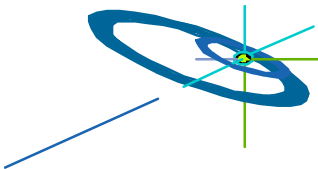# Protecting Sensible Biomedical Resources within the ViroLab Virtual Laboratory

Onur Kalyoncu,
Matthias Assel

High Performance Computing Center – HLRS
University Stuttgart
assel@hlrs.de

Outline

The ViroLab Project

Motivation

Virtual Laboratory Architecture

ViroLab Data Access and Integration

ViroLab Security Infrastructure

Data Resource Protection

Conclusions

H L R S

The ViroLab project

- Funded by EC within the 6th Framework Programme in the area of integrated biomedical information for better health
- 12 partners from 8 different European countries
- 3 years project (2006-2009)
- Experts from multiple disciplines (Physicians, virologists, epidemiologists, computer scientists)
- *Develop a "Virtual Laboratory" for medical experts that allows clinical studies, medical knowledge discovery, and decision support for HIV drug resistance*
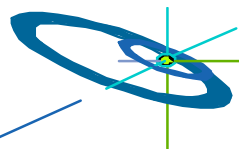
H L R S
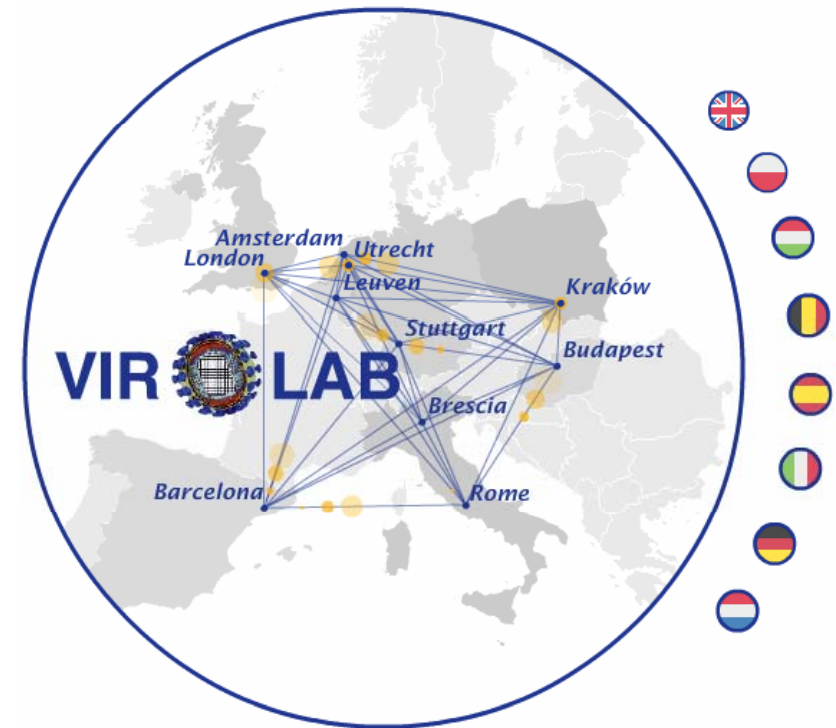
Motivation

What we had…

- Distributed teams/groups/researchers
- Distributed resources providing **heterogeneous** data/information and capabilities
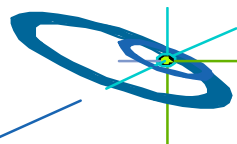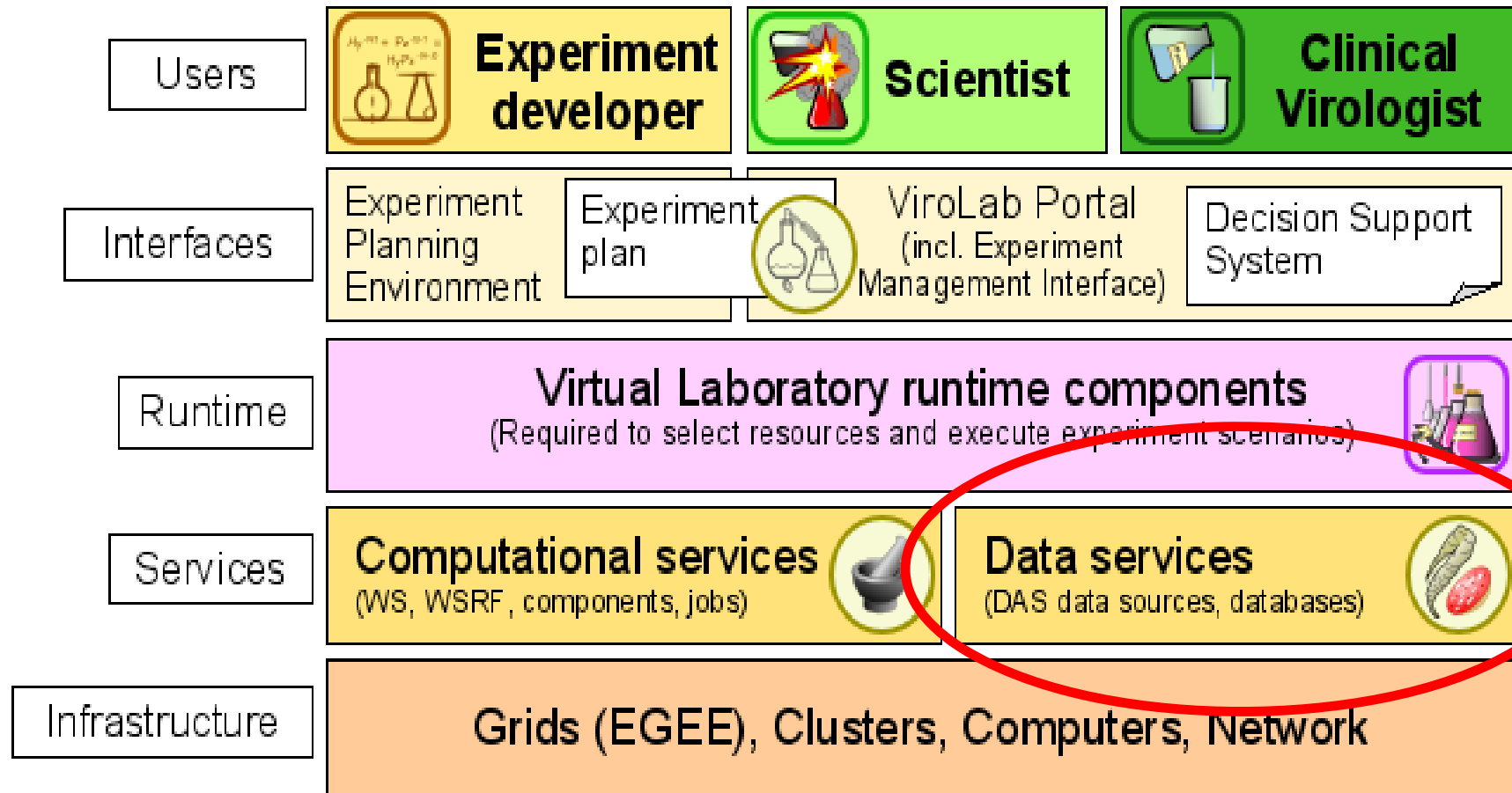- Distributed applications and workflows

But: we have a common goal…

What we need…

- Integration of users, data, workflows, applications, resources into one sophisticated environment
- Interdisciplinary collaboration and research
- Dynamic, on-demand and secure accessibility of resources and knowledge

H L R S

Virtual Laboratory Architecture

Users

| Experiment developer | Scientist | Clinical Virologist |

Interfaces

Experiment Planning Environment | Experiment plan | ViroLab Portal (incl. Experiment Management Interface) | Decision Support System

Runtime

Virtual Laboratory runtime components
(Required to select resources and execute experiment scenarios)

Services

Computational services
(WS, WSRF, components, jobs)

Data services
(DAS data sources, databases)

Infrastructure

Grids (EGEE), Clusters, Computers, Network

H L R I S

ViroLab Data Access and Integration

- Usage of established HIV database management system: RegaDB
- Data conversion, extraction, and anonymisation occur within each hospital
- Set of virtualisation services - Data Access Services (DAS) - that allows users to perform several activities on dispersed data resources
- Single/central entry point for all data requests representing the only "visible" and accessible system
- Secure data exchange and proper access control for certain resources
- Integrated with existing frameworks (Shibboleth, OGSA-DAI) to ease development and improve functionality
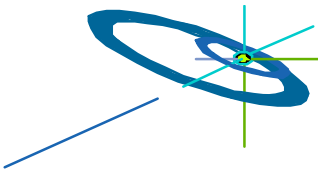
H L R S
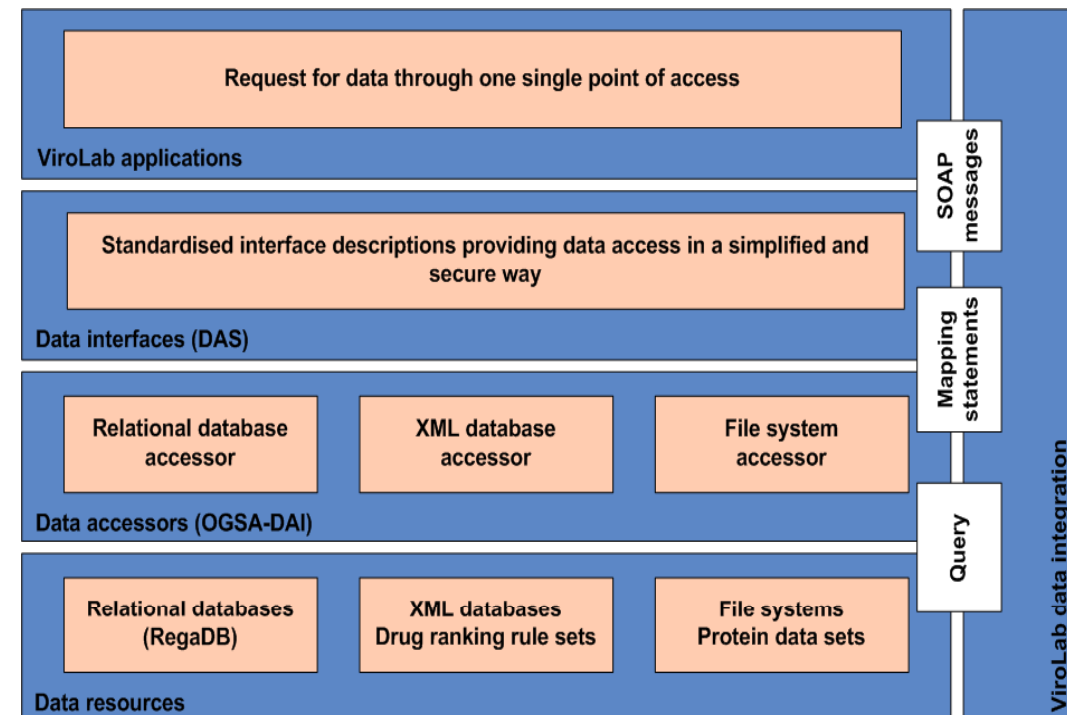
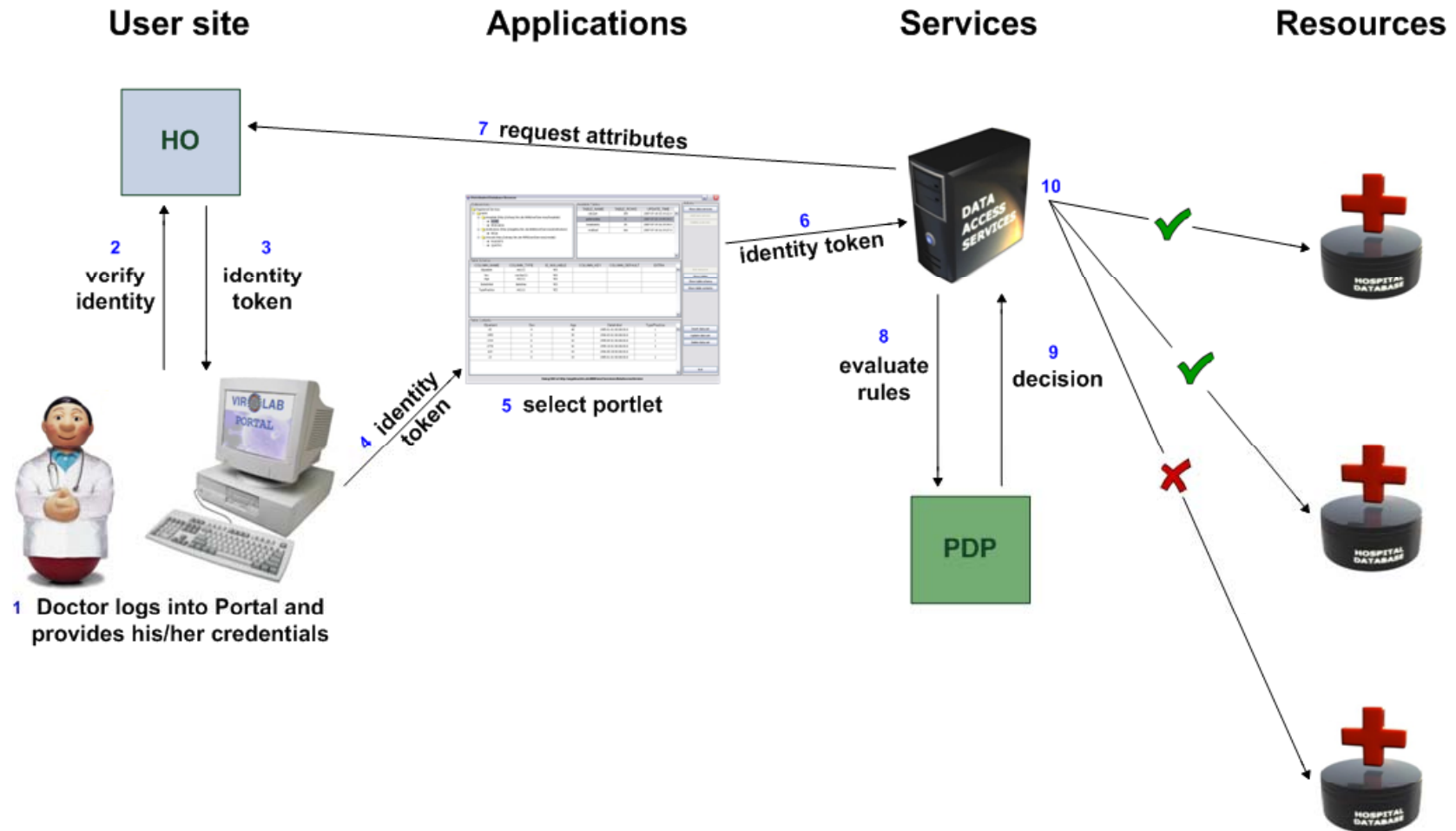# ViroLab Data Access and Integration
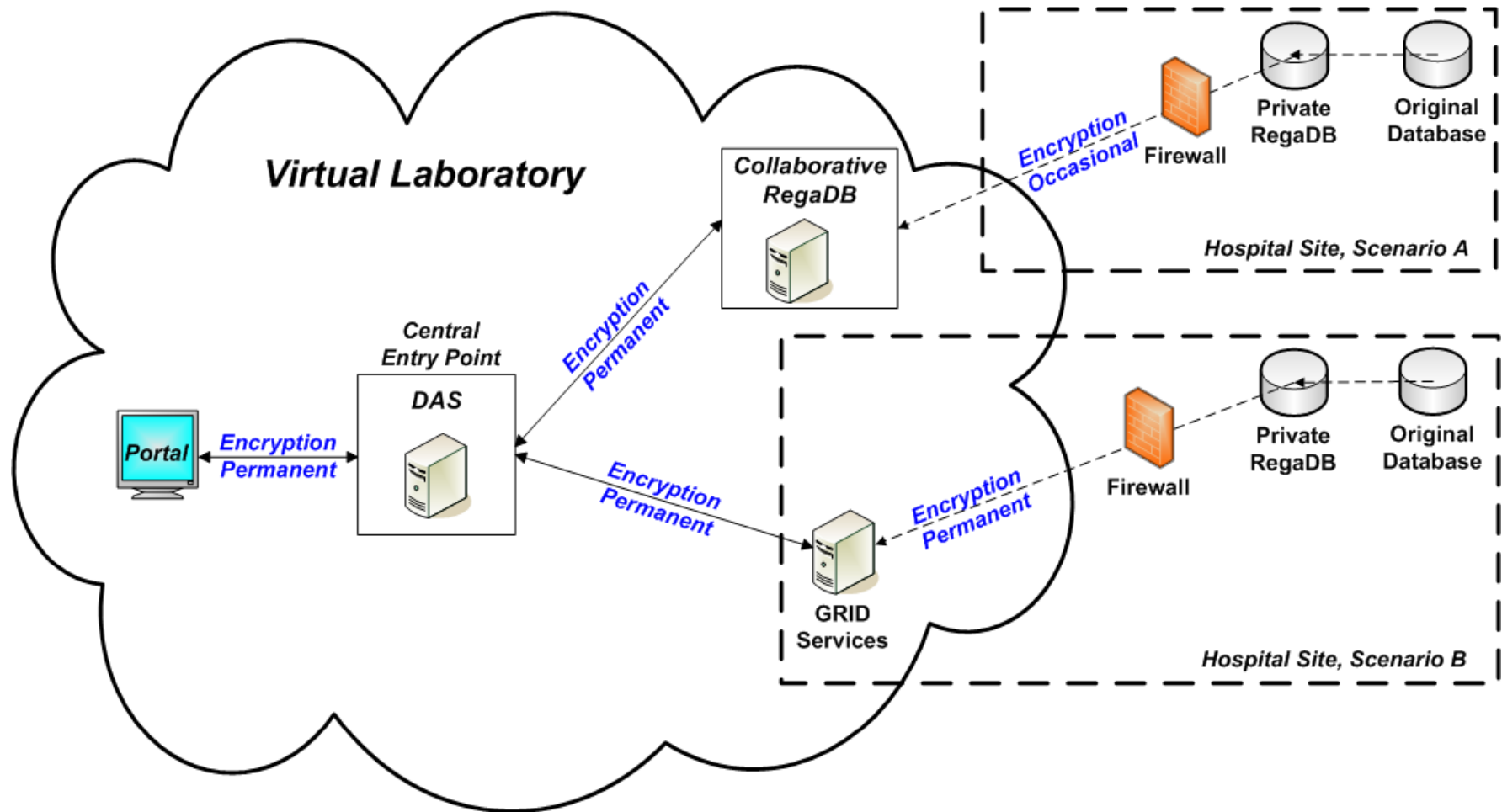
ViroLab Security Infrastructure

- Access to virtual laboratory functionalities is provided through the ViroLab Portal

- Two-step authentication and authorisation procedure

- Authentication based on Shibboleth

    - Decentralised and dynamic Virtual Organisation (VO)

    - Single-Sign On

    - Trustworthiness among the members of the Shib federation through metadata exchange (technically) and signed documents (legally)

    - Home organisations are responsible for users' identity management

    - communication through SAML

    - Possibilities for authentication: Username/Password or X509 certs

- Each resource can be secured by setting a proper policy

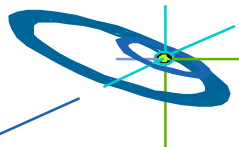- Attribute-based access control using XACML specifications at the corresponding service provider site

H L R S

ViroLab Security Architecture

User site   Applications   Services   Resources

HO

7 request attributes

DATA ACCESS SERVICES

10

2 verify identity

3 identity token

6 identity token

VIROLAB PORTAL

4 identity token

5 select portlet

8 evaluate rules

9 decision

PDP

1 Doctor logs into Portal and provides his/her credentials
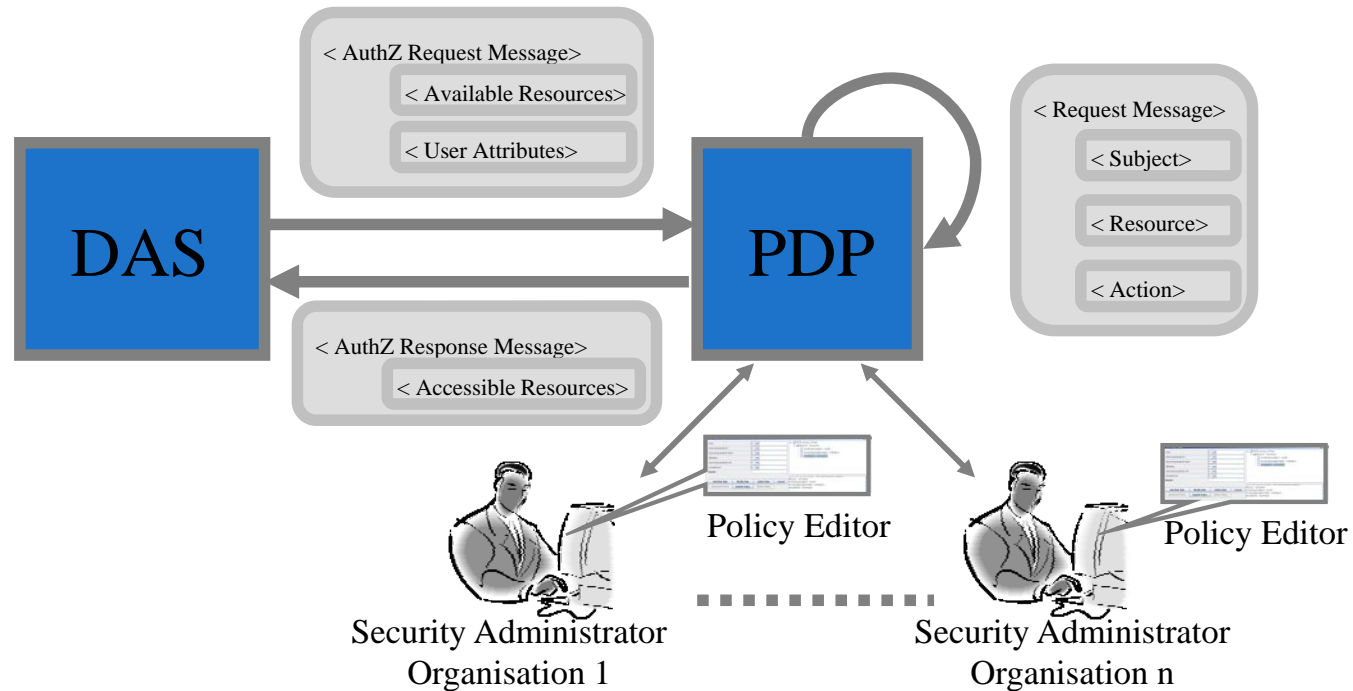
HOSPITAL DATABASE

H L R S

Data Resource Protection - Approach

- Final authorisation decision up to the data resource's owner
- Access control handled with the aid of so-called access control policies
- Policies implemented using established policy description language: XACML
- Attribute-based access control approach:

  The policies contain a set of rules specifying the required attributes (conditions) to become authorised for certain resources
- User-friendly graphical interface for dynamically adding, updating, removing policies
- Automatic notification in case of changing policies
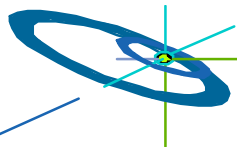
  -> transparent re-authorisation

H L R S

Data Resource Protection - Implementation

< AuthZ Request Message>

< Available Resources>

< User Attributes>

< Request Message>

< Subject>

< Resource>

< Action>

DAS

PDP

< AuthZ Response Message>

< Accessible Resources>

Policy Editor

Policy Editor

Security Administrator
Organisation 1

Security Administrator
Organisation n

H L R S

Conclusions

- Collaborative working environment to foster cross-organisational data exchange, communication, and research for infectious diseases

- Decentralised security architecture

- Usage of existing standards and technologies

- Creation of simple and/or highly detailed access control policies

- One standard access control policy language (XACML)

- Flexibility and dynamicity during the security management through VO approach and attribute-based access control

- Fast and easy generation, change, and upload of policies through nice and user-friendly graphical interface

- Future developments will further strengthen

  - Fine-grain access control

  - Encrypted policy management

  - Trust management
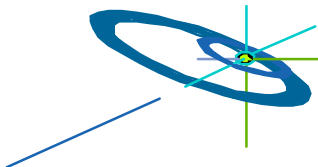
H L R S

Where to find more about ViroLab?

http://www.virolab.org

http://virolab.hlrs.de
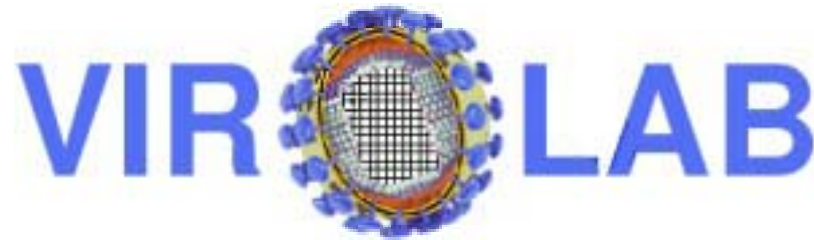
http://virolab.cyfronet.pl

Thank you for your attention.

Any questions?

H L R S