Identity Federation: security for multiple services in a trusted environment.

...enabling a community of interest...

Elio Molteni
President of AIPSI
info@aipsi.org
Introduction to AIPSI

What is Identity Federation

The benefits

Key standards & specifications

The USA Government case
What is AIPSi?

- AIPSi is the Italian chapter of ISSA®
- More than 13,000 experts in the world
- Association of professional people

ISSA® - With active participation from individuals and chapters all over the world, the Information Systems Security Association (ISSA) is the largest international, not-for-profit association specifically for security professionals. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.
Goals of AIPSI

- Organization of educational forums
- Documents and special publications
- Exchange of experiences among national and international members
- Reference point for security experts recruitment
- Cooperations with other professional organizations
Let’ us start on “Identity Federation”
Allow information-sharing transactions in a secured and trusted environment:

- government to citizen
- government to business
- government to government

..and Identity is the fundamental!
Preserve privacy ensuring data security

Simplify access to services and applications

Reduce the need to manage multiple sets of identity credentials

Reduce the cost and complexity of managing identities

Enable dynamic creation and management of trusted relationships
Benefits of Identity Federation

Customer/citizen convenience
- Improved user experience & eased application access with SSO

Reduced costs
- Improved Leveraging identity management practices of “actors”
  - Identity proofing
  - Credential issuance
  - Forgotten/lost credentials
- Reduced password related Helpdesk costs
- Increased usage of lower cost Web applications
- Need for credentials lowers Web application usage
- Avoidance of federated SSO technology “one-offs”
Enhanced security

- Leveraging of “stronger” regularly used & better proofed credentials
- Credential explosion is inherently insecure
- Identity Provider controls user credential & thus access to Service Provider application
  - Former users immediately lose access to federated applications since they must come through the IdP
- Use of enterprise class security building blocks
What is Identity Federation?

Federation enables users and applications to work across autonomous internal business units, external business partners and other third-parties seamlessly as if they were part of the same security domain, while in fact the domains remain independent!

From technical point of view (communications)

From business point of view (relationships)

From policy point of view (trust)
How Identity Federation works

- A user being redirected to another domain’s protected Web applications
- Transfer of security information handled invisibly to the user
- Provides SSO across domains: Community Federations

How Identity Federation works

www.other_PA.com

Security Product

www.PA.com

Authenticate Here

Redirect
SSO

User

Internet
Groups of “related” organizations come together to create a federation “community”
Who is Federating?

Government agencies worldwide for eGovernment
- USA, Ireland, Norway, Austria, New Zealand...
- Eased citizen access to government services

B->B
- Health management, employee benefits, pension providers, travel services, web conferencing, payroll services, insurance, specific ASPs, & many others...

B->E (link internal portals around world)
- Internal federation for large, geographically distributed organizations

B->C (consumer information services)
- Via wireless phones & cable TV
- Early stage projects
Key Standards & Specifications

- **Security Assertion Markup Language (SAML)**
  - Standard managed by OASIS
  - Provides for the sharing of security information between domains
  - Protocol & ticket together enable federation

- **Liberty Alliance**
  - Alliance of many sponsor companies
  - ID-FF – Portion of Liberty that enables browser-based federations

- **WS-Federation**
  - Plans for ADFS implementing WS-Federation in late 2005
The USA Government case

An example of Community Federations

Coming from
Educause Net@EDU Annual Meeting
February 7, 2005
Absent a National ID and unique National Identifier, the e-Authentication initiative will establish trusted credentials/providers at determined assurance levels.
GSA* is organizing E-Authentication effort

- Providing technical & business framework for federal agencies to federate with each other
- Will be extended to other external & commercial entities

Goal

- Driving agency applications on-line for citizens, businesses, & government users
- 30 agencies in the process of federation enabling applications
- Enable federation for as many as 6K-7K agency applications
- Wants to avoid each agency having to issue credentials for its users

Status

- In initial production

GSA* General Services Administration
### E-Gov Agenda

#### Government to Govt.
1. USA Service
2. EZ Tax Filing
3. Online Access for Loans
4. Recreation One Stop
5. Eligibility Assistance
   - Online
6. Wireless Networks
   - Online

#### Lead
- SSA
- Treasury
- DoED
- DOI
- FEMA
- Labor

#### Government to Business
1. Federal Asset Sales
2. Online Rulemaking Management
3. Simplified and Unified Tax and Wage Reporting
4. Consolidated Health Informatics
   - (business case)
5. Business Gateway
6. Int’l Trade Process Streamlining

#### Lead
- GSA
- EPA
- Treasury
- HHS
- SBA
- DOC

#### Cross-cutting Infrastructure: eAuthentication GSA

#### Government to Citizen
1. e-Vital (business case)
2. Grants.gov
3. Disaster Assistance and Crisis Response
4. Geospatial Information One Stop
5. Wireless Networks

#### Internal Effectiveness and Efficiency
1. e-Training
2. Recruitment One Stop
3. Enterprise HR Integration
4. e-Travel
5. e-Clearance
6. e-Payroll
7. Integrated Acquisition
8. e-Records Management

#### Lead
- OPM
- OPM
- GSA
- OPM
- GSA
- NARA
Identity Federation: security for multiple services in a trusted environment.

Enabling a community of interest...

Elio Molteni
President of AIPSI
info@aipsi.org

www.aipsi.org
www.issa-italy.org