Access rights management and access control for BioCASE

Lutz Suhrbier[1]
Email: suhrbier@inf.fu-berlin.de

Ekaterina Langer[1], Markus Döring[2]
Anton Güntsch[2], Walter Berendsohn[2]

1) Freie Universität Berlin
Networked Information Systems,
Department of Mathematics and Computer Science
WWW: http://nbi.inf.fu-berlin.de

2) Freie Universität Berlin
Department of Biodiversity Informatics,
Botanic Garden and Botanical Museum

WWW: http://www.bgbm.org

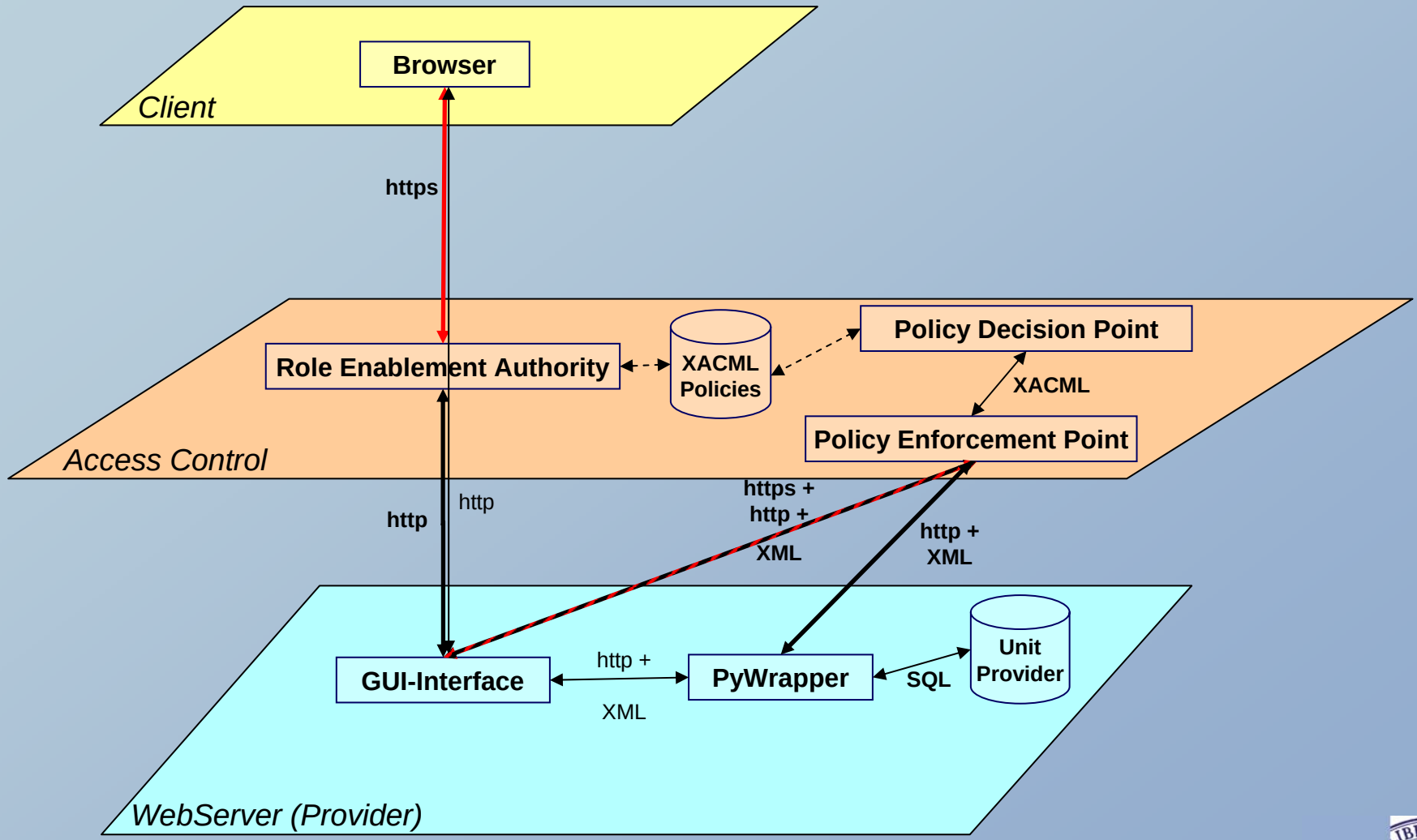
Overview

- Tasks and requirements
- Overview of the current solution
  - System architecture
  - XACML terminology
  - Authentication and access control
  - Access rights management
- Next Steps

Tasks and Requirements

- Development of authentication services for system access
  - restricted data access to specified end-users
  - (Re)use the same infrastructure as for general access (i.e. BioCASE/PyWrapper, ABCD)
- Specification of appropriate rights and their further management
- Base the services on XML security formats and protocols
  - eXtensible Access Control Markup Language (XACML) [OASIS]
    - XML based languages for the definition of access control policies and decision requests and responses
    - Role Based Access Control profile provided
  - XML Signature (XMLSig) and XML Encryption (XMLEnc) [W3C]
    - Specification for digitally siging and encryption of XML documents
    - Permits multi user, selective and fine granular operations on XML documents

Architecture of the current solution



Some XACML terminology

- Policy Enforcement Point (PEP)
  - entity protecting a resource (e.g. unit provider)
  - sends XACML-requests to a Policy Decision Point (PDP)
  - requests mainly base on attributes: subject, action & resource
- Policy Decision Point (PDP)
  - examines the request and retrieves applicable XACML-policies
  - grants access according to the evaluation of applicable policies
- Role Enablement Authority
  - Defined in the XACML Role based access control profile v2.0
  - Evaluates the roles assigned to a given user

Authentication and Acces Control

- Authentication
  - Public Key Infrastructure (PKI)
    - Currently issuing of X.509-certificates for providers and users
    - Integration of further hierarchical layers possible (e.g. national)
    - Build up on OpenSSL
  - Secure Socket Layer (SSL)
    - Uses X.509-certificates
    - Permits client and server authentication via https protocol
- Role Based Access Control realised through PEP
  - Role assignment processed by the Role Enablement Authority
  - Using these role assignments, the PEP acts as an Application Level Firewall on the BioCASE protocol according to policies specified by the provider and permits
    - Blocking of BioCASE requests (e.g. search requests on specific concepts)
    - Filtering of BioCASE responses (e.g. localisation info for protected species)

Access rights management

- Specification of XACML-policies
- A role manager provides policy management facilities to the system administrators of the providers
  - Role manager is a command line tool for the specification of

    Roles

    ```
    create biocase role client
    ```

    Role assignments

    ```
    add biocase roleassignments expert-assignments assignment
      client "CN=BioCASE Client, OU=NBI, O=FU-Berlin, L=Berlin,
      ST=Berlin, C=DE" client
    ```

    Role permissions

    ```
    add biocase rolepermissions client-request permission
    deny_scan_UnitDigitalImage
    http://www.tdwg.org/schemas/abcd/1.2/DataSets/DataSet/Uni
    ts/Unit/UnitDigitalImages scan-request deny
    ```

  - Syntax will be enhanced for BioCASE in the next steps

Next Steps

- Improvement of policy evalution functionality
- Data source authenticity and confidentiality
  - Introduce XML-Signature/Encryption to protect BioCASE protocol including its content (response)

Further information

- **Today: Computer demonstration 14:30 h**

- Website
  - http://nbi.inf.fu-berlin.de/research/SYNTHESYS

Using XML-Security