XML-Sicherheitsdienste für GBIF-D

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

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

Überblick

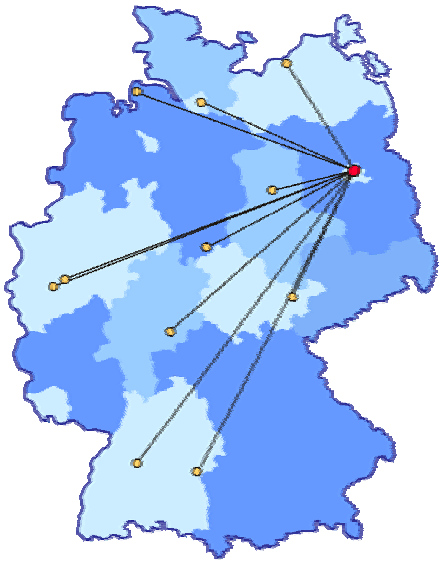
- Aufgaben im Projekt
- Besonderheiten von GBIF und der BioCASE-Architektur
- Analyse der Benutzeranforderungen
- Konzept zur Absicherung der Kommunikation in GBIF-D
- XML-basierte Sicherheitsstandards
- Transfer von Informatikkompetenz in GBIF
- Ausblick
  - Erweiterung um Rechtemanagement und Zugriffskontrolle
  - Publikationen

Arbeitspakete im Projekt

- AP1: Absicherung der Daten- und Nachfragekommunikation
  - Vertraulichkeit
  - Integrität
  - Nicht-Abstreitbarkeit

  } von Daten und Nachfragen
  - Authentizität der Datenquellen
- AP2: Rechteverwaltung und Zugriffskontrolle
  - Authentifizierung von Anwendern
  - Differenzierte Zugriffspolitiken für Datenanbieter und -nachfrager
  - Nur autorisierter Zugriff auf Ressourcen
- AP3: Transfer von Informatik-Kompetenz in GBIF

Kennzeichnend für GBIF und BioCASE



- Heterogenität von
  - Soft-/Hardware-Plattformen
  - Datenbankmanagementsystemen
- unterschiedlicher Stand der Technik
- Variierender Stand der IT-Kenntnisse bei den Datenanbietern
- Bereitstellung der Daten auf freiwilliger Basis
- Knappe finanzielle Ressourcen
- Überwiegend öffentlich zugängliche Daten
- XML-basiertes Anfrage/Antwort-Protokoll (BioCASE)
- XML-basiertes Datenaustausch-Schema (ABCD)

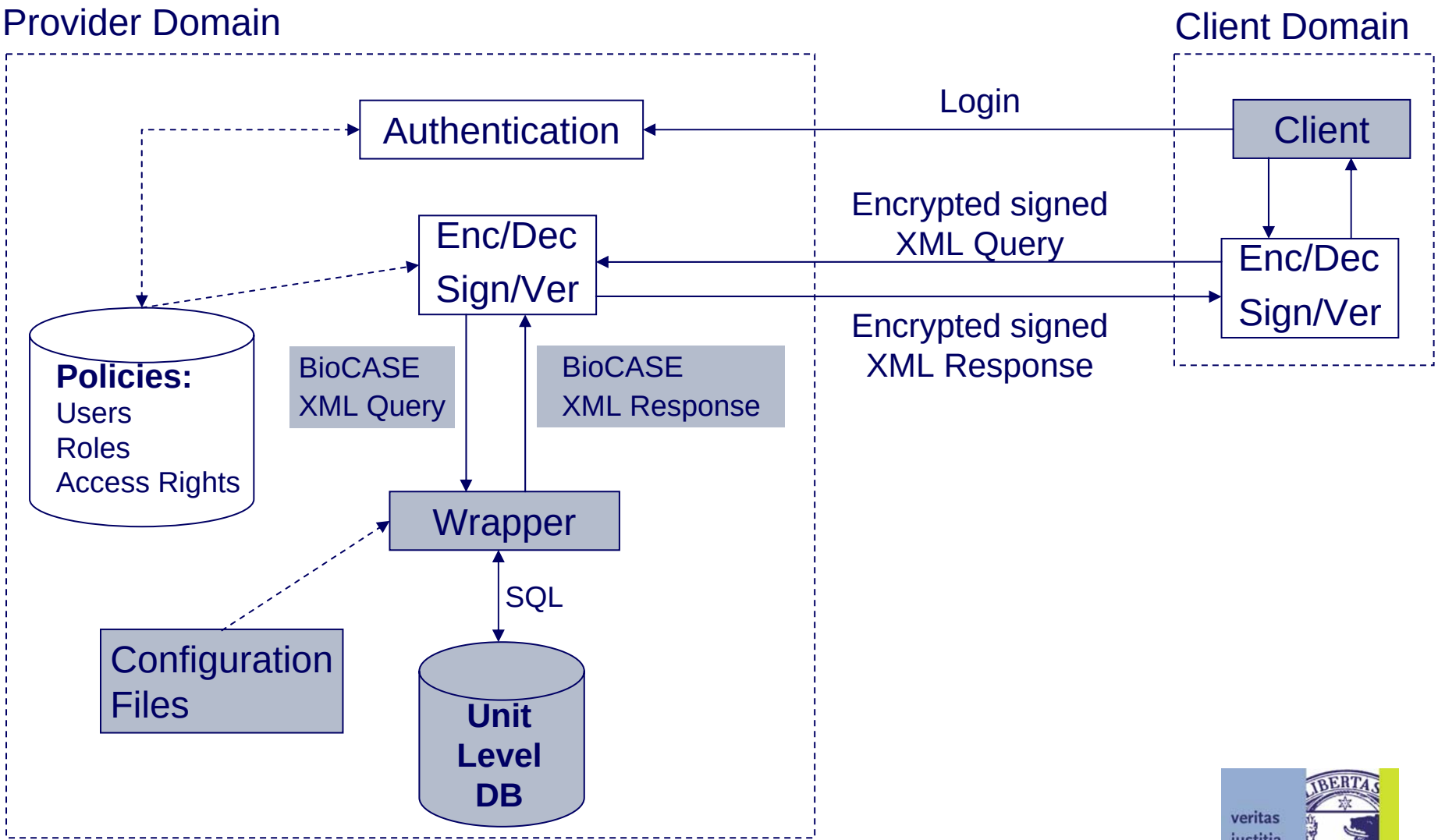
Erweiterung durch Sicherheitsdienste

- Ausschöpfen des vollen Potentials des GBIF-Informationssystems
  - Anbindung der kompletten Biodiversitätsdaten, limitierter Zugriff auf sensitive Informationen für Berechtigte
  - Modifizierende Fernzugriffe und Annotationen durch berechtigte Experten
  - Übermittlung vertraulicher 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

Analyse der Benutzeranforderungen

- Persönliche Interviews mit Entwicklern der BioCASE-Software und des ABCD-Schemas am BGBM
- Elektronische Befragung von Datenanbietern
  - Erstellung des Fragenkatalogs und Versenden per E-Mail
  - Breite Basis für die Anforderungsanalyse
    - GBIF, SYNTHESYS, BioCASE Projektpartner
    - 93 Kontaktpersonen aus 61 Organisationen
  - Zeit- und Finanzressourcen sparend
  - Grundlage für einen fortzusetzenden Dialog mit den Anwendern
- Auswertung der Ergebnisse
  - 47% Rückmeldung
  - Analyse

Konzept Sicherheitsdienste für GBIF-D



XML-Sicherheitsstandards I

- **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 digitale Signaturen
  - Signieren/Verifizieren ganzer XML-Dokumente oder von Dokumententeilen
  - 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

XML-Sicherheitsstandards II

- **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 Access Control Markup Language (XACML)**

  [OASIS standard since February 2003]
    - XML-basierte Spezifikation von Autorisierungspolitiken gegenüber Objekten und deren Durchsetzung
    - XML-Vokabular um Zugriffsregeln auf Ressourcen zu definieren
    - Request/Response-Protokoll um Zugriffskontrollentscheidungen zu ermitteln

XML-Sicherheitsstandards III

- **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

- **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.

AP3: Transfer von Informatikkompetenz in GBIF

- Abstimmungstreffen mit den Koordinatoren der IT-Fachgruppe, Berlin 16.07.2004
  - Zusammenarbeit der IT-Fachgruppe und der AG NBI
  - Themen für zukünftige Workshops
- Vorträge für den Workshop "Spezifikationen zum Datentransfer und zukünftige Datenfluss-Szenarien" der IT-Fachgruppe, Berlin 28.-29.10.2004
  - ”Web Services: Eine kritische Einführung”, Dr. Klaus Schild, NBI
  - ”XSLT: Transformation von XML-Dokumenten”, Dr. Klaus Schild, NBI
  - ”XML-Sicherheitsmechanismen für den Datentransfer in GBIF”, Ekaterina Langer

Weitere Informationen

- http://nbi.inf.fu-berlin.de/research/GBIF-D/
- Wissenschaftliche Publikationen zu diesem Thema:
  - R. Tolksdorf, L. Suhrbier, E. Langer:
    Designing XML Security Services for Biodiversity Networks
    Tagungsband DACH Security 2005 gemeinsame Arbeitskonferenz von Deutschland, Österreich und der Schweiz
  - R. Tolksdorf, L. Suhrbier, E. Langer:
    Integration of XML Security Services in a Biodiversity Information System
    Eingereicht für die Tagung Sicherheit 2005 der Gesellschaft für Informatik