



GDI-DE

Spatial Data Infrastructure Germany

- Security Issues -

OGC Security Working Group
Paris, July 9th, 2007

Geschäfts- und Koordinierungsstelle GDI-DE
(Coordination Office GDI-DE)
ronald.mordhorst@bkg.bund.de



- 1 Introduction: SDI Germany / INSPIRE

- 2 Requirements
 - 2a Why do we need Security?
 - 2b Where do we need Security?
 - 2c Who does need Security?
 - 2d Until when shall security be implemented?
 - 2e Which standards can be used for what?

- 3 Are standards missing?

- 4 Discussion



1 Nation (Federation)

with parliament (legislature),
administration (executive
authority), judicial power

16 States („Länder“)

each with parliament
(legislature), administration
(executive authority), judicial
power

14.000 Municipalities

with many rights of self-
government





Federation

- BKG Frankfurt ●
- BKG (GDZ) Leipzig ●
- Federal Authorities

16 States

- SDI Initiatives ●
- SDI Network ● and SDI Offices

14.000 Municipalities

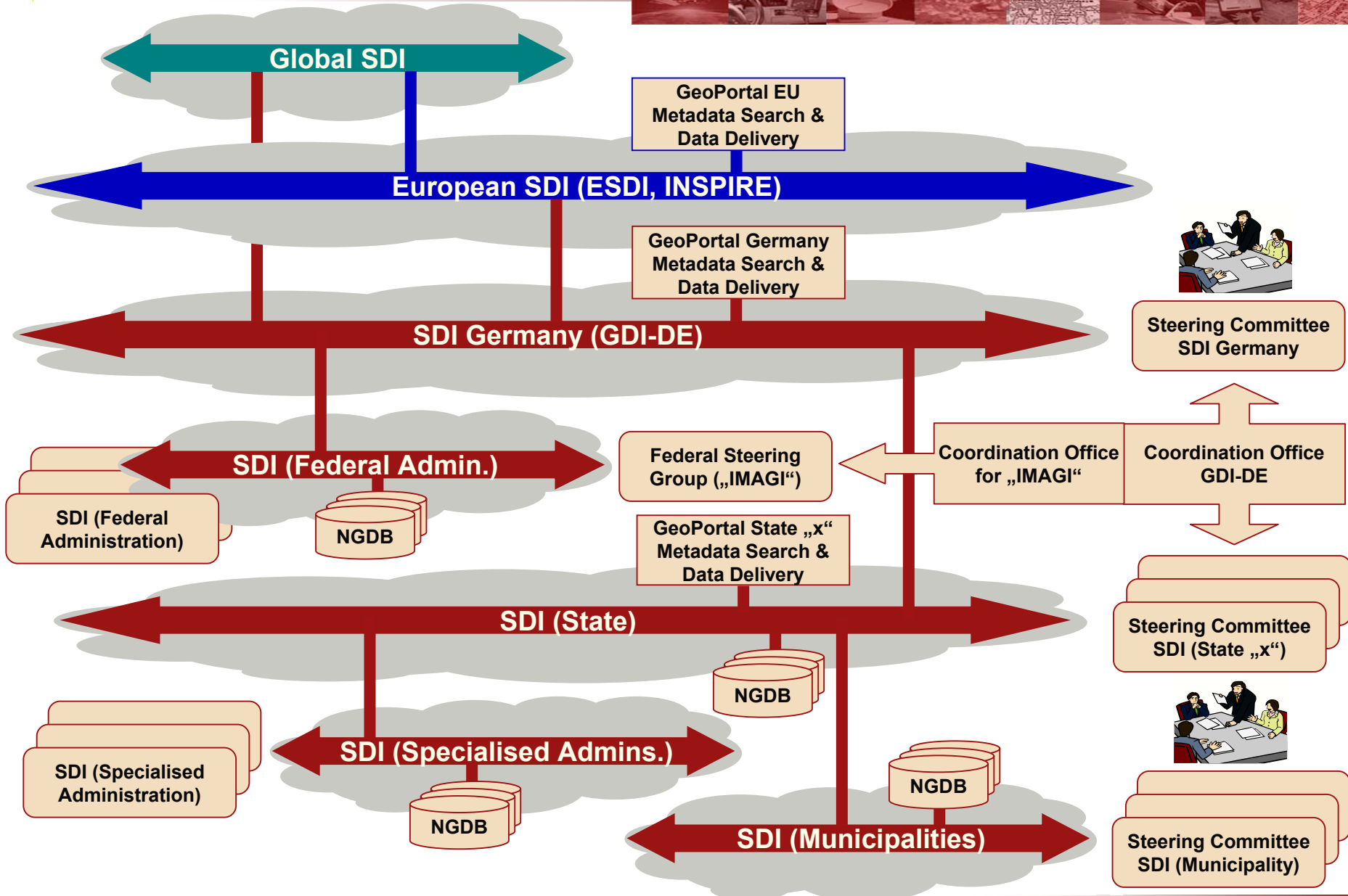
- SDI Initiatives,
- Cooperations

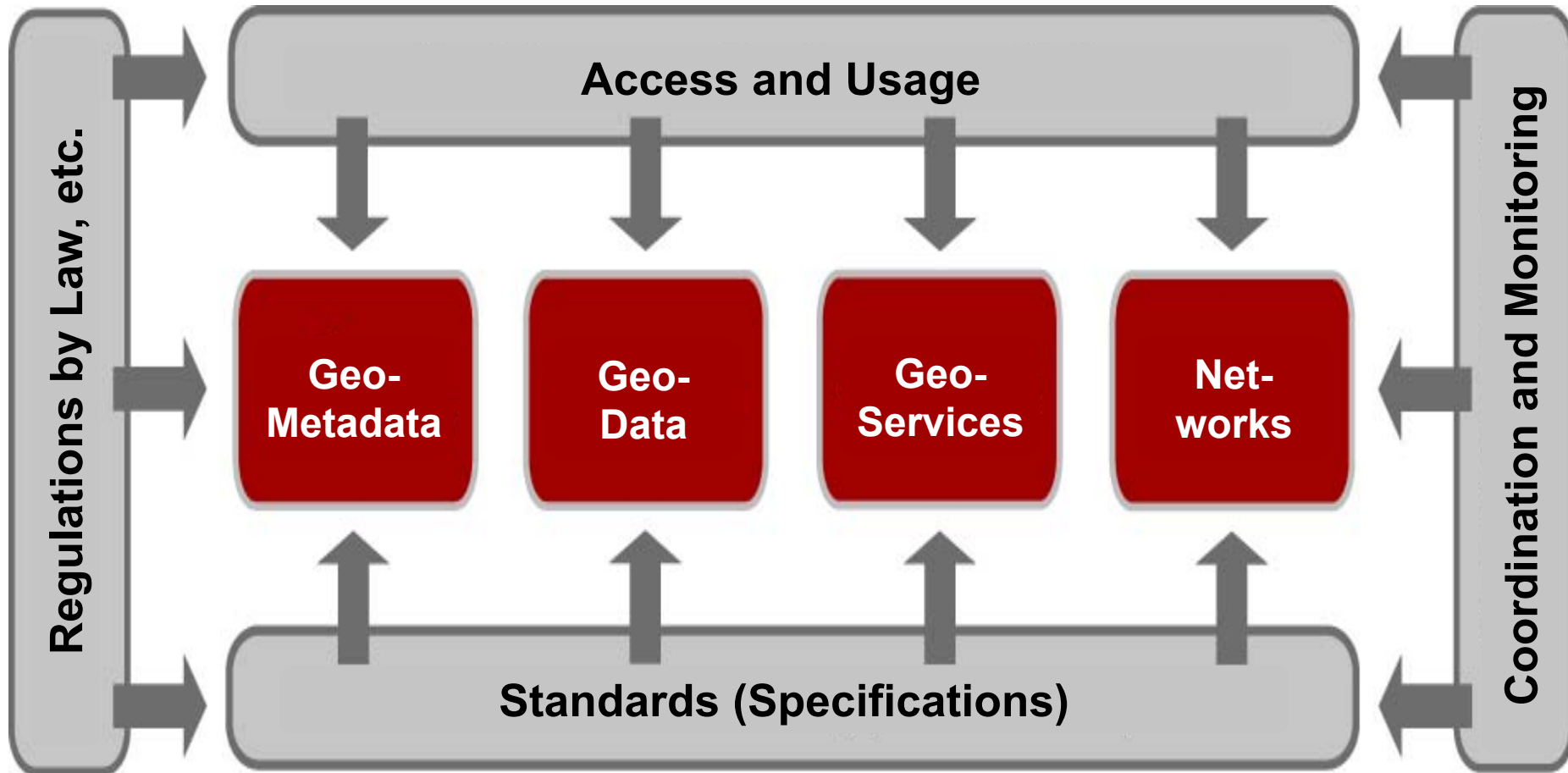
Geoinformation industry

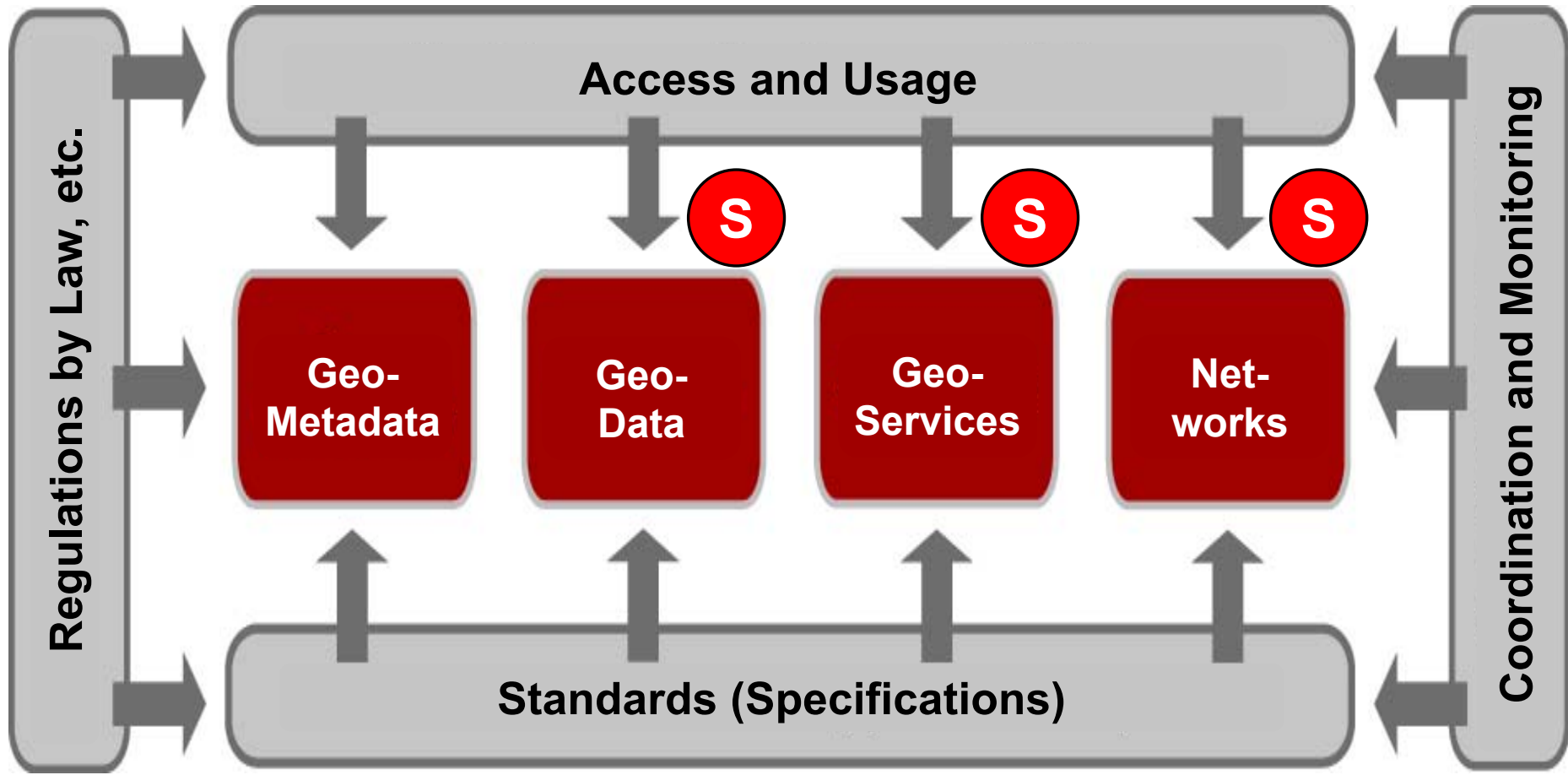
- GIW Office ●
- GDI Model projects
- Cooperations



Technical and Organisational Structure of SDI Germany

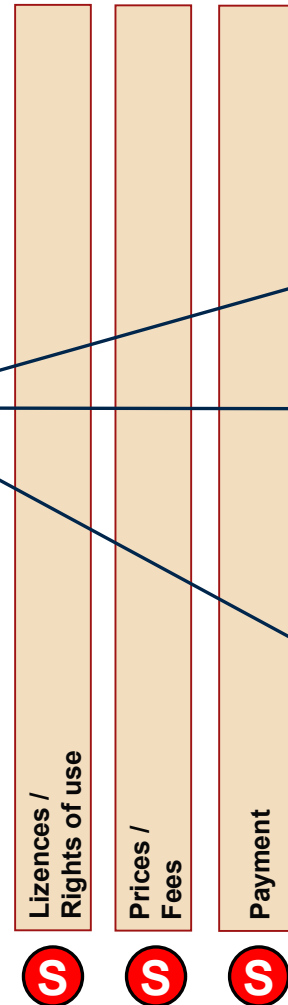




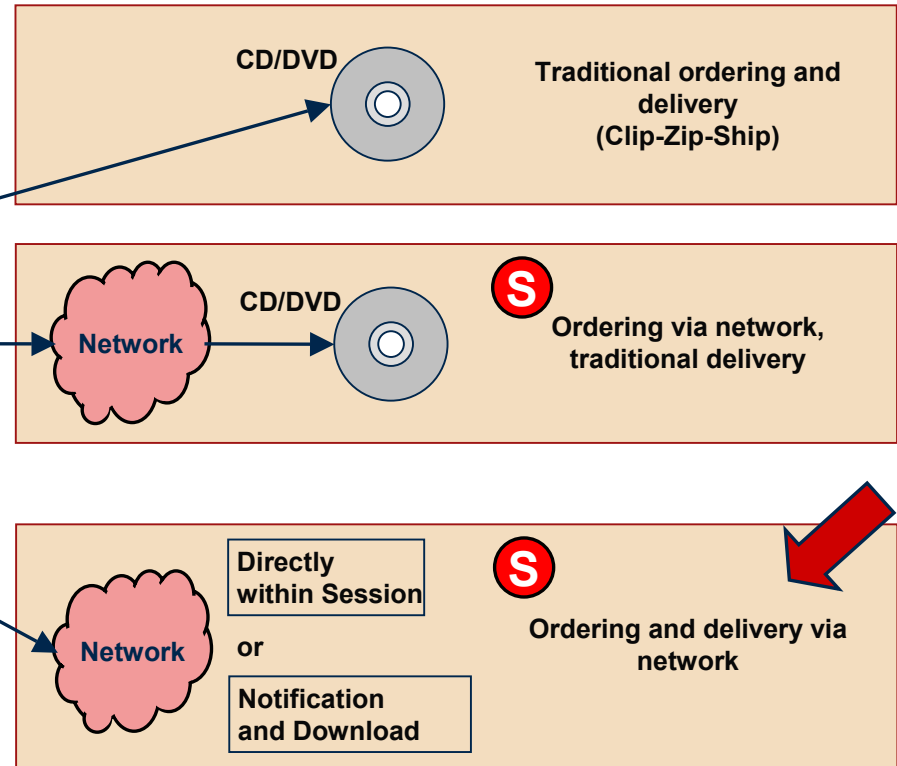
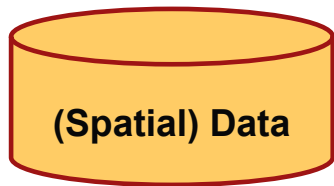




General Functions (optional)



Ordering & Delivery





Architecture of Spatial Data Infrastructure Germany Version 1.0_EN

2007

A concept for sharing, access and use of
spatial data and spatial data services,
across the various levels of public authorities
and
across different sectors of eGovernment in Germany








Spatial Data Infrastructure Germany



specs. not sufficiently developed

specs. and solutions not sufficiently developed

<i>Grading</i> <i>Function</i>	<i>GDI-DE mandatory</i>	<i>GDI-DE optional</i>	<i>GDI-DE prospective</i>
Data and management functions	<ul style="list-style-type: none"> • Metadata catalogues: Registration and lookup of spatial data, geoservices and applications • Provision of vector data • Provision of raster data • Gazetteer 		<ul style="list-style-type: none"> • Registers  • Thesauri • Sensor data 
Visualisation	<ul style="list-style-type: none"> • 2D-Visualisation 	<ul style="list-style-type: none"> • 3D-Visualisation 	
General functions		<ul style="list-style-type: none"> • Service monitoring • Access control  	<ul style="list-style-type: none"> • Ordering functions  • License management 
Applications		<ul style="list-style-type: none"> • Geoportals 	
Information models	<ul style="list-style-type: none"> • National spatial data base (NGDB) • Defined CRSs • Description of spatial resources • Defined data formats (vector, raster) 		<ul style="list-style-type: none"> • Common license model



- Access control services require an enhancement of the communication protocols (e.g. using cryptographic techniques) between user and service.
- The Simple Object Access Protocol (SOAP) supports nearly all requirements for a safe communication. Other, more specialised specifications make use of SOAP as basic technology. A well-known example is the Web Service Security Specification (WS-S).
- The architecture recommends to use WS-S with SOAP as communication protocol and to use at least for the transport of descriptions of subjects (so-called digital identities) compatible standards (e.g. SAML).

Recommended Implementation Specifications

- OASIS Security Assertion Markup Language (SAML) V2.0
(Download: <http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip>)
- OASIS eXtensible Access Control Markup Language (XACML) V2.0
(Download: <http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-ALL.zip>)
- OASIS Web-Service Security Core Specification 1.1
(Download: <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>)



General Questions in the Security (and Safety) Context



- Effort spent in creation of data
- Effort spent in software & systems
- Annual data maintenance cost
- Annual system cost
- ...

**How many man-years
spent ?**

Value in € ?

Example 1: SDI of Some German States

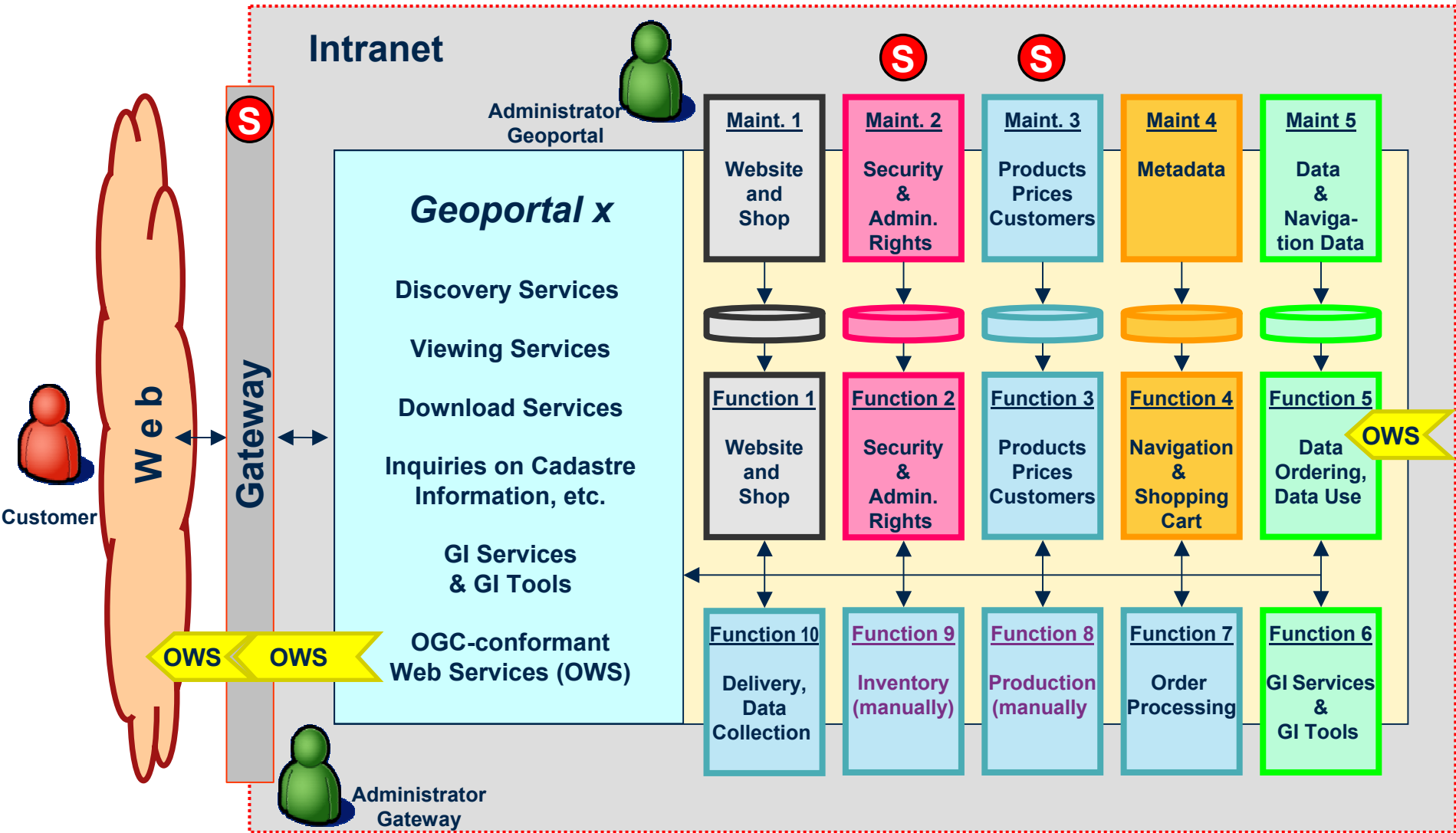


Example 1: SDI of Some German States



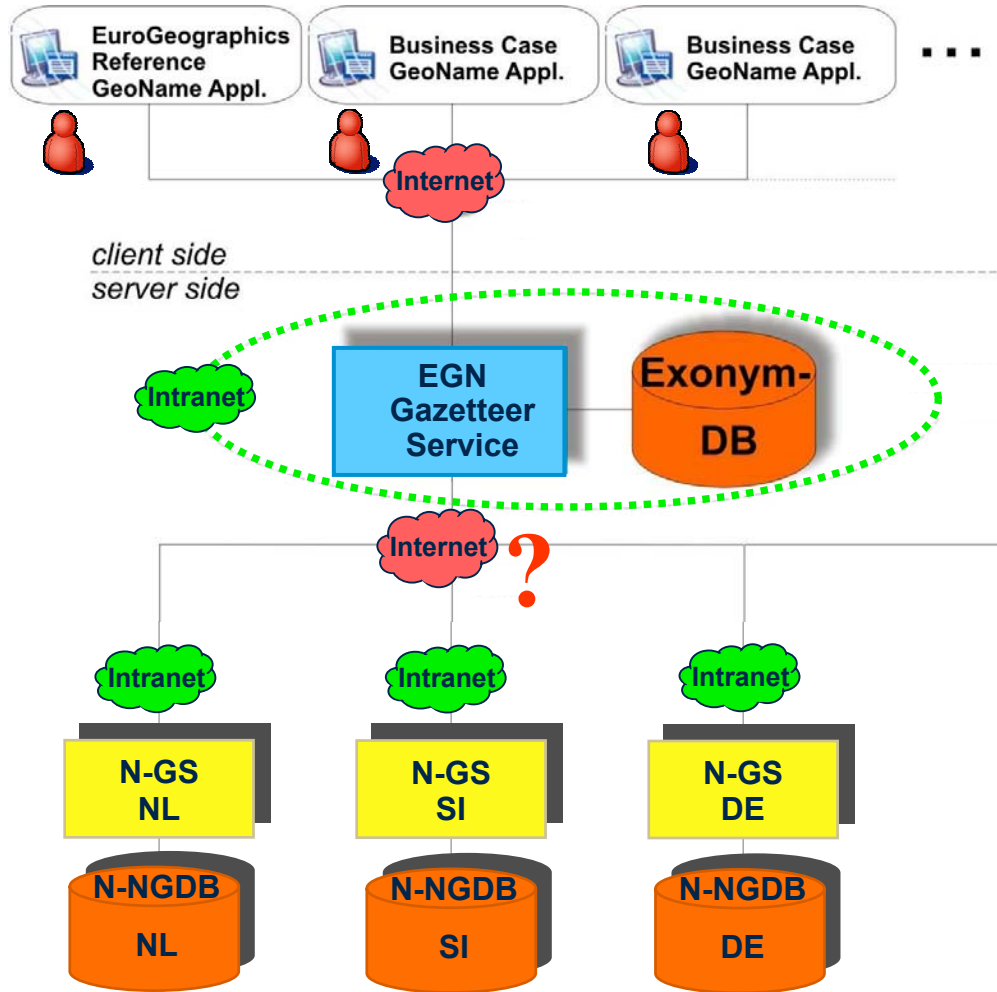
1. Link to Gateway
2. Authenticate
3. Discovery (user-dependent)
4. Selection (Layers, Bounding Geometries, ...)
5. Combination of Layers, etc.
6. Calculate Price (underlying Price Model) ← optional
7. Contract between Data Owner and User (e.g. Terms of Use, Copyright)
8. Delivery (or online usage)
9. Invoicing ← optional
10. Payment ← optional

Functional Structure Geoportal x

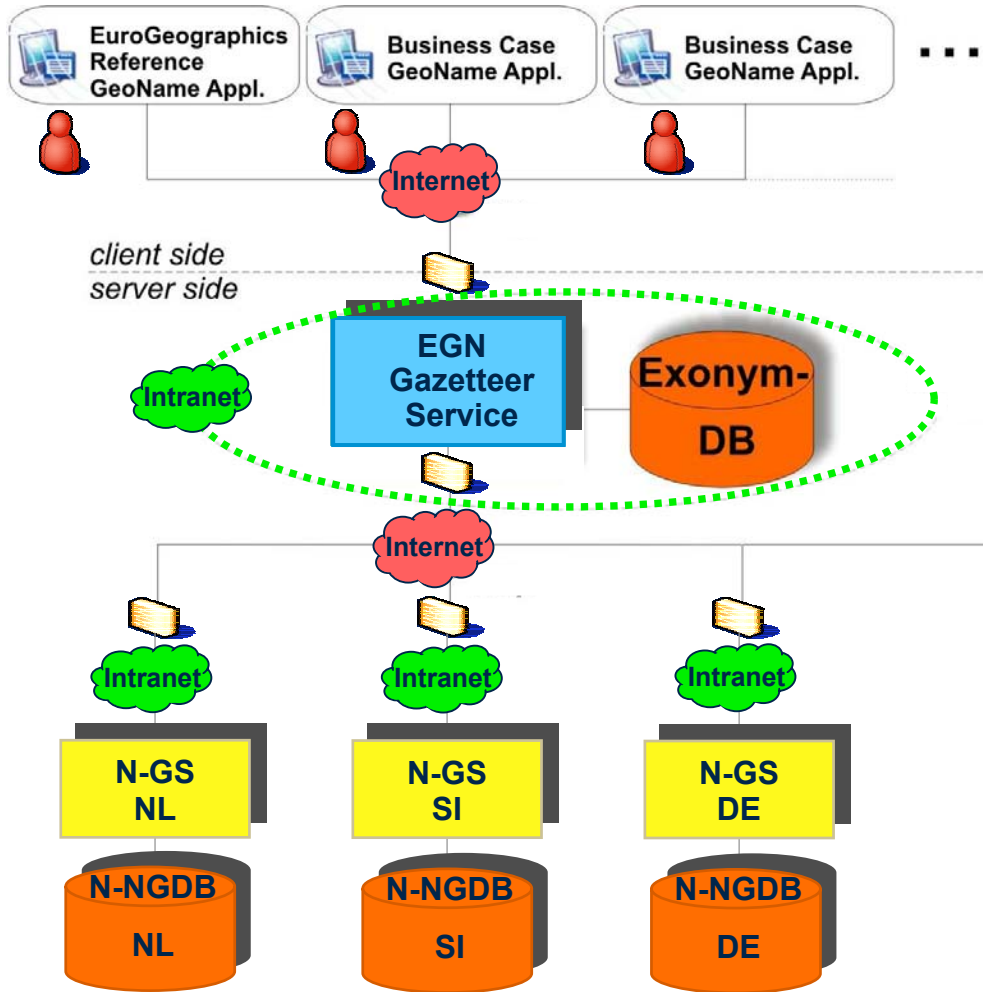




Example 2: EuroGeoN Multinational SDI Service (WFS-based)

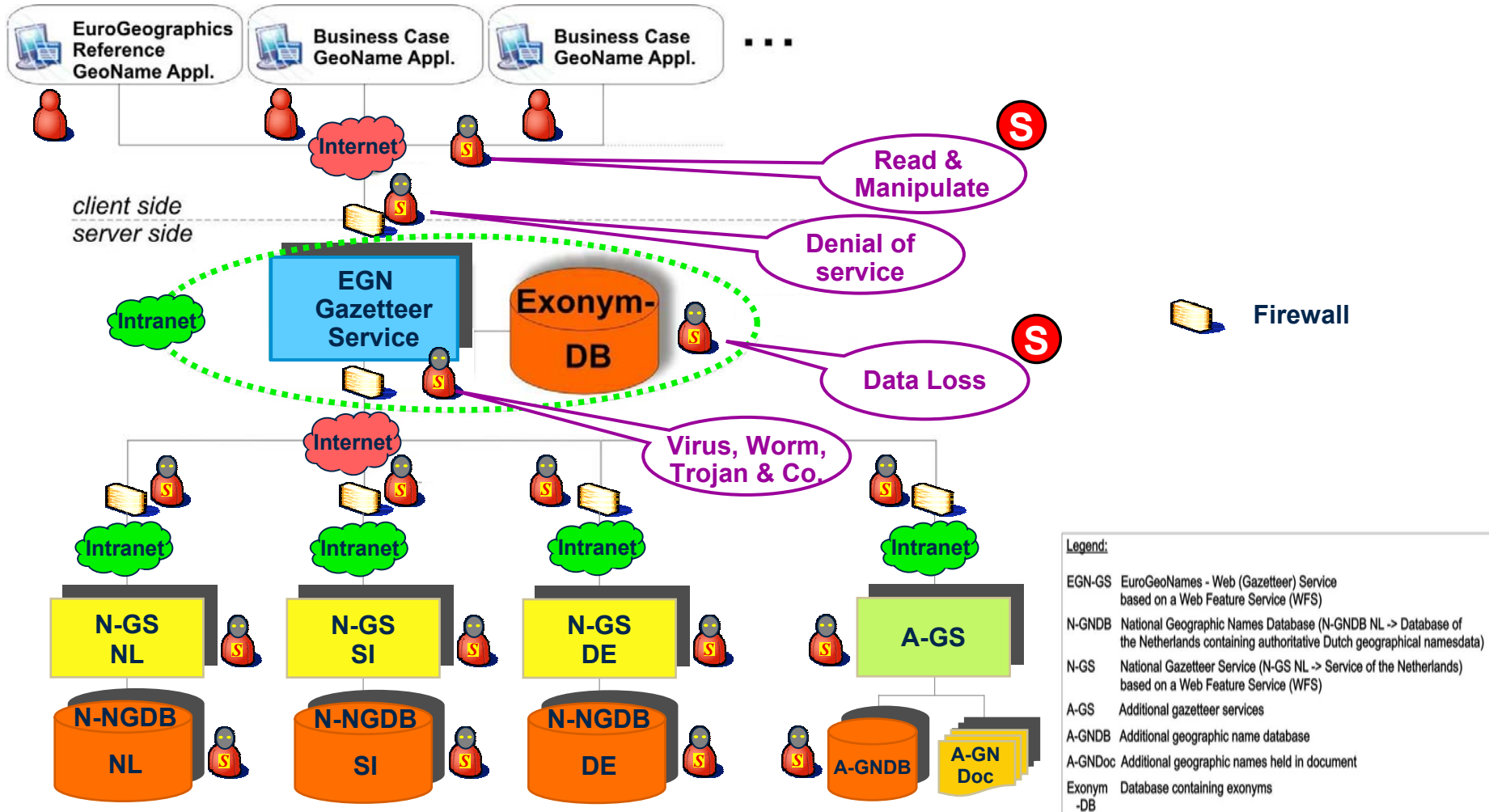


- Legend:**
- EGN-GS EuroGeoNames - Web (Gazetteer) Service based on a Web Feature Service (WFS)
 - N-GNDB National Geographic Names Database (N-GNDB NL -> Database of the Netherlands containing authoritative Dutch geographical names data)
 - N-GS National Gazetteer Service (N-GS NL -> Service of the Netherlands) based on a Web Feature Service (WFS)
 - A-GS Additional gazetteer services
 - A-GNDB Additional geographic name database
 - A-GNDoc Additional geographic names held in document
 - Exonym-DB Database containing exonyms

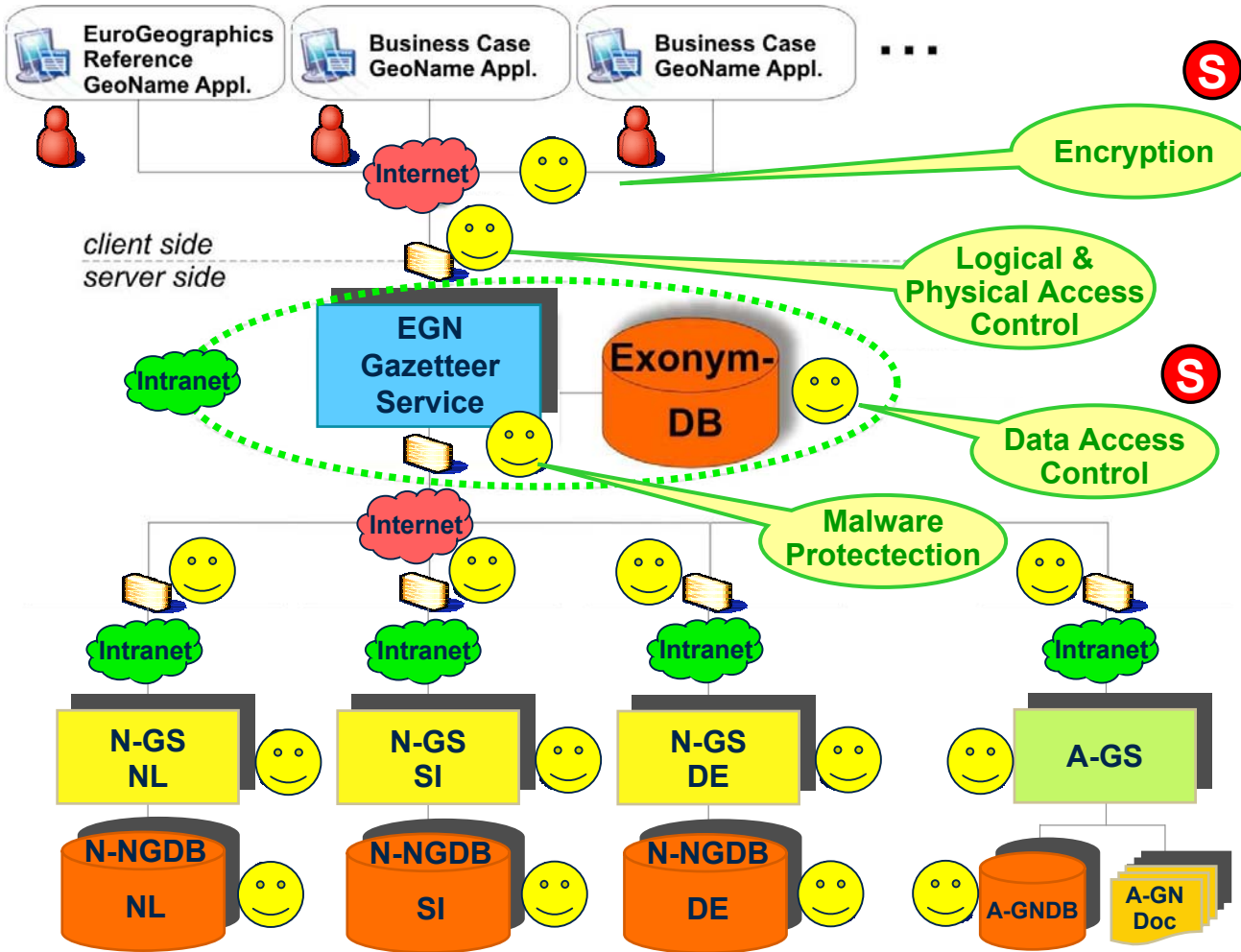


 Firewall

- Legend:**
- EGN-GS EuroGeoNames - Web (Gazetteer) Service based on a Web Feature Service (WFS)
 - N-GNDB National Geographic Names Database (N-GNDB NL -> Database of the Netherlands containing authoritative Dutch geographical namesdata)
 - N-GS National Gazetteer Service (N-GS NL -> Service of the Netherlands) based on a Web Feature Service (WFS)
 - A-GS Additional gazetteer services
 - A-GNDB Additional geographic name database
 - A-GNDoc Additional geographic names held in document
 - Exonym-DB Database containing exonyms



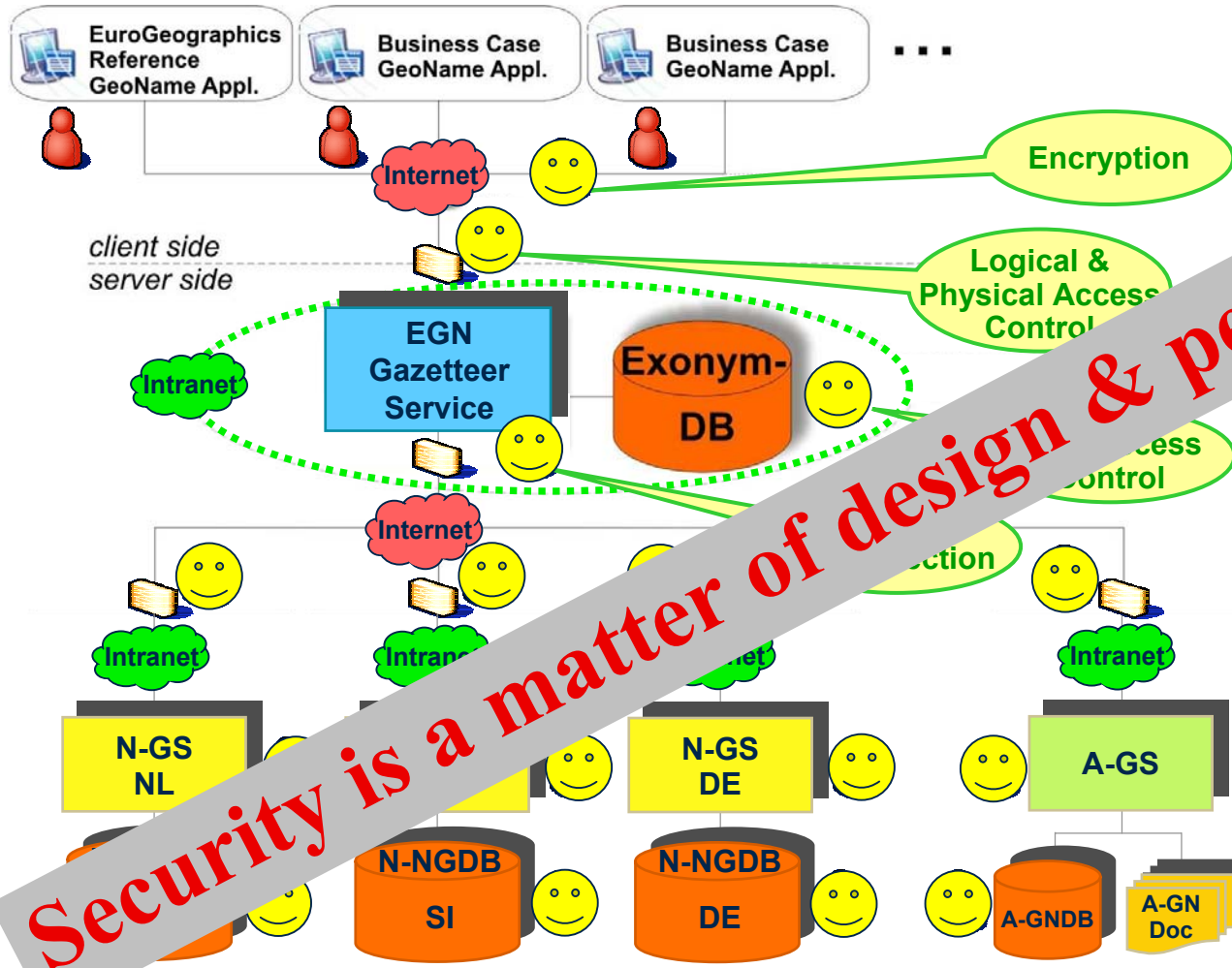
Possible countermeasures



Countermeasures are necessary at EGN central site and at EGN decentral sites and within applications

- Legend:**
- EGN-GS EuroGeoNames - Web (Gazetteer) Service based on a Web Feature Service (WFS)
 - N-GNDB National Geographic Names Database (N-GNDB NL -> Database of the Netherlands containing authoritative Dutch geographical namesdata)
 - N-GS National Gazetteer Service (N-GS NL -> Service of the Netherlands) based on a Web Feature Service (WFS)
 - A-GS Additional gazetteer services
 - A-GNDB Additional geographic name database
 - A-GNDoc Additional geographic names held in document
 - Exonym Database containing exonyms
 - DB

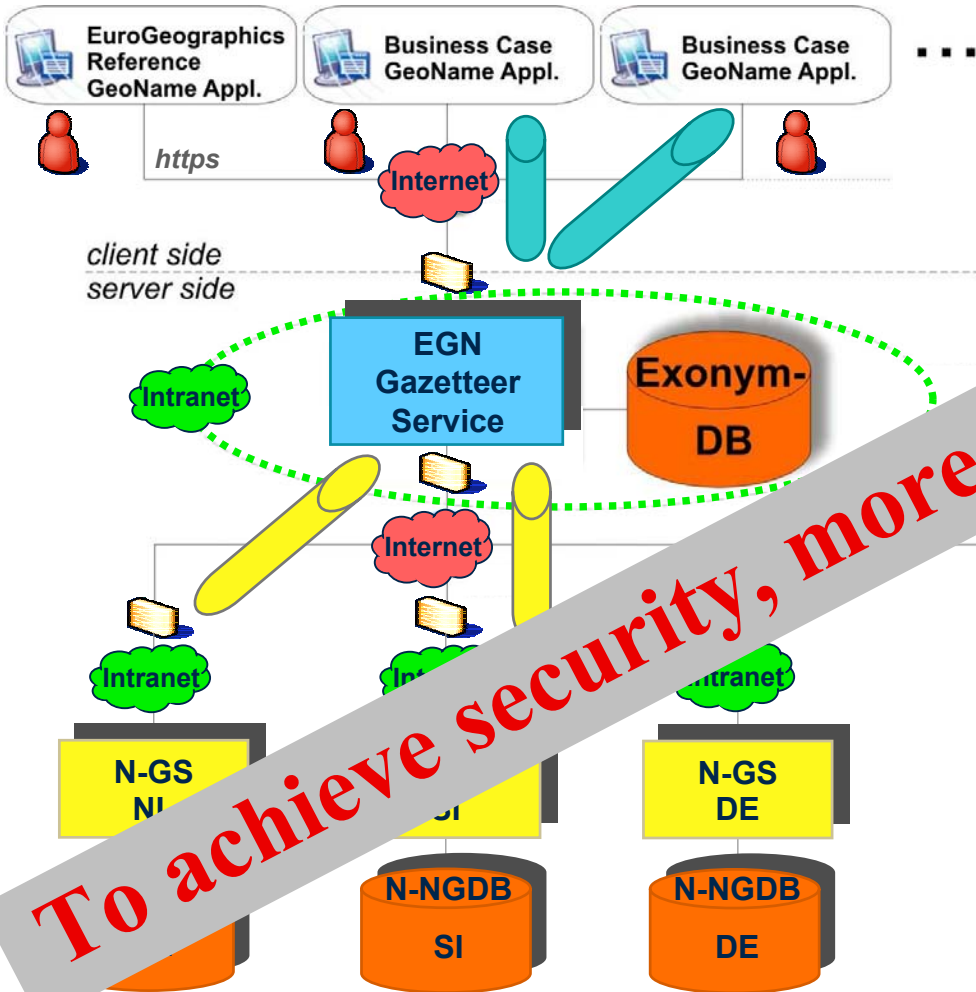
Will the smilies come by themselves?



Countermeasures
 If necessary
 at EGN central site
 and
 at EGN decentral sites
 and
 within applications

Security is a matter of design & permanent effort

- Legend:**
- EGN-GS EuroGeoNames - Web (Gazetteer) Service based on a Web Feature Service (WFS)
 - N-GNDB National Geographic Names Database (N-GNDB NL -> Database of the Netherlands containing authoritative Dutch geographical namesdata)
 - N-GS National Gazetteer Service (N-GS NL -> Service of the Netherlands) based on a Web Feature Service (WFS)
 - A-GS Additional gazetteer services
 - A-GNDB Additional geographic name database
 - A-GNDoc Additional geographic names held in document
 - Exonym-DB Database containing exonyms



To achieve security, more than that is necessary.

- Legend:**
- EGN-GS EuroGeoNames - Web (Gazetteer) Service based on a Web Feature Service (WFS)
 - N-GNDB National Geographic Names Database (N-GNDB NL -> Database of the Netherlands containing authoritative Dutch geographical namesdata)
 - N-GS National Gazetteer Service (N-GS NL -> Service of the Netherlands) based on a Web Feature Service (WFS)
 - A-GS Additional gazetteer services
 - A-GNDB Additional geographic name database
 - A-GNDoc Additional geographic names held in document
 - Exonym-DB Database containing exonyms



- **Define different classes of users**
- **Define, what users are allowed to do**
- **Specify desired level of security**
- **Determine, which softwares are involved**
- **Determine appropriate measures**
- **Refine planning**
- **Build / Test / Implement / Operate**



Kontakt:

Ronald Mordhorst
Geschäfts- und Koordinierungsstelle GDI-DE
Bundesamt für Kartographie und Geodäsie
Richard-Strauss-Allee 11
60598 Frankfurt
Tel: 069 / 6333-477 (oder -258)
E-Mail: ronald.mordhorst@bkg.bund.de

Information / Service:

www.gdi-de.org

www.imagi.de

www.bkg.bund.de

www.geoportal.bund.de / www.geodatensuche.de

www.geodatenzentrum.de