GÉANT Data Protection Code of Conduct SAML 2.0 profile

For Service Providers established in European Union, European Economic Area and countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC

Version 1.1, 24 October 2014

The work leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

1. Introduction

This profile defines REQUIRED, RECOMMENDED, and OPTIONAL behavior for deployments supporting the Data Protection Code of Conduct. This deployment profile is based on the Organization for the Advancement of Structured Information Standards (OASIS) SAML 2.0 specifications [SAML2 Core, SAML2META]. It also references elements defined in [SAML2MDUI], and makes use of an Entity Category element defined in Entity Category Specification: Data Protection Code of Conduct [CoCEntityCategory]. The requirements from those specifications are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

This document is supplemented by the non-normative Notes on Implementation of INFORM/CONSENT GUI Interfaces [CoCGUI] document which outlines the current best practice in the implementation and deployment of Identity Provider side modules for attribute release and user consent.

Note that the SAML features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. SAML Metadata Requirements for SP Entities

1. mdui Requirements:
    1. SPs MUST provide at least one `mdui:PrivacyStatementURL` value.
    2. It is RECOMMENDED that SPs provide at least one `mdui:DisplayName` value.
    3. It is RECOMMENDED that SPs provide at least one `mdui:Description` value.
    4. For all mdui elements, at least an English version of the element MUST be available, indicated by an `xml:lang="en"` attribute.
2. Attribute-related Requirements:
    1. SPs MUST provide `RequestedAttribute` elements describing attributes (and, optionally, requested values) relevant for the SP. The `RequestedAttribute` elements MUST include the optional `isRequired="true"` to indicate that the attribute is necessary.
    2. If the SP requires just one or some particular value(s) of an attribute (such as, `eduPersonAffiliation="member"`), the SP MUST use the `saml:AttributeValue` element to indicate that value(s).
3. SPs MUST provide an Entity Category attribute [CoCEntityCategory] value asserting compliance with the Code of Conduct.

2.1 Display name

A short descriptive name of the service, if possible without abbreviations. It SHOULD be meaningful both to the users of the service and to readers not affiliated with the service.

This value may be displayed by various GUIs in order to identify the service.

Examples:

- Helsinki University's Moodle learning management system
- University of Tübingen's Weblicht tool for linguistics research

2.2 Description

A description which summarises the service provided. It SHOULD be meaningful both to the users of the service and to readers not affiliated with the service.

This value may be displayed by various GUIs in order to summarise the purpose for which the service processes personal data.

It is RECOMMENDED that the length of the description is no longer than 140 characters.

Examples:

- SAS-download gives access to SAS®-software for qualified users.
- bibliotek.dk gives access to all public Danish libraries, and allows users to search for and order materials.
- WebLicht is a chaining tool for linguistics research. It provides an execution environment for automatic annotation of text corpora.

2.3 Privacy Statement URL

A URL which resolves to a document that is the service's Privacy Policy.

This value may be displayed by various GUIs as a clickable link for the end user to provide more information on how the service processes personal data. See Privacy policy guidelines for Service Providers [CoCPrivacyPolicy] for more information.

The `PrivacyStatementURL` MUST resolve to a document which is available to browser users without requiring authentication of any kind.

2.4 Requested Attribute

Zero or more elements specifying attributes and, when applicable, attribute values requested by this service. Having no `RequestedAttribute` element in place implies the service does not request any attributes.

If the Service Provider supports both SAML 1.x and SAML 2.0 protocols, it SHOULD list requested attributes using only the SAML 2.0 attribute naming conventions [MACEDirAttrProf].

- Note: The underlying SAML 2.0 metadata standard is unable to express the attribute requirements of such a Service Provider. The recommendation above is intended to minimise the chance of interoperability problems arising. It is further RECOMMENDED that such a Service Provider uses the SAML 2.0 protocol when possible rather than SAML 1.x.

A necessary attribute is indicated using the `isRequired="true"` XML attribute. In the context of this Data protection Code of Conduct, an attribute is required only if it is both relevant and necessary for enabling access to the service.

`isRequired="false"` or a missing `isRequired` XML attribute indicates the attribute is optional (relevant, but only useful or desirable).

See What attributes are relevant for a Service Provider [CoCAttributes] document for assistance on the necessary and optional attributes. See also Data protection good practice for Home Organisations [CoCHomeOrg] document for a good practice on managing the release of attributes flagged as necessary or optional.

Note: Introduction to Code of Conduct [CoCIntroduction] proposes to defer the support to attributes flagged as optional to Phase 2.

2.5 Entity Category: Data protection Code of Conduct

An Entity Category attribute as defined in the Entity Category Specification: Data Protection Code of Conduct [CoCEntityCategory].

3. SAML Metadata Requirements for IDP Entities

IdPs MUST provide an Entity Category support attribute [CoCEntityCategory] value asserting that they are willing to interact with Service Providers conforming to the Code of Conduct.

4. Examples

Only related elements and attributes are presented.

Example (Service Provider):

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://filesender.example.org/">
   <Extensions>
      <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
         <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion”
            Name="http://macedir.org/entity-category"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
         </Attribute>
      </EntityAttributes>
   </Extensions>
   <SPSSODescriptor>
      <Extensions>
         <UIInfo xmlns=”urn:oasis:names:tc:SAML:metadata:ui”>
            <DisplayName xml:lang="fi">FileSender</DisplayName>
            <DisplayName xml:lang="en">FileSender</DisplayName>
            <Description xml:lang="fi">FileSender tarjoaa helpon tavan jakaa suuria tiedostoja.</Description>
            <Description xml:lang="en">FileSender offers an easy way to share large files with anyone.</Description>
            <PrivacyStatementURL xml:lang="fi">https://filesender.example.org/privacy-fi.html</PrivacyStatementURL>
            <PrivacyStatementURL xml:lang="en">https://filesender.example.org/privacy-en.html</PrivacyStatementURL>
         </UIInfo>
      </Extensions>
      <AttributeConsumingService>
         <RequestedAttribute
            FriendlyName="displayName"
            Name="urn:oid:2.16.840.1.113730.3.1.241"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            isRequired="true"/>
         <RequestedAttribute
            FriendlyName="eduPersonPrincipalName"
            Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            isRequired="true"/>
         <RequestedAttribute
            FriendlyName="mail"
            Name="urn:oid:0.9.2342.19200300.100.1.3"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            isRequired="true"/>
      </AttributeConsumingService>
   </SPSSODescriptor>
</EntityDescriptor>
```

Example (Identity Provider):

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://idp.example.org/">
   <Extensions>
      <EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
         <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            Name="http://macedir.org/entity-category-support"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</AttributeValue>
         </Attribute>
      </EntityAttributes>
   </Extensions>
</EntityDescriptor>
```

References

[CoCAttributes]	Data protection Code of Conduct, “What Attributes Are Relevant for a Service Provider”, <https://wiki.refeds.org/display/CODE/What+attributes+are+relevant+for+a+Service+Provider>
[CoCEntityCategory]	Data protection Code of Conduct, “Entity Category Specification”, Version 1.1, 24 October 2014
[CoCGUI]	Data protection Code of Conduct, “Notes on Implementation of INFORM/CONSENT GUI Interfaces”, <https://wiki.refeds.org/pages/viewpage.action?pageId=1606095>
[CoCHomeOrg]	Data protection Code of Conduct, “Data Protection Good Practice for Home Organisations”, <https://wiki.refeds.org/display/CODE/Data+protection+good+practice+for+Home+Organisations>
[CoCIntroduction]	Data protection Code of Conduct, “Introduction to Code of Conduct”, <https://wiki.refeds.org/display/CODE/Introduction+to+Code+of+Conduct>
[CoCPrivacyPolicy]	Data protection Code of Conduct, “Privacy Policy Guidelines for Service Providers”, <https://wiki.refeds.org/display/CODE/Privacy+policy+guidelines+for+Service+Providers>
[MACEDirAttrProf]	MACE-Dir, “SAML Attribute Profiles”, April 2008.
[SAML2 Core]	OASIS, “Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0”, 15 March 2005. Document Identifier: saml-core-2.0-os, <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
[SAML2META]	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, with various addenda, and in associated specifications.
[SAML2MDUI]	SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0.

Document History

Changes from Version 1.0 Errata 1, 10 June 2014

- Introduced a mandatory Entity Category support attribute for Identity Providers.
- Corrected links in the References section.

Changes from Version 1.0, 14 June 2013

- Removed white space characters from the <AttributeValue>, <mdui:DisplayName>, <mdui:Description> and <mdui:PrivacyStatementURL> elements in the Examples section and reformatted the example.