Security, Integration and Implementation

EUBIROD Training Lectures Part 3: Implementation and Usage

Peter Beck, Philipp Perner

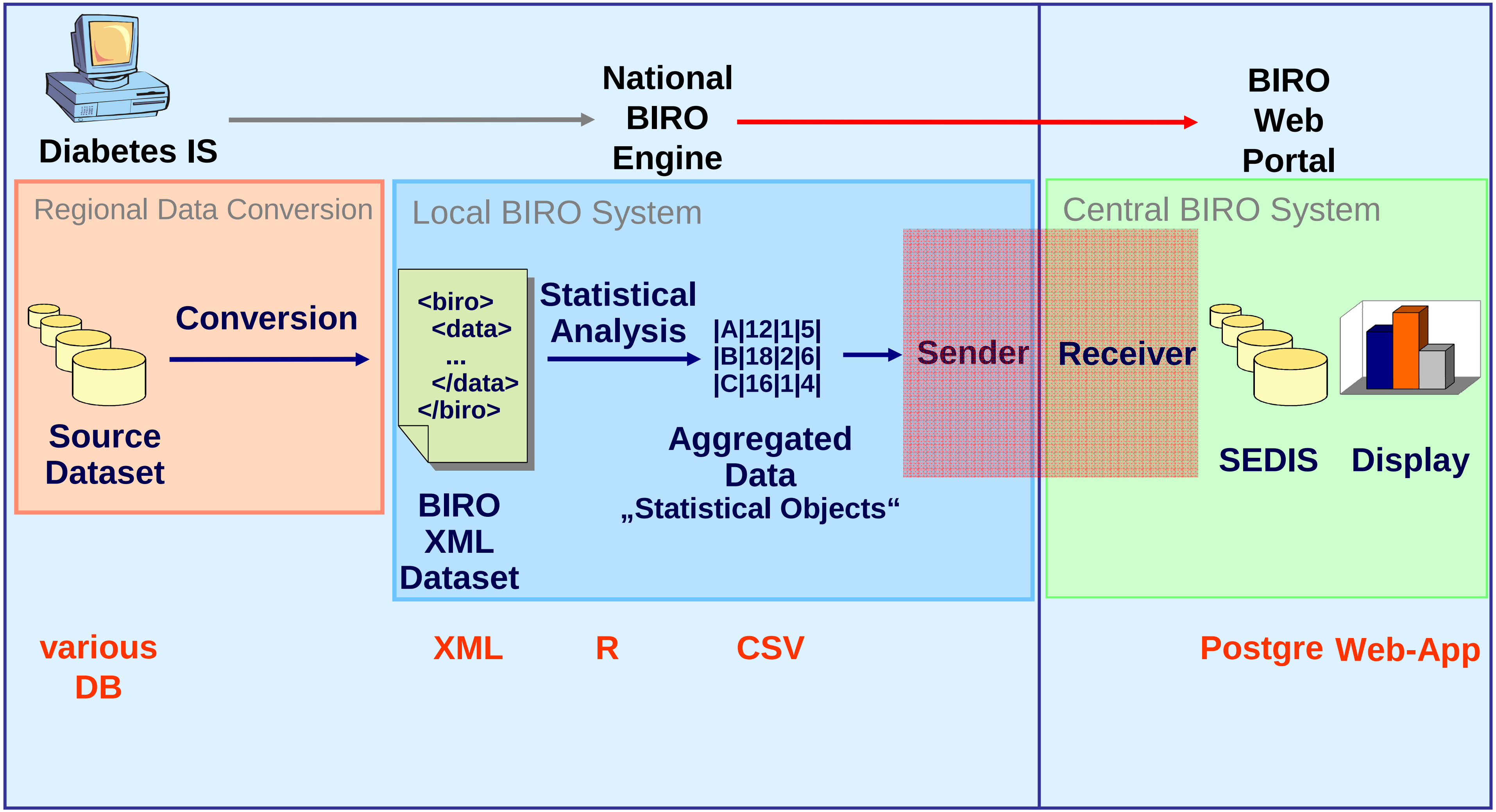
Kuwait City, 2nd-4th May 2009

Agenda

- Requirements
- Technology
- Security
- Integration
- Implementation

BIRO Academy

B.I.R.O. Architecture



Diabetes IS

National BIRO Engine

BIRO Web Portal

Regional Data Conversion

Conversion

Source Dataset

Local BIRO System

```
<biro>
  <data>
    ...
  </data>
</biro>
```

BIRO XML Dataset

Statistical Analysis

```
|A|12|1|5|
|B|18|2|6|
|C|16|1|4|
```

Aggregated Data „Statistical Objects“

Sender

Receiver

Central BIRO System

SEDIS

Display

various DB

XML

R

CSV

Postgre

Web-App

Security Requirements

Security Services according to ISO/OSI 7498-2

- Authentification
- Authorization
- Confidentiality
- Data Integrity
- Non-Repudiation

Security Technologies

- Encryption
- Digital Signatures
  - Public Key Cryptography (Key Pair)
  - Hash Algorithm

Communication Software Technology Requirements

- Selection Criteria
  - – Open, platform independent standard
  - – XML-based communication
  - – Use over Internet protocol(s)
  - – Availability of open source implementations
  - – Security (encryption, digital signatures)

Communication Software Chosen Technology

- Web-Services
  - Use SOAP Message Standard
    - Open W3C standard
  - SOAP messages are XML files
  - Transport protocol is HTTP(S)
  - Open Source SOAP frameworks exist for J2EE platform
    - Apache Axis2
  - Open Source Implementation of OASIS WebServiceSecurity specifications: Apache Rampart
    - XML encryption (XMLEnc)
    - XML signature (XMLsig)

WebService-Security

- Security on Transportation Layer
  - Communication via SSL + HTTP
- Security on Application Layer
  - Apache Rampart supports Public Key Cryptography
    - X.509 Certificates for Partners
  - Encryption/Signature of BIRO Data-Transfers to meet security requirements

Security Summary

- Authentication / Authorization
  - Public Key Certificates
- Confidentiality
  - Encryption HTTPS / SSL
  - Encrypting XML content before submission using XMLEnc
- Integrity and Non-Repudiation
  - Transmission integrity: HTTPS / SSL
  - Signature of the content before submission using XMLSig by sender

- Application

- Transport

Integration - Status

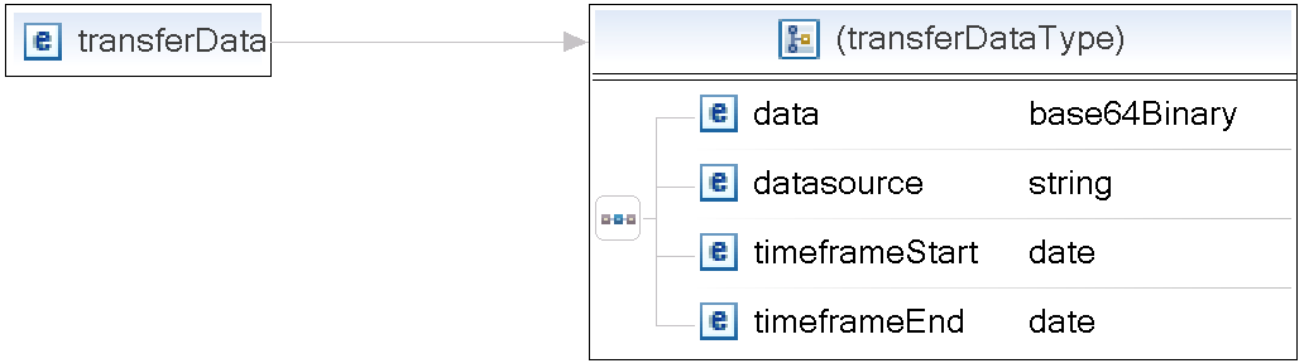
- Organizational level
  - – no additional network configuration (e.g. Firewalls)
  - – No additional tools necessary (VPN, FTP, …)
- Technical level
  - – Standardized Interface for WebService-Invocation
  - – All-In-One solution for BIRO-Box possible

Integration - Future steps

- Software-Updates as convenient as possible for partners
- Integrated Build-process of the BIRO-Box
- Eliminating partners‘ duty of configuring Communication-Software parameters

Implementation – Local Engine

- Local-Engine („BIRO Box“ Application)
  - Small Java Library integrated into BIRO-Box to provide security
  - Invoking WebService from BiroBox
  - Message *transferData* with actual dataitems



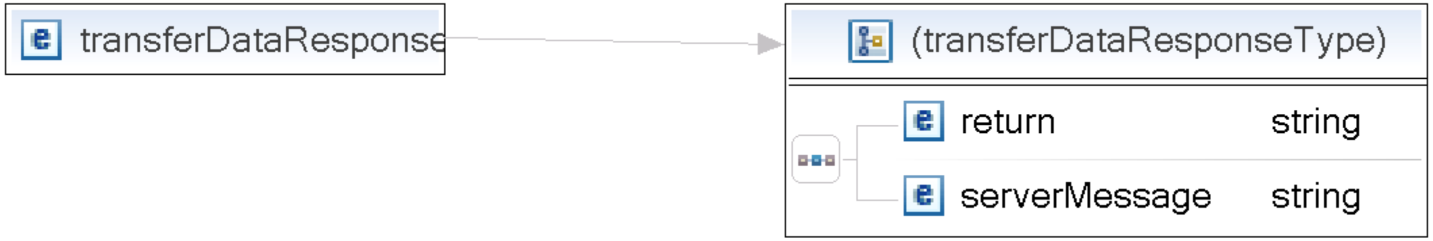
transferData

(transferDataType)

data	base64Binary
datasource	string
timeframeStart	date
timeframeEnd	date

Implementation – Central Engine

- Central-Engine
  - Apache-Tomcat Server running the WebService
    - Server configuration for HTTPS
    - Installation of Open Source Frameworks: Axis, Rampart…
  - Message *transferDataResponse* with status of sent message



Implementation – Future steps

- Currently one message implemented
- Management-Messages for general local/central-Engine communication
  - e.g. Software-Version, Transfer-Status (asynchronous), …

BIRO Academy

EUBIROD

Executive Agency fo Health an Consumer

Kuwait City, 2nd-4th May 2009