GÉANT Data Protection Code of Conduct

Entity Category Specification

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 1.2, 12 October 2015

Introduction

The EU Data Protection Directive (95/46/EC) sets the legal framework for attribute release within the European Union and European Economic Area. For more information on the requirements imposed, see Introduction to Data protection directive [DirectiveIntroduction].

The Data Protection Code of Conduct sets out practices for meeting the requirements of the Data Protection Directive. It defines a set of rules to be followed by Service Providers wishing to receive user attributes from the Identity Providers managed by Home Organisations. It is expected that Home Organisations will be more willing to release attributes to Service Providers asserting the conformance to the Data Protection Code of Conduct. For more information, see Introduction to Code of Conduct [CoCIntroduction].

This document defines a SAML 2.0 Entity Category attribute [SAML2EntityAttr] for Service Providers that claim conformance to the Data Protection Code of Conduct and a SAML 2.0 Entity Category support attribute for Identity Providers that are willing to interact with Service Providers conforming to the Data protection Code of Conduct.

Syntax

The following URI is used as the Attribute Value for the Entity Category attribute and Entity Category support attribute:

```
http://www.geant.net/uri/dataprotection-code-of-conduct/v1
```

Semantics

By asserting membership in the Entity Category, a Service Provider claims

- that it is bound by
    - the data protection laws in the European Union or European Economic Area, or
    - a third country's domestic data protection laws which have been recognised by the EC as ensuring an adequate level of protection [ECWhiteList], or
    - an international commitment into which a third country has entered and which has been recognised by the EC as ensuring an adequate level of protection [ECWhiteList],
- that it has committed to the Data Protection Code of Conduct for Service Providers [CoCforSP], and
- that it conforms to the SAML 2 Profile for the Data Protection Code of Conduct [CoCSAML2]

By asserting the Entity Category support attribute, an Identity Provider claims that it releases the requested attributes to a Code of Conduct committed Service Provider without administrative involvement.

Provenance

When an Entity's registrar (normally the Entity's home federation) registers the Entity's assertion of membership in the Entity Category it must perform at least the checks defined for a home federation operator in the Operator guidelines document [CoCOperatorGuidelines].

No requirements are defined for the provenance of an Identity Provider's Entity Category support attribute.

Examples

Entity Category attribute (Service Provider):

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

Entity Category support attribute (Identity Provider):

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

Usage

Enable Home Organisations / Identity Provider administrators to easily set up a global attribute filter policy for Service Providers committed to the Code of Conduct.

For related configuration examples, see

- Code of Conduct Cookbook [CoCCookbook].

- InCommon's R&S category [InCommon].

- Shibboleth configuration instructions by SWAMID [SWAMID].

References

75

[CoCCookbook]   Data protection Code of Conduct, "Data protection Code of Conduct Cookbook",
                    <https://wiki.edugain.org/Data_Protection_Code_of_Conduct_Cookbook>

[CoCforSP]   Data protection Code of Conduct, "Code of Conduct for Service Providers",
                    <https://wiki.refeds.org/display/CODE/Code+of+Conduct+for+Service+Providers>

[CoCIntroduction]   Data protection Code of Conduct, "Introduction to Code of Conduct",
                    <https://wiki.refeds.org/display/CODE/Introduction+to+Code+of+Conduct>

[CoCOperatorGuidelines] Data protection Code of Conduct, "Operator guidelines",
                    <https://wiki.refeds.org/display/CODE/Operator+guidelines>

[CoCSAML2]   Data protection Code of Conduct, "SAML2 profile for the Data Protection Code of Conduct", Version
                    1.1, 24 October 2014

[DirectiveIntroduction] Data protection Code of Conduct, "Introduction to Data protection directive".
                    <https://wiki.refeds.org/display/CODE/Introduction+to+Data+protection+directive>

[ECWhiteList]   European Commission, "Commission decisions on the adequacy of the protection of personal data in
                    third countries", <http://ec.europa.eu/justice/data-protection/international-
                    transfers/adequacy/index_en.htm>

[InCommon]   InCommon federation, "Configure a Shibboleth IdP to Support R and S", <
                    https://spaces.internet2.edu/display/InCFederation/Research+and+Scholarship+IdP+Config >

[SAML2EntityAttr] Young, I., Johansson, L., Cantor, S., "The Entity Category SAML Entity Metadata Attribute Types",
                    August 2012, <http://macedir.org/draft-macedir-entity-category-00.txt>

[SWAMID]   SWAMID, "GEANT Data Protection Code of Conduct",
                    <https://wiki.swamid.se/display/SWAMID/GEANT+Data+Protection+Code+of+Conduct>

Document History

Changes from Version 1.1, 24 October 2014
- Removed references to the Safe Harbour arrangement that has been invalidated by the European Court of Justice.
- Corrected links in the References section.

Changes from Version 1.0 Erreta 1, 10 June 2014
- Introduced an Entity Category support attribute and a related example.
- Corrected links in the References section.

Changes from Version 1.0, 14 June 2013
- Reformatted the Examples section to remove misleading white spaces from the <AttributeValue> element