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

Version: 1.0

Abstract:

The following whitepaper describes the different potential options to access identity-based web services in Inter-federation (Inter-CoT[1]) scenarios; i.e., when there is no business relationship between the service requestor and the service provider AND such relationship cannot be inherited from a commonly-trusted third party, such as in typical federation cases - Intra-CoT.

Even if there is such lack of direct business relationship, final interoperability is still possible by (indirect) inheritance of the trust relationship existing among the entities operating the different CoTs.

The solutions proposed in this whitepaper are especially interesting in certain scenarios, such as those associated to roaming situations in the telecommunications industry. They can also be applicable to other industries, such as the eHealth or eGovernment sectors.

Filename: access-to-identity-enabled-services-in-inter-cot-scenarios-v1.0.pdf

[1] CoT – Circle of Trust

Editors:

Carolina Canales-Valenzuela, Ericsson
Sampo Kellomäki, Symlabs

Contributors:

Fulup Ar Foll, SUN
Conor Cahill, Intel
Gaël Gourmelen, Orange
Mikko Laukkanen, Teliasonera
Rob Lockhart, IEEE-ISTO
Antonio Navarro, Symlabs
Pat Patterson, SUN

Notice:

Contents

1 Introduction

The goal of the present paper is to describe the scenario where an application (Service Provider B, SP-B, working as web service consumer WSC-B) wants to access an identity-enabled service (Web Service Provider, WSP-A), and both of them belong to different Circles of Trusts (CoT, as defined in [LibertyGlossary]) or federations. Due to this, it is assumed that, although no direct business agreement exists between SP-B/WSC-B and SP-A/WSC-A, some sort of business agreement exists between the entities operating the IdPs/DSs of both CoTs.

This document explores different mechanisms to achieve this, in particular:

1. **Discovery Service Proxying**: There exists a trust relationship between the entities operating the DSs of both CoTs, 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).

Note that in all of the three scenarios, apart from some sort of business relationship between "distinguished" members of the different CoTs (e.g,, the IdP-DSs), there is a need to be able to establish a direct or derived trust relationship at the PKI level. See [TrustModelsGuidelines] for further information about trust relationships.

Regarding the scenario of a heavily firewalled environment, it seems to be a requirement that each CoT manages its own SPs and firewalling rules. The other CoT's administrators should not have to make any "per SP" configuration.

2 Description

2.1 SSO Using IdP Proxying

The figure below depicts this scenario.

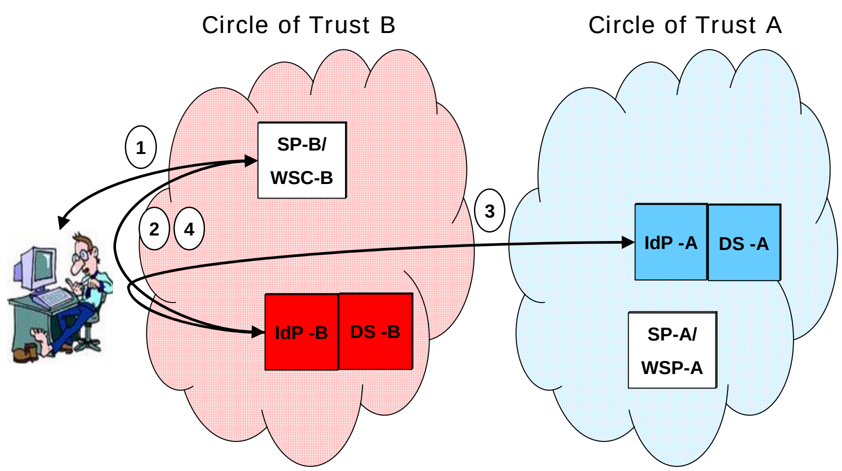

Figure 1: SSO in Inter-CoT (Inter-federation) scenario

In brief, and according to the IdP Proxying functionality as described in [SAMLCore2]:

1. Albert, a user with an account at IdP-A, accesses a page on SP-B which is in the CoT of IdP-B.
2. The SP-B logically contacts IdP-B. Given that SP-B is in the CoT of IdP-B, the access control is natural. This requires a firewall hole between Albert and IdP-B.
3. IdP B proxies the authentication of the user, Albert, to IdP-A by using HTTP redirect. The firewall has to have a hole from Albert to IdP-A. (This seems to be the usual case inside a given CoT.)
4. IdP-B trusts IdP-A to authenticate the user and consumes the assertion from IdP-A and then issues a new assertion to SP-B (including Albert's federation handle as understood by SP-B), i.e., the SP-B only needs to trust the leader of its own CoT, the IdP-B.

The assertion from IdP-B towards SP-B has discovery bootstrap information pointing to DS-B. Such information can be used to discover services in CoT-B and to perform Discovery Proxying to find services in CoT-A. See Section 2.2.1 "Web Services Invocation Using DS Proxying."

In the Inter-CoT Discovery approach in Section 2.2.2, IdP-B would include a reference to Albert's DS (DS-A) in the assertion returned to SP-B. Such DS-A EPR is extracted from the SAML token provided by IdP-A.

2.2 Access to Identity-enabled Web Services

Once SP-B has obtained a valid SSO token for Albert (containing references to, at least, DS-B, but maybe also to DS-A), SP-B tries to discover and access some web services exposing resources belonging to Albert (e.g., profile information for service personalization). These web service providers are located in Albert's CoT (CoT-A, exclusively, not in CoT-B).

2.2.1 Web Services Invocation Using DS Proxying

The figure below depicts this scenario.

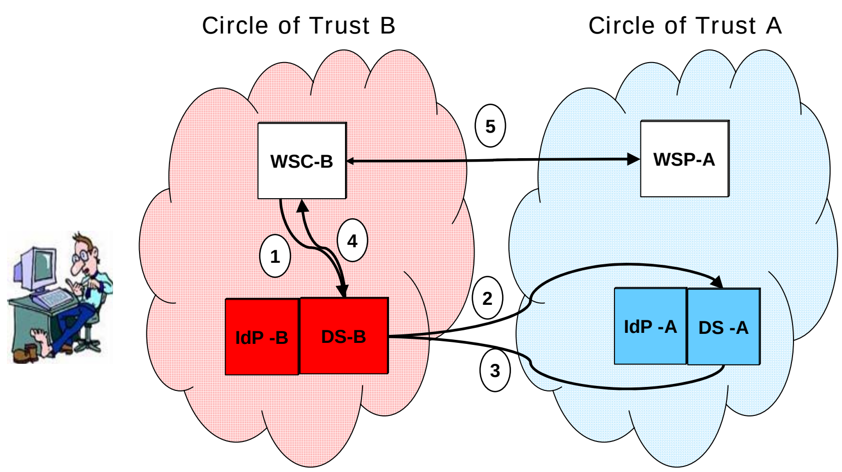

Figure 2: Inter-CoT (Inter-federation) Access to Id-based web services via DS Proxying

1 SP-B, acting as WSC-B, wants to invoke an identity service of Albert (ultimately provided by WSP-A, but SP-B doesn't know about this, yet). It starts by sending a discovery request to DS-B (the CoT agreements establish that this bootstrapping information is always present in the SSO token). Since DS-B is the natural member of CoT of SP-B, a firewall hole will exist.

2 DS-B detects that Albert does not belong to its CoT, but to another CoT, and proxies the discovery request to DS-A.

DS-B adds a new field to the discovery request indicating that this is a proxied request from WSC-B. DS-A can then make the appropriate credential/access decisions based upon that info.

Note that this indication is not standard and would require to be specified as an extension of the DS Query operation (a new element inside the Query element, part of the RequestedService element).

How does DS-B know that it is supposed to use DS-A, and how it is to access DS-A? Several possibilities exist here. The first one corresponds to the "official" recommendation of the standard. The rest represent a non-exhaustive enumeration of possible examples, and are provided for informational purposes, only:

a Due to previous business agreements, DS-B is aware of the information necessary to query the DS of the users of CoT-A (DS-A's EPR preconfigured upon set up).

b IdP-B, when it consumed the assertion from IdP-A, stashed the DS-A bootstrap from IdP-A somewhere where DS-B can find it. This, however, requires that DS-B caches such information for each of the users of CoT-A accessing services of CoT-B.

c DS-A reference (EPR) was included in the SSO token provided to SP-B as part of DS-B bootstrap info (e.g., in an AttributeStatement of the SAML token to be presented to DS-B). SP-B includes such a token in its request to DS-B, and DS-B is able to extract such DS-A information from the token. This alternative has the advantage that it does not require DS-B to cache DS-A information for each of the users of CoT-A.

3 DS-A issues WSP-A EPR which includes necessary security token(s) for access to WSP-A by WSC-B, and returns that to DS-B. Note that the SubjectConfirmation element of such tokens (assuming SAML tokens) should be set to WSC-B/SP-B, rather than DS-B, as would normally be the case.

A firewall hole is needed between DS-B and DS-A. This is feasible because there is only one DS in CoT-B, and often DS-B and IdP-B are the same machine so the hole may already exist to facilitate IdP proxying. There is no need to open a hole between WSC-B/SP-B and DS-A.

4 DS-B response to WSC-B/SP-B.

5 WSC-B/SP-B calls WSP-A presenting the token provided by DS-B.

WSP-A validates the token (assuming SAML token) according to the processing guidelines in [SAMLCore2], i.e., validation of SubjectConfirmation element, validation of signature in the token as signed by DS-A (who is a natural CoT partner of WSP-A), etc.

Regarding validation of the SubjectConfirmation element, this is an implementation-specific detail which can be materialized by means of multiple mechanisms, but, in general, all of them are based on ensuring that WSC-B's certificates matches the presenter of the token, for instance by:

a Verifying that the CommonName in the WSC-B/SP-B's TLS certificate is the proper prefix of WSC-B/SP-B's Provider ID, as reflected in the intended SubjectConfirmation field of the SAML token.

b Verifying that the CommonName in the WSC-B/SP-B's signing certificate (assuming the request was signed) is proper prefix of WSC-B/SP-B's ProviderID, as reflected in the intended SubjectConfirmation field of the SAML token.

For the signature and certificate checks in (a) and (b) to work, the certificates have to be issued by some CA which WSP-A is willing to trust. (Presumably, this CA can be trusted to enforce required policies.)

2.2.2 Inter-Federation (Inter-CoT) Discovery

In this case, WSC-B obtains a direct reference to DS-A, and is therefore able to directly query such entity. DS-B works as a trust broker, in this case, by generating a token that will be used to bridge trust between WSC-B and DS-A. Note that such token could be issued with different possible subject confirmation mechanisms (e.g., it could be a bearer token, a HoK token, etc). This depends on the deployment scenario, and the degree of trust being required by the different entities. In a “degenerated” model, WSC-B could not need to present any security token in order to access DS-A (being trust-established by some other mechanisms, such as by extending the “Authentication” trust level, as reflected in [TrustModelGuidelines]: WSC-B simply proves to be the owner of a certificate issued by a Certification Authority that DS-A is willing to trust, directly or indirectly, together with providing Albert’s handle in DS-A.

The following diagram reflects the associated message flow:

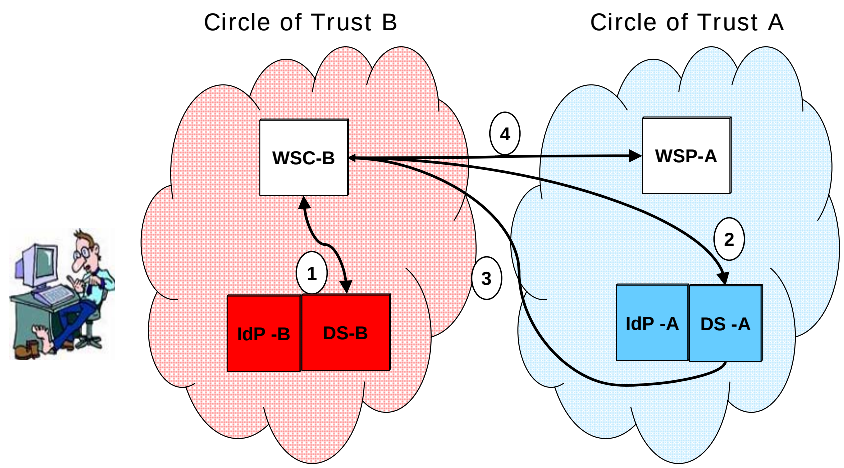

Figure 3: Inter-CoT Access to Id-Based Web Services via Inter-CoT Discovery

1 SP-B, acting as a WSC, queries DS-B asking for Albert's identity service. As a result of this DS query, it obtains all the information and associated credentials/tokens (EPR) to contact, directly, DS-A with IDP-B/DS-B acting as a Trusted Third Party helping to authenticate SP-B/WSC-B towards DS-A: See the description on different models, above. As reflected in the descriptive text of this section, such credential could be:

a a SAML HoK token,

b a bearer token (SAML or otherwise),

c no security credential but rather an identity token conveying Albert's handle in DS-A ("degenerated" model), in case the trust between DS-A and WSC-B could be established in some other way, as mentioned above.

Note that the DS-A EPR information could also be obtained as a result of the SSO operation (directly returned by IdP-B/DS-B, according to CoT-B bylaws applying to users belonging to CoT-A), and therefore this step would not be needed.

2 SP-B/WSC-B will directly contact DS-A, and authenticate itself through any of the authentication mechanisms defined in the Liberty ID-WSF specifications. This will also depend on the type of token generated by DS-B; for instance, by proving possession of the key reflected in the SAML HoK assertion signed by IDP-B/DS-B, in case (1.a) above.

DS-A validates the received <wsse:Security> header that authenticates SP-B/WSC-B as it trusts IDP-B/DS-B, based on the Inter-CoT trust relationship that exists between IDP-B/DS-B and IDP-A/DS-A.

Note that in the “degenerated” model, the validation of the identity token conveying Albert’s handle in DS-A might not directly help to build trust between WSC-B and WSP-A. Trust will instead be directly from already existing trust on the PKI infrastructure.

3 DS-A, in turn, returns WSP-A’s EPR with associated credential to enable SP-B/WSC-B to query WSP-A (no security token in “degenerated” model, simply WSP-A contact information including Albert’s identity token for WSP-A).

4 SP-B/WSC-B directly contacts WSP-A, and can authenticate itself according to the mechanism specified in WSP-A’s EPR, as provided by DS-A (for instance, relying on the SAML HoK assertion signed by DS-A). A full description of this peer-authentication functionality is provided in [LibertySecMech20].

WSP-A validates the received <wsse:Security> header that authenticates SP-B/WSC as it trusts DS-A (both entities belonging to the same CoT).

2.2.3 Direct Access

As stated in previous sections, in this scenario, WSC-B would query DS-B, and would be able to obtain a direct reference (together with the appropriate credentials) to access WSP-A. This would be equivalent to saying that WSP-A is directly registered in DS-B, which is therefore factually-equivalent to belonging to CoT-A (business relationship between DS-B and WSP-A, DS-B works as trust broker between WSC-B and WSP-A).

This scenario is, in practical terms, equivalent to the Intra-CoT scenario. Therefore, no further description seems to be needed.

2.3 Metadata Distribution in Inter-CoT Scenarios

Interoperability in federated scenarios typically requires agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so forth. In these types of scenarios, this information is usually described as metadata information, and it becomes even more relevant in Inter-CoT environments. Even if the different network entities will have commonly shared this sort of information with the members of its own CoT, for interoperability purposes, however, it seems necessary that all or at least some part of such metadata information is also made available to partners of another CoT with whom there is no *a priori* business relationship, but one could be established *on the fly*. In practice, there are several potential ways of distributing such information, let’s name a few for informational purposes:

a **Push from Central Authority**: A central authority (perhaps the DS/IdP operator) pushes the authorized metadata to the members of its own CoT.

This could be by means of LDAP replication, synchronizing flat files[3] with the metadata in XML format (as standardized by the OASIS SSTC), or some other types of enterprise synchronization procedures.

b **Pull from central authority**: This is very similar to the previously described mechanisms (Push) and much of the database backend standardization discussion applies.

c **Well-Known-Location (**WKL, as defined in [SAMLMeta2], Section 4.1 "Publication and Resolution via Well-Known Location") **plus PKI**: Ubiquitous use of a Well-Known-Location to get metadata and then use PKI to trust it.

d **Well-Known-Location plus central authority distribution of trusted ProviderIDs**: Ubiquitous use of a well-known-location to get metadata and then use central authority to distribute list of trusted ProviderIDs (push or pull).

The main advantage of this approach is that the trust list is very simple so even junior system administrators are likely to get it right. Ideally, the format of this list should be standardized (one proposal would be: first line: "issuerprovid:issuenumber:expiry:futexp," followed by ProviderIDs of members of the CoT, one per line, separated by Unix newline (0x0a)). However, given the simplicity of this approach, even a non-standard format is unlikely to cause any problems.

The main disadvantage of this approach is that the well-known-location approach is not supported by many vendors (or, at least, as part of the default product configuration).

e **Well-Known-Location for metadata, OCSP for trust**: Ubiquitous use of WKL to get metadata and then use OCSP [RFC2560] to check trust from central authority.

[2] For instance, by making use of tools such as “rsync," see http://rsync.samba.org/

3 Conclusion

In summary, access to identity-based web services in scenarios where there is no direct business relationship between the service requestor and the service provider can be achieved by leveraging a previously-existing business relationship established between some “distinguished” members of the CoT (for instance, the entities operating the IdP-DS).

As an example, this seems to be of special applicability in roaming scenarios typical of the telecommunication industry, by leveraging (and possibly extending) the already-existing agreements among the different operators. It can also be of applicability to other industries, such as the eHealth or eGovernment sectors.

To conclude, all the scenarios described in this paper are fully interoperable and can be achieved by direct applicability of the Liberty Alliance’s specification set, with the following exception:

- Section 2.2.1(DS Proxying), extension of the RequestedService element inside the DS Query operation is needed in order to signal to DS-A that the entity to be presenting the DS-A-generated token (WSC-B) is different from the DS requestor (DS-B).

Some other enhancement proposals (although not explicitly required for interoperability):

- Inter-CoT Metadata distribution, define the format of the file containing the list of trusted ProviderIds, to be distributed by the central authority of each CoT.

Even if these specific topics are not directly addressed by the standard, it seems rather immediate to handle them as proprietary extensions in specific deployments.

4 References

[LibertyGlossary] Hodges, Jeff, eds. "Liberty Technical Glossary," Version v2.0, Liberty Alliance Project (30 July, 2006). http://www.projectliberty.org/liberty/content/download/868/6180/file/liberty-glossary-v2.0.pdf

[LibertySecMech20]. Hirsch, Frederick, eds. "Liberty ID-WSF Security Mechanisms Core," Version 2.0 errata v1.0, Liberty Alliance Project (09 July, 2007)., http://www.projectliberty.org/liberty/content/download/893/6255/file/liberty-idwsf-security-mechanisms-core-2.0-errata-v1.0.pdf

[TrustModelGuidelines] OASIS “Trust Models Guidelines," John Linn (RSA) et al, http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf

[SAMLCore2] Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds. (15 March 2005). "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," SAML V2.0, OASIS Standard, Organization for the Advancement of Structured Information Standards, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C., eds. (June 1999). "X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP," RFC 2560, The Internet Engineering Task Force, http://tools.ietf.org/html/rfc2560

[SAMLMeta2], Cantor, Scott, Moreh, Jahan, Philpott, Rob, Maler, Eve, eds. (15 March 2005). "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0," SAML V2.0, OASIS Standard, Organization for the Advancement of Structured Information Standards http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf