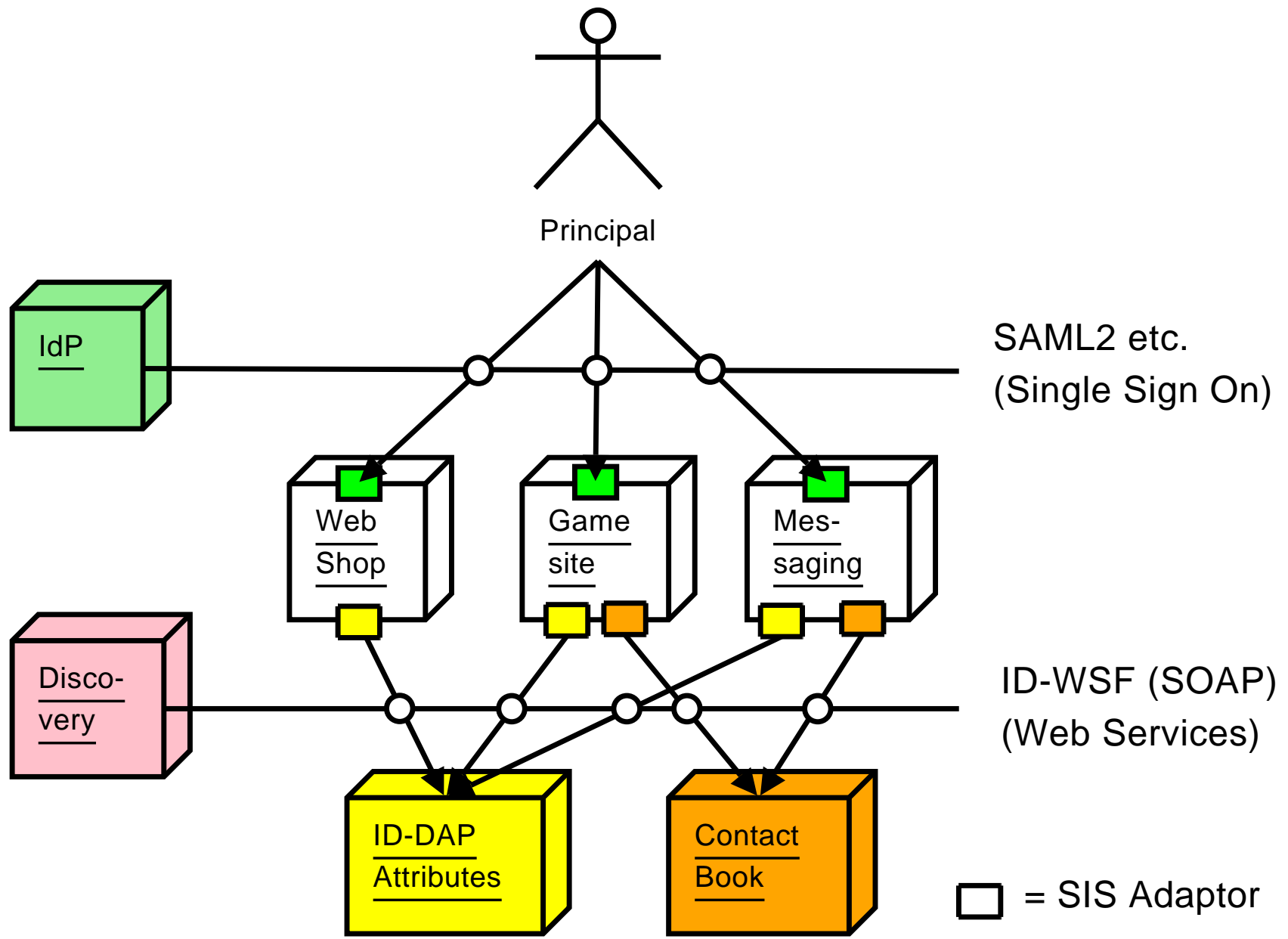


Liberty eGovt BOF

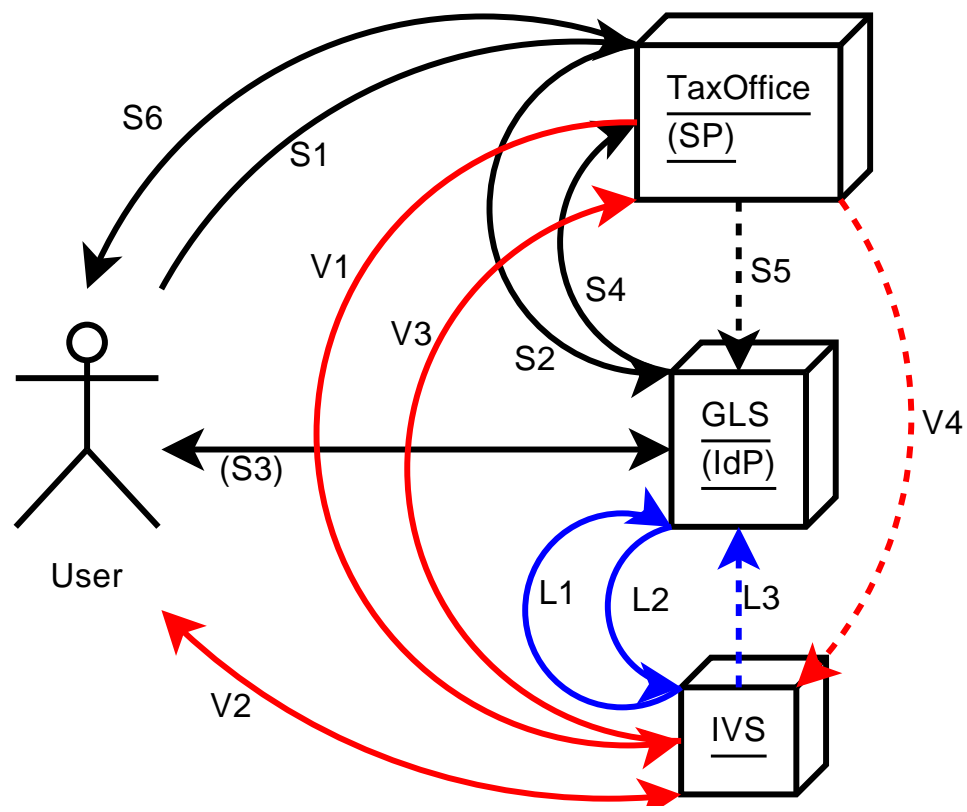
Santa Clara, March 10, 2008

Sampo Kellomäki (sampo@symlabs.com)



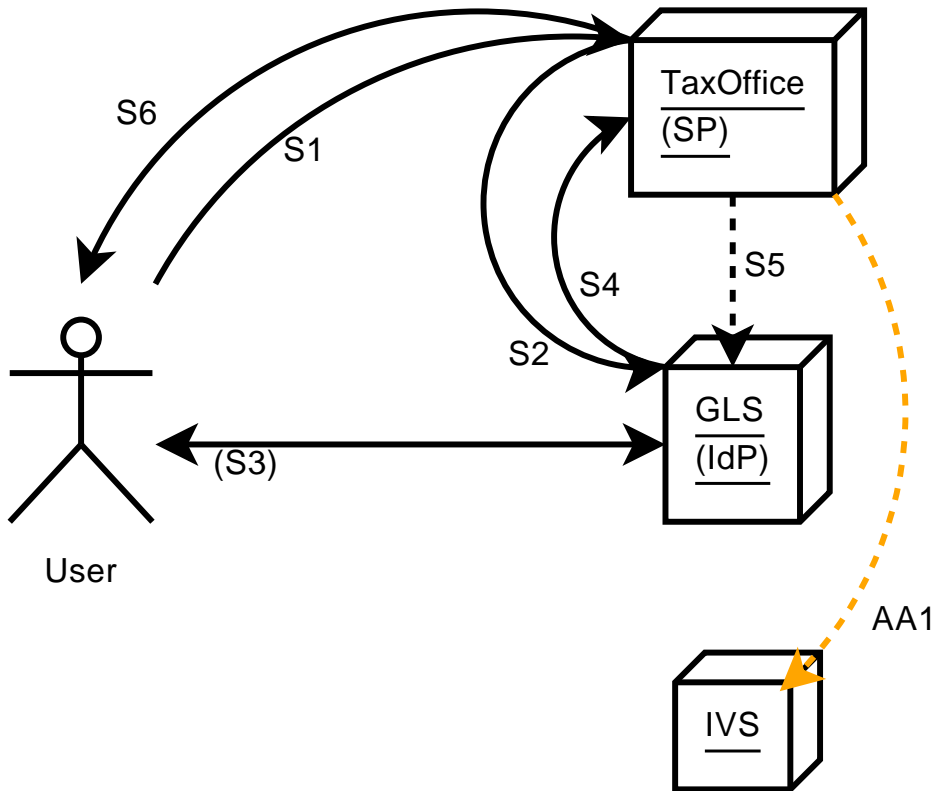
eGovt SIG: One Year Later

- Pushed to OASIS the authentication contexts
 - What is the status on these?
 - Any plans by governments to actually adopt them?
- "Query Extension for SAML AuthnRequest" ready to go to SSTC
- "Profile for Use of DisplayName" ready to go to SSTC
- Several eGovt profile documents have matured
- Still no full consensus on scope (narrow vs. wide)
- Still no full clarity on Artifact vs. POST



- Direct Two IdPs Approach
- S1 User accesses SP
 - S2 SP redirects to GLS (IdP)
 - S3 GLS authenticates user
 - S4 GLS redirects user to SP with artifact
 - S5 SP uses back channel to get SAML assertion
 - V1 SP needs to provision user, redirect to IVS
 - L1 IVS redirects user to GLS for authentication
 - L2 GLS already has user session, redirect back to IVS
 - L3 IVS gets the SAML assertion using back channel
 - V2 IVS asks user consent for attribute release
 - V3 IVS redirects user to SP with artifact
 - V4 SP fetches the attributes as SAML assertion
 - S6 SP delivers government service to user

v0.4 (SK, 20070617)



IVS as SAML Attribute Authority Approach

S1 User accesses SP

S2 SP redirects to GLS (IdP)

S3 GLS authenticates user

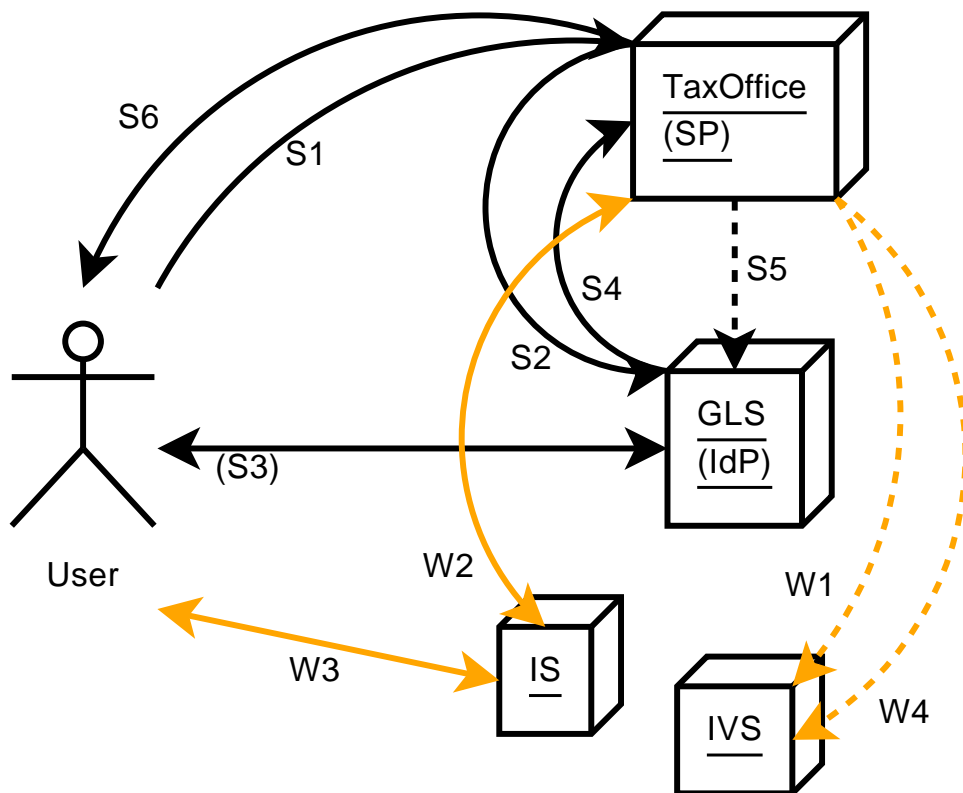
S4 GLS redirects user to SP with artifact

S5 SP uses back channel to get SAML assertion

AA1 SP performs attribute query using identifier
obtained in S5 (id is shared between GLS and IVS)

S6 SP delivers government service to user

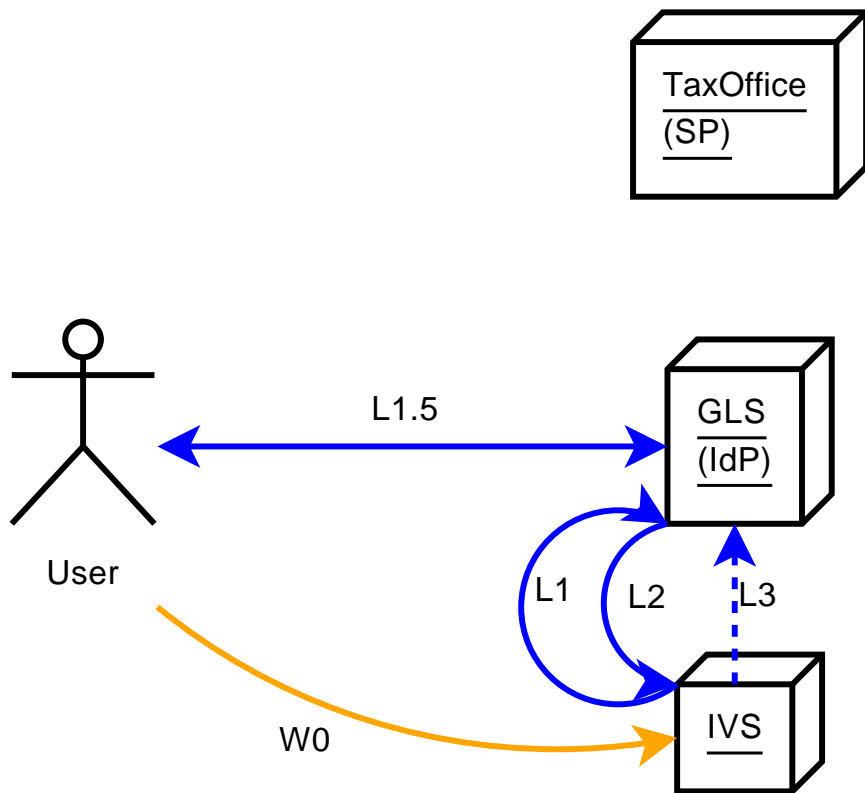
v0.4 (SK, 20070617)



WSF Call with Web Interaction Approach

- S1 User accesses SP
- S2 SP redirects to GLS (IdP)
- S3 GLS authenticates user
- S4 GLS redirects user to SP with artifact
- S5 SP uses back channel to get SAML assertion
- W1 SP needs to provision user, call IVS
- W2 In return to W1 IVS requests user to be redirected to Interaction Service
- W3 IS asks user to select attributes to release
- W4 SP retries the Web Service call to IVS, this time successful as the confirmation exists.
- S6 SP delivers government service to user

v0.4 (SK, 20070617)



Preparatory Step for WSF Approach

W0 User registers at IVS and links his GLS identity

L1 IVS redirects user to GLS for authentication

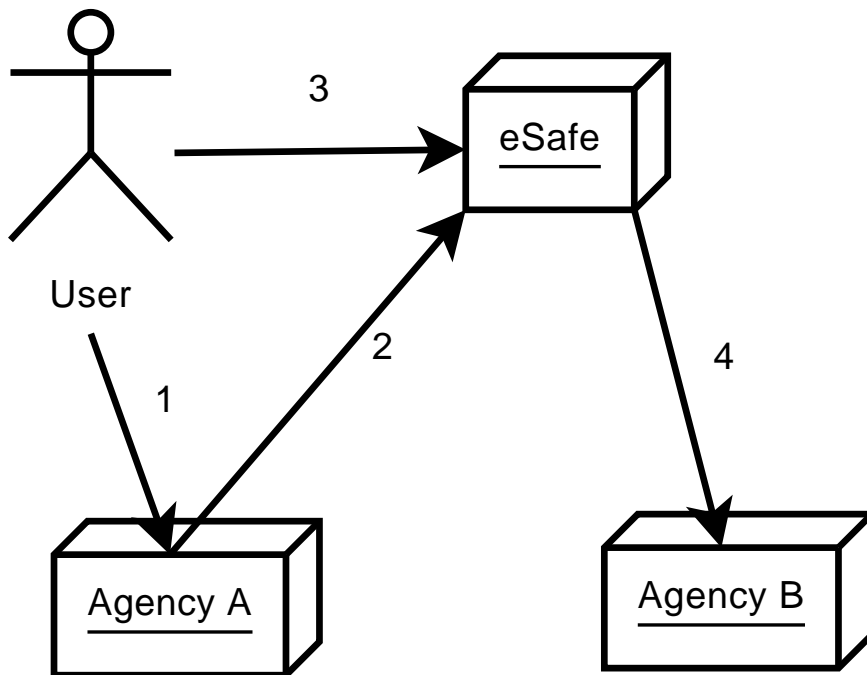
L1.5 GLS authenticates the user (if no session)

L2 Redirect back to IVS

L3 IVS gets the SAML assertion using back channel

Now user has a pseudonym at IVS.

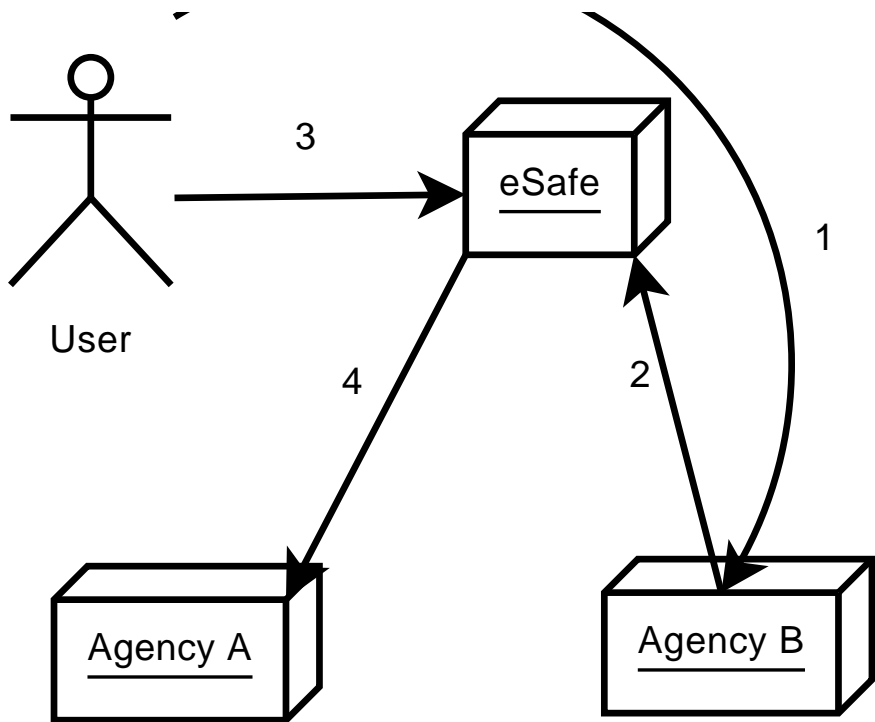
v0.4 (SK, 20070617)



eSafe Pull Model

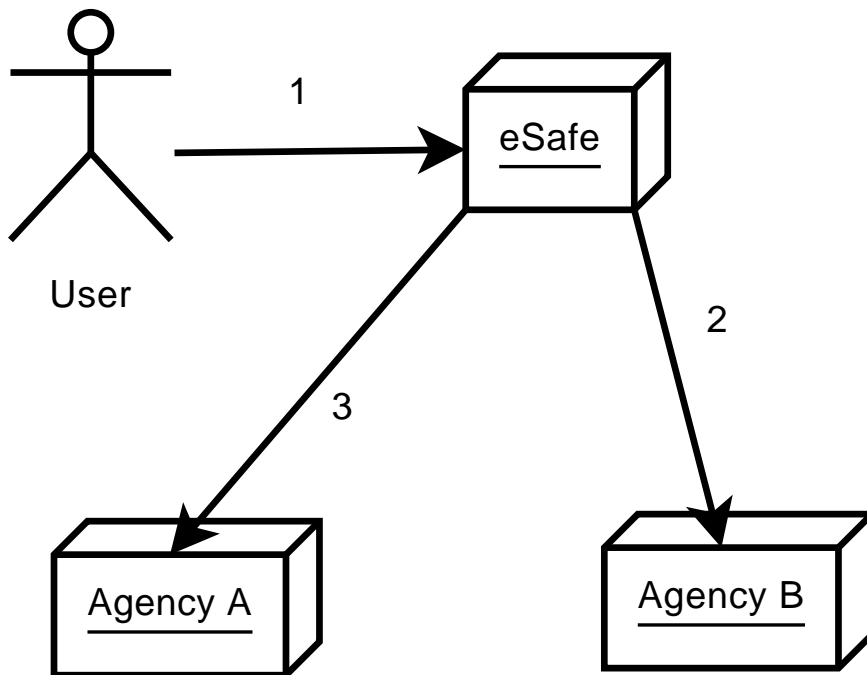
1. User request operation that needs data from Agency A
2. Agency A tries to get it from eSafe
3. eSafe asks user consent
4. eSafe gets the data from Agency B and relays it back to Agency A so that original operation can complete.

N.B. If data is already in eSafe, step 4 is omitted.



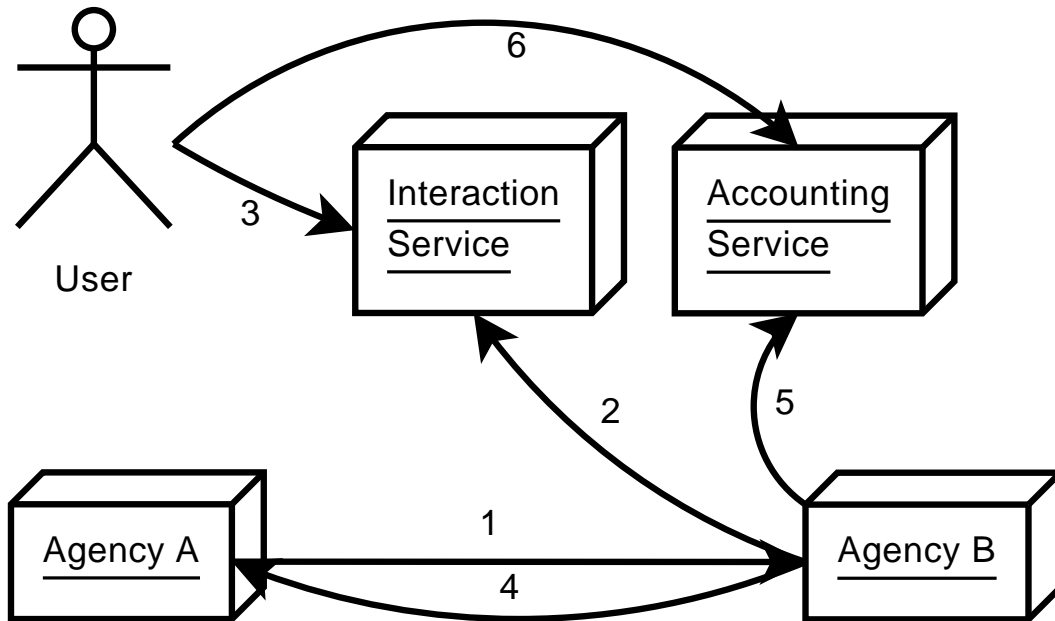
eSafe Push model

1. User goes to data and sends it to Agency A
2. Agency B sends the data to eSafe
3. eSafe asks users consent for sharing
4. eSafe sends the data to Agency A. Presumat Agency A can now complete some operation that was pending required data.



eSafe Portal Model

1. User triggers an operation at eSafe. eSafe knows that the operation is executed at Agency A, but involves data available from Agency B
2. eSafe fetches the data (if not already in eSafe)
3. eSafe pushes the data to Agency A and instructs it to perform the operation.



Direct Data Sharing Between Agencies

1. Agency A requests information
2. Agency B requests user consent
3. User consents to release
4. Agency B releases information
5. Agency B reports release to Accounting
6. Later, user sees audit log

4 Liberty Tool Pack

- SAML SSO
 - Unique or
 - Sector based or
 - even pseudonymous IDs
- ID-WSF web services
 - discovery as authorization point
 - same ID properties as SSO
- ID Mapping Service or SAML ID Mapping
 - Connect sector based IDs
- People Service
 - act in role
 - delegation
- "Managed" Digital signatures based on strong SSO / DSS

- non-repudiation in the Norway sense

5 Acronym Expansion

ID-WSF Liberty Alliance Identity Web Services Framework

IdP Identity Provider (SAML role, asserting party)

SP Service Provider (e.g. web site) (SAML role, relying party)

CoT Circle of Trust: a group of SPs and the IdP(s) they trust

WSC Web Services Client

WSP Web Services Provider

DS Discovery Service

TokM Token Mapping Service

PS People Service

EPR End Point Reference (URL + metadata and possibly credentials)