Summary of Attribute Release Requirements

One of the challenges faced by all federations at the moment is the need to improve the flow of attributes between IdPs and SPs for a wider range of use cases to be addressed by federations. A recent discussion on the REFEDS mailing list led to a long conversation about the approaches currently being used by federations to support attribute release.

The following is a summary of the list discussion and some thoughts on how to progress these issues.

Discussion topics

--- Using existing Entity Categories ---

At the time of writing, only InCommon and SWAMID (http://wiki.swamid.se/display/SWAMID/Entity+Categories) have made much progress with the use of Entity Categories. It was noted that both had a category for "collaborative services for researchers and scholars" but that the definitions and requirements were slightly different. Tom Scavo explained that InCommon had specifically chosen the word 'scholarship' and not education due to the precise meaning of the category and would recommend that other federations follow suit. SWAMID have an additional requirement that members of this category must also be part of one of the safe data processing categories. InCommon do not have this issue due to the differences in data protection laws in Europe and the US.

It was noted that Entity Categories are mostly intended to address the 'bundle' approach - i.e. send everything or don't participate. Although granularity has been introduced in some use cases, it is supposed to be a bullet approach to address the problem of attribute flow. It also noted that categories are built around generalised use cases: an IdP deciding to "release attributes to the X category" is making a decision based on participation in that use case, not just a yes/no on everything the federation operator might think is acceptable across the whole set of possible use cases.

For any interfederation use cases, it will be necessary to have transferable Entity Categories that work across the federation boundaries.

"UPDATE FROM RENATER, APRIL 2013:"

The InCommon Technical Advisory Committee will recommend a new category called the "Service by Affiliation Category" to the Steering Committee. Quoting the draft definition of the category:

"The Service by Affiliation (SbA) category identifies service providers that benefit InCommon member institutions' community members (faculty, staff, students, and others) based solely on their affiliation with their institutions. For example, a software company might offer discounts to university students and faculty. Institutions that support the Service by Affiliation Category add value for their community members by facilitating access to these services with very little administrative overhead."

RENATER have defined SP categories within their federation. They have two kinds of categories: type of service (groupware, elearning, e-documentation, etc) and target population (national, community, local). This information is populated by SP admins while registering their SP. Categories is used for 1) publishing purpose (classification of SPs on the federation web site) and 2) generating Shibboleth attribute filters that IdP use instead of maintaining filters manually.

--- Problems for the Proxy Approach ---

It was noted that the TERENA SP Proxy approach raises specific problems when it comes to asking for attributes to be released as it doesn't allow any granularity for the different services it protects. This means it has trouble meeting the 'is required' standard for release.

--- Declaring Attribute Requirements and the FedOp role ---

Many federations have some sort of process in place for listing the attribute requested by SPs. This ranges from simply asking SPs to note these in an AttributeConsumingService element in metadata, to more formal requests that are checked and audited by federation, to processes as part of an automated federation registry. It is clear that there is little consistency across federations as to process.

Federations are also adopting different processes for helping IdPs manage the release of attributes. This includes everything from simply presenting information, to providing attribute filter files (SWITCH, Renater). It was noted that a more dynamic approach to attribute filters is now available for Shibboleth as part of the Configure+a+Shibboleth+IdP+to+Support+R+and+S+Shibboleth-ImpoSupportRandS-%E%BF%EF%BB%BFReleaseaDynamicSubsettingR%25SBundle u[Approve software].

One of the benefits of having some level of FedOp role within the process of attribute release is part of an IdP risk assessment. It was noted the IdPs benefited greatly from having a clear process to point at and say 'this is why we are releasing' rather than depending on individual administrators to make unguided value judgements (which has led to poor levels of release).

The RequestedAttribute element was discussed at length. General opinion was that this should not be relied upon as a mechanism to address the problems of attribute release and flow, but the opinion was not unanimous.

The [[Data protection CoC|Data protection Code of Conduct]] recognizes those SPs who reside in EU/EEA and are committed to the data protection directive. The Code of Conduct isn't an Entity Category (such as Research and Scholarship) and doesn't define any attribute bundles. The Code of Conduct relies on RequestedAttribute elements in metadata as the mechanism to ensure minimal disclosure.

"UPDATE FROM RENATER, APRIL 2013"

RENATER have limited use cases of attribute filters that group SPs by type of services; most IdPs use attribute filters that gather SPs regarding their target population (national, all). Currently the federation metadata neither includes RequestedAttribute elements (to declare user attributes expected by an SP) nor SP categories.
Now that Shibboleth IdP (2.4.0) natively includes the feature mentioned below as a uApprove plugin, we might give up the attribute filters generation approach and complete our federation metadata with RequestedAttribute and SP categories.

RENATER also have use cases of SPs targeted at a group of IdPs. The SP needs a subset of the federation metadata to build its Discovery Service. The IdP needs attribute filtering for the groups it belongs to. Some group of universities are even building their own federation to achieve this. RENATER would like to provide some kind of sub-federation service, provided by our national federation registry. The federation metadata (or sub-federation metadata) could include categories to tag SPs/IdPs belonging to such groups of entities.

"UPDATE FROM DFN, APRIL 2013"

Since the DFN-AAI metadata management system provides support for entity categories only since recently, there's only one entity category in productive use. It is used by an IT infrastructure project[1] to build a virtual sub-federation, implementing both SP- and IdP-side filters based on this entity attribute value. Currently, this specific category is only available for entities listed on a whitelist maintained by the technical project coordinator and which is consumed by the federation's metadata management system at regular intervals. DFN planning to implement a similar mechanism for supporting the CoC entity category. The PrivacyStatementURLs (SPs only) are regularly harvested and checked for references to the relevant CoC version. Every entity positively checked is added to a list which is used to toggle the availability of the CoC category.

=== Auditing / Processing Attribute Requirements ===

It was noted that the proposed REFEDS Federation Operator Procedures template should include a section on standard processes for dealing with checking attributes requested by SPs and auditing entity categories. The big problem that exists here is that we have disparate practice across all federations at this point in time and it will be difficult to align them.

Audit / checking can mean everything for checking for accuracy / typos, to checking whether the assertion is in some sense true. The more stringent and demanding such checks will be, the more likely it is that the FedOp will at least share liability for any misuse of data resulting from relying on such information.

For larger federations, the type of per SP checking that is possible in smaller environments is something that cannot be achieved in general and is not seen as scalable. Where federations are running audits or check on attributes requested, we need a common way of understanding to what level. Does this happen only at registration, are SPs asked to redclare, are random checks carried out to ensure that information is as documented?

It was noted that the [[Data protection CoC|Data protection Code of Conduct]] work has the concept of a "coarse check" by the Federation Operator [[Federation operator's guidelines|as part of its supporting documentation]]. It also defines a process of defining [[What attributes are relevant for a Service Provider]].

As noted in the work to process template / recommendation processes around FOP, it is important for us to improve our understanding of trust in the interfederation space by improving the ways in which we can consume and interpret federation metadata registration policies and other such processes.

How can we ensure that the points of process are equal?

"<blockquote>If your federation makes a promise to your metadata consumers that an SP's RequestedAttribute attributes in metadata are "not only" what the SP themselves claimed "but also" reasonable for the SP's business purposes, then unless a partner federation's definition is the same then you can't "trust" that metadata, and you're probably going to want to filter out the RequestedAttribute (and AttributeConsumingService) before republishing: Ian Young</blockquote>"

== Is this a Service / Cert Mark? ==

Do we need something to represent these ideas outside of the metadata in the form of a service mark / cert mark? This would be a 'sign' that could be recognised by organisations and end users to know that they can make sensible decisions about releasing data.

== Proposed Actions for REFEDS ==

* When available, move the [http://macedir.org/draft-macedir-entity-category-00.txt macedir.org] draft into the REFEDS RFC Stream.
* Focus on shared values within a namespace, based on federation declared categories.
* Define common entity category descriptions for Research and Scholarship and the Code of Conduct as first two well understood areas.
* Role out these entity categories with willing federations.
* Continue discussions to include other candidate categories (mostly in the nren-service / hei-service / student-service space).