Federated Identity Management based on LIBERTY

http://www.celtic-fidelity.org
Agenda

• What is the Fidelity project
• Fidelity Objectives
• Project Implementation
• Most Important Project Findings
• Live Demo
What is the Fidelity project?

A cooperative R&D project sponsored by EUREKA/CELTIC and several European governments

Project development time frame: April 2005-December 2006

Results from the project will be exploited after project end by business lines of consortium members

Fidelity partners

Operators
- telenor
- france telecom
- orange
- TeliaSonera

Industry
- ERICSSON
- ITALTEL
- gemalto

SMEs / Universities
- linus
- tb-security
- oslo university college
- moviquity
Objectives of Fidelity project

- Demonstrate the **technical viability** of the Liberty approach in a pan-European context by setting up four CoTs with mobile operators as IdPs in an **heterogeneous** infrastructure
- Demonstrate the **interoperability** of **identity roaming/interconnection** between Identity Providers and Service Providers in CoT /interCoT using realistic scenarios
  - SSO, ID federation, attribute sharing
- Study **legal, privacy**, and socio-economical issues in Inter-CoT environments
- **Interoperability** between different **authentication** methods
- Include **smart cards** as authentication devices and attribute storages
- Introduce support for **non-HTTP** services
  - Example: VoIP
Fidelity project approach

• **Articulate project developments around a full range of scenarios**
  – *Representative* from real use-cases, involving simple to complex situations
  – Enabling to test a *wide range* of Liberty concepts
  – Focusing on InterCoT *interoperability* aspects
  – Based on *off-the-shelf, heterogenous*, multi-vendor IT infrastructure

• **Scenario requirements to cover the following issues**
  – Use Liberty Alliance approach and include both ID-FF and ID-WSF schemes, with *alternative implementation* options
  – Put *security, trust and confidentiality* as a top priority in the scenarios
  – Meet EU and national *legislation requirements* in implementation
  – Support *different authentication levels* in mobile and web environment
  – Enable access independency
Example: The Spanish CoT

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>1.4.2_04</td>
</tr>
<tr>
<td>Redhat</td>
<td>FC 4</td>
</tr>
<tr>
<td>Apache HTTP Server</td>
<td>2.0.54</td>
</tr>
<tr>
<td>SourceID ID FF 1.2 Java Toolkit</td>
<td>2.0</td>
</tr>
<tr>
<td>Ericsson IDP, DS, SP, WSP</td>
<td></td>
</tr>
</tbody>
</table>
• Flexible User Consent Module:
  – Technology vendors should provide a flexible user consent module which must be
    available and adaptable to all ID-SIS service and Attribute Provider (not only for
    Personal Profile). The user must know that he is in control of his personal data

• Interaction service – Multiple User Consent
  – How to deal with services that require attributes from various WSP for its service
    (Example: Car Rental Service require Credit Card info, Calender Info, Personal Profile
    Info)

• Liberty Specifications contain many options
  – Authentication Context Class versus Authentication Context Statement
  – Adding more attributes can be done in various ways, but some present implementations
    put restrictions
    Liberty specifications contain a lot of options and this complicates the multi-
    vendor deployment. Liberty should define some “profiles” (as a set of options)
    which may be based on the type of use cases to be supported, or business
    model(s) to be supported
Project Findings 2 (6)

• Metadata
  – Current IDP implementations do not always follow Liberty specifications
  – A slight mismatch was found between XSD schema and written specifications

• Liberty uses redirection heavily, but browsers can define a limit in its preferences
  – Could result in error in service execution

• Limited Size of Relaystate
  – “SHOULD NOT EXCEED 80 BYTES” hence business attributes should not be used in URLs due to this limitation

• InterCoT Service Discovery
  – Three methods exist: Direct Proxying / DS Chaining / Direct Access
    (not all supported by products used in Fidelity)
  – Fidelity selected Direct Access with PKI based trust model for all ID-WSF/FF InterCoT traffic which enables business model for InterCoT attribute sharing between V-SP and H-WSP
    Technically, this is implemented by using hierarchical certificate path validation (RFC3280)
Project Findings 3 (6)

• Resolving Home CoT of a user
  – Simple for End-User (no or few clicks)
  – Full proof process did not exist, but Fidelity tried a number of solutions.

• Authentication of users across CoT boundaries and between IDP’s
  – mapping of methods into three levels with algorithm -> independence of method / CoT
  – maintain simplicity for SP implementations

• Fidelity used many authentication methods
  – userid-password
  – SIM-EAP with/without PinCode  (Mobile phone/SIM methods used to authenticate also PC users)
  – WPKI
  – PCPKI
  – GPRS Authentication
  – ...

which can be exchanged across CoT boundaries
Project Findings 4 (6)

- The Liberty Specifications are a sound base for InterCoT deployment scenarios but some product implementations are not yet fully commercial grade.

- MultiVendor environments (Ericsson IDP, SUN AM, FTRD IDP, HP, Open Source Source-ID) are very complicated and PnP is something of the future.

- Liberty Interoperability and Conformance tests should be enhanced and made more stringent for IDP-proxy feature.

- Liberty conformance tests should be enhanced and hardened, especially for interCoT scenarios.

- Liberty actors (IDP, DS, SP, WSP, Interaction Module) should independently specified and implemented in order to enable a custom framework composition.
But what about the SP’s?

- SP Toolkit is mandatory for getting acceptance in the market place
  - Service Provider toolkit and tools for configuration and administration should be designed and developed in a SP-centric manner in order to favour Liberty adoption by existing Service Providers
  - Provided guidelines when to use one-time identifier or federated identity
    - Users who already have a local account on a SP can federate it with their IDP’s account
    - One-time access is always related to punctual attribute sharing (e.g.: Auto-fill a form, Retrieve user geolocation, etc.)

And how about the end-user?

- a huge task is still ahead for the IDP owners to:
  - Identification of the Circle of Trust / Branding
  - Make the user understand mechanisms of CoT and CoCoT
  - Recognizing that an SP belongs to user’s CoCoT
  - CoT as everyday’s Object: Concept of Key Holder and Master Key?

- Coherency/Consistence presentation of the whole process
  - Entering the CoT, Attribute management of many WSP’s, Federation/De-Federation

Master Key = IDP credentials

Key = SP credentials

CoCoT logo/brand

CoT logo/brand
Project Findings 6 (6)

- Fidelity worked with business case analysis
  - IntraCOT with Telco as IDP
  - Internal Enterprise
  - Inter-CoT
  - Mobile-fixed collaboration
- Common Costs Savings on Customer management & implementation for SP’s ..
- Reduced administration for service execution, “free” increase of “subscriber base” ..
Conclusions

Overall no *major problems found*

No more questions like:
- Does Federated Identity technology actually work?
- Are the specifications mature enough?

→ Technically InterCoT scenarios are possible

but:
- How can I integrate the technology in my business processes?
- How do I market this technology?
- soft “issues” like how to educate the end-users, how to gain the confidence of the end-users,…

The Liberty Specifications are mature for implementing InterCoT scenarios