THE LIBERTY ALLIANCE PROJECT

Fulup Ar Foll, Principal Engineer
Liberty Technical Expert Group

Master Architect, Global Software Practice
Sun Microsystems, Inc.

Importance of Identity

Why do we need Liberty

- Most of Added Value Services need identity
- The most basic element in a high-value relationship with customers, employees, citizens or business partners
- Has to be managed with great care to proactively fight fraud and identity theft
- Common mechanisms to handle identities are required

Importance of Federation

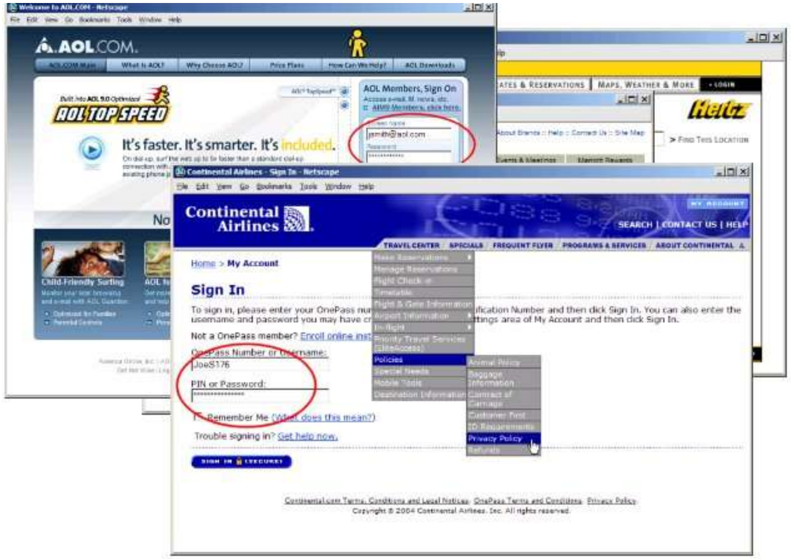
Loosely Identity connection is a MUST.

- Federation is the way the world works today (drivers license, national ID, SIM cards…)
- Federation facilitates scalable, efficient, user-friendly, cross-domain Identity Management
- Without Identity Management, federation fails… interactions and transactions become more difficult, if not impossible
- Federation is a foundation for pseudonymous and anonymous secure business relationship

Principal/EndUser Vision

Too complex

- ✗ Login and password proliferation
- ✗ Information attribute redundancy
- ✗ Personal information management
- ✗ Data privacy
- ✗ Security



Home > My Account

Sign In

To sign in, please enter your OnePass nu… …ification Number and then click Sign In. You can also enter the username and password you may have cr… …ttings area of My Account and then click Sign In.

Not a OnePass member? Enroll online inst…

OnePass Number or Username: JoeS176

PIN or Password: ***************

Remember Me (What does this mean?)

Trouble signing in? Get help now.

Continental.com Terms, Conditions and Legal Notices OnePass Terms and Conditions Privacy Policy

Copyright © 2004 Continental Airlines, Inc. All rights reserved.

Enterprise Considerations

Two dimensions

- Managers - Decisions Maker
  - Web Services SOA framework.
  - Loosely couple identification.
  - Commercial software stack.
- Architect - Implementers
  - Outsourcing of application
  - Easier integration of partners
  - Extend panel of services
  - An answer to some security concerns

Why Liberty ?

- A free standard focusing on:
  Privacy, Security, Interoperability
- An industrial reality:
  Certified products, Already proven in production
- *Customer requirement* (i.e. Norway Gouv. RFQ)

Kravspesifikasjon for PKI i offentlig sektor
Versjon 1.02 , Januar 2005

Krav 10.5.1 Autentisering

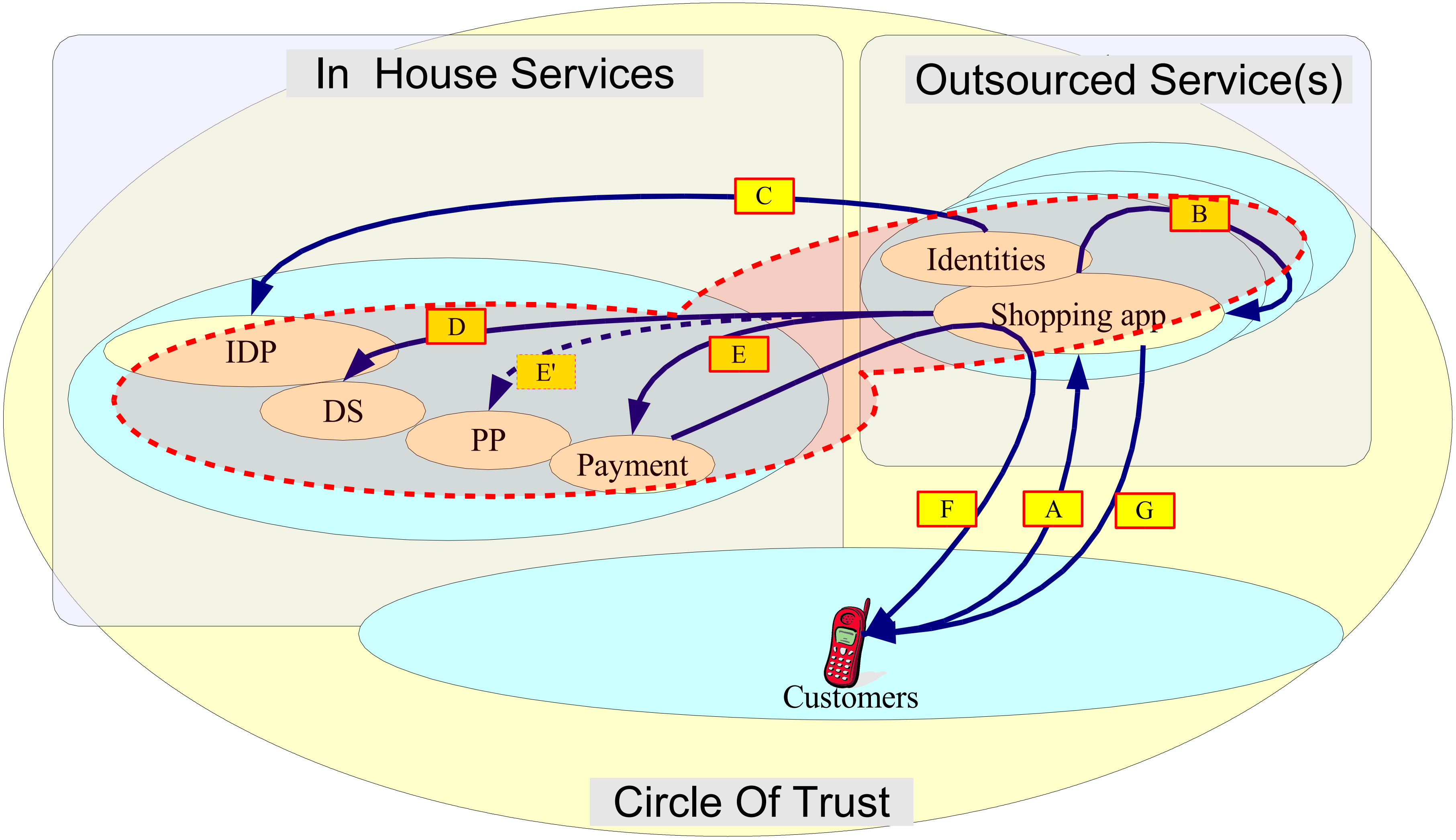
Det skal tilbys en ”Identity Provider” i henhold til Liberty Alliance spesifikasjoner. Løsningen skal beskrives. Det skal angis hvilke versjoner og overordnede funksjoner som støttes.

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 shalll be described. It shall be indicated which versions and which high level functions are supported.

Basic CoT *(outsourcing of services)*



Qualification

Before doing anything,identify what type of deployment it will be !

- Who will serve as an SP? IDP?
- Will users of SP act on their own behalf or do users belong to an enterprise?
- Will each SP allow federation to each IDP or will it be an IDP proxy situation?
- Failure to clarify this at the beginning will lead to a lot of confusion and cross-purpose discussion.

Account Creation/Federation

Which one, How to

- Manual user registration and federation
  - Good for individual consumer case when no enterprise third party to bulk federate for them.
  - Will require very good instructions/explanation
- Bulk account creation and/or federation
  - Programmatically mimic LDAP/SGDB entries
  - Generate login/passed – never used by user
  - Cookie indicating preferred IDP will be missing
  - List of IDPs page may therefore be needed
  - Lengthy list of IDPs (i.e.100++) cumbersome
  - Consider use of customer-specific or IDP-specific start page or URL.

Access Control

SP is responsible for securing access.

For each SP, identify data needed for access control decisions and where it will come from.

- For individual consumers may come from user.
- For outsourcing scenario, data needed may be split between SP and IDP.
  - Attributes can be sent in a bulk feed.
  - SP application can use SAML
  - Can use provisioning/sync solution between SP and IDP to better leverage capabilities of an access management type of product.

Support

How to support someone you don't know ?

For each SP and IDP, identify potential user issues, and how support will be provided by SP and IDP.

- User cannot login, can't access app, data wrong,...
- Identify how users will report a problem
- Identify first responder, escalation paths
- Identify how each responder will
  - Be able to identify user's account
  - Be able to contact user later to ask more questions
  - Gets tricky if user has different ID at SP and IDP
  - User likely to forget SP ID when accounts federated

Logout

Local and/or Global logout both possible

- Bigger issue than it initially seems
- Providing just one may cause issues
  - Users do local logout, leave global session, walk away from browser
  - Users might avoid use of global logout thinking they have more work to do.
  - Best to support both, educate users on differences
  - If you must do just one, choose global logout

SSO expectations

Sign Sign One & Simplified Sign One

- Set expectation appropriately
  - Logins to hardware devices
  - Logins to networks (VPNs etc)
  - Logins to applications
  - Different levels of authentication (i.e. single versus dual factor)
- “Simplified Sign On” may be better term

Monitoring

- Obvious
  - Monitor HW, OS on all component servers (app, authN service, authZ service, storage)
- Proactive
  - Monitor CPU, number of connections, response time and set acceptability threshold values for each.
- Possible Glitch
  - Monitor federated login with synthetic transactions. IDP may be best positioned to do so if access to IDP is restricted.

Business Agreements

- Many other legal documents typically exist
  - Sales contracts, Purchase Orders, Statements of Work, Service Level Agreements, Contract approvals, Consulting Services agreements etc.
- Liberty-related agreements need to relate to other agreements
- Add Liberty-specific terms to existing SOW/SLA templates
  - Liberty compliance, adding/removing COT members, joining other COTs, federation, authN levels, session timeouts, adding/removing users, policy enforcement

Production Deployment

- There is a world of difference between doing this in a lab and the real world. Deploy and test as early as possible in the 'real' environment.
- Hardened environments
- Firewalls & firewall rules
- Network & Load balancers
- Router ACLs
- Certificates
- DNS and mappings

Liberty Summary

- A free standard focusing on:
  - *Privacy*
  - *Security*
  - *Interoperability*
- An industrial reality:
  - *Certified to latest spec products available*
  - *Already proven in production*
- Return of experience available
  - *Deployment paper*
  - *Consulting services*

http://www.projectliberty.org/

Fulup Ar Foll
fulup@sun.com