Mon Service Public

- Case study and Mapping to SAML/Liberty specifications

Gaël Gourmelen - France Telecom
23/04/2007
Agenda

- Brief presentation of the "Mon Service Public" project (main features)

- Detailed use-cases:
  - SSO and Federation
  - Attribute sharing
  - Liberty flows
  - Focus on "Mon Service Public" specificities regarding Liberty Alliance specifications or implementations of these specifications (products)
A personalized portal mon.Service-Public.fr will enable every citizen to set up his or her own home page to access all the online public services of concern to him or her. Users will thus be able to access all their official paperwork.
1. Central Access Point
2. Single Sign On

Global Identity Management Solution based on Liberty Alliance specifications

Identity Federation, no Unique Identifier

One MSP account / several authentication ways (user / pwd, SMS challenge, certificates)

Federation with different kinds of eGov accounts

MSP

Account Dupont

Account Durand

M ME DURAND

M DUPONT

Other e-ID

Services provided by public sectors

Health Care
- Refund
  - Personal account M Dupont- N° 85651

Job agency
- Researches
  - Personnal account N° 15646746

Tax administration
- Tax account
  - Family account Durand - N° 654832

Seamless adm
- Changement d’adresse
  - Procedure Id N° 694125

Personal account M Dupont- N° 85651

Procedure Id N° 694125

Tax account

Family account Durand - N° 654832

Researches

Personnal account N° 15646746

Refund

Health Care
An e-Safe / briefcase to store personal data and dematerialized official documents (diplomas, civil register certificates, etc…) which the user can obtain from the civil service and submit to the authorities to complete other procedures.
A Dashboard to give the end user a unified perception of his / her interactions with public services: messaging, documents, information...

1. Central Access Point
2. Single Sign On
3. Personal Data Storage and Exchange
4. Focal Communication Center
Agenda

- Brief presentation of the "Mon Service Public" project (main features)

- Detailed use-cases:
  - SSO and Federation
  - Attribute sharing
  - Liberty flows
  - Focus on "Mon Service Public" specificities regarding Liberty Alliance specifications or implementations of these specifications (products)
Use-cases: SSO & Federation

- **The SSO and Federation processes** can be both initiated from "Mon Service Public" portal (dashboard) or from "partner site".
Use-cases: SSO & Federation

- The kinematics are the same in both cases (if initiated from the dashboard, the user is first redirected to the "partner site" – SP).
Use-cases: SSO & Federation

- Standard use of the Liberty Alliance ID-FF specifications (ID-FF 1.2)
  … with however the following specificities:

- **Requirement:** One single account on the "Mon Service Public" portal (IDP) can be federated with multiple accounts on SP side.

- The Liberty Alliance ID-FF specifications **do not prevent** the implementation of this requirement **but** in that case the "link" between the multiple accounts at a same SP is established and maintained on SP side only (as according to ID-FF specifications, for one single account on the IDP, only one federation alias is associated to one SP).

  *This was considered as not acceptable (mainly from privacy and user experience standpoints)*

*The decision has been taken to instead support "multi-federation" on IDP side (and thus managing multiple federation aliases on IDP side for one single IDP account and one given SP)*
Use-cases: SSO & Federation

This has some impacts on:

- Management and storage of federations on IDP side.

  bob@msp
  ✓ ANPE : Alias=123 Index=0
  ✓ ANPE : Alias=456 Index=1
  ✓ CAF : Alias=998 Index=0
  ✓ …

- SSO & Federation Interfaces exposed by "Mon Service Public" IDP.
  - Specific processing rule associated with the parameter "NameIDPolicy=federated" of a <lib:AuthnRequest>.
  - Introduction of a new parameter during SSO from the dashboard to enable the IDP to identify the right federation ("FederationIndex").
Use-cases: SSO & Federation

- SSO from the "Mon Service Public" portal/dashboard:

  1. **Initiate SSO process** (with requested authentication context)
  2. **Authentication of the principal** (if necessary)
  3. **artifact**
  4. **<lib:Authnrequest> + FederationIndex**
  5. **<samlp:Request>**
  6. **<samlp:Response>**
  7. **FederationIndex**
  8. Initiate SSO process (with requested authentication context)
Use-cases: Attribute sharing

- The partner sites (SPs/WSCs) will rely on the Liberty Alliance ID-WSF framework to query the principal's e-Safe / briefcase (SP/WSP) to provide the following features:
  - Automatic form filling (and update)
  - Retrieval of dematerialized documents that can be needed to complete the procedures at these partner sites
  - …
Use-cases: Attribute sharing

The user wants to auto-fill the form or attach a document to the current procedure.

ID-FF one-time federation flows (redirection) if needed

ID-WSF 1.1 Interaction Service
Use-cases: Attribute sharing

- Again, this is a **standard use of the Liberty Alliance specifications** (ID-WSF 1.1).

- **Just wanted to highlight the two following points:**
  - The ID-WSF framework is not only used to exchange attributes or profile data but also **documents** (binary content).
  - The interaction with the principal (through the "ID-WSF 1.1 Interaction Service" protocol) is not only used to collect consent but also to **select the document** to be exchanged.
Some other interesting use-cases exist, related to:

- **Inter-COT (IDP to IDP federation with bi-directional SSO)**
- **People Service (contacts)**
- ...

Thank you !