

# EuroGeoNames Workshop on Architecture and Security

BKG, Frankfurt a.M.  
3 Mai 2007

## Agenda

- TOP 1: Introduction
- TOP 2: EGN Architectural model in detail
- TOP 3a: Security Aspects I
- *Coffee Break (ca. 10.40)*
- TOP 3b: Security Aspects II
- TOP 4: Access Control
- *Lunch Break (ca. 12.30)*
- TOP 5: Conclusions TOP 2 – TOP 4
- TOP 6: Follow-up Actions
- TOP 7: Miscellaneous
- *End of Workshop (15.00)*

# EuroGeoNames Workshop on Architecture and Security

## **TOP 3: Security Aspects**

BKG, Frankfurt a.M.  
3 Mai 2007

## Table of Content

- Disambiguation:  
„security“ vs. „access control“
- EGN Security Concept  
Network and Firewall requirements
- EGN Access Control Concept  
Access control requirements

## Disambiguation: Why security?

- Protecting goods and services
- Protecting systems and infrastructures
- Put effort in protection instead of dealing with damages

## Disambiguation: types of security threats

- Hacking and Malware (Viruses, etc.)  
→ Firewalls
- Interfering with messages along network connections  
→ https
- Unauthorized acces to service, unauthorized retrieval of information  
→ user authentication, access control

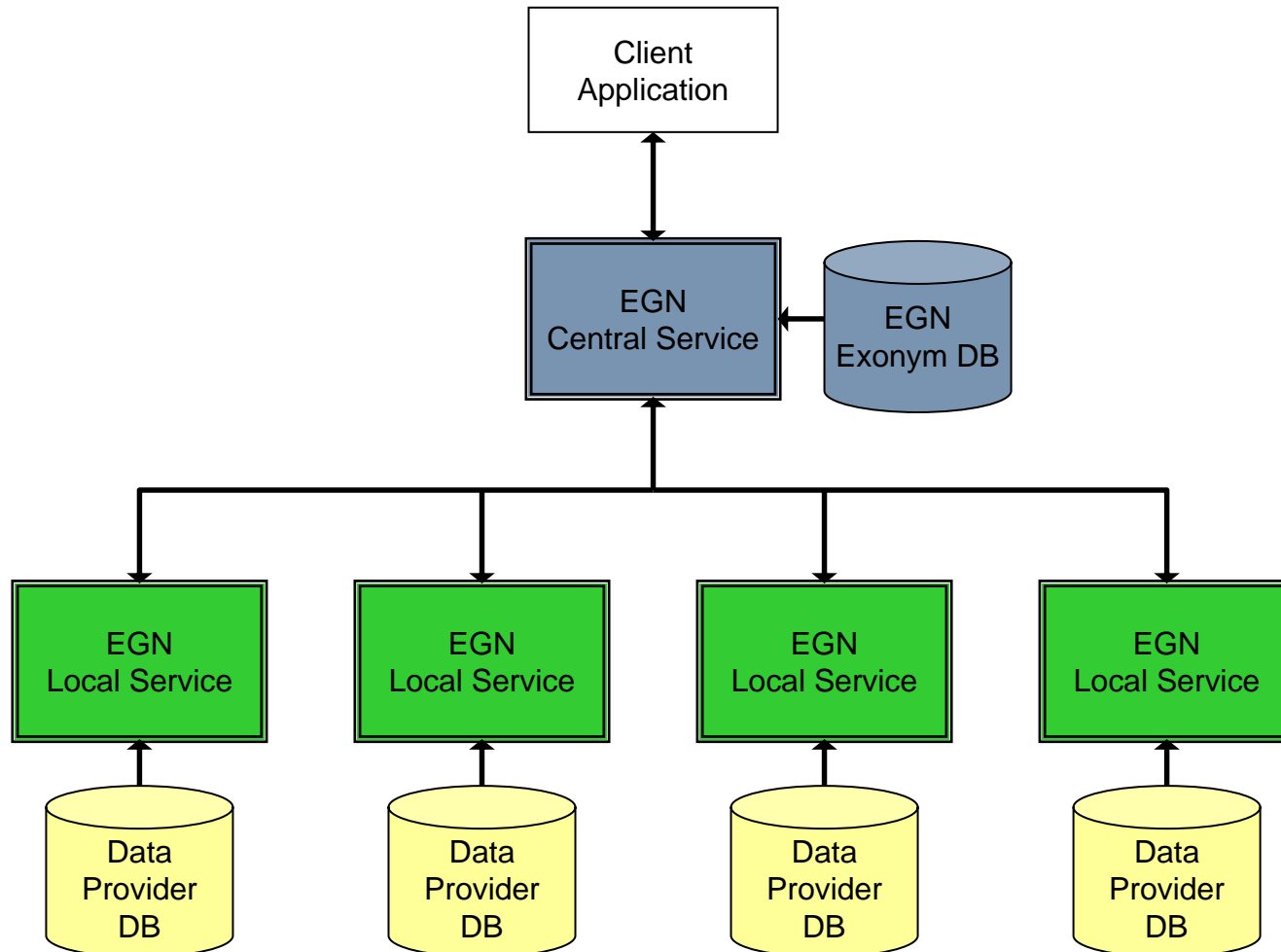
## Measures in Use at NMCAs

- Firewall (13/15)
  - Application level gateway (5/15)
  - Packet filter system (8/15)
  - DMZ (11/15)
- Message encryption
  - At transport level (https) (10/15)
  - At message content (XML encryption, XML signature)
- User authentication, access loggin

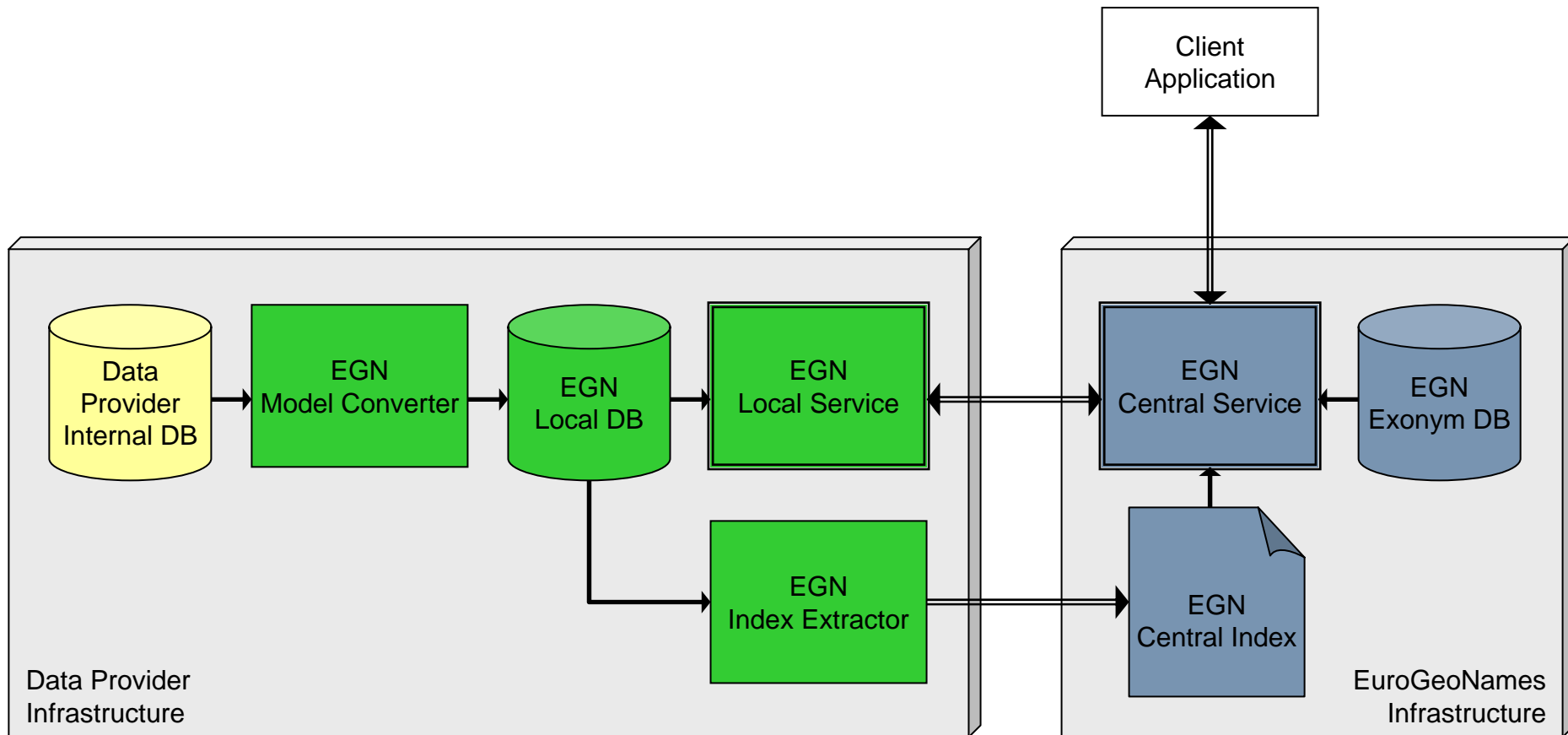
## Measures in Use at NMCAs

▪ <u>Firewall</u>	<u>13</u>
▪ <u>Applic.level gateway</u>	<u>5</u>
▪ <u>Packet filter systems</u>	<u>8</u>
▪ <u>dmz</u>	<u>11</u>
▪ <u>ssl</u>	<u>6</u>
▪ <u>https</u>	<u>10</u>
▪ <u>VPN</u>	<u>2</u>
▪ <u>Apache</u>	<u>9</u>
▪ <u>Tomcat</u>	<u>6</u>
▪ <u>J2EE</u>	<u>1</u>
▪ <u>Java</u>	<u>5</u>
▪ <u>ssh</u>	<u>7</u>
▪ <u>sftp</u>	<u>6</u>
▪ <u>high availability</u>	<u>8</u>

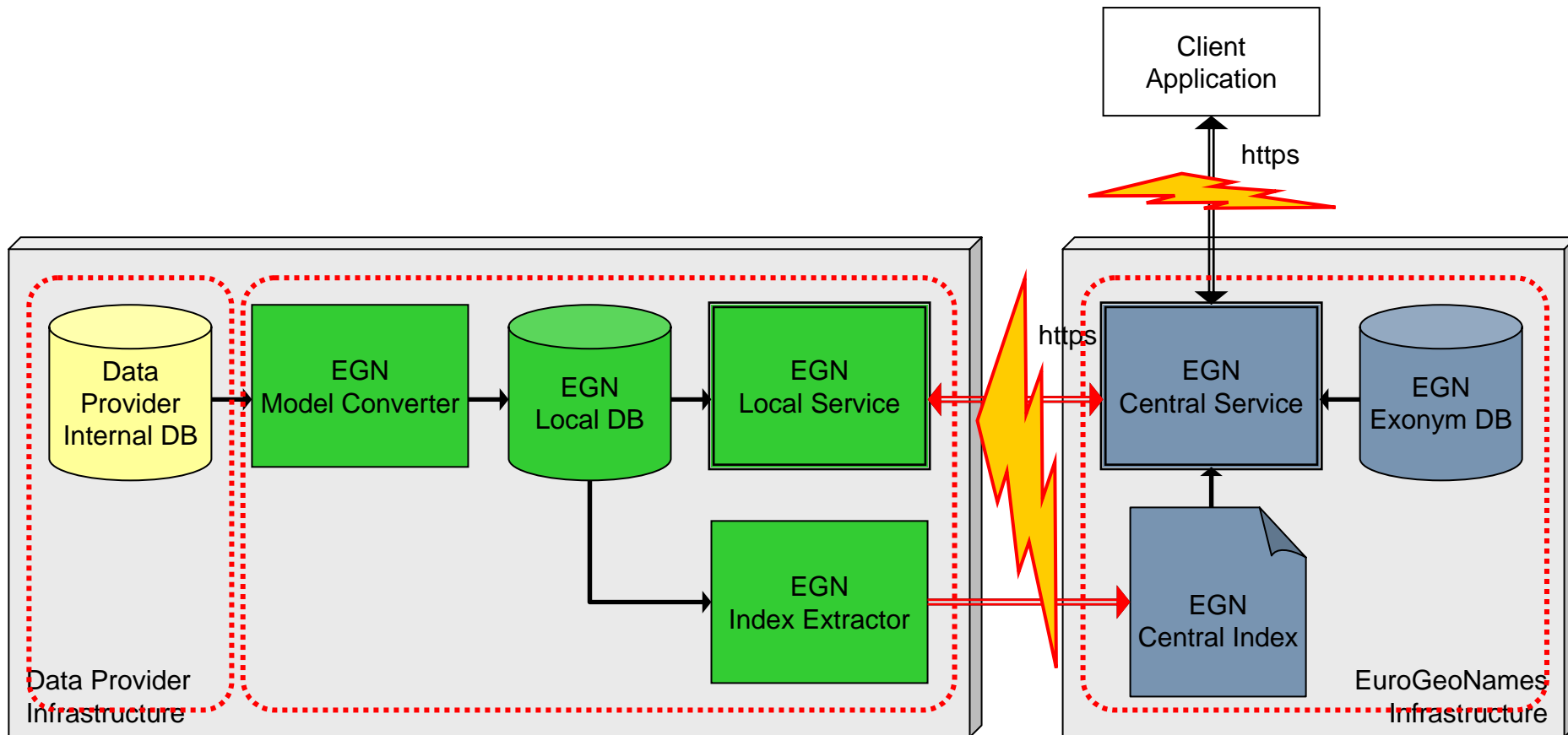
## Proposed Architecture – Overview



## Propose Architecture – Detail



# EGN Security Concept



## EGN Security Concept

- Using existing technology, successful strategies
- In agreement with all data and service providers
- Suggested security model as shown on previous slide:
  - Client application connects through https
  - Central service protected through Firewall
  - Secure connection between central and local services
  - Secure connection for EGN index extraction
  - Security to be ensured at central service

## EGN Access Control Concept

- Access control requirements  $\leftrightarrow$  business model
- Business model in development, final early 2008
- Basic building blocks must be taken into account now

## **EGN Access Control Concept – Example of EGN usage**

- Web portal for tourism
- User can search for a particular place
- Application shows a map of the place
- Application offers various information on the place
  
- EGN service is used for search functionality

## EGN Access Control Concept – Example of EGN usage

- Parties involved:
  - User of the Web portal
  - Provider of the Web portal

## EGN Access Control Concept – Example of EGN usage

- Parties involved:
  - User of the Web portal → end user
  - Provider of the Web portal → value adding reseller (VAR)
  - → EGN
  - → NMCA

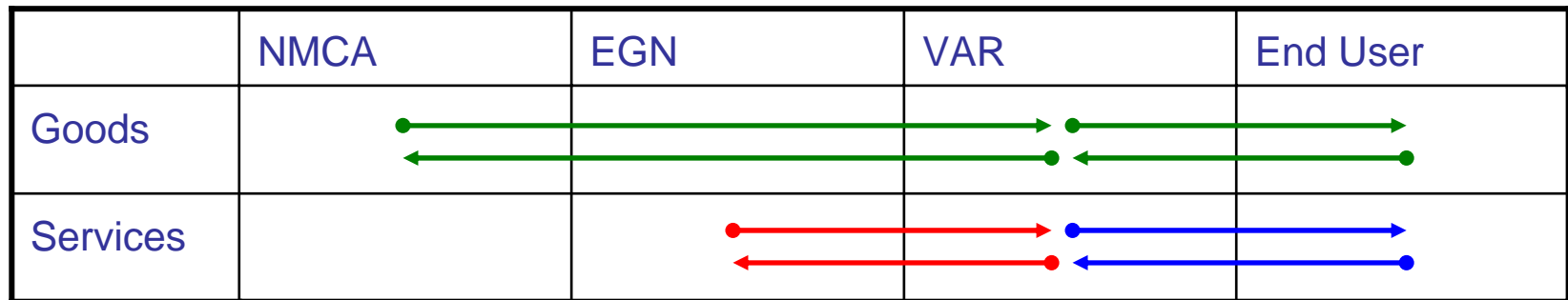
## EGN Access Control Concept – Revenue stream

- To be traded:
  - Goods = geonames data
  - Service = internet gazetteer service

## EGN Access Control Concept – Revenue stream

	NMCA	EGN	VAR	End User
NMCA	X	X	X	X
EGN	–	X	X	X
VAR	Uses goods for VAR-service	Uses EGN- service	X	X
End User	Uses goods via VAR-service	–	Uses VAR- service	X

## EGN Access Control Concept – Revenue stream



- A. EGN offers EGN service to VARs
- B. VARs offer VAR service to end users
- C. NMCAs offer geonames data to VARs & end users

## **EGN Access Control Concept – Access control requirements**

**A. EGN offers EGN service to VARs**

**A.1 which VAR integrates EGN service**

**A.2 number of request from each VAR**

**A.3 blocking requests of individual VARs**

## **EGN Access Control Concept – Access control requirements**

C. NMCAs offer geonames data to VARs & end users

C.1 amount of data requested from each VAR

C.2 amount of data requested by each end user

C.3 blocking requests of individual VARs

C.4 blocking requests of individual end users

C.5 restricting access for VARs and end users  
with respect to area, scale, feature type, etc.