>

OIO WS-Trust Deployment Profile

Version 1.1

Agency for Digitisation
February 2017

Content >

Document History

Date	Version	Initials	Changes
09-06-2009	0.9	SPN	Document ready for OIO public hearing
08-09-2009	1.0	TG	Document updated after public hearing (only editorial changes)
22-01-2017	1.1	TG	Improved clarity of requirements by usage of RFC 2119. Binding switched to OIO IDWS SOAP profile instead of Liberty Basic SOAP Binding, References to deprecated Liberty Profiles have been removed and references have been updated.

Introduction

This profile describes how to deploy the OIO WS-Trust profile in the Danish eGovernment sector. It specifies bindings, policies, mapping of claims to OIOSAML attributes and other details.
Note that the profile only is relevant for accessing a Security Token Service (STS) in a foreign security domain. This profile does not prescribe which bindings to use when accessing an STS that resides in the same security domain as the requester.

Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in RFC2119.

The following abbreviations are used:

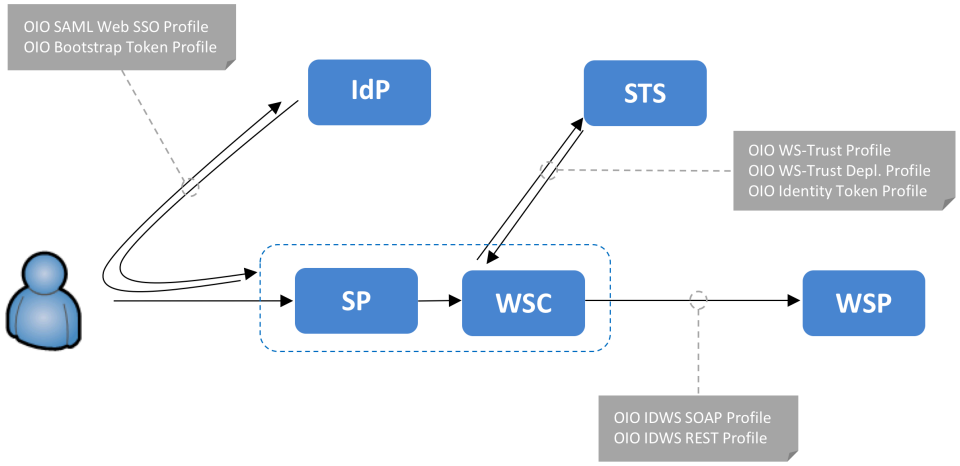
- Identity Provider (IdP) - a federated authentication service (typically based on SAML 2.0).
- Service Provider (SP) - a web application or portal allowing federated log-in using an Identity Provider.
- Security Token Service (STS) - a service issuing security tokens for web service invocations (typically based on WS-Trust).
- Web Service Consumer (WSC) - an application or client that needs to invoke a foreign identity-based web service in context of a particular user.
- Web Service Provider (WSP) - a provider of an identity-based web service that allows access based on a security token issued by a trusted STS.

Related profiles

A number of other documents are closely related:

- The [Scenarios] document describes the overall business goals and requirements within Danish eGovernment and shows how the different OIO profiles are combined to achieve these.
- The [OIO-WST] document contains a profile of WS-Trust specifying restrictions on WS-Trust messages and details regarding processing rules.
- The OIO SAML Profile for Identity Tokens [OIO-IDT] defines requirements for security tokens issued by Security Token Services.

The figure below illustrates the "big picture" of OIO IDWS profiles in a typical scenario:



The reader is assumed to be familiar with WS-Trust [WST] and SAML.

Deployment Requirements

Binding

When deploying the [OIO-WST] profile a binding is required. This profile mandates use of the OIO IDWS SOAP Binding [OIO-SOAP].

In essence, the OIO IDWS SOAP Binding implies:

- A request message MUST include the following SOAP headers: `<wsa:MessageID>` and `<wsse:Security>`.
- A response message MUST include the following SOAP headers: `<wsa:MessageID>`, `<wsa:RelatesTo>` and `<wsse:Security>`.
- The security header MUST include a `<wsu:Timestamp>` containing a `<wsu:Created>` element.
- Request and response messages MUST be signed and the signature MUST cover all SOAP headers, all security tokens and the SOAP body.
- Security tokens in the form of SAML Assertions or BinarySecurityTokens containing certificates MAY be included to authenticate the sender/user and/or establish trust in the sender's signing key.
- If the message includes holder-of-key assertions, the key referenced in the assertion MUST match the key that signed the message.
- A secure transport protocol (e.g. TLS) MUST be used.

Note the above list is informational – the normative requirements and further details can be found in the profile document [OIO-SOAP].

Bootstrap token

The [OIO-WST] profile does not specify how a rich client or service provider obtains a bootstrap token for the user that can be presented to the (initial) Security Token Service.

This profile recommends the following approaches:

1. In case the service provider has a web application or portal where the user has logged in via web SSO (as specified in OIO-SAML), the service provider SHOULD extract the bootstrap token from the authentication assertion issued by the SAML Identity Provider. (The bootstrap token is embedded as an attribute).
2. In case of a rich client, the bootstrap token SHOULD be obtained from either:
    a) An authentication server on the same physical network as the user. The user will authenticate to this server using the authentication mechanism deployed on the local network (e.g. Kerberos).
    b) An external Security Token Service that allows authentication using the user's OCES digital signature.

All bootstrap tokens SHOULD be SAML 2.0 assertions conforming to the OIO Bootstrap Token Profile [OIO-BOOT].

Co-located STS

When an STS is co-located with an Identity Provider (as specified in OIO-SAML) it is RECOMMENDED that the STS does not issue security tokens unless the user has a valid browser session with the Identity Provider.

Further, issued tokens SHOULD not have a life time exceeding the life time of the web SSO session.

Issued Tokens

All security tokens issued by the STS SHOULD follow the OIO SAML Profile for Identity Tokens [OIO-IDT].

Mapping Claims to OIOSAML Attributes

The OIO WS-Trust profile describes how claims in the `wst:Claims` element for the issued token should be specified using the `ic:ClaimType` element. This element allows claims to be specified using a URI.

Since OIOSAML defines URIs for its attribute names, the OIOSAML attribute URIs SHOULD be used also in WS-Trust requests for OIO Identity Tokens (see above paragraph). When requesting claims / attributes not defined in OIOSAML (e.g. sector-specific attributes), the claim URIs MAY follow the naming conventions defined in OIOSAML.

Example: a `wst:RequestSecurityToken` message could include the following element:

```
<wst:Claims
    wst:Dialect="http://schemas.xmlsoap.org/ws/2005/05/identity">
    <ic:ClaimType
            Uri="dk:gov:saml:attribute:CprNumberIdentifier"/>
</wst:Claims>
```

in order to get an assertion issued containing the `CprNumberIdentifier` attribute defined in OIOSAML.

Security Policy

Web Service Providers SHOULD define their requirements for tokens and claims using a WS-SecurityPolicy [WS-SP] file and make it available through the mechanisms defined in WS-MetadataExchange [WS-MDX].

This allows dynamic retrieval of policy and subsequent obtaining necessary security tokens. Web Service Consumers are however not required to fetch the security policy dynamically. It is expected that requirements for token issuers and claims will be fairly static for many eGovernment deployments, and here it is viable to manually configure the STS endpoint and requested claims in the Web Service Consumer.

Certificate Policies

It is recommended that all Security Token Services use OCES Company- or Function[1] certificates [OCES-CP] when signing issued security tokens.

Certificate Validation

All relying parties MUST perform a revocation check on X.509 certificates used to sign security tokens or messages.

[1] Also known as VOCES- and FOCES certificates.

References

[WST] "WS-Trust 1.3", OASIS Standard, 19 March 2007.

[WS-SP] "WS-SecurityPolicy 1.2", OASIS, July 2007.

[WS-MDX] "Web Services Metadata Exchange Version 1.1", August 2006.

[WST-OIO] "OIO WS-Trust Profile 1.1", Danish Digitisation Agency.

[OCES-CP] https://www.nemid.nu/dk-da/om-nemid/historien_om_nemid/oces-standarden/oces-certifikatpolitikker/

[Scenarios] "Identity-Based Web Services – Scenarios", Danish Digitisation Agency.

[OIO-SOAP] "OIO IDWS SOAP Profile V1.1", Danish Digitisation Agency.

[OIO-BOOT] "OIO Bootstrap Token Profile V1.1", Danish Digitisation Agency.

[OIO-IDT] "OIO SAML Profile for Identity Tokens, V1.1", Danish Digitisation Agency.