Introduction to Code of Conduct

Contents

1. Background

Service Providers in the identity federations for higher education and research are reporting problems in receiving necessary user attributes from his/her Home Organisations (see for instance: Federated Identity Management for Research Collaborations). Data protection concerns are believed to be a major reason for Home Organisations' hesitation to release attributes.

This Data protection Code of Conduct describes an approach to meet the requirements of the EU data protection directive. This Code of Conduct is a joint effort by the GN3 project (SA3 task 3 "eduGAIN") and REFEDS.

2. Contents

The Data protection Code of Conduct consists of these normative documents:

1. Code of Conduct for Service Providers. The principles to which a Service Provider commits when it asserts that its processing of personal data is compliant with this Data Protection Code of Conduct.
2. Entity category attribute definition: Data protection Code of Conduct. This document defines a SAML 2.0 metadata Entity Category attribute which is then used in the Data Protection Code of Conduct.
3. SAML 2 Profile for the Code of Conduct. This document describes a profile of SAML 2.0 metadata to support the Code of Conduct.

In addition, there are several accompanying informative, non-normative documents:

1. Introduction to Data protection directive An general introduction to EU Data protection directive's relevant sections.

1. Managing Data Protection Risks Using the Code of Conduct. This document identifies data protection risks and proposes approaches to manage them.
2. Privacy policy guidelines for Service Providers. This document assists the Service Providers to develop a Privacy Policy document expected in this Code of Conduct.
3. What attributes are relevant for a Service Provider. This document assists the Service Providers to assess what attributes they can request from the Home Organisations.
4. Data protection good practice for Home Organisations. This document assists the Home Organisations to reduce their attribute release risks.
5. Operator guidelines. This document describes the federation and interfederation operator's role in the Code of Conduct.
6. Handling non-compliance. This document suggests actions in the case of having doubts that a Service Provider is ignoring the Code of Conduct to which it has committed.
7. Notes on Implementation of INFORM/CONSENT GUI Interfaces. This document supplements the Code of Conduct by suggesting features for the Identity Providers' attribute release/consent modules.

3. How Does the Code of Conduct Achieve its Goals?

The Code of Conduct describes an approach whereby both Home Organisations and Service Providers can acquire confidence that the other party is meeting its data protection requirements:

- Both the Home Organisation and the Service Provider must comply with the requirements specifically imposed on them by the Data protection directive and by national law.
- The Service Provider commits to the Code of Conduct for Service Providers.
    - If the Service Provider is located within the EU/EEA, the local laws already bind the Service Provider to most of the requirements presented in this the Code of Conduct. The Code of Conduct can be seen mostly as a division of responsibility to ensure the data protection law's requirements are met.
    - The use of this Code of Conduct is not encouraged for attribute release to non-EU/EEA Service Providers and Service Providers outside countries/arrangements that do not guarantee adequate data protection. Instead, refer to the Model contracts of European Commission.
- The Service Provider asks, via its SAML 2.0 metadata elements, for Attributes that are necessary for the legitimate interests of the Service Provider to provide the service to the end user. It indicates this legal grounds by labeling these attributes as "isRequired=true".
- To inform the end user of processing his/her personal data, the Service Provider includes a prominent link to its Privacy Policy e.g. on its front page.

- The Service Provider's commitment to the Code of Conduct document may assist the Home Organisation to achieve confidence that the risk of releasing Attributes to such a Service Provider is acceptable because it can see that the attribute processing done at the Service Provider meets the requirements of the Directive.

4. Phased Implementation

This section suggests and provides reasoning for a phased implementation, where the release of optional extra attributes is deferred to a later phase. See I ntroduction to Data protection directive for background information.

4.1 Thoughts on the Current Situation

1. There are already many Service Providers which require Attributes to be asserted by a trusted Identity Provider. There is significant interest in encouraging Identity and Service Providers to use Attribute release, when appropriate and done in a manner consistent with each party's risk appetite.
2. In the short term, deployability is the primary goal. The Code of Conduct should give maximum confidence to both the Home Organisations and the Service Provider with minimum cost for both of them.
3. There is a need for a scaleable approach to providing Home Organisations with the information they need when deciding whether or not to release attributes to a specific Service Provider.
4. Consensus on Phase 1 has to involve both Service Providers and Home Organisations. Both parties must be comfortable with the approach in order for it to see broad adoption. It is inevitable that any framework is going to be a trade-off between maximising functionality and maximising adoption; a dialogue between Service Providers and Home Organisations is required to work out where the sweet spots are in that range.
5. Experience in some federations seems to indicate that there are very few (approaching none) use cases that require the use of optional extra Attributes released on user consent. Using necessary Attributes has been sufficient.
6. Requiring user consent to the release of optional Attributes would make widespread deploy significantly less likely since doing consent properly requires both the Home Organistations and Service Providers to implement new systems (so increased cost).
    a. Service Providers need to be able to identify attributes as "necessary" or "optional".
    b. Identity Providers need to install a consent module which supports the concept of releasing optional extra attributes on user consent.
    c. Identity Providers needs to signal that user consent has been obtained.
    d. Service Providers need to be able to verify that user consent has been obtained.

4.2 Phase 1 Approach

1. Deploy a voluntary participation model for constraining risk. Encourage all parties to addess their responsibilities within the Code of Conduct.
2. Home Organisations and Service Providers should rely on **the necessary for the legitimate interests legal grounds** for requesting and providing Attribute release.
    a. This approach would be much simpler than **user consent**, for both Home Organisations and Service Providers.
    b. This approach seems to match the experience so far.
3. **Defer release of optional extra Attributes** based on user consent until Phase 2.
    a. Introducing consent, even as an optional possibility for Home Organisations and Service Providers, would add significant complexity to the framework. A unilateral statement by the Service Provider that did not rely on matching action by the Home Organisation would no longer be sufficient. The added burden exceeds the value at this point in time.
    b. Explaining all of the additional complexity without creating an immense amount of confusion for everyone may be too difficult.
    c. If an Service Provider really wants an optional attribute, it should obtain it directly from the user.

4.3 Specific Phase 1 Steps

The Code of Conduct for Service Providers lists the criteria that Service Providers must meet in order to state that they are committed to this Code of Conduct. For Home Organisations aiming at making use of this Code of Conduct, Data protection good practice for Home Organisations provides good practices which would help the Home Organisations to meet the requirements set by the Data protection directive. A Home Organisation can decide to ignore these good practices. However, doing so creates risk for the Home Organisation, not the Service Provider.

Federations are proposed to

1. Help Service Providers **to populate necessary SAML 2.0 metadata elements**, such as MDUI information
2. Help and encourage Service Providers to understand a simple privacy policy document and its role, and then publish a privacy policy.
3. **Help Home Organisations understand** the Code of Conduct model and become comfortable with it.
4. **Help Home Organisations configure** their Identity Provider to use the Code of Conduct model.

5. About the Preparation Process of this Code of Conduct

Specifically,

- The eduGAIN project and REFEDS attribute release workgroup have developed the Code of Conduct as a joint project process.
- The intention has been to keep the process open, including public commenting, workshops and consultations. The goal is to make the Code of Conduct generally approved among the community.

- The eduGAIN project is discussing with the Article 29 working party (WP29) of EU on the possibilities to submit the Code of Conduct to the working party for approval. Approval by WP29 would further legitimize the use of the Code of Conduct in EU.
- The generally approved Code of Conduct would then be made available for federations, Home Organisations and Service Providers.
- Adopting the Code of Conduct would be purely optional for federations. Service Providers and Home Organisations are always able to use whatever alternative means (e.g. bilateral agreements) to fulfill the obligations imposed by the data protection laws.
- The goal of having the CoC generally approved is to remove obstacles from wide adoption and to avoid the eduGAIN project and REFEDS attribute release workgroup being held liable for the contents of the Code of Conduct. Obtaining "general approval" would further legitimize the use of the Code of Conduct in EU.