Meeting requirements for person identifiers from Grid resource providers

To obtain editing access to this space (working group members only), see instructions at http://middleware.internet2.edu/docs/internet2-spaces-instructions-200703.html

Grid Use Cases

(The information in this section was provided by Jim Basney <jbasney at ncsa dot uiuc dot edu>)

The grid use case considered here actually spans two projects with somewhat different attribute requirements:

1. Go TeraGrid (attribute requirements)
2. CILogon (attribute requirements)

Both grid service providers require a **persistent, non-reassigned identifier**. Preference is for ePTID (simply because it is non-reassigned by definition) but ePPN will suffice (with some understanding about the reassignment policy).

TeraGrid knows the GivenName and SurName already, but CILogon doesn't, so CILogon requires GivenName and SurName (or DisplayName) in addition to the identifier. Thus the fact that ePTID is non-correlatable is mostly irrelevant in the case of CILogon since other correlatable attributes are required.

As of November 16, 2010, Go TeraGrid trusts 31 InCommon identity providers:

- 12 IdPs provide ePTID
- 14 IdPs provide ePPNs that are never re-assigned
- 5 IdPs provide ePPNs that are re-assigned in some circumstances

"So far it's just a small sample of the InCommon membership. I'd be very interested to see InCommon survey all members about whether they support ePTID (and if they have plans to, and if not, why)."

Grid RP administrator requirements on person identifiers in federated use cases

1. The identifier must be *persistent* (as opposed to *transient*) over time. This does **not** mean the identifier is permanent. Indeed, either the IdP or the user may choose to discontinue use of the identifier at any time.
2. Once an Identity Provider has asserted a persistent identifier for a particular real world person, the IdP should not *reassign* that identifier to a different individual. If the IdP does reassign identifiers, the IdP must accommodate the RP's need to manage reassignment-based risks.

"Participants are expected to keep internal logs with accurate date/time stamps that allow for security incident response. In particular, an Identity Provider should be able to identify the specific individual associated with an opaque identity presented to a Service Provider."

Issues to be addressed:

- eduPersonPrincipalName weakens privacy by its easy associativity and by the fact that all RPs receive the same value
- eduPersonTargetedID is difficult to implement and deploy, and therefore it is not widely supported by IdPs (at least in the U.S.)
- a significant proportion of InCommon IdPs assert eduPersonPrincipalName that is not reassigned
- both sets of attribute requirements above are difficult (if not impossible) to encode in metadata as a coherent set of `<md:RequestedAttribute>` elements

Possible resolution of issues:

- Have each IdP determine the minimum number of years before a previously assigned eduPersonPrincipalName will ever be reassigned to a different individual. Call this the "ePPN non-reassignment interval" and recommend that it be published in a well known and accessible place.
- Promote broader support for eduPersonTargetedID
- Define a new identifier with the required properties