XML-Sicherheitsmechanismen für den Datentransfer in GBIF

Ekaterina Langer Lutz Suhrbier
Prof. Dr.-Ing. Robert Tolksdorf

Freie Universität Berlin
Institut für Informatik
Netzbasierte Informationssysteme
mailto:atanasso@inf.fu-berlin.de
http://nbi.inf.fu-berlin.de/research/GBIF-D/

 © Ekaterina Langer, FU-Berlin

Überblick

- Grundlagen der IT-Sicherheit
- Ziele und Besonderheiten von GBIF
- Aktueller Zustand der BioCASE-Architektur
- XML-basierte Sicherheitsstandards
  - Kurze Vorstellung
  - Vorteile
  - Beispiele
- Systemarchitektur nach der Integration von Sicherheitsdiensten
- Ausblick
  - Absicherung der Kommunikation
  - Erweiterung um Rechtemanagement und Zugriffskontrolle

© Ekaterina Langer, FU-Berlin

IT-Sicherheit

- IT-Sicherheit = Safety + Security
- Security: Schutz vor Schäden, die durch beabsichtigte und mit Intelligenz betriebene Angriffe auf IT-Systeme entstehen
- Potenzielle Gefahren für die Kommunikation im Internet
  - Abhören geheimer Informationen
  - Manipulieren von Daten- und Nachrichten
  - Fälschen der Absenderdaten
  - Abstreiten von abgeschickten Nachrichten

© Ekaterina Langer, FU-Berlin

Kernanforderungen und Techniken der IT-Sicherheit

- Ein sicheres System soll
  - Authentifizierung von Anwendern
  - Nur autorisierter Zugriff auf Ressourcen
  - Vertraulichkeit von Daten und Nachrichten
  - Integrität von Daten/Nachrichten
  - Authentizität von Datenquellen
  - Nicht-Abstreitbarkeit von Nachrichten

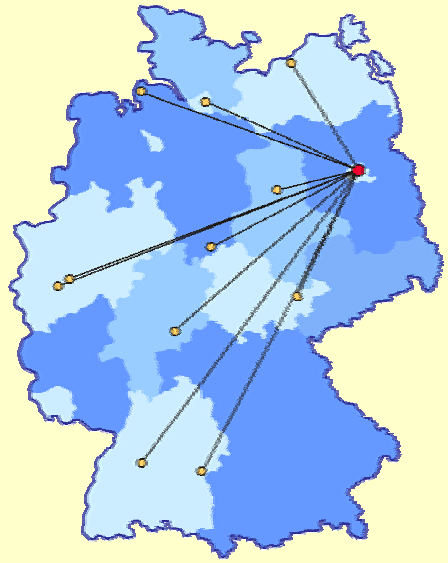
  gewährleisten.

- Mechanismen
  - Zugangskontrolle
  - Rechteverwaltung, Zugriffskontrolle
  - Verschlüsselung
  - Finger Print

  +
  - Digitale Signatur

GBIF-D

- Ziele der GBIF-Initiative:
  - weltweite Vernetzung und Bereitstellung der vorhandenen Daten zur biologischen Vielfalt über das Internet
  - Steigerung der Effizienz der Biodiversitätsforschung
  - Unterstützung der Prioritätensetzung bei Forschungs- und Naturschutzvorhaben

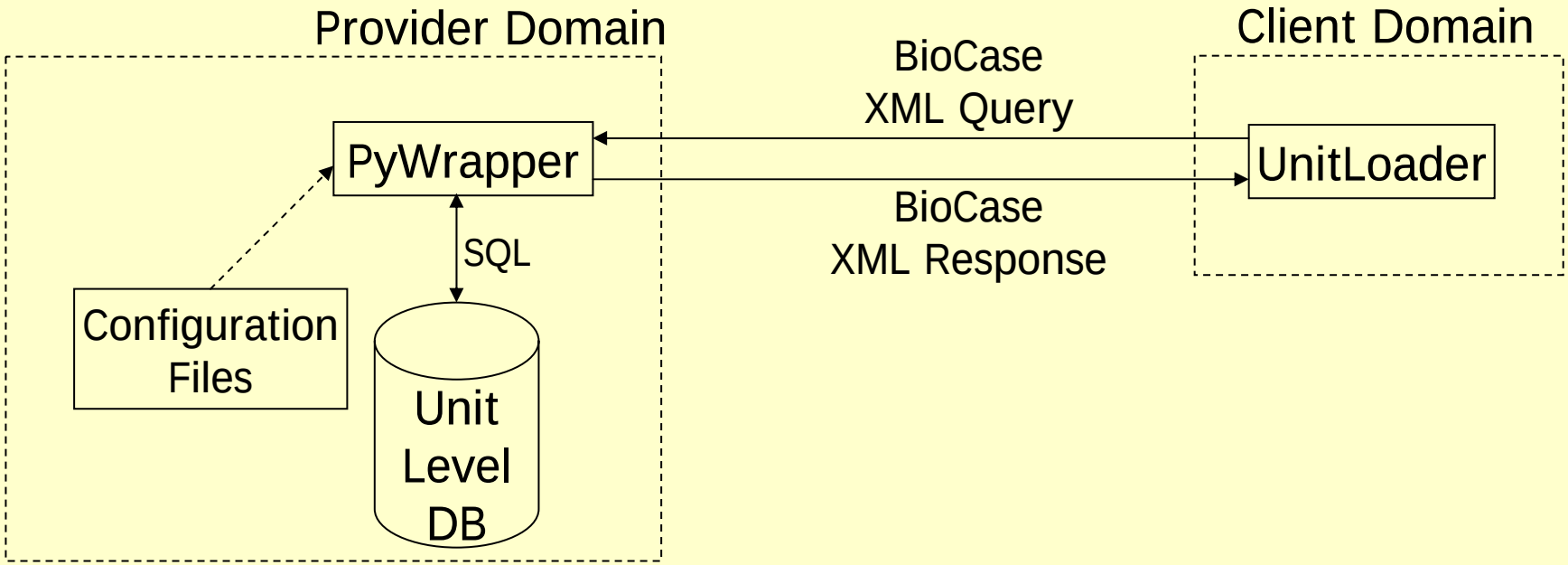


- GBIF-Besonderheiten
  - Heterogenität von Plattformen, DBMS, IT-Systemen und –Kenntnissen bei den Datenanbietern
  - Bereitstellung der Daten auf freiwilliger Basis
  - Hauptsächlich öffentliche Daten
  - Knappe finanzielle Ressourcen

© Ekaterina Langer, FU-Berlin

Aktueller technischer Stand

- Abstraktion von der Vielfalt eingesetzter DBMS auf Seiten der Datenanbieter durch Kapselung mit der Wrapper-Komponente
- XML-basiertes Anfrage/Antwort-Protokoll
- XML-basiertes Datenaustausch-Schema



© Ekaterina Langer, FU-Berlin

Erweiterung durch Sicherheitsdienste

- Wozu überhaupt Sicherheitsdienste?
  - Bereitstellung auch sensibler Biodiversitätsdaten, Zugriff nur für Berechtigte
  - Universeller Einsatz des Systems
    - Modifizierende Fernzugriffe auf die Daten durch berechtigte Experten
    - Berichte an Behörden

- Authentifizierung von Benutzern und Zugriffskontrolle auf die Ressourcen anhand von rollenbasierten Politiken
- Sichern der Kommunikation durch
  - Vertraulichkeit und Integrität der übertragenen Daten
  - Authentizität der Datenquellen
  - Nicht-Abstreitbarkeit von Nachrichten
- Kennzeichnung/Durchsetzung von Eigentumsrechten (IPR) durch digitales Rechtemanagement

© Ekaterina Langer, FU-Berlin

XML-basierte Sicherheitsstandards

- **XML Encryption** [W3C Recommendation since 10.12.2002]
  - Vertraulichkeit von XML-Daten durch Verschlüsselung
  - Verschlüsselung ganzer XML-Dokumente oder fein abgestuft z.B. von Elementgruppen, einzelnen Elementen oder Elementinhalten (selektive Verschlüsselung)
  - Unterschiedliche Schlüssel für verschiedene Teile eines Dokuments, so dass geheime Abschnitte des Dokuments nur für bestimmte Empfänger lesbar (End-to-End-Security)

- **XML Signature** [W3C Recommendation since 12.2.2002]
  - Integrität und Verbindlichkeit von XML-Daten durch Anwendung digitaler Signaturen
  - Signieren/Verifizieren ganzer XML-Dokumente oder von Dokumententeilen, aber auch von beliebigem nicht-XML Inhalt
  - Digitale Signaturen werden persistenter Bestandteil des Dokuments und somit dauerhaft verifizierbar
  - Alle per URI referenzierbaren Datenobjekte flexibel mit verschiedenen Optionen (enveloped, enveloping oder detached) signierbar

© Ekaterina Langer, FU-Berlin

Beispiel Digital Signatur

```
<Signature Id="SignatureExample“
   xmlns="http://www.w3.org/2000/09/xmldsig#">
   <SignedInfo>
    <CanonicalizationMethod
       Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <Reference  URI=“#envelopedData">
        <Transforms>
            <Transform
                Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </Transforms>
        <DigestMethod
                Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
    </Reference>
</SignedInfo>
<SignatureValue>MC0CFFrVLtRlk=reIZS5...</SignatureValue>
```


© Ekaterina Langer, FU-Berlin

Beispiel Encryption

```
<KeyInfo><KeyValue><DSAKeyValue>
    <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
</DSAKeyValue></KeyValue></KeyInfo>
<Object Id="envelopedData">
  <OrchidRecord>
    <HigherTaxon TaxonRank="Family">Orchidaceae</HigherTaxon>
    <ScientificName>Orchis x feinbruniae</ScientificName>
    <AuthorString>Baumann & Dafni 1979</AuthorString>
    <GatheringSite>
      <ContinentOrOcean>Asien</ContinentOrOcean>
      <Country>IL</Country>
      <NamedAreaName>Galiläa</NamedAreaName>
      <Location>
        <EncryptedData Id="Loc"  Type="http://www.w3.org/2001/04/xmlenc#Content"
                       xmlns="http://www.w3.org/2001/04/xmlenc#">
          <EncryptionMethod  Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
          <CipherData><CipherValue>8QoRT8+=jhdsTdu35WQ...</CipherValue></CipherData>
        </EncryptedData>
      </Location>
    </GatheringSite>
  </OrchidRecord>
</Object>
</Signature>
```


© Ekaterina Langer, FU Berlin

Weitere XML Sicherheitsstandards

- **XML Key Management Specification (XKMS)**

  [W3C Candidate Recommendation since 5.4.2004]

  - Spezifiziert die Verwaltung von öffentlichen Schlüsseln und Vertrauenszusicherungen
  - zwei XML-basierte Request/Response-Protokolle:
    - XKRSS: Generierung und Registrierung öffentlicher und privater Schlüssel
    - XKISS: Auffinden und Verifikation öffentlicher Schlüssel bzw. Zertifikate.

- **eXtensible rights Markup Language (XrML)**

  [ContentGuard specification, contributed to OASIS, OeBF and MPEG-21 as foundation for digital rights language]

  - XML-basierte Spezifikationsgrammatik zur Beschreibung von Rechten und Bedingungen, die mit der Nutzung digitaler Ressourcen (Software, Services, Hardware) verbunden sind.

© Ekaterina Langer, FU-Berlin

SAML

- **Security Assertion Markup Language (SAML)**

  [OASIS Standard since September 2003 (SAML V 1.1)]

  - XML-basiertes Request/Response-Protokoll für den Austausch von Autorisierungs- und Authentifizierungsinformationen
  - Definiert ein XML-Vokabular zur Formulierung von:
    - Authentifizierungsaussagen: Zusicherungen über Subjekte (Menschen, Rechner), die eine Identität in einer Sicherheitsdomäne nachgewiesen haben
    - Autorisierungsaussagen: Aussagen über das Recht eines Subjekts bestimmte Aktionen auf eine Ressource auszuführen
  - Eindeutige Identifikatoren (URNs) für Authentifizierungsmechanismen und Autorisierungsaktionen

© Ekaterina Langer, FU-Berlin

Beispiel SAML

- Autorisierungszusicherung:

```
<Assertion> [...]
  <AuthorizationDecisionStatement
    Resource= "http://www.herbarium.com/orchidee" Decision="Permit">
    <Subject><NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.0:assertion#emailAddress">
        john@botanik_inst.de
      </NameIdentifier>
    </Subject>
    <Action Namespace="urn:oasis:names:tc:SAML:1.0:action:rwedc">
      Read
    </Action>
    <Evidence>
      <AssertionIDReference>LOG-Abc12Z</AssertionIDReference>
    </Evidence>
  </AuthorizationDecisionStatement>
  <ds:Signature>XML Signature for assertion</ds:Signature>
</Assertion>
```

Nach Frederick Hirsch: Getting Started with XML Security,
http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html

© Ekaterina Langer, FU-Berlin

XACML

eXtensible Access Control Markup Language (XACML) [OASIS standard since February 2003]

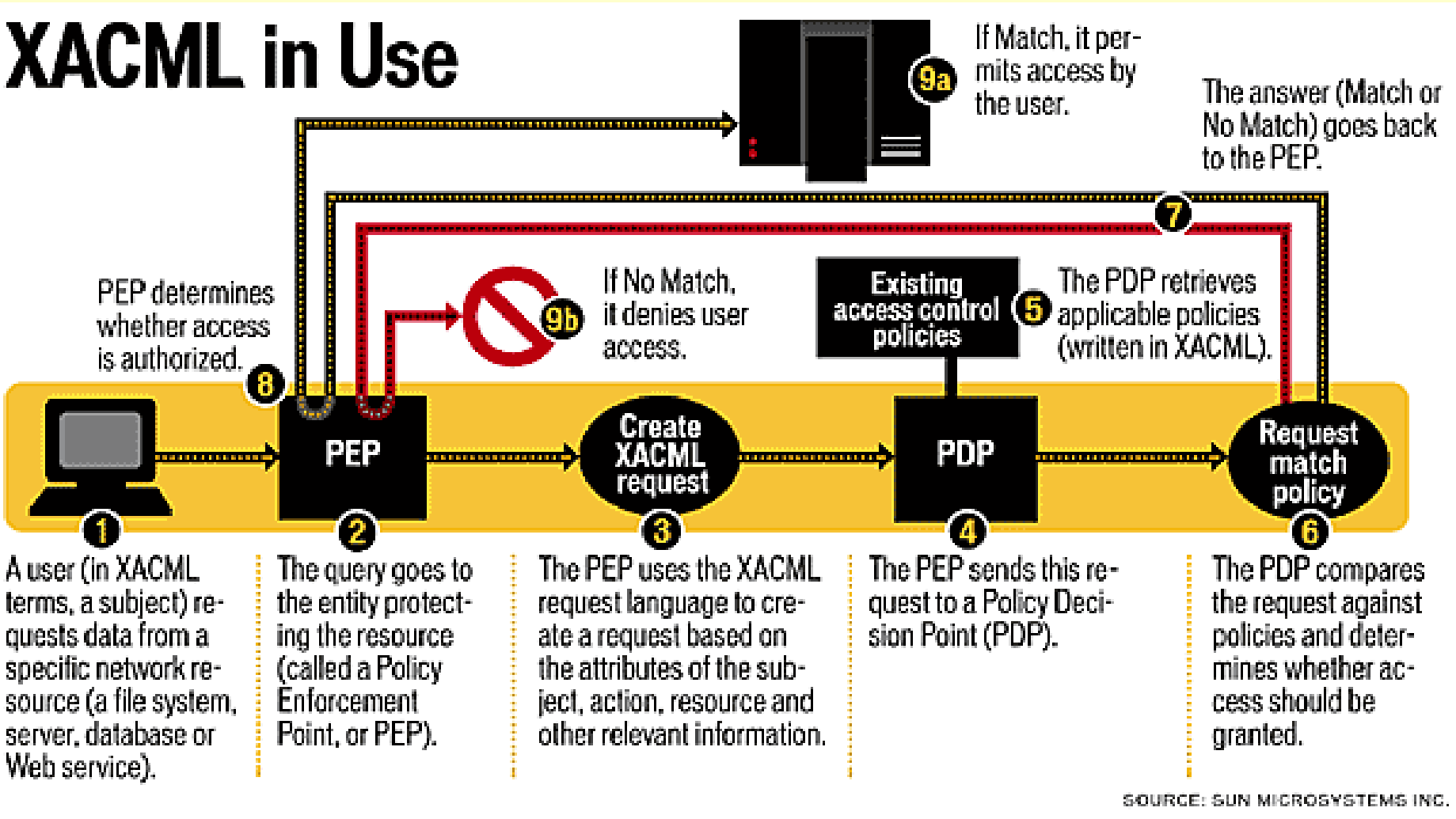
- Definiert ein Basisschema inklusive Namensraum, um in XML Autorisierungspolitiken (Zugriffskontrolle) gegenüber ebenfalls in XML definierten Objekten zu beschreiben

- XML-Vokabular um Zugriffsregeln auf Ressourcen zu definieren

- Request/Response-Protokoll um Zugriffskontrollentscheidungen zu ermitteln
  - Request = Anfrage, ob eine bestimmte Aktion erlaubt ist
  - Reponse = Ergebnis auf Basis definierter Sicherheitspolitiken
    - Permit => Aktion erlaubt
    - Deny => Aktion verboten
    - Indeterminate => Ein Fehler lässt keine Entscheidung zu
    - Not Applicable => Anfrage kann nicht beantwortet werden

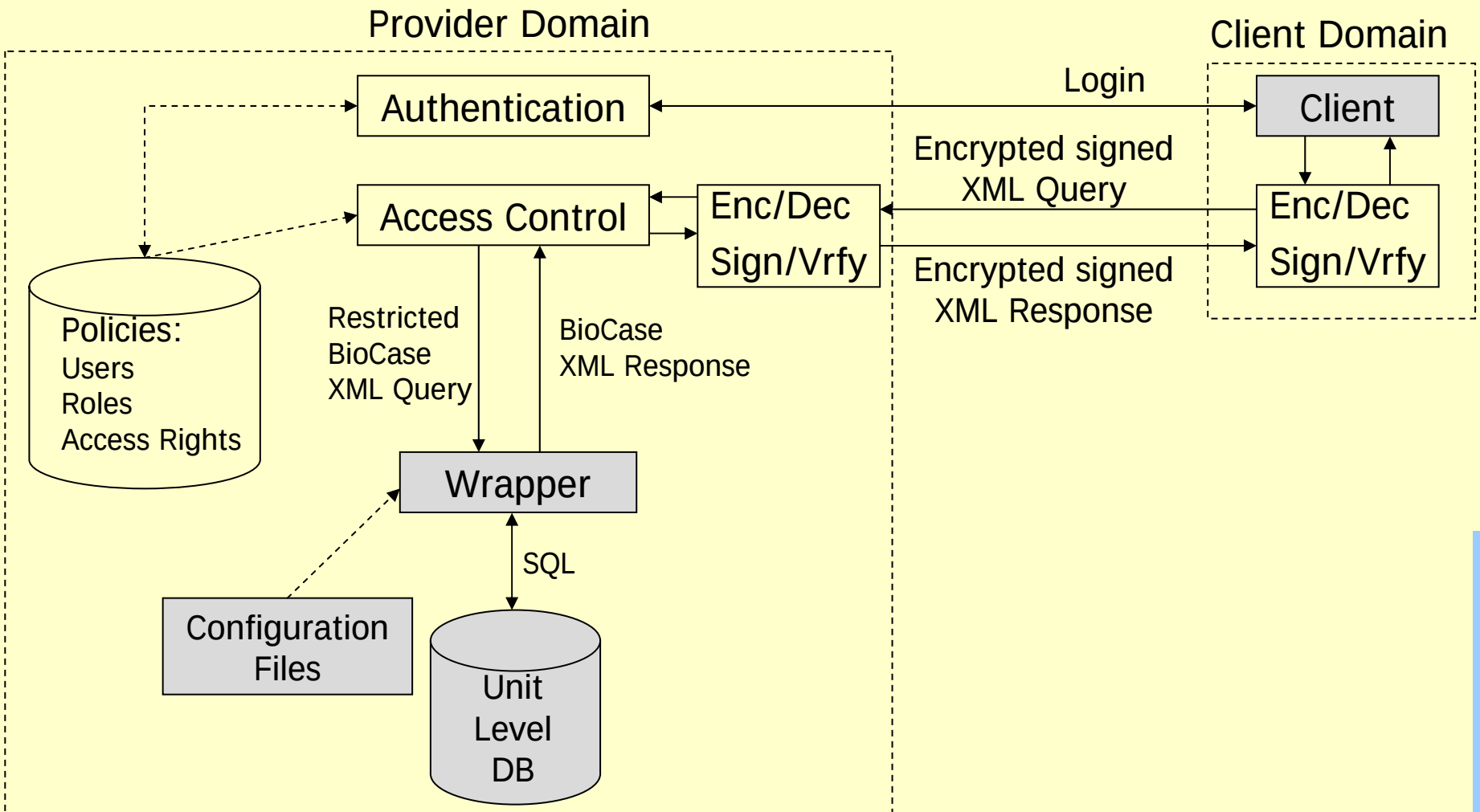
© Ekaterina Langer, FU-Berlin

XACML in Use



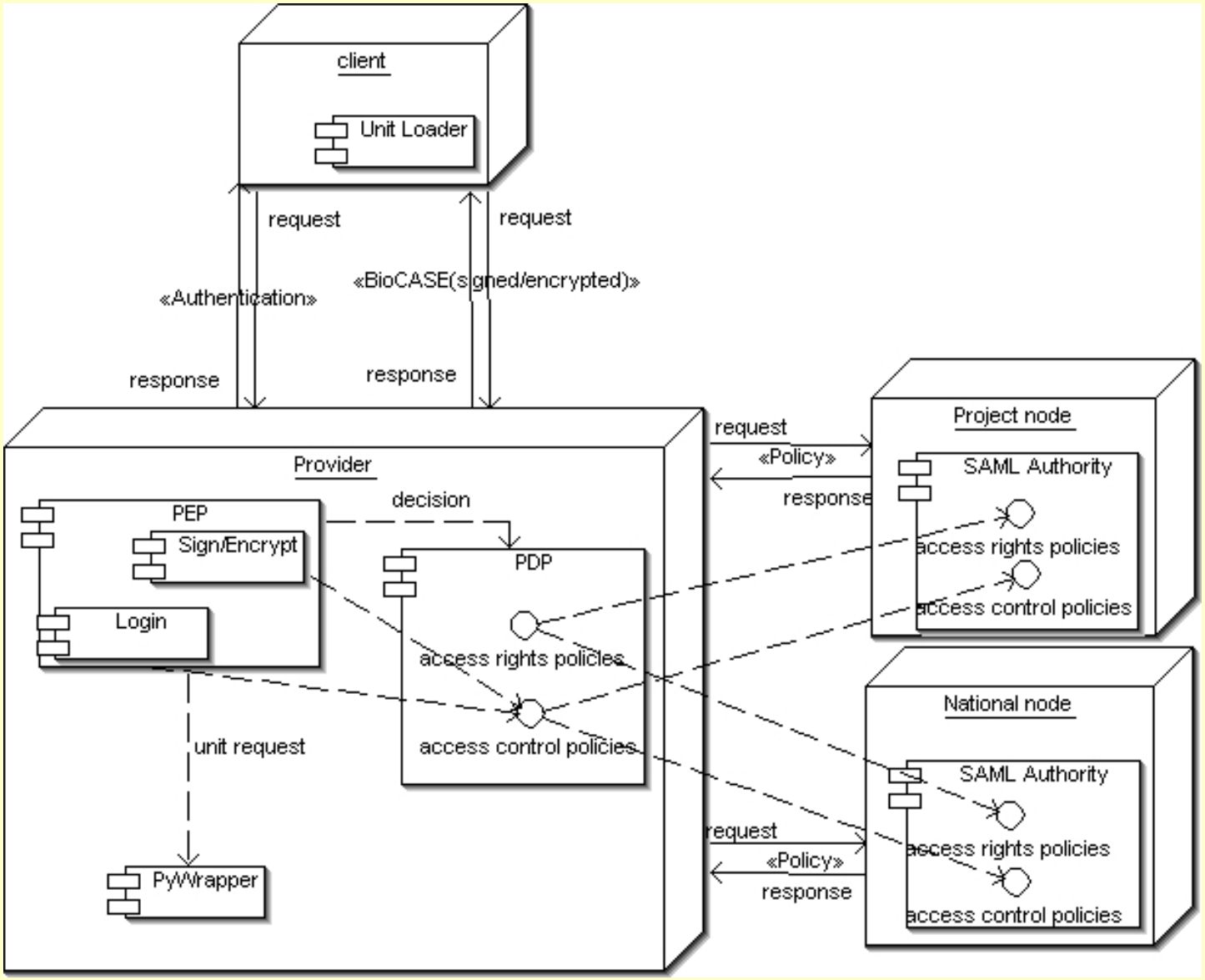
 © Ekaterina Langer, FU-Berlin

Sicherheitsdienste GBIF - Grobe Architektur



© Ekaterina Langer, FU-Berlin

Konzept zur Integration von Sicherheitsdiensten, Zugriffskontrolle und Rechtemanagement



Weitere Informationen

- http://nbi.inf.fu-berlin.de/research/GBIF-D/

- Eingereichte wissenschaftliche Publikationen zu diesem Thema:
  - Eingereicht für die Tagung Sicherheit 2005 der Gesellschaft für Informatik

    R. Tolksdorf, L. Suhrbier, E. Langer: Integration of XML security services in a biodiversity information system

  - Eingereicht für DACH Security 2005 gemeinsame Arbeitskonferenz von Deutschland, Österreich und der Schweiz

    R. Tolksdorf, L. Suhrbier, E. Langer: Designing XML Security Services for Biodiversity Networks

© Ekaterina Langer, FU-Berlin