Government Public Administration (GPA) Federated Authentication Guidelines

SAML 2.0 Implementation Profiles and Operational Modes

Date: 1st July 2011
Version: v1.0
Department: Technology and Systems Governance
Document Control Information

01. Document reference
TSG-GDL-Government Public Administration Federated Authentication Guidelines-v1.0.doc

02. Document type
Guideline

03. Security classification
Public

04. Synopsis
This document provides information on the supported SAML 2.0 implementation profiles and operational modes.

05. Document control

<table>
<thead>
<tr>
<th>Author</th>
<th>Change controller</th>
<th>Distribution controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology and Systems Governance</td>
<td>Technology and Systems Governance</td>
<td>Technology and Systems Governance</td>
</tr>
</tbody>
</table>

This document may be viewed and/or downloaded from the IMS On-Line, which maintains the latest issues of all documents and forms.

06. Authorisation

<table>
<thead>
<tr>
<th>Issuing authority</th>
<th>Approval authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology and Systems Governance</td>
<td>Technology and Systems Governance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature / Date</th>
<th>Signature / Date</th>
</tr>
</thead>
</table>

07. Modification history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 1.0</td>
<td>01/07/2011</td>
<td>First release of the document</td>
</tr>
</tbody>
</table>

08. Acknowledgements
N/A

09. References

[DK-SAML] OIO Web SSO Profile V2.0, IT- og Telestyrelsen.


2.0, OASIS Standard.

http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf


[ITTArch] Anbefaling om fælles arkitektur for tværgående autenticitetssikring.

[ITTAuthLevel] Vejledning vedrørende niveauer af autenticitetssikring.

[ITTAtrib] Anbefaling til kerneattributter for bruger.

[ITTUID] Anbefaling til unik id-nøgle.


[EgovSAMLProf] SAML Artifact Profile as an Adopted Scheme for E-Authentication.


[NistElAuth] Electronic Authentication Guideline,NIST Special Publication 800-63 Version 1.0.1

10. Distribution list
N/A
# Table of Contents

DOCUMENT CONTROL INFORMATION ............................................................................................................................................... I

TABLE OF CONTENTS .................................................................................................................................................................. III

01. GPA FEDERATED IDENTITY PROVIDER (IDP) CAPABILITIES ................................................................. 4
  01.1 SAML 2.0 SUPPORT ........................................................................................................................................................ 4

02. LIBERTY ALLIANCE EGOV 1.5 PROFILE SUPPORT .................................................................................. 5

03. PROFILES .................................................................................................................................................................. 6
  03.1 WEB BROWSER SSO PROFILE .............................................................................................................................. 6
      03.1.1 User Agent accesses Resource ............................................................................................................................... 6
      03.1.2 Service Provider Determines Identity Provider ........................................................................................................... 6
      03.1.3 Service Provider sends <AuthnRequest> ..................................................................................................................... 7
          03.1.3.1 Location of Identity Provider .................................................................................................................................. 7
          03.1.3.2 Binding Selection ...................................................................................................................................................... 7
          03.1.3.3 Signing the Request .............................................................................................................................................. 7
      03.1.4 Identity Provider Authenticates Principal ................................................................................................................... 7
          03.1.4.1 Single Sign-On ........................................................................................................................................................... 7
          03.1.4.2 Selecting Authentication Mechanism ...................................................................................................................... 7
      03.1.5 Identity Provider sends <Response> ......................................................................................................................... 8
          03.1.5.1 Processing Rules ..................................................................................................................................................... 8
          03.1.5.2 Assertion Contents ............................................................................................................................................... 8
          03.1.5.3 Location of Service Provider .................................................................................................................................. 8
          03.1.5.4 Bindings .................................................................................................................................................................. 8
          03.1.5.5 Signing .................................................................................................................................................................. 8
      03.1.6 Service Provider grants or denies access ............................................................................................................... 9
  03.2 IDENTITY PROVIDER DISCOVERY PROFILE .................................................................................. 9
      03.2.1 If Automated Discovery Fails ................................................................................................................................. 9
  03.3 SINGLE LOGOUT PROFILE ......................................................................................................................... 9
      03.3.1 Local Logout Requirements ....................................................................................................................................... 10
01. **GPA Federated Identity Provider (Idp) Capabilities**

### 01.1 SAML 2.0 Support

The table consists of the SAML conformance and operational modes that are supported by the current **Government Public Administration Federated Identity Provider**.

**NOTE:** The message component is not always included when it is obvious from context.

<table>
<thead>
<tr>
<th>profile, &lt;message(s)&gt;, binding</th>
<th>Operation Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IdP Lite</td>
</tr>
<tr>
<td>Web SSO, &lt;AuthnRequest&gt;, HTTP redirect</td>
<td>MUST</td>
</tr>
<tr>
<td>Web SSO, &lt;Response&gt;, HTTP POST</td>
<td>MUST</td>
</tr>
<tr>
<td>Web SSO, &lt;Response&gt;, HTTP artifact</td>
<td>MUST</td>
</tr>
<tr>
<td>Artifact Resolution, SOAP</td>
<td>MUST</td>
</tr>
<tr>
<td>Enhanced Client/Proxy SSO, PAOS</td>
<td>MUST</td>
</tr>
<tr>
<td>Name Identifier Management, HTTP redirect (IdP-initiated)</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, SOAP (IdP-initiated)</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, HTTP redirect</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Name Identifier Management, SOAP (SP-initiated)</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>Single Logout (IdP-initiated), HTTP redirect</td>
<td>MUST</td>
</tr>
<tr>
<td>Single Logout (IdP-initiated), SOAP</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>Single Logout (SP-initiated), HTTP redirect</td>
<td>MUST</td>
</tr>
<tr>
<td>Single Logout (SP-initiated), SOAP</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>Identity Provider Discovery, (cookie)</td>
<td>MUST</td>
</tr>
</tbody>
</table>
02. Liberty Alliance EGOV 1.5 Profile Support

The Liberty Alliance EGOV 1.5 Profile is also supported. More conformance details can be found at the following link.

http://projectliberty.org/liberty/content/download/4711/32210/file/Liberty_Alliance_eGov_Profile_1.5_Final.pdf
03. Profiles

03.1 Web Browser SSO Profile

This chapter contains a profile which is a further specialization of the Web Browser SSO Profile from [SAMLProf]. Unless stated explicitly, all messages, policies, processing rules etc. of the original profile are inherited.

The steps in the basic scenario covered by the profile are illustrated in the figure below (figure from [SAMLProf]):

![Figure 1: Steps in basic SSO](image)

In the following, each step will be described in detail including specifics of bindings and processing rules.

03.1.1 User Agent accesses Resource

This profile contains no restrictions on this step as it is governed by the HTTP protocol. Note that a resource may be requested via a link or frame from the portal, but it will still result in plain HTTP(s) request from the user agent to the Service Provider.

As in the SAML profile, the RelayState mechanism MAY be used by the Service Provider to associate subsequent profile exchanges with the original request. However, for privacy reasons this parameter must not reveal any details of the request (i.e. it must be opaque).

03.1.2 Service Provider Determines Identity Provider

In the original OASIS SAML profile, this step is implementation dependent and a number of different options exist. In this profile, the step MUST follow the described in section 3.2. This will help to ensure that the architecture is open towards multiple Identity Providers.
03.1.3 Service Provider sends <AuthnRequest>

03.1.3.1 Location of Identity Provider

In order to send the request, the Identity Provider’s single sign-on service must first be located. The SAML profile states that metadata MAY be used for this purpose but for this profile this is a must. No prior exchanges between Service and Identity Providers should take place without prior establishment of legal- and business agreements and exchange of metadata.

03.1.3.2 Binding Selection

The SAML profile allows a selection of different bindings; this profile mandates use of HTTP Redirect binding with DEFLATE encoding based on the deployment experiences from the American e-Authentication initiative. The HTTP exchange MUST take place over (one-way) SSL / TLS to ensure confidentiality of the request (integrity and authenticity is provided by digitally signing the request as described in the next subsection).

03.1.3.3 Signing the Request

In the original OASIS SAML profile, signing of the request is optional. In this profile, digital signing of the request is mandatory and should be performed using the Service Provider’s signature whose certificate is exchanged as part of the metadata.

Since HTTP Redirect binding with DEFLATE encoding is used, the signature MUST be located in the “Signature” query string described by this binding instead of in the request XML message.

03.1.4 Identity Provider Authenticates Principal

This step is governed by the requirements to the individual Identity Provider.

03.1.4.1 Single Sign-On

If the Identity Provider already has a valid session with the user, authentication of the user should not be performed and instead single sign-on be used. Exceptions to this are:

- The user may have chosen to opt-out of single sign-on via his preferences with the Identity Provider.
- The Service Provider may have included the ForceAuthn attribute in the request with a value of “true”. This instructs the Identity Provider to re-authenticate the user even if he already has a session. The Identity Provider MUST honour this attribute.
- The Service Provider may have included the IsPassive attribute with a value of “true”. This instructs the Identity Provider and client not to take over the user interface. The Identity Provider MUST honour this attribute. If the <AuthnRequest> cannot be processed without taking over the user interface (e.g. because there is no current SSO session with the user), the Identity Provider MUST send a response with a status code of urn:oasis:names:tc:SAML:2.0:status:NoPassive.

03.1.4.2 Selecting Authentication Mechanism

An Identity Provider may support several authentication mechanisms each providing a different assurance level for the user’s identity. Examples are username/password login, authentication via digital signatures bound to certificates, PIN code login etc.

It is not allowed for Service Providers to specify the requested level of authentication via extensions to the <AuthnRequest> message as this may be problematic for many software products to handle. In a future update of the profile this restriction may be lifted, so that requested level of authentication can be included in the <AuthnRequest> message.

---

1 The service provider certificate may be obtained from MITA or else the certificate must be issued from an industry recognised certification authority.
Instead, an Identity Provider MAY deploy different logical IdP services with different end-points and let the Service Provider choose between these. Alternatively, an Identity Provider MAY let the user select among different mechanisms interactively or let the choice be a part of the user’s preferences.

Details about end-points will be advertised via metadata exchanged when a Service Provider joins the federation. The level of authentication for each end-point will be communicated out-of-band (not part of SAML metadata).

03.1.5 Identity Provider sends <Response>

When an Identity Provider processes a request and produces a response, it must follow the rules defined in this section.

03.1.5.1 Processing Rules

Only Service Providers with prior agreements may be served by the Identity Provider.

If the Identity Provider receives an AuthnRequest from a Service Provider with which it has no agreement the request MUST be rejected with a proper error message.

If the Identity Provider wishes to return an error, it MUST NOT include any assertion in the <Response> message. Otherwise, if the request is successful, the <Response> element MUST conform to the following:

- The <Issuer> element MAY be omitted, but if present it MUST contain the unique identifier of the issuing Identity Provider; the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
- A successful response MUST contain exactly one <Assertion> with exactly one <AuthnStatement> element. Each assertion's <Issuer> element MUST contain the unique identifier of the issuing Identity Provider; the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. If the IsPassive attribute is set and control of the user interface is needed, the following status code MUST be returned urn:oasis:names:tc:SAML:2.0:status:NoPassive.

The background for the above restrictions is limitations in COTS products and a desire to make the profile easy to deploy.

03.1.5.2 Assertion Contents

The assertion included in a response must follow one of the two attribute profiles described later in this profile. Specifically, the assertion MUST state the level of authentication achieved.

03.1.5.3 Location of Service Provider

In order to send the response, the Service Provider’s assertion consumer service must first be located. The SAML profile states that metadata MAY be used for this purpose but in this profile this is a must.

03.1.5.4 Bindings

The OASIS SAML profile allows several different bindings; this profile mandates use of the HTTP POST binding based on the deployment experiences from the American e-Authentication initiative. The HTTP exchange MUST take place over (one-way) SSL / TLS to provide for confidentiality of the request (integrity and authenticity is provided by digitally signing the request).

03.1.5.5 Signing

The response message SHOULD NOT be signed using the Identity Provider’s signing key. Instead, the embedded Assertion is required to be signed.
03.1.6 Service Provider grants or denies access

The Service provider receives and processes the response message with the enclosed assertion. In addition to the processing mandated by the SAML profiles, the Service Provider must check that the level of authentication in the received assertion is equal to or higher than the level required by the resource requested by the user.

Based on this information from the assertion, it creates a session with the user and performs an authorization decision for the resource originally requested by the user. If the access check is successful, the requested (web) resource is returned to the user.

03.2 Identity Provider Discovery Profile

The Identity Provider Discovery Profile described in [SAMLProf] enables a Service Provider to discover which Identity Providers a principal is using with the web browser SSO profile.

The profile relies on a cookie that is written in a domain common between Identity Providers and Service Providers in a deployment. The cookie contains a list of Identity Provider identifiers and the most recently used IdP should be at the end of the list.

GPAIdp directly adopts the profile and requires conforming Service and Identity Providers to support it. This will facilitate an open architecture where multiple Identity Providers can be leveraged.

The cookie must be transient such that it is not stored between browser sessions.

The name of the common domain is to be determined by the federation organization that the entity is part of.

03.2.1 If Automated Discovery Fails

There may be situations where a Service Provider cannot discover an Identity Provider via the above mechanism. For example, the user may not yet have a session with an Identity Provider or may have deleted the cookies in his browser.

In such a situation, the Service Provider can select its default Identity Provider. If the Service Provider supports multiple Identity Providers, he may prompt the user to select Identity Provider.

03.3 Single Logout Profile

SAML 2.0 supports the concept of single logout and describes both a Single Logout Protocol in [SAMLCore] and a Single Logout Profile in [SAMLProf]. These allow Identity- and Service Providers to terminate multiple user sessions by exchanging <LogoutRequest> and <LogonResponse> messages. In this way, a user can perform near-simultaneous logout to all Service Providers whose session originate from a particular Identity Provider (i.e. "single logout"). The user may either contact a Service Provider or an Identity Provider to initiate the logout.

The figure below from [SAMLProf] shows an example message flow:
Figure 2: Message flow during Single Logout

Note: The translucent “user agent” illustrates that the message exchange may pass through the user agent or may be a direct exchange between system entities, depending on the SAML binding used for Single Logout.

The possible variations in the OASIS Single Logout Profile pertain to which binding is used. The choices are SOAP binding, HTTP Redirect, HTTP POST, and Artifact binding. Note that the OASIS profile clearly distinguishes between the first request from Service Provider to Identity Provider (which is strongly recommended to use a front-channel binding) and subsequent message exchanges.

In GPA authentication scenario, the following restrictions must be followed:

- HTTP Redirect binding MUST be used for the first request going from a Service Provider to an Identity Provider. This will allow the Identity Provider to determine the user session by e.g. reading browser cookies.
- Either HTTP Redirect or SOAP Binding MUST be used for subsequent request/response messages from the Identity Provider to a Service Provider.
- All Service Providers and Identity Providers MUST support the HTTP Redirect binding.
- Support for SOAP Binding is optional for Service Providers.
- Support for SOAP Binding is mandatory for Identity Providers.
- All request and response messages MUST be signed.
- Communication MUST be secured using client-authenticated (two-way) SSL / TLS.

03.3.1 Local Logout Requirements

In addition to the Single Logout profile described above, each Service Provider should also offer local logout for stand-alone applications to the user. A local logout means that the user will be logged out of the local Service Provider application only. The Service Provider will not send any `<LogoutRequest>` message, and the user will keep any active session with the Identity Provider and other Service Providers unless they expire on their own.

Note that for Service Providers who are part of a portal, a local logout may not make sense and may be handled as part of the portal framework instead.