Security aspects of the Fidelity project

Prof. Manel Medina
Miguel Colomer
Antoine de Poorter
Sandra García
Contents

• Fidelity Project goals
• Web services Roaming architecture
  – Liberty Alliance Protocol suits
• Security Requirements
• Threats & countermeasure Solutions:
  – Security Policy
• Security Evaluation Tools
• Testing Scenario
• Conclusions
Fidelity project goals

• Fidelity: Federated Identity Management
• Celtic / Eureka awarded project
• Proof of concept about interoperability of LA specs. in heterogeneous infrastructure
• Identity federation concept
• Sharing attributes in pan European context
Inter-CoT use case

SSO & Attribute sharing

Federation

One time id

Authenticationservices (smart cards, SW,....)

Identifier / WSP

Identification Provider

Discovery Service

Web Service Provider(s)

Trusted SPs

Identifiers

SP Service Provider(s)

IDP

Identifier / WSP

DS

Authentication services (smart cards, SW,....)

One time id

SSO

Attribute sharing
Book a hotel use case

Scenario options:
- WSP placed on a smart card
- Registration of attributes
- Confirmation in Calendar
- Wallet and re-authentication (stronger authentication)
- Payment of hotel room

Basic technical features:
- ID-FF (SSO, SSO proxy)
- One time ID
- User Interaction for Home CoT discovery
- User/password authentication
- WSP invocation
- Interaction service
Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles.

Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)
Security Requirements

• Roaming of web services
  – Show the technical feasibility of a large scale implementation

• Identity federation and Single Sign On
  – Produce best practices recommendations to guarantee the adequate security to involved actors

• Personal Data Protection
  – Show that seamless authentication and attribute sharing across CoT boundaries is possible

• Explore the applicable EU legislation
  – Identify relevant environments
  – Produce recommendations for the technical mechanisms and legal agreements
Technical Approaches (I)

To meet the Security requirements, LA provides the following tools:

• Single Sign-On and Federation Protocols
• Proxy Identity
• Discovery Service
• Personal attributes transfer authorisation
Technical Approaches (II)

- Artifact Profile management
- Authentication mechanisms
- Access Control Policy
- Use of smart-cards
- Pseudonimity and Anonymity management
Security Aspects: Threats

Identity management threats only:
• Client Session hijacking
• User Identity theft
• Phishing Service Provider identity
• Phishing Identity Provider identity
Solutions: Security Policy

• 1: Principal authentication and access security policy.
• 2: Principal, Service Provider and IDP data protection security policy.
  – Secured storage and access to personal data
• 3: Service Provider, IDP and WSP access security policy.
  – Trusted PKI usage
  – Mutual authentication
  – Certificate revocation
• 4: Business practice security policy.
• 5: Operation security policy.
Security Evaluation Tools

• Specific:
  – Fake IdP, DS, SP
  – Non-valid certificates

• Non-specific:
  – Sniffing
  – Web browser and applications attack tool
  – DNS spoofing or DNS cache poisoning
  – Hacking tools
  – Password cracking
Specific Testing scenario

Fake SP as WSP (AP)

Visited CoT

Visited IDP
Test suit

• Network sniffing:
  – SSO and SLO.
  – Create and remove federation.
  – DS publishing and querying.
  – User attributes querying.
  – IDP to IDP (in InterCoT) communications.

• Fake components simulation:
  – SP to (AP, DS, IdP)
  – IdP to IdP
Concluding remarks

• Fidelity & LA proof of concept provide trustworthiness to:
  – **End users**: accessing their home or **roamed services**, with different levels of **anonymity**, and **guaranteed preservation** of personal data
  – **Service Providers**: **Non-repudiation proofs** that the attribute providers are providing the **right information** about the end-user
  – **IdP**: **Service level agreements** signed with other IdP, will guarantee that their **liability** will be kept always **under control**

• Innovative mobile user identification and attribute sharing solutions based on smart-cards has been tested:
  – Integration of Liberty components on smart-card

• Testing methodology has proven efficiency in checking the right installation choices:
  – PKI authentication context initialisation
  – Policy checking