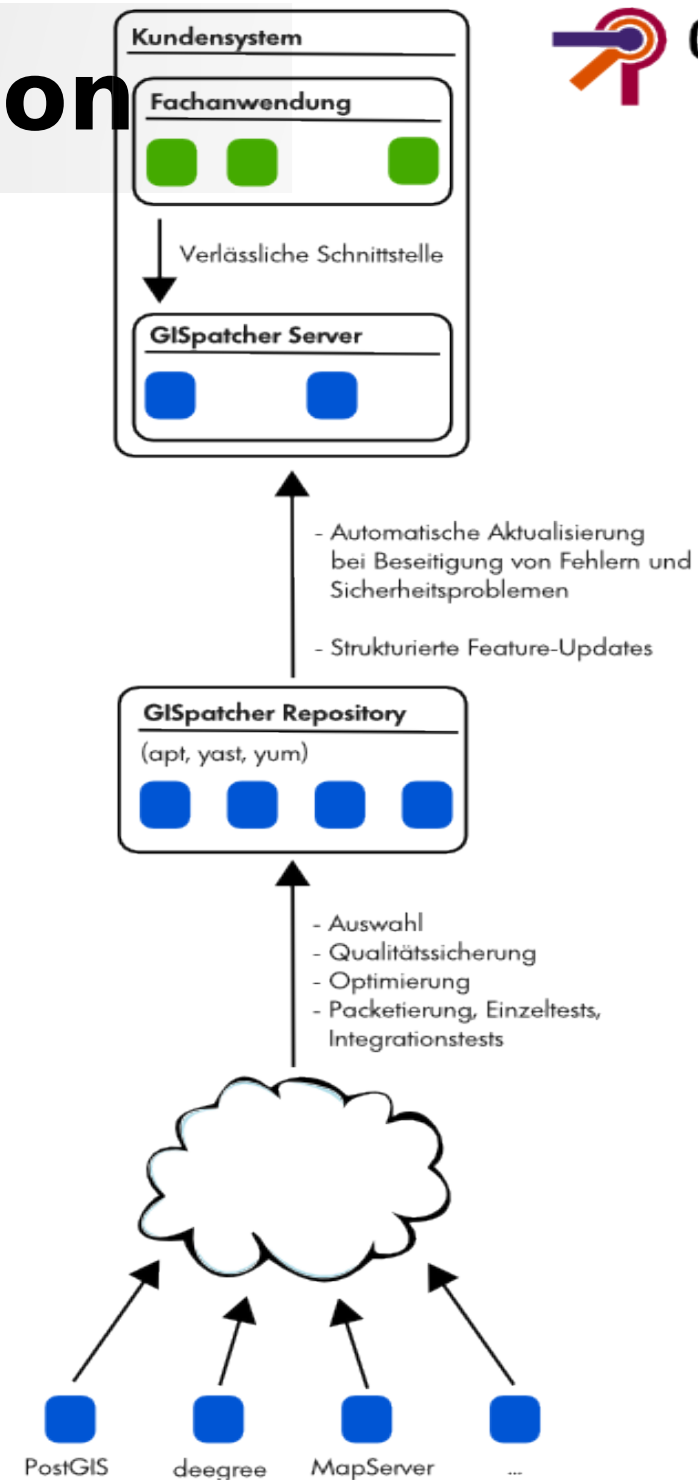
- **Authentifizierung**

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

- Absicherung Kommunikation Klienten - Server (SSL)
- Authentifizierung (wer)
- Autorisierung (was)
- Abrechnungsmechanismus (wieviel)
- Herstellerunabhängig (Freie Software, „Open Source“)
- Minimalinvasiv für Server und Klienten-Programme, möglichst unkompliziert
- Plattformunabhängig (Windows, Linux, ...)
- nach Möglichkeit bekannte und bewährte Technik nutzen

- Pflege und Wartung der Installation
 - Große Installationen müssen wartbar bleiben
-> Paketmanagement
 - Verlässliche Versionen mit definierten Zuständen
- Einfache Pflege der Benutzerverwaltung
- Abrechnungsnachweise und Billing
 - Kundenbezogene Abrechnung (nach AdV)
 - Anbindung an Reportingwerkzeug möglich
- Lösung: GISpatcher (<http://www.gispatcher.com>)

GISpatcher- Funktion



- Alle GISpatcher-Produkte sind
 - Frei (über https) als Pakete verfügbar (derzeit Debian Lenny, OpenSuse 10.3)
apt.gispatcher.com / rpm.gispatcher.com
 - qualitätsgesichert, signiert
 - versioniert in einem definierten Zustand
- GISpatcher-Server
 - Geodatenbank (PostGIS)
 - Absicherungskomponente (deegree OWSProxy / deegree U3R)
 - Accountingkomponente (OSAAS)

- Alle Dienste laufen in einer eigenen Tomcat-Umgebung
 - Separat herauf- und herunterfahrbar
 - Eigenständiges Logging
 - Clonen von OWSProxy-Containern automatisiert möglich.
- Jar-Dateien (deegree2.jar etc.) werden in shared/lib abgelegt, dadurch effektive Speichernutzung
- Update-Pfad über Betriebssystem frei wählbar

GISpatcher Appliance



- Ready-to-use Installation
- Display mit Statusanzeige und Server-Infos
- Über ein getrenntes Netz konfigurierbar (Webschnittstelle)
- Skalierbar

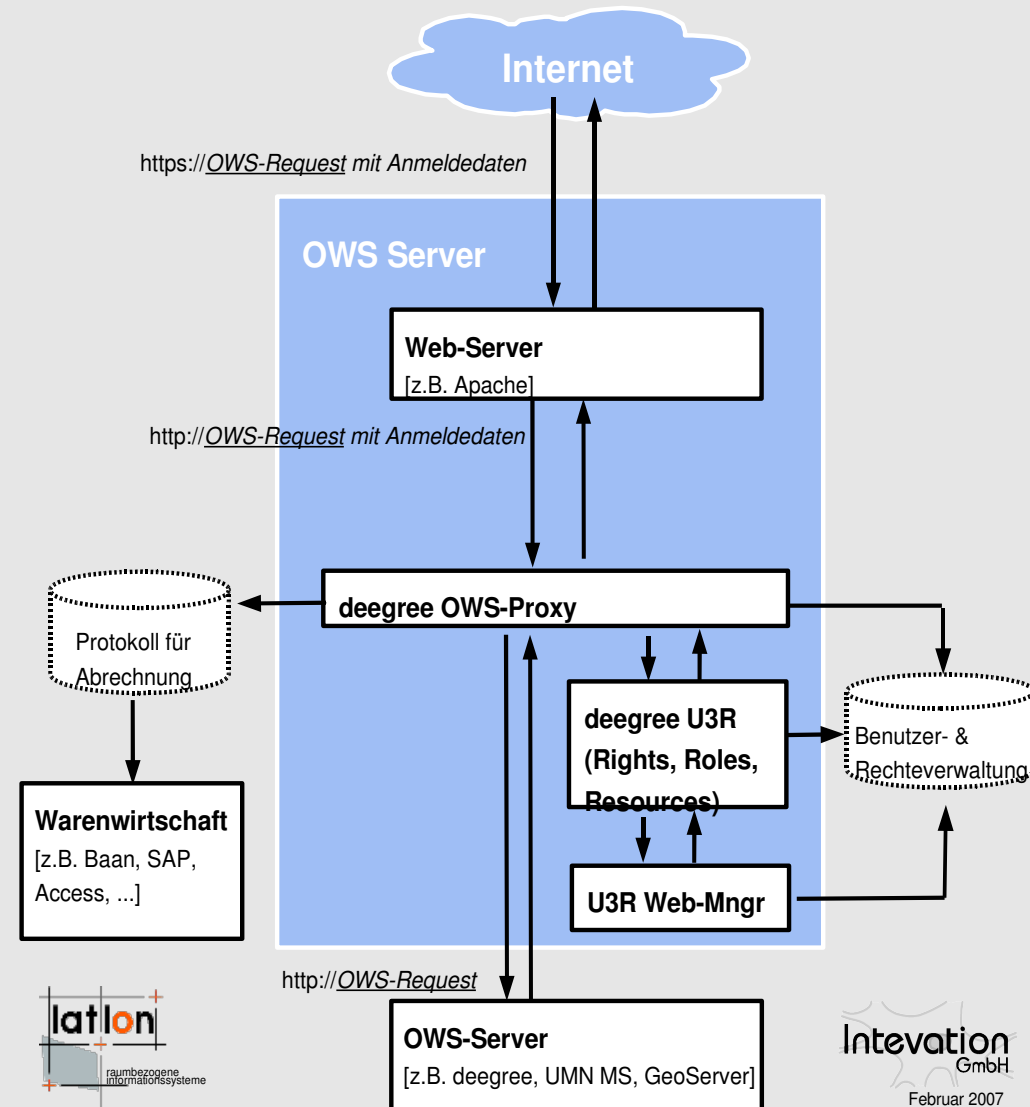


Komponenten: deegree OWSProxy



- Nutzerbasierte Absicherung durch transparenten Proxy
- Jeder WMS-Server absicherbar (UMN MapServer, Geoserver, deegree, ...)
- Gut skalierbar

deegree OWS-Proxy und deegree U3R: Security-Erweiterung für



Komponenten: deegree U3R



- Absicherungskomponente mit Web-Interface zum Benutzermanagement

Services Benutzer Gruppen Rollen Logout (SEC_ADMIN)

Services-Editor

Typ: WMS WFS

Eingabe:

| Nr. | Titel <> | Adresse <> | Typ <> | Aktion |
|-----|----------------------------|--|--------|----------------------------------|
| 1 | Frida Osnabrück DemoServer | http://demo.intevation.org/cgi-bin/frida-wms | WMS | Löschen Aktualisieren Bearbeiten |

Services Benutzer Gruppen Rollen Logout (SEC_ADMIN)

Rollen-Editor

Rollen

- SEC_ADMIN
- meier
- schmidt**

zugewiesene Gruppen

- schmidt

verfügbare Gruppen

- SEC_ADMIN
- meier

Services Benutzer Gruppen Rollen Logout (SEC_ADMIN)

Rechte-Editor

Definieren Sie hier, welche Informationsebenen für die Rolle 'schmidt' freigeschaltet sein sollen

Service: Frida Osnabrück DemoServer (WMS)

Freigeschaltete Layer

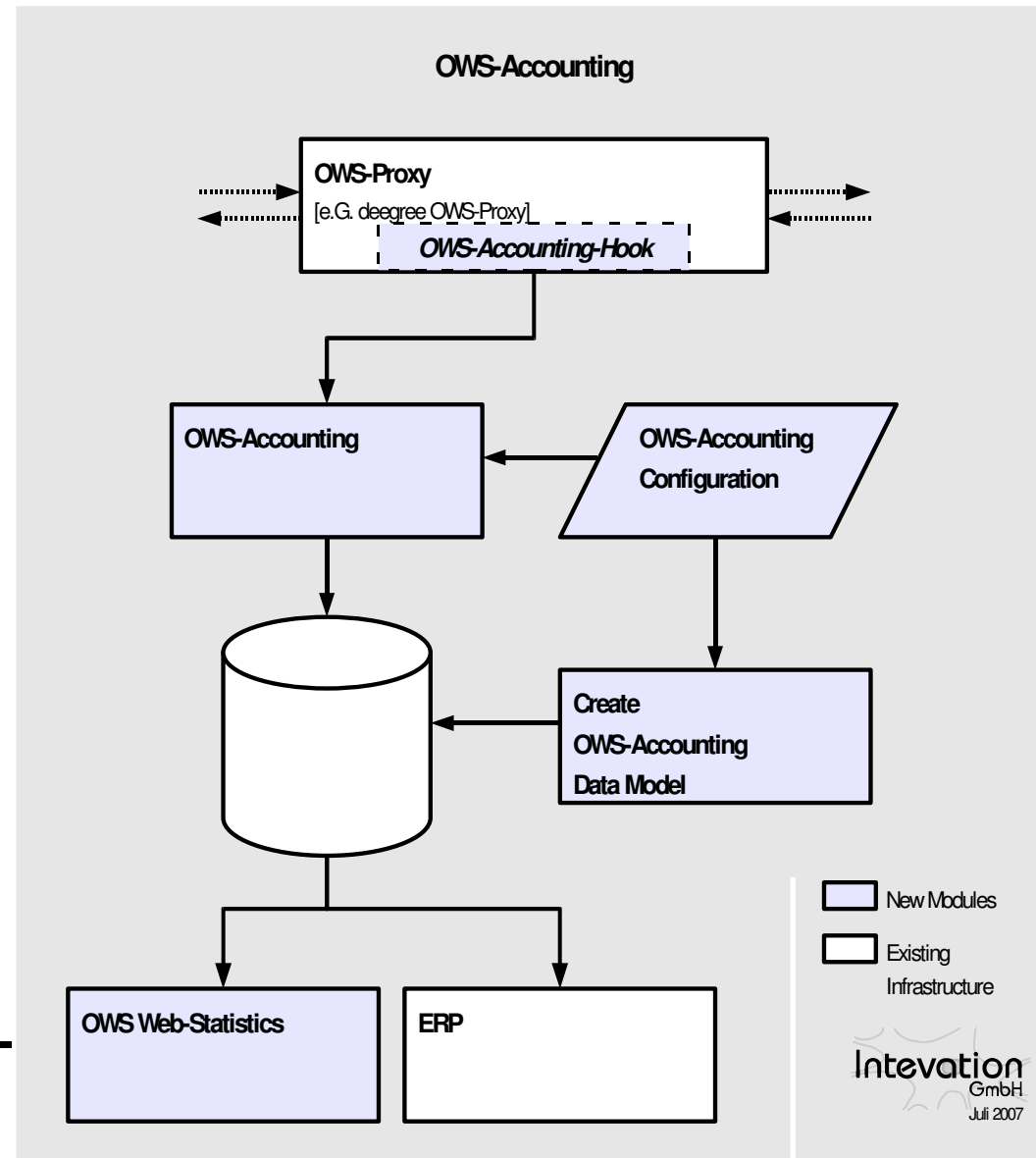
| Nr. | Name <> | Titel <> |
|-----|---------------------|--------------------|
| 1 | gruenflaechen | Grünflächen |
| 2 | gewaesser | gewaesser |
| 3 | gewaesserpolyl | Gewässerflächen |
| 4 | gewaesserlinien | Gewässer |
| 5 | sehenswuerdigkeiten | Sehenswürdigkeiten |

Gesperzte Layer

| Nr. | Name <> | Titel <> |
|-----|----------------------|--------------------------------|
| 1 | Osnabrueck | Frida Osnabrück DemoServer |
| 2 | strassenall | strassen |
| 3 | sonststrassenhinten | Sonstige Straßen (Hintergrund) |
| 4 | nebenstrassenhinten | Nebenstraßen (Hintergrund) |
| 5 | hauptstrassenhinten | Hauptstraßen (Hintergrund) |
| 6 | bundesstrassenhinten | Bundesstraßen (Hintergrund) |
| 7 | autobahnhinten | Autobahnen (Hintergrund) |
| 8 | sonststrassen | Sonstige Straßen |
| 9 | nebenstrassen | Nebenstraßen |
| 10 | hauptstrassen | Hauptstraßen |
| 11 | bundesstrassen | Bundesstraßen |
| 12 | autobahn | Autobahn |

Komponenten: OSAAS

- OGC Statistics and Accounting System: Abrechnungskomponente
- Nutzerdaten in ERP verfügbar
- Jede Anfrage an den gesicherten Dienst wird mitprotokolliert
- Vielfältige Auswertemöglichkeiten



<http://wald.intevation.de/projects/osaas>

Was wird kommen?



- Weitere Entwicklungsschritte:
 - einfache Dokumentation der Einrichtung
 - Eingliederung weiterer Module in GISpatcher Server
 - UMN MapServer
 - deegree WFS-Server
 - ...
 - Ggfs. Windows-Installationswerkzeug

- Sicherheit bringt Komplexität, daher auf Wartbarkeit achten!
 - Standardisierte Pakete
 - Qualitätsgesichert und bestens getestet
 - Update-Pfad klar definiert
 - Transparenter Entwicklungspfad
- <http://www.gispatcher.com>

Vielen Dank!



Fragen?

Intevation GmbH

Stephan Holl

<stephan.holl@intevation.de>

Neuer Graben 17

49074 Osnabrück

0541 - 335083 663