Access to Identity-Enabled Web Services in Cross Border, Inter-Federation Scenarios

Conor Cahill, Intel
Carolina Canales-Valenzuela, Ericsson
Sampo Kellomäki, Symlabs
Mikko Laukkanen, TeliaSonera
Use Cases and Business Motivation

Mikko Laukkanen, TeliaSonera
A Single Circle of Trust

Benefits for the different actors by using Liberty technologies

- Fees for WSP access
- Potentially a large and trusted customer base consisting of trusted SPs
- Potentially a large and trusted customer base (consisting of IdP customers)
- Outsourcing of authentication and verification of user's identity (precondition of user joining a CoT)
- Customers authenticated in a secure and possibly strong way
- Attributes available about the customers
- No multiple credentials to remember
- Single Sign-on experience
- Attribute management
- Permission-based attribute sharing
- Anonymity
- Trusted SPs
- New business opportunities for the operator (Authentication and DS services, hosting of user's identity-based services)
- Business agreements with SPs and WSPs

Customer relationship

SP/WSC

Business agreement

IdP + DS (+ WSP)

WSP

Circle of Trust

Customer

gets
attributes, accesses identity Web-services

Business agreement

grants attributes

Fees for WSP access

Potentially a large and trusted customer base consisting of trusted SPs

New business opportunities for the operator (Authentication and DS services, hosting of user's identity-based services)

Customer relationship

SP/WSC

Business agreement

IdP + DS (+ WSP)

WSP

Circle of Trust

Customer

gets
attributes, accesses identity Web-services

Business agreement

grants attributes

Fees for WSP access

Potentially a large and trusted customer base consisting of trusted SPs

New business opportunities for the operator (Authentication and DS services, hosting of user's identity-based services)
Interconnected Circles of Trust (Inter-CoT)

Extra benefits for the different actors in the case of Inter-CoT

- Even larger trusted customer base consisting of all customers of the interconnected IdPs
- Possibility to provide a personalized service to an enlarged customer base
- Local credentials and local attributes for accessing foreign services
- Single Sign-On experience among all Circles of Trust
- Large set of trusted SPs of other Circles of Trust
- New business opportunities for IdPs
- Even larger customer base consisting of trusted local and foreign SPs

Customer relationship

Business agreement

Accesses and grants attributes

Accesses and grants attributes

Accesses and grants attributes

IdP + DS (+ WSP)

IdP + DS (+ WSP)

IdP + DS (+ WSP)

IdP + DS (+ WSP)

SP/WSC

WSP

WSP

Circle of Trust B

Circle of Trust A

Even larger trusted customer base consisting of all customers of the interconnected IdPs

Possibility to provide a personalized service to an enlarged customer base

Local credentials and local attributes for accessing foreign services

Single Sign-On experience among all Circles of Trust

Large set of trusted SPs of other Circles of Trust

New business opportunities for IdPs

Even larger customer base consisting of trusted local and foreign SPs

Customer relationship

Business agreement
Business opportunities and use cases

- **Business to customers (B2C) sector**
  - Operators as IdPs and roaming between operator CoTs
    - Hotel booking, sight and restaurant locators, ...
- **Business to business (B2B) sector**
  - E-Government services within a country and between countries
    - For instance, access to the user’s records hosted by another department of the administration
  - E-Healthcare
    - For instance, access to the user’s medical records available in a CoT hosted by another hospital. Also, the pharmaceutical industry is a great example:
      - See [http://www.projectliberty.org/liberty/content/download/2827/18948/file/Alamillo_20CATCert_20-%20Alamillo.pdf](http://www.projectliberty.org/liberty/content/download/2827/18948/file/Alamillo_20CATCert_20-%20Alamillo.pdf) for an excellent example from the Catalan Health Service for an ePrescription service.
- **Universities**
  - Cooperation between universities, e.g., student exchanges
- **Outsourcing of certain (authentication) services**
  - E.g., banks could outsource strong authentication to an operator
- **Enterprises sector**
  - IdP hierarchy or mesh within (large) organizations
Inter-CoT – challenges

- **Business challenges**
  - How to get actors (SPs and IdPs) co-operate in order to realize the Inter-CoT use cases?
  - How should the branding be handled for Inter-CoT?

- **Technical challenges**
  - How can foreign IdP find home IdP for customer authentication?
  - How can foreign SP/WSC find (home) DS for finding WSPs?
  - How can (home) DS trust request from foreign SP/WSC?
  - How can (home) WSP trust request from foreign SP/WSC?
Intra-Federation Use Case

- My addressing info is centralized in a single on-line service
  - Ensure consistency
  - **User-centric**: All info under my control
- No direct business relationship between Amazon.com and My Addressing Info, but TeliaSonera working as **Trusted Third Party**
Inter-Federation Use case

- No direct trust between Boogle Maps and TeliaSonera’s Location
- Leverage Telefónica and TeliaSonera business agreement
In order to understand the solution, it is assumed that the audience is, at least, familiar with:

- SAMLv2 and another typical IdM technologies
- Liberty ID-WSFv2
1. **Discovery Service Proxying**: There exists a trust relationship between the entities operating the DSs of both CoTIs, trust is established by proxying WSC-B’s discovery request through DS-B towards DS-A.

2. **Inter-Federation (Inter-CoT) Discovery**: In this case, it is assumed that WSC-B obtains a direct reference to DS-A, trust is established between both entities by leveraging the already existing trust (business) relationship between DS-A and DS-B.

3. **Direct Access**: In this case, DS-B is able to directly provide a reference to WSP-A, however, this effectively implies that WSP-A is registered in DS-B, and therefore both entities factually belong to the same CoT (any sort of business relationship between them is implied).
Discovery Service Proxying

- Pre-condition: SAMLv2 IdP Proxying happened previously, and so WSC-B has DS-B EPR
- Flow:
  0. Restaurants nearby my current location?
  1. Albert’s Location service?
  2. Albert’s Location service [Requestor = WSC-B]?
  3. Albert’s Location Service EPR [including token for WSP-A]
  4. Albert’s Location Service EPR [including token for WSP-A]
  5. Albert’s Location [including token for WSP-A]?
Discovery Service Proxying - Details

- Fully standard, works out of the box with current specifications, with the exception of.....

- ....Step 2, DS Lookup Query between DS-B and DS-A needs to convey WSC-B’s identifier (apart from the requestor’s, DS-B), for DS-A to be able to appropriately generate token for WSP-A
  - Extension of the DS Query operation (a new element inside the Query element, part of the RequestedService element)
  - Easily implementable as proprietary extensions in specific deployments
Inter-Federation (Inter-CoT) Discovery

- Pre-condition: SAMLv2 IdP Proxying happened previously, and so WSC-B has DS-B EPR
- Flow:
  0. Restaurants nearby?
  2. Albert’s Location service [including token for DS-A, if needed]?
  3. Albert’s Location Service EPR [including token for WSP-A, if needed]
  4. Albert’s Location [including token for WSP-A, if needed]?
Direct Access

- WSP-A registered in DS-B, therefore this is implicitly equivalent to WSP-A belonging to Circle of Trust B.
- Equivalent to Intra-Federation (single-CoT) scenario, “normal” focus of ID-WSF
Conclusions

- Fully standard technology
  - Exception of minor detail in Discovery Service Proxying
- Up and running, working out of the box
  - Full list of products that have passed the Liberty Interoperable certification program is available here: http://www.projectliberty.org/liberty/liberty_interoperable/interoperable_products
- Addresses the needs of organizations of different sectors of the industry, looking to leverage inter-federations for accessing trusted identity Web services even when there is no business relationship between the service requestor and the service provider
Questions?

THANK YOU!