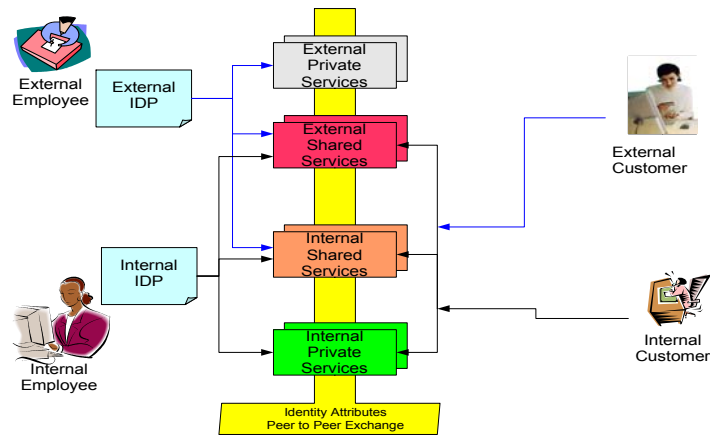


Identity Federation & Web Services

Fulup Ar Foll, Sun Microsystems
fulup@sun.com

Why Federation



Why Standard & Interoperability Matter

•Global Connectivity

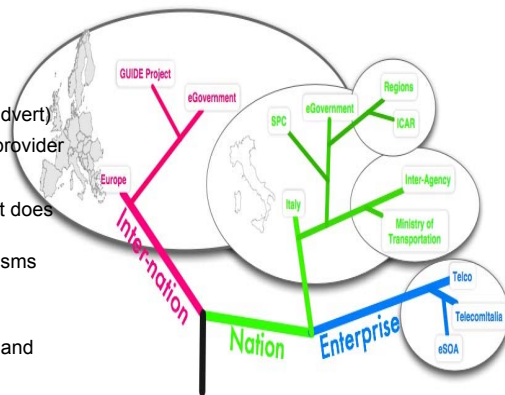
- Across repository, domain, ...
- Seamless to User (complexity advert)
- Want to be both consumer and provider

•Increasing Demand for ID

- Every one want your Identity, but does users want it ?
- Need adequate privacy mechanisms before exposing it.

•Heterogeneous world

- Multi vendors, services provider and consumers are heterogeneous.
- Multi channel, cross devices, cross networks, ...



3

A high level Interoperable standard

•ID-FF: Identity Federation Framework

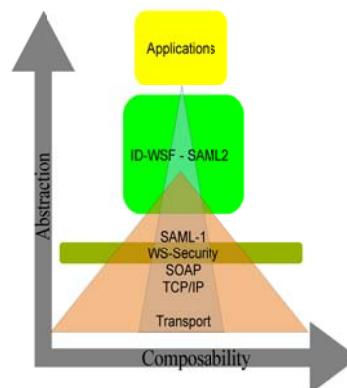
- "Liberty Federation"
- Focused on human-to-application interaction
- Now converged with SAML V2.0

•ID-WSF: Identity Web Services Framework

- Focused on application-to-application interaction

•ID-SIS: Service Interface Specs

- ID-SIS plus ID-WSF equals "Liberty Web Services"
- Defines particular useful services
- Personal profile, geolocation...



4

Design goals

- A standards-based architecture for Federation & identity web services
 - Ecosystems of services that expose interfaces on behalf of individual users' identities
- Privacy and Security as a 1st class citizen
 - Identity information requests access-controlled
 - Minimal disclosure of identity information
 - Protection against disclosure of identifiers
- Flexible foundation for application development
 - Across security domains and computing platforms
 - Across time, allowing for service location flexibility

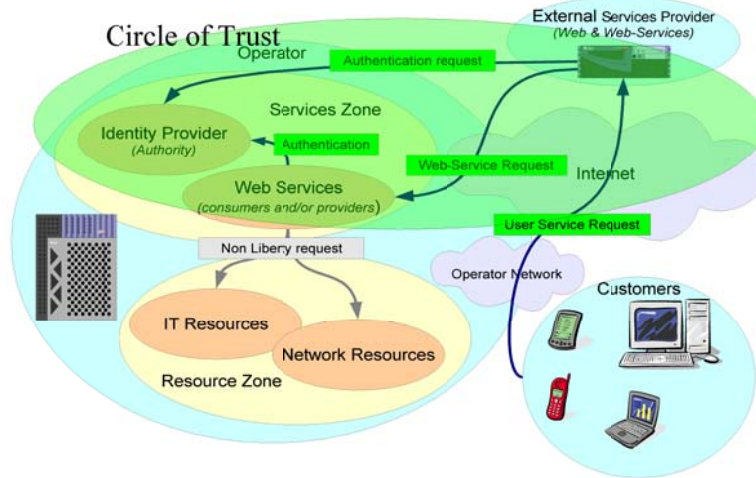
5

Privacy is a MUST

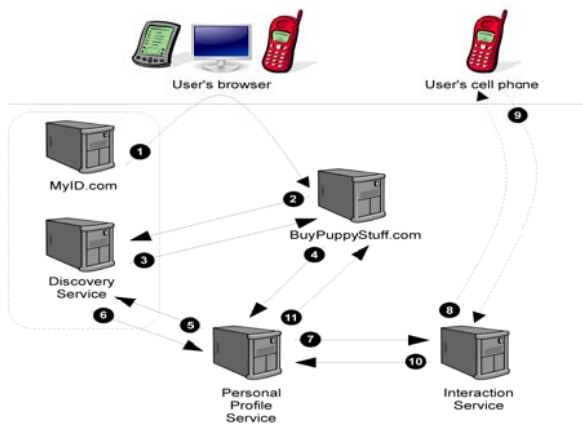
- Ensuring that your data is shared on your terms by:
 - Capturing your usage directives and consent status in service messages
 - Allowing for interaction with you at critical junctures to obtain your consent and privacy policies
 - Interaction Service, Interaction Redirect
- Inhibiting correlation of your activities by:
 - Offering different pseudonyms to different parties
 - Identity Mapping Service
- Protecting your data in transit
 - WS-Security for confidentiality

6

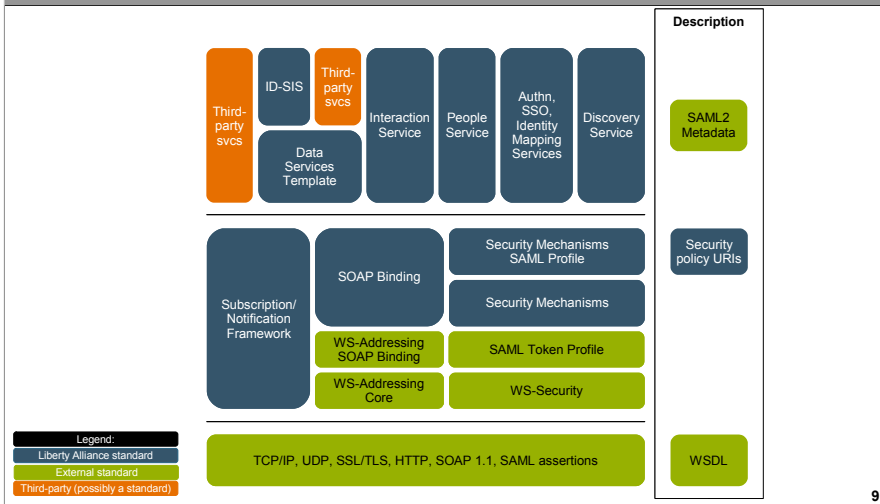
Global Architecture



An all-singing, all-dancing sample flow



Protocol architecture piece-parts



9

Major benefits of ID-WSF's design

- Peer to Peer (no big brother)
- Authentication, authorization, and application of usage policy against consumers of identity data
- User privacy through use of pseudonyms
- Dynamic service discovery and addressing
- Common web services transport mechanisms to apply identity-aware message security
- Abstractions and optimizations to allow anything – including client devices – to host identity services
- Unified data access/management model for developers
- Flexibility to develop arbitrary new services
- Identity model for social network & cross users (ID-WSF2)

10

ID-WSF 2.0: What's new ?

- Features

- Cross-user transactions
- Asynchronous & messaging
- Subscription/Notification
- Adoption of SAML2

- Components

- Framework enhancements
 - Adoption of WS-Addressing
 - Multi-user invocation context
- People Service
 - Who are my "friends"?

11

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

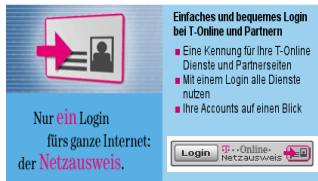
12

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

Technology is Mature


T-Online Netzausweis



Einfaches und bequemes Login bei T-Online und Partnern

- Eine Kennung für Ihre T-Online Dienste und Partnersiten
- Mit einem Login alle Dienste nutzen
- Ihre Accounts auf einen Blick

Nur ein Login fürs ganze Internet: der **Netzausweis**.

Login 

[? Hilfe zum Netzausweis](#)

T-Online Netzausweis

Der aktuelle Status Ihrer Dienste **Netzausweis Überblick anzeigen**

Das Passwort-Chaos besiegen



Zwei Ex-Chaoten sagen aus: **mehr**

Mein T-Mobile Login

Bitte geben Sie Ihre Benutzerdaten ein

Benutzername [\[vergessen?\]](#)

Passwort [\[vergessen?\]](#)

Freischaltcode eingeben >

 [Details >](#)

Liberty Alliance ID-WSF 1.1



Le projet de portail Mon.Service-Public.fr doit permettre à l'utilisateur - personne physique ou morale - l'accès à une gamme cohérente et étendue de services dans un environnement personnalisé, et ce dans des conditions permettant de créer la confiance.

Une version pilote a été développée et testée par 500 usagers mi 2006. Après des conclusions plutôt positives sur cette expérimentation et l'intérêt du service, la phase de réalisation du système "grand public" a été lancée.



Identity Federation & Web Services

Fulup Ar Foll
fulup@sun.com