OPEN STANDARDS and IMPLEMENTATIONS for e-GOVERNMENT INTEROPERABILITY FRAMEWORKS

Adomas Svirskas\textsuperscript{2}, Cédric Hébert\textsuperscript{1}, Jelena Isačenkova\textsuperscript{2}

\textsuperscript{1}SAP Labs France, \textsuperscript{2}Institut Eurécom
Sophia-Antipolis, France

OASIS Symposium, April 28\textsuperscript{th} 2008, Santa Clara, USA
Tutorial Outline

- Tutorial objectives
- General business context of the project
- Indicative examples to motivate the framework
- Conceptual model
- Technical context
- Chosen specifications
- Overview of the implementation
Tutorial Objectives

- Overview of the EU Member States public agencies e-collaboration requirements and a particular case study - Europol/Eurojust collaborations
- Presentation of the main concepts of the proposed solution
- Discussion of the relevant technologies and standards, implementation options, decision making
- Sharing implementation experience
In a Nutshell

- **The business context**
  - EU IST FP6 project R4eGov - [www.r4egov.eu](http://www.r4egov.eu)
  - Collaboration among 27 EU member states governments

- **The technology context**
  - SOA and Web 2.0 based solutions
  - Web Services, Grid & Rich Internet Applications

- **The main issues**
  - On-demand Interoperability
  - Privacy, Security and Trust

- **Proposed approach**
  - Lightweight standards-based interoperability framework with emphasis on basic enforceable security
The Business Context

- EU IST FP6 project R4eGov - [www.r4egov.eu](http://www.r4egov.eu)
- Government agencies of the 27 EU Member States need to be able to *e-collaborate*
- The agencies are very independent, autonomous and protective of their data
- *Growing number of regulations are in effect*
- *The equilibrium between individual interests and common goals needs to be found and procedures put in place accordingly*
EUROPOL-EUROJUST CASE STUDY
The Hague Programme Vision

The Principle of Availability

- Throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and

- The law enforcement agency in the other Member State which holds this information will make it available for the stated purpose

- The Hague programme is a five-year programme for closer co-operation in justice and home affairs at EU level from 2005 to 2010
The Principle of Availability

- The methods of exchange of information should
  - Make full use of new technology
  - Be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (online) access, including for Europol, to existing central EU databases such as the SIS

- New centralised European databases should only be created on the basis of studies that have shown their added value.
The Three Protocols

- **Money laundering protocol** will make it possible for Europol to deal with money laundering as such, with no need to identify at a previous stage the predicate offence to which it is related. The implementation of this protocol will remove the legal restriction in several member states in the provision of intelligence related to suspicious transactions reported to the Financial Intelligence Units and will give Europol the possibility to cross-match the intelligence on those suspicious transactions at the EU level that have resulted in law enforcement investigations.

- **Joint Investigation teams protocol** will allow the member states to cooperate in an innovative and more efficient way in international investigations. Europol will be in a position to assist the investigations as the joint investigation teams will include Europol officials in a support capacity. This does not mean that Europol representatives may use any coercive power but that they can support with crime analysis, expertise, his services and products.

- **Danish Protocol on AWFs**, improving the functioning of the AWF legal framework based on the lessons learned during the first years of implementation and making Europol an easier tool and more user-friendly organization to work with for the law enforcement agencies interested in sharing intelligence on crime groups.
Civil Liberty Concerns

- "The free market in access to data/intelligence will rely on "self-regulation" by the law enforcement agencies and make accountability almost meaningless"

- "The law enforcement (police, immigration and customs) and security agencies will have unfettered access to any data held within the EU and, as is increasingly hinted at, with "friendly" non-EU states too"

- "The "principle of availability" sweeps away external checks and controls over the exchange of information and intelligence. In effect the agencies will be "self-regulated" with the all the dangers of misuse and abuse."

The case study provides an illustrative example of interactions between Europol, Eurojust and Competent Authorities in Member States.

Focus on interactions between different organisations, as opposed to internal ones.

Consider areas where interoperability is more critical for the success of the overall process.

Security and privacy requirements are of key importance for Europol & Eurojust.
Europol-Eurojust Case Study
Europol-Eurojust Case Study

1. Interaction Flow 2 – Eurojust access to AWF:

- **Europol**
  - LB
  - CMx
  - IMT4
  - SCx
  - IS
  - IxS
  - AWF

- **Eurojust**
  - NM
  - ENU
  - MS CA
  - College
  - JIT
  - CMS
  - TWF

**Using the message exchange system, Europol LBs (contacting the MS CA through the ENU) approve association of Eurojust to Europol AWF in the context of the Eurojust case**

**Eurojust NM requests association of Eurojust to Europol AWF in the context of the Eurojust case**

**Europol owner of AWF grants access to the AWF by Eurojust**

**Eurojust access AWF**

**Information is uploaded in the CMS**

**In a coordination meeting, in the context of the same Eurojust case, Eurojust NMs decide to request access to Europol AWF**
Europol-Eurojust Case Study

- The interactions between Europol and Eurojust have interesting interoperability requirements, which makes them useful as a general case study, with solutions applicable to other areas of eGovernment:
  - Multi-national exchange of information subject to different legal requirements
  - Access by an organization (Europol/Eurojust) to information managed by the other (Eurojust/Europol)
  - Collaboration in the context of interrelated Eurojust and Europol cases
Key Elements of the Case Study

- Addressing key interoperability barriers, whose resolution would add more value to the overall process
- Simplified, focusing on key aspects and ignoring details that are not strictly relevant
- Principle of availability as defined in the 3 Protocols
- Exchange of information complying with confidentiality, data protection and security requirements (including data classification)
- Identity and access management issues, with identities managed by different organisations (Eurojust and Europol) having to interact and exchange data
- Case management, considering the interactions between Eurojust and Europol case management systems *(CMS, including TWF for Eurojust, and InfoEx and AWF for Europol)*
- Interactions between workflows in Eurojust and Europol
Key Requirements

- Workflows:
  - All workflows can be developed into automatic process interaction, with human control points
  - Flexible application of workflows, with human judgement determining changes in workflows or deciding one of several workflows to be applied in certain circumstances
  - Partial visibility of internal workflows

- Functional aspects:
  - Secure information exchange
  - Collaboration and Case Management
Key Requirements

- Type of interactions:
  - Currently Asynchronous interactions, where identity management can significantly improve response times
  - Long running interactions, with requests and responses separated by long periods of time, but still requiring correlation within specific cases

- Identity and access management
  - Identification and authentication when a Eurojust/Europol information system is accessed by an external user
  - Role Based Access Control (access based on role and not only identity, where the role is asserted by a trusted party), with roles being defined and managed by multiple organisations
  - Based on standards compatible with Web Services standards (i.e. SAML / WS-*)\(^\d\), e.g. considering the possibilities of applying identity federation standards
  - Consideration of overall identity and access management architecture, including audit (so that the role of the user is recorded in audit logs)
R4eGov-Europol/just Synergy

- Europol/Eurojust provide to R4eGov an area of practical applications with clear value for European citizens

- Provide adequate input to R4eGov work-packages

- Make use of R4eGov outputs and deliverables within Europol own projects and initiatives

- Participate in R4eGov project management and review activities, ensuring the alignment of R4eGov objectives, activities and deliverables with the needs and priorities of Europol & Eurojust
THE MAIN CONCEPTS
The Case Study Distilled

Mutual Legal Assistance Collaboration Scenario
The MLA Scenario

1. The Europol National Unit of country A asks for support from Eurojust (EJ) National Member of country A regarding the execution of measures for protection of a witness in a criminal proceeding. The measure is to be executed in country B.

2. Europol National Unit A makes a written request of assistance (witness protection) to EJ National Member A.

3. The EJ National Member A opens a Temporary Work File in the CMS.

4. The EJ National Member A contacts EJ National Member B forwarding the request of assistance.

5. The EJ National Member B contacts the responsible national authority of country B. Steps are taken by the responsible national authority to provide the requested assistance.
The Requirements Distilled

- There is a need for federated domains of trust, which would provide:
  - Repeatable procedures of data exchange compliant with the policies and regulations
  - Means of controlled access, accountable usage
  - Overarching support of data authenticity and confidentiality
  - Support for auditing of data usage
  - Preservation of privacy
Collaborative Interactions
(Private/Public/Federated)

Choreography domain

Federated Collaboration domain

Orchestration domains

Administration domains

Public

Public

Public

$P_{prvA}$

$P_{prvB}$

$P_{prvC}$

$P_{public}$

$P_{public}$ – Public Business Protocol

$P_{prvA-C}$ – Private Integration Protocols
Collaboration Pattern Variations

- Rigid workflows to automate repeatable procedures, eliminate unnecessary human work and mistakes
- Ad-hoc creative information manipulation, collective knowledge creation - towards Enterprise (Government) Social Computing
- Collecting, Publishing, Tagging - towards Enterprise (Government) Mash-ups
The Technical Context

- **Proliferation of Service Oriented Architecture (SOA) solutions**
  - Data as (composite) services
  - Data services aggregated from different sources on-demand (mash-ups)

- **Social factors of ICT usage**
  - Data is *easier to obtain and harder to protect*
  - Technical innovations come (and go) fast
  - People use the ICT tools *less responsibly, as toys*

- **Collaborative interactions occur in this context**
Potential Solutions

- Defining and enacting business protocols (choreographies & orchestrations)
  - Defining public protocols first
  - Deriving public protocols from private processes/public interfaces

- Enhancing these protocols in order to increase levels of security and provable compliance of multi-party collaborations

- Institute controls, which enhance transparency of the interactions and allow controlling the way the key data is processed, distributed, retained, and accessed in day-to-day operations
Interoperability in R4eGov

- Interoperability is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" – IEEE Standard Computer Dictionary

- Scope of interoperability approaches: How much agreement/shared collaboration design is necessary to prepare "interoperability at run time"?
  - **Unbounded approach**, artificial intelligence / "perfect" Ontology approach
    - Partners can send each other “everything”, they will understand the terms expressed in the ontology
  - **Limited approach**
    - Collaboration spheres between selected partners
      - E.g. all parties involved in Europol/Eurojust scenario
    - Partners in collaboration sphere agree on certain formats (metamodels) for documents, organizational units etc.
    - If automated, flexible processes are wanted:
      - partners collaborate in design phase of collaboration, e.g. for shaping suitable process chunks / services
  - **De-central approach**
    - Describe possibilities/interfaces of individual public administrations rather than global processes
    - **Inside-Out approach** rather than **Outside-In approach**
    - Aligned with Service-oriented architecture
Interoperability in R4eGov

Public Administration A

Organization

Data
Process
Function
Output

Business Interoperability Interface

Communicate
Comprehend
Adapt
Validate

Technical Interoperability Gateway

Executable private processes

Public Administration B

Organization

Data
Process
Function
Output

Business Interoperability Interface

Communicate
Comprehend
Adapt
Validate

Technical Interoperability Gateway

Executable private processes
Interoperability in R4eGov

Public Administration A
- Private process
- Interface for partners
- Goals
- Internal goals
- Goals that require collaboration
- Conceptual Private Information (EPC)
- Conceptual Interface (EPC)
- Conceptual global model (EPC)
- Technical Private Information (BPMN)
- Technical Interface (BPMN)
- Technical global model (BPMN)
- Executable Private Information (BPEL)
- Executable Gateway Specification (BPEL)
- Set of verified, complementary BPEL interfaces

Public Administration B
- Private process
- Interface for partners
- Goals
- Internal goals
- Goals that require collaboration
- Conceptual Private Information (EPC)
- Conceptual Interface (EPC)
- Conceptual global model (EPC)
- Technical Private Information (BPMN)
- Technical Interface (BPMN)
- Technical global model (BPMN)
- Executable Private Process (BPEL)
- Executable Gateway Specification (BPEL)
Interoperability in R4eGov

- Each PA can query the repositories of its partners for certain documents, processes etc.
- EP and EJ could agree to implement the global process XY as specified in repository Z.
- To support monitoring and analysis the Business Interoperability Interface (BII)-Repository also comprises information to correlate conceptual and BPEL processes.
**Standardisation Objectives**

- R4eGov is committed to the adoption of open standards, and intends to build upon and/or extend interoperability specifications where possible
  - ensure that R4eGov framework uses relevant standards and interoperability guidelines
  - ensure that R4eGov results contribute to the future developments of standards in relevant areas

- **Why standardisation matters:**
  - way to promote and achieve interoperability between technologies across different organizations and vendors
  - interoperability is a key requirement in today’s multi-vendor market (need balance between agreed functionality, competitive advantage, and need for interoperability)
  - standardisation is an important part of successful exploitation
Interoperability Solution Requirements

- Standards-based (IETF, W3C, OASIS)
- Simple & Lightweight – not only for rocket scientists
- Flexible – usable in great variety of environments
- Easily configurable (no need for 50 in-house developers)
- Transparent (like a phone PBX- on tap, not on top)
Interoperability Solution Principles

- SOA approach, naturally
- Event-based infrastructure for integration
- Web services and Enterprise Service Bus (ESB)
THE SOLUTION
Full Interoperability Framework
General Interoperability Architecture
Interop Enactment Environment

Manageable...
Interoperability Distilled

Participant A

- Legacy System
- Some other service
- BPEL engine

Interop Gateway

Participant B

- Legacy System
- BPEL engine

Interop Gateway

Simple...

- Management
- Monitoring
- Operation mapping
- Security
- Choreography enactment
- Business rule support

Orchestration

Business protocol
Extended IOP Gateway Architecture

Web services application server - IOP Gateway

- Message Validation
- Security
- Logging
- Dispatch
- Encryption
- Logging
- Privacy Support
- Security

Internal Domain

- ESB
  - Flexible, Loosely Coupled Back-end Integration
  - Service Mediation
    - Service Virtualization
    - Message Mediation
    - Content-Based Routing
    - Logging
    - Message Transformation
    - Validation
    - Fine-grained Access control

- Back-end Systems/Wrappers
  - Back-end Adapter
  - Java Service
  - .Net Service

- Mediator (CBR)
- Mediator (Security)
- Mediator (Logging/Monitoring)

Back-end Systems

- Composite BPEL Services

WS-Security
WS-Policy
WS-SecurityPolicy
WS-Addressing
WS-SecureConversation
WS-ReliableMessaging
WS-Trust
WS-*...
Implementation Tools
Axis2/Synapse & WSO2

Synapse
Logging, routing, transformation, management, security

SynapseEnvironment API

Axis2
RM  Addressing  Security  MTOM
What is an ESB?

“Any to any data connectivity and transformation (including Web services) built on an advanced, proven, reliable middleware infrastructure”
ESB Management Functions

- Apache Synapse/WSO2 ESB can ensure:
  - Logging
  - Tracking - adding headers
  - Authentication and Authorization
  - Schema validation
  - Monitoring and statistics
  - Failover, retry and load balance
SECURITY
The Issues

- SOA is known to be and can be vulnerable
  - This vulnerability can impact customer's data privacy, integrity, reliability and availability

- Failures/misuses are very costly
  - Impacts customer satisfaction, trust and loyalty, future revenues, ...even enterprise's stock price
  - Regulation breaches end up in legal battles

- Security/compliance with the regulations needs to be a business enabler
Key Requirements

- **Type of interactions:**
  - Currently **Asynchronous** interactions, where identity management can significantly improve response times
  - **Long running** interactions, with requests and responses separated by long periods of time, but still requiring correlation within specific cases

- **Identity and access management**
  - **Identification and authentication** when a Eurojust/Europol information system is accessed by an external user
  - **Role Based Access Control** (access based on role and not only identity, where the role is asserted by a trusted party), with roles being defined and managed by multiple organisations
  - Based on **standards compatible with Web Services** standards (i.e. SAML / WS-*), e.g. considering the possibilities of applying identity federation standards
  - Consideration of overall identity and access management architecture, including audit (so that the role of the user is recorded in audit logs)
Collaborating Parties do Have Different Security Requirements
Tiered Security Architecture

Web services application server - IOP Gateway

ESB
- Flexible, Loosely Coupled Back-end Integration
  - Service Mediation
    - Service Virtualization
      - Message Mediation
        - Content-Based Routing
        - Logging
        - Message Transformation
        - Fine-grained Access control
  - Message Mediation
  - Message Transformation

Internal Domain
- Back-end Systems/Wrappers
  - Back-end Adapter
  - Java Service
  - .Net Service
  - Proxy Service
  - E-Mail Server

Back-end Systems
- Internal workflow

Access Control Decision Making
- Context Handler
- PDP
- PAP
- Mediator (CBR)
- Mediator (PEP)
- Obligation Service

Request
- Message Validation
- Inward PEP
- Logging
- Dispatch

Response
- Encryption
- Logging
- Privacy Support
- Outward PEP

Protection and threat prevention

Access Enablement

Internal workflow
- BPEL Composite Services

Flexible, Loosely Coupled Back-end Integration
Basic Security Architecture

Access Control
Decision Making
Context Handler
PDP
PAP

Mediator (CBR)
Obligation Service
Policy DB

Mediator (PEP)

Request
Response

ESB
Flexible, Loosely Coupled Back-end Integration
Service Mediation
- Content-Based Routing
- Logging
- Message Transformation
- Fine-grained Access control

Protection, threat prevention, access control

Partner A
Back-end Systems/Wrappers
Policy DB
Mediator (CBR)
Mediator (PEP)
Request
Response

Partner B
Internal Domain
IOP Gateway
ESB
Back-end Systems/Wrappers

Flexible, Loosely Coupled Back-end Integration
Service Mediation
- Content-Based Routing
- Logging
- Message Transformation
- Fine-grained Access control

Web services
E-Mail Server
Proxy Service
Net Service

BPEL Composite Services

Internal workflow

A. Svirskas, C. Hébert, J. Isačenkova, OASIS Symposium 2008, April 28th, Santa Clara, USA
Standards, Specifications

- Authenticity, confidentiality
  - WS-Security
  - WS-Policy
  - XML Encryption, Digital signatures

- Identity management, Access Control
  - Security Assertion Markup Language - SAML
  - Extensible Access Control Markup Language - XACML
Standards, Specifications

- While understanding and using most of WS-* specs is relatively easy, practically it opens a number of technical issues to solve.
- Consistency and maturity of some specs are still evolving.
- Providing standard-based access control solution in distributed systems is not straightforward and requires a good knowledge of:
  - A couple of specs
  - Basic security concerns (digital signatures, encryption)
  - Access control models
WS-Security

- WS-Security fully covers the requirements with signing and encrypting particular SOAP message parts
- Implemented within Apache Rampart
- Well supported by WSO2 WSAS and ESB
- Configurable using WS-Policy
Access Control Model - RBAC

User A

User B

User C

Role I

Role J

Role K

Permission 1

Permission 2

Permission 3

Session

Session a

Session b

Session

Permission 1

Permission 2

Permission 3
AC Reference Framework - XACML
Existing AC solutions

- Proprietary solutions, e.g.
  - Open PERMIS
    - Uses own access control policy language
    - X.509 AC based authorization, now supports SAML
  - Shibboleth
    - Limited RBAC model support
    - Focused on privacy
- XACML-based solutions - emerging, e.g.
  Axiomatics Delegent
Access Control Enforcement

- Delegent AC suite, Axiomatics AB
Inter-domain Authorization

- Transmission of credentials between domains

- Choice of technologies
  - X.509 Attribute Certificates
  - SAML

- Both of them are not trivial in implementation
Authorization: choice of technology

X.509 Attribute Certificates

- Mature security considerations
- Attributes include Authentication Information, Identities, Role, Group and are extendible
- Similar to X.509 based PKI
- Can support delegation and certificate chains
Authorization: choice of technology II

- SAML
  - XML authorization framework
  - Is widely used now and will be used more in future
  - Good bridging with access control module (SAML 2.0 specifies the mapping with XACML)
  - Fits well into SOA specifications 'zoo' (WS-Security, WS-Trust and others)
  - Wide range of use cases
Motivation of Choice

- Attribute certificates
  - Can be XML-based
  - Clear Well understood structure

...but...

- SAML makes multi-party collaboration solution flexible
- Open for innovative SOA-oriented security solutions (research)
Distributed Roles

- Inter-domain access control is based on distributed (global, public) roles
- Participants need to agree on the set of commonly used roles
- Resource owners need to announce which distributed roles are needed to access which resources
- Resource consumers need to know this in order to map internal user credentials to external roles and build requests
Distributed Role-based Access Control

PEP  Policy Enforcement Point
PDP  Policy Decision Point
PAP  Policy Administration Point
PR   Policy Repository
dRole Distributed Roles Policy
Distributed Role-based Access Control

Request along with user ID and distributed roles
Privacy Preservation in dRBAC
Steps on the Sender’s Side

System A ➔ ESB ➔ PEP ➔ PDP ➔ ReqBuilder ➔ RoleMapper ➔ IOP GW A

- request
- authorisation
- XACML auth. req.
- authorization decision
- build external attributes
- get distributed roles
- request with external attributes
- attribute assertion
- sign & encrypt
- decision
- sign & encrypt
- send OUT
- msg sign & encrypt
- REQUEST
Steps on the Receiver's side

IOP GW B  
PEP
PDP
PEP
ESB
System B

REQUEST  
msg decrypt & verify  
request  
authorisation  
decrypt & verify  
XACML auth.req.  
authorisation decision  
decision  
target service invocation
IMPLEMENTATION
Implementation Experience

- This part of the tutorial will be a demonstration of experience with particular products, mentioned earlier:
  - Web services engine - WSO2 WS Application Server
  - ESB - WSO2 ESB
  - Access control - Axiomatics Delegent
Conclusions & Future Work

- This work is aiming to integrate a number of interoperability & security solutions into a practical framework
- Modern Web services and ESB solutions are used for implementing the framework
- Work is in progress to implement a prototype based on this framework
Credits

- R4eGov project partners, in particular:
  - Henrik Plate, SAP Labs France
  - Abdelkrim Boujraf, Unisys Belgium
  - Joerg Zieman, DFKI, Germany
  - Hannah Lee, University of Hamburg
  - Filippo Angelucci, Europol
Thank you!

www.r4egov.eu

adomas.svirskas@eurecom.fr, adomas@svirskas.com
cedric.hebert@sap.com
jelena.isachenkova@eurecom.fr