The ReFEDS/GÉANT Code of Conduct (CoC)

An Approach to Compliance with the EU Data Protection Directive

Steve Carmody
April 23, 2012
What is the Code of Conduct?

• An Approach to simplify interoperation when releasing attributes
• Allow IDPs and SPs to become confident that partners are operating in compliance with the EU data protection
Goals of the Code of Conduct

• Make it as simple as possible for campus users to easily access remote sites requiring attributes.
• Find an appropriate balance between risk and value for all parties.
• Provide suggestions to Federations, IDPs, and SPs on Business Practices that are believed to be consistent with the EU data protection directive and its interpretations.
• Provide suggestions that would allow interoperation between parties around the world, not just within the EU.
Approach

• Use the EU data protection law as the starting point
• Develop a design that
  • provides all parties with sufficient assurance that parties they interoperate with are meeting their privacy-related responsibilities,
  • is able to tolerate and recover from incidents and misbehaving entities,
  • is scaleable (avoids requiring bilateral contracts between all parties)
• Note -- in the absence of a contract that defines responsibilities for each party there will be non-zero risk for all parties.
When you think about the EU data protection…

• What image comes to mind?
A Mass of Snakes?
Something about which there is no consensus?
A Opportunity to Get Away From the Office?
EU Data Protection Requirements

• Both parties have specific responsibilities under the Directive
• Both parties MAY need to be assured that the other party has met its obligations
  • IDPs need to "implement appropriate ... organizational measures" to ensure that release does not result in unlawful processing by others
  • v1 of the CoC has been constructed so that SPs do NOT need any assurance from the IDP about what it has done
The General Idea

• SP commits to meeting its requirements under the CoC
  • The CoC is a set of specific operating requirements derived from the EU Data Protection Directive
  • SP indicates this commitment in its metadata element
  • This is self-declared by the SP (self-audit)
• SP only asks for attributes that are adequate, relevant and not excessive to the Service
• IdPs can make a decision to release attributes based on their local risk management procedures
Specific Steps

- Both the IDP and the SP must comply with specific requirements. (Introduction to Data protection directive, section 12)

- The SP signs and publishes the *Code of Conduct for Service Providers*.
  - If the SP is located within the EU/EEA, this does NOT impose any additional restrictions or constraints on the SP.
  - The SP is stating that it is operating in compliance with those requirements.
Specific Steps (more)

- The SP asks, via its SAML 2.0 metadata elements, for Attributes that are required for the **legitimate operation of the SP**. It indicates this legal grounds by labeling these attributes as "isRequired=true".

- The SP includes a **prominent link** on its front page to its Privacy Policy, which lists the required Attributes, and describes how they are used.
  - This INFORMs the user about attribute release.

- The SP's signed Code of Conduct document may convince the IdP that the risk of releasing attributes to such an SP is acceptable.
Specific Steps (more)

- The IDP may also decide to INFORM the user.
  - SP’s name and identity (=>mdui:Displayname, mdui:Logo)
  - SP’s purpose (=>mdui:Description)
  - mdui:PrivacyStatementURL
  - a list of attribute names/values (c.f. uApprove)
To use 'GakuNin-Test-Fed Test SP1 (md:ServiceName)', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.

**Digital ID Card**

<table>
<thead>
<tr>
<th>Mandatory information for using the service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>edupersonprincipalname</td>
</tr>
<tr>
<td>organizationname</td>
</tr>
<tr>
<td>organizationalunit</td>
</tr>
<tr>
<td>edupersonaffiliation</td>
</tr>
<tr>
<td>edupersonentitlement</td>
</tr>
</tbody>
</table>

- I always check the information to be sent. This time I agree to send the information.
- I agree that the information same as this time will be sent automatically to this service in the future.

[Options to continue or cancel.]
The Documents .... Required

- Code of Conduct for Service Providers.
- SAML 2 Profile for the Code of Conduct.
  - Describes how to use various elements in order to remain compliant with the CoC
The Documents ... Suggestions

- Privacy policy guidelines for Service Providers.
- What attributes are relevant for a Service Provider.
- Data protection good practice for Identity Providers.
The Documents ... Suggestions

• Federation operator's guidelines.
• Handling non-compliance.
• Notes on Implementation of INFORM/CONSENT GUI Interfaces.
The Documents … Suggestions

• The REFEDS survey on the use of MDUI elements
Process for Adoption

• The eduGAIN project and REFEDS attribute release workgroup have developed the Code of Conduct as a joint project process.
• The process is open, including public commenting, workshops and consultations. The goal is to make the CoC **generally approved** among the community.
• The eduGAIN project is initiating discussions with the Article 29 working party (WP29) of EU on the possibility of submitting the CoC to the working party for approval or comment.
• The generally approved CoC would then be made available for federations, Home Organisations and Service Providers.
Process for Adoption

• Adopting the CoC 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 to wide adoption
  • avoid the eduGAIN project and REFEDS attribute release workgroup being held liable for the contents of the CoC.
  • further legitimize the use of the CoC in EU.
Status

- Public commenting, workshops and consultations are underway
- At the REFEDS meeting, May 2012, we will open the Official Public Comment period, through August 1
- Publish v1.0 in the Fall, 2012
We Are All in this Together ..... 

• But it's not so difficult!
Comments, Feedback:

- Send email to:
  - [refeds-attribute-release@refeds.org](mailto:refeds-attribute-release@refeds.org)
  - [edugain-policy@geant.net](mailto:edugain-policy@geant.net)