

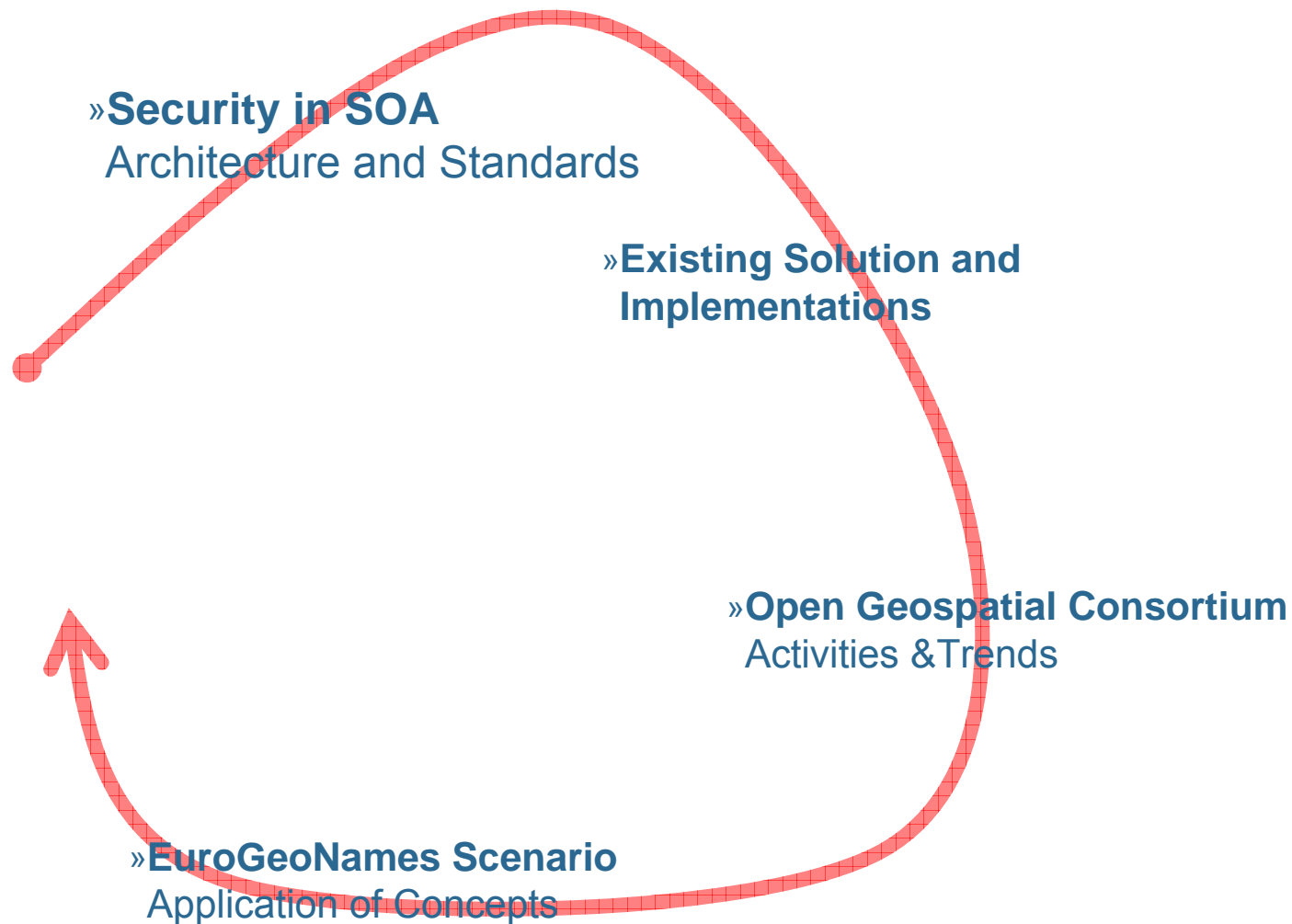


Service-based Access Control in Spatial Data Infrastructures

Jan Drewnak

con terra GmbH, Münster

Roadmap



What's it all about

➔ **Apply Authentication & Authorization to OGC Services**

needed for (almost) any business case

required for paid content

required for non-public content

provide user-specific “views” onto a service

➔ **Do not touch existing software**

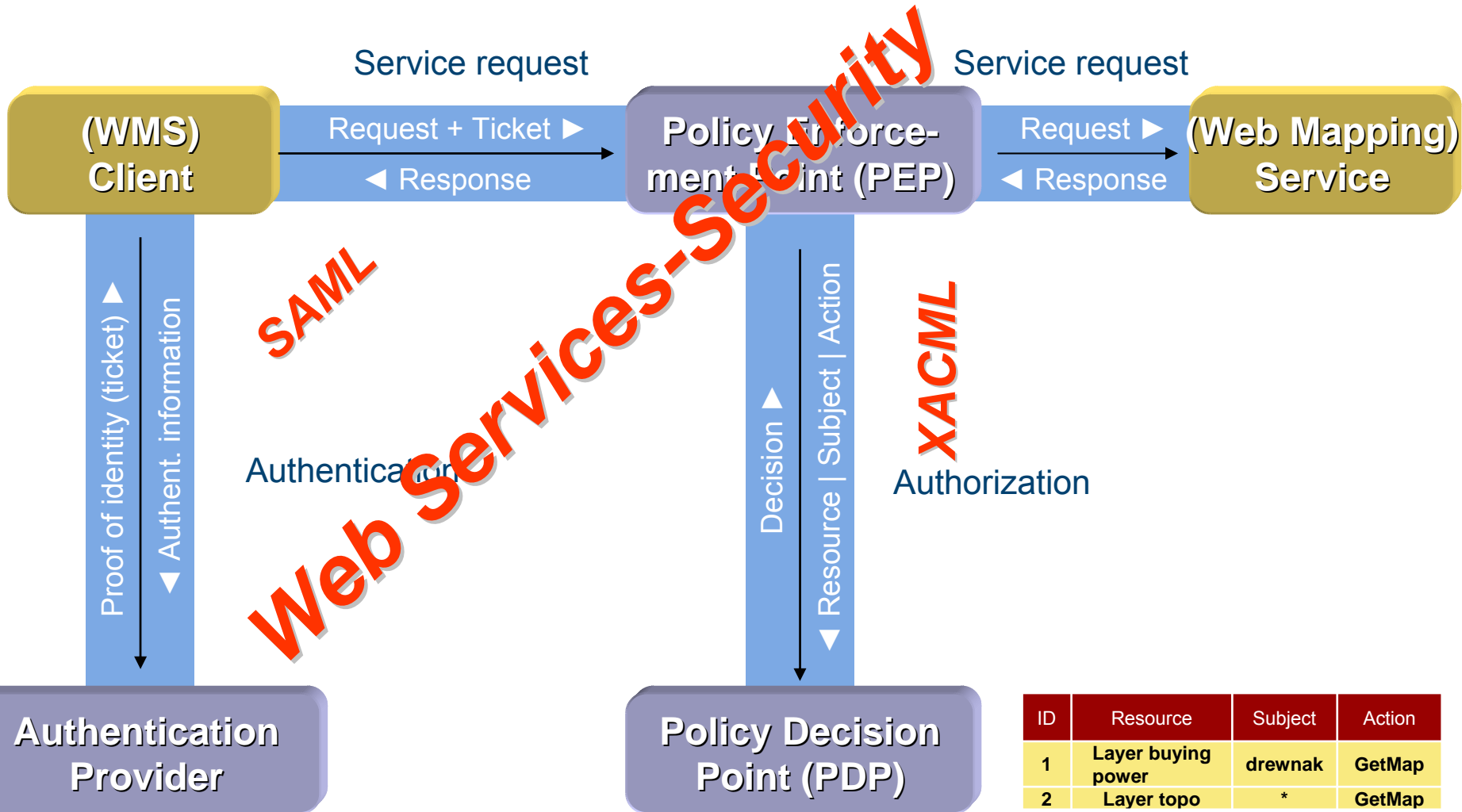
Support of standard OGC interfaces

Easy application of Authentication & Authorization to existing scenarios

➔ **But first...**

... how do they deal with these issues in the rest of the web services universe?!

Security handling in SOA



SAML: Security Assertions Markup Language

- ➔ Generic expression language to describe and **communicate approved user information**
- ➔ Specified by the OASIS industrial consortium
First version Nov. 2002
- ➔ Central SAML document contains assertions about users

E.g. assertion: *Jan Drewnak was authenticated by password by GeoClearingHouse, Inc. at 2007-03-5, 11 am. His e-mail address is drewnak@conterra.de*

XACML: eXtensible Access Control Markup Language

- ➔ **Generic expression language to describe policies (permissions/denials)**
- ➔ **Specified by the OASIS industrial consortium (Organization for the Advancement of Structured Information Standards)**
- ➔ **Complex (but powerful)**
- ➔ **GeoXACML extends XACML by ...**
 - ... adding functions and data types
 - ... defining a resource model
- ➔ **Well-defined XACML syntax allows to implement generic PDPs (-> SunXACML)**

“As long as your policies are expressed in (core) XACML, a policy decision can be made by any PDP”

WS-S – General info

- ➔ **Specifies, how to add security relevant information to SOAP messages**

Application of *XML Encryption(W3C)* and *XMLSignature(W3C)* plus “security tokens”

- ➔ **Specified by the OASIS industrial consortium**

- ➔ **Profiles for recent version 1.1**

Username Token | X.509 Token | SAML Token | Kerberos Token
REL (Rights Expression Language) Token

- ➔ **WS-S advantage: Security information is included in the SOAP *header*, the real payload in the body remains unmodified**

SOAP based service specifications need not to be modified to enable WS-S

Adoptable to SDI? From the technical perspective...

- ➔ **Problem: Common approaches are focused on „real“ web services (use of SOAP protocols etc.)**
- ➔ **OGC services are plain and crude (mostly limited to the HTTP protocol)**

Web service security is not fully applicable

- ➔ **OGC clients are plain, too!**

A possible approach...

- ➔ Understand security as an **extension** of existing spatial data infrastructures
- ➔ Use security standards that are established within the IT sector as far as possible
- ➔ Be open for changes!
 - GeoDRM is evolving
 - OGC service interfaces will get mapped to SOAP (sometimes)
 - Support different standards/technologies for policies and identities
 - Interfaces may change
- ➔ **But: provide support for existing standards (and thus solutions)**

GDI NRW Solution

➔ 2001: First concepts published in GDI NRW

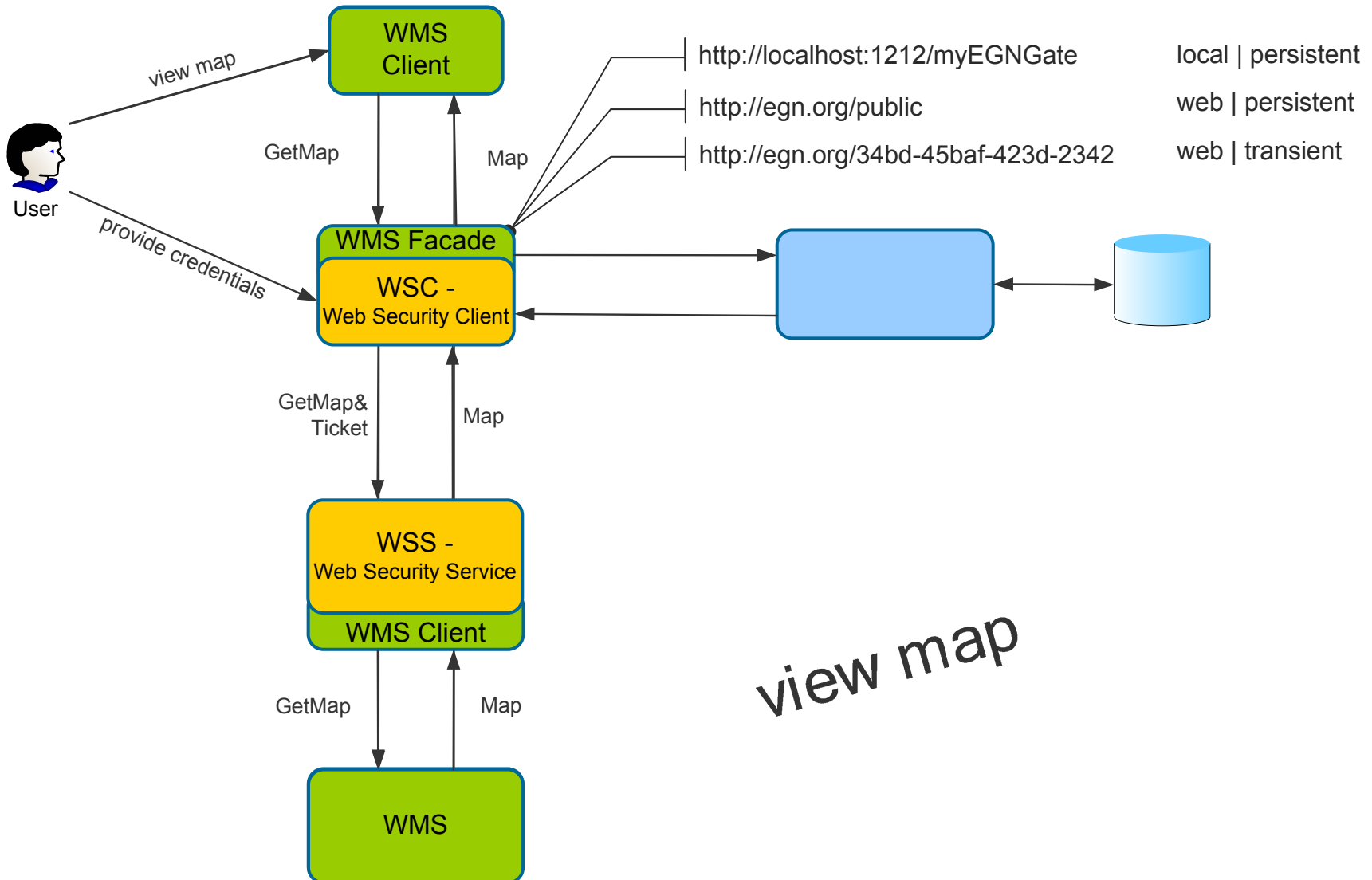
➔ 2002: GDI NRW Testbed II

Specification of

Web Authentication Service (WAS)

Web Security Service (WSS)

General Architecture



view map

V
C

Implementations

➔ 52°North Open Source Software Initiative

Basic implementations of WSC | WAS | WSS
current release allows protection of WMS layers

➔ con terra sdi.suite securityManager

based on open source implementations
protection of WMS | WFS(-T) | ArcIMS | ArcGIS Server
spatial authorization for WMS | WFS | ArcIMS
administration tools

➔ Interceptor concept

Authorization module that encapsulates knowledge about service-specifics, e.g. WFS vs. WMS requests

Tasks for example: Filter out layers, feature types, attributes, ...

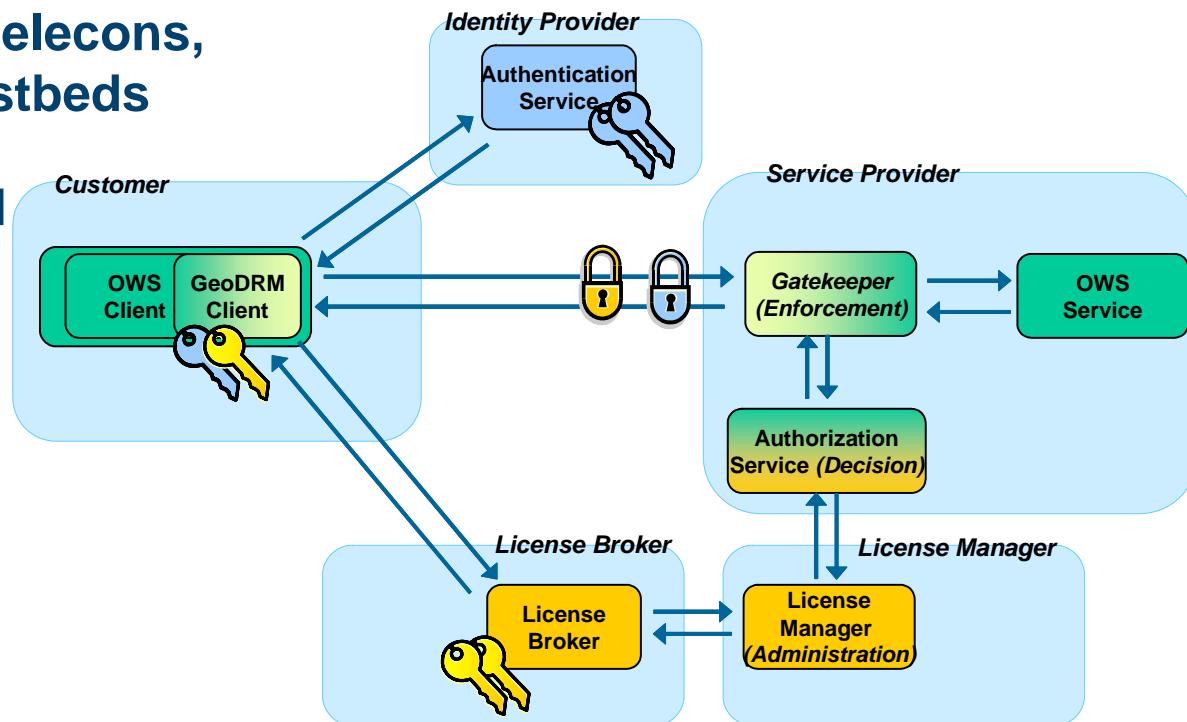
Interceptors are deployed in the WSS, which is just a “runtime environment”

OGC – Trends in Access Control

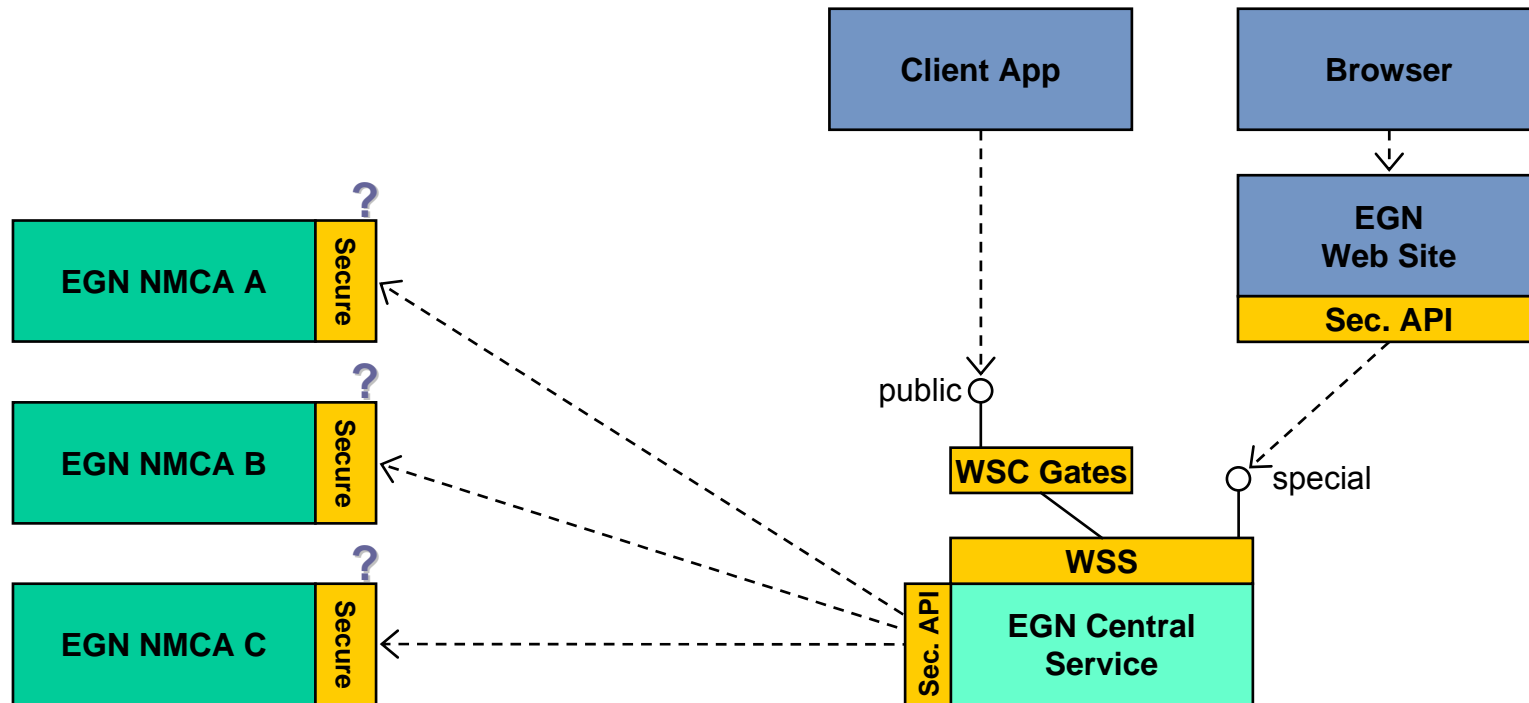
- ➔ GeoDRM Working Group since 2004
- ➔ Goal: evaluate and develop security solutions for OGC Web Services
- ➔ Activities: meetings, telecons, participate in OWS testbeds
- ➔ Result OWS-4 testbed

☹ Applies to SOAP services

☺ Applies WS-S



Just a (EGN) Scenario



Projects Using Introduced System (con terra / 52°North)

- ⇒ **Forestal GIS (InFoGIS),**
State Forestal Agency, Baden-
Wuerttemberg
- ⇒ **Geodatenatlas Steinfurt & Borken,**
Districts of Steinfurt/Borken,
Germany
- ⇒ **Metainformation System Hesse,**
Hessische Zentrale für
Datenverarbeitung
- ⇒ **LoG-IN (Interreg III Project),**
Consortium Leiedal (BE), Norfolk
(UK), Rotenburg/Wümme (DE)
- ⇒ **INSPIRE@EC**
European Commission (Eurostat)
- ⇒ **Joint Project 2005,**
Dortmund, Münster, Steinfurt,
Borken, Coesfeld, Bottrop
- ⇒ **Hydrological GIS (GGInA),**
Federal Agency for Hydrology of Germany
- ⇒ **Management of Environmental Data**
(OSIRIS), Rheinland-Pfalz
- ⇒ **Geoportal Croatia,**
State Geodetic Agency (Kroatien)
- ⇒ **Geocommunicator.gov,**
Bureo Of Landmanagement (USA)
- ⇒ **City of Bottrop**
- ⇒ **KABAS,**
State Environmental Agency, North Rhine-
Westfalia
- ⇒ **sdi.suite securityManager, con terra GmbH**
- ⇒ **52°North Open Source Initiative**



Dipl.-Geoinf.
Jan DREWNAK

con terra GmbH
Muenster

drewnak@conterra.de
www.conterra.de

Thanks for your attention!

Questions?