CoC FedOp Perspective

A FedOp Perspective on the Code of Conduct Service Category

This document gives a brief FedOp perspective on the Code of Conduct service category. These issues were discussed on the Interfederation WG call on November 6, 2013.

The Interfederation WG Charter contains the following deliverable:

> *Review and adopt the US-EU Code of Conduct to address privacy and attribute release.*

That deliverable is perhaps overly prescriptive since the Code of Conduct service category is not easily operationalized within the InCommon Federation.

The Code of Conduct has been formulated as a service category. Some federations have already implemented a Code of Conduct service category and there is a concrete proposal within the REFEDs community to standardize it:

https://refeds.terena.org/index.php/Entity_Category_CoC

As you skim the above document, you will quickly realize that the Code of Conduct (CoC) is actually multiple levels of documents, each bearing its own set of requirements. Consequently, it's difficult to isolate the complete set of requirements associated with the CoC service category.

Recommendation: Consolidate the Code of Conduct spec in a single document (similar to what's been done with the REFEDs R&S spec).

A notable requirement is that the SP MUST include a `PrivacyStatementURL` in its metadata, and moreover, the FedOp is required to perform the following substantive action:

> *Checks that the Service Provider's Privacy Policy document is available and indicates commitment to the Code of Conduct*

before tagging the SP with the CoC entity attribute. Legal will probably have to review any certification process that is put into place. It is not known if legal will have to review each application submitted, to determine compliance with CoC. A possible pre-emptive action would be the following:

Recommendation: Standardize the Code of Conduct language that the SP must include in its Privacy Statement.

The requirements around `<md:RequestedAttribute>` elements in metadata are likewise notable in that it appears the InCommon Federation will have difficulty meeting them, at least as things stand now. First let's give some technical background.

Shibboleth and simpleSAMLphp treat `<md:RequestedAttribute>` elements in metadata differently. (AFAIK commercial software doesn't recognize them at all.) Out of the box, the simpleSAMLphp IdP automatically releases the requested attributes listed in SP metadata. Apparently this is desired behavior in EU hub-and-spoke federations (which is where you find significant deployments of simpleSAMLphp). OTOH the latest version of the Shibboleth IdP (which is the dominant software solution in the InCommon Federation) can leverage requested attributes in metadata but like all attribute release policy in Shibboleth, that requires explicit action by the deployer.

More importantly, in the InCommon Federation we support `<md:RequestedAttribute>` elements in metadata *for informational purposes only*. AFAIK there are no IdPs that leverage these elements in SP metadata. In fact, our recommended practice is to release the entire minimal subset of R&S attributes to ALL SPs.

Furthermore, we do NOT support the `isRequired` XML attribute on the `<md:RequestedAttribute>` element in metadata. There was an extended debate about that when R&S was being launched. The upshot is that `isRequired="false"` by default (according to the schema), and therefore any given requested attribute is optional by default. This means that EU IdPs won't be releasing attributes to an InCommon CoC SP any time soon, since entities in the InCommon Federation will have difficulty supporting the attribute release mechanism called out in the CoC service category spec.

Bottom line: The attribute bundle approach used by R&S is a more rational approach to attribute release.

Recommendation: Avoid the use of `<md:RequestedAttribute>` elements in metadata to operationalize the Code of Conduct category. Consider using the attribute bundle approach instead.

Given recent discussion on the REFEDs mailing list, apparently there are others in the community that agree.