Liberty Alliance
What's Next

Fulup Ar Foll
Master Architect
Global Software Practice
Sun Microsystems
What's About Federation

• **Federation of providers** (CoT), a group of entities providing services who signed agreement, in order to make life of shared customers/users (*Principal*) more simple.
  - accept Principal identity authentication to be done once per session (*SSO*) and by a shared authority (*IDP*)
  - Accept to provide service knowing only an “avatar” of principal identity (*Opaque Handle/Federation Key*). This non significant pointer on principal identity allowing service provider (*SP*) to know that “it is him” without knowing “who he is”.

• **Federation**: a weak link that allow to map a principal avatar identity used by a service provider to the effective principal identity know only from the authority of authentication (*IDP*).

• **Federated Identity**: The data/attributes at the service provider attached to a principal identity avatar.
Standard and Convergence

Liberty Alliance
- Phase 1: July 2002
- ID-FF v.1.1: January 2003
- ID-FF v.1.2: November 2003
- SAML v.2.0 use/testing: April 2005

OASIS SSTC
- SAML v.1.0: November 2002
- SAML v.1.1: September 2003
- SAML v.2.0: March 2005

Internet2 Shibboleth
- Shib v.1.0/1.1: July/August 2003
- Shib v.1.2: April 2004

OASIS Contribution

Sun Confidential: Internal Only
OASIS SAML 2.0 Concepts

Profiles
- Combining protocols, bindings, and assertions to support a defined use case

Bindings
- Mapping SAML protocols onto standard messaging or communication protocols

Protocols
- Request/response pairs for obtaining assertions and doing ID management

Assertions
- Authentication, attribute, and entitlement information

Authn Context
- Detailed data on types and strengths of authentication

Metadata
- IdP and SP configuration data
Global Liberty Architecture

Identity Provider
- Authentication
- Federation
- Discovery service
- Policies/Authorization

Identity Services
- Geolocation
- Personal Profile
- ....

Service Provider
- web content
- games
- merchant site
- ....

Circle Of Trust

Principal
- customer
- employé
- game user
- ....

Auth. Pts

Legacy/existing Infrastructure

Other CoTs

Liberty ID-FF/SAML-2.0
Liberty ID-WSF
Not Specified by Liberty
Liberty Technical Framework

- **ID-FF (Identity Federation Framework)**
  - Federation/Defederation
  - SSO (*single & simplified Sign On*) / SLO (*single logout*)
  - Authentication context & Attributes
  - Metadata

- **ID-WSF (Identity Web Service Framework)**
  - Authentication Service
  - Discovery Service
  - DST (Data Service Template)
  - Interaction Service

- **ID-SIS (Identity Service Interface)**
  - Personal profile, Geoloc, Presence, Contact Book, ...
ID-WSF 2.0: Cross-User

- Extended Invocation Context to include:
  - Invocation Identity
    - Who is submitting the request
  - Target Identity
    - Who’s resource is targeted in the request
  - Sender
    - Server sending the request
  - Destination
    - Server receiving the request
ID-WSF-2: People Service

- Identity Federation between *individuals*
  - Paul establishes a connection with Carolina
- Supports Invocation of another user’s service
  - Carolina can access Paul’s Calendar (w/permission, of course)
- Group (Collection) management
- Invitation model for cross-IDP federations
Why Choosing Liberty?

- **Fit your requirements:**
  *Free & Open standard, Privacy, Security, Interoperability*

- **An industrial reality:**
  *Certified products, Already proven in production*

- **You're not in a position of choosing:**
  *Costumer chooses for you !!!*

---

**Kravspesifikasjon for PKI i offentlig sektor**
*Version 1.02, Januar 2005*

**Krav 10.5.1 Autentisering**

Det skal tilbys en "Identity Provider" i henhold til Liberty Alliance spesifikasjoner. Løsningen skal beskrives. Det skal angis hvilke versjoner og overordnede funksjoner som støttes.

**Requirements Spec. for PKI in Public Sector**
*Version 1.02, January 2005*

**Requirement 10.5.1 Autentication**

*It shall be offered an "Identity Provider" according to Liberty Alliance specifications. The solution shall be described. It shall be indicated which versions and which high level functions are supported.*
Liberty Alliance
What's Next

Fulup Ar Foll
fulup@sun.com