An upcoming change in the attribute structure

SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

Tr&Id WG Meeting, Berne, 15 May 2019

How to Identify Users in AAI?

Use a unique (identifier) attribute:

- swissEduPersonUniqueID
- mail
- eduPersonPrincipalName
- eduPersonUniqueId
- eduPersonTargetedID
- **subject-id (New!)**
- **pairwise-id (New!)**

swissEduPersonUniqueID (urn:oid:2.16.756.1.2.5.1.1.1)

Examples	112359@switch.ch 6D31303-134363-53001@uzh.ch
Unique	
Non-Reassignable	
Opaque	(not the case for subset of users of some universities)
Persistent	
Targeted	
Usage	SWITCHaai, very well supported and widely used in CH
Comment	😀 Still most reliable identifier in SWITCHaai ☹ Not available outside CH

mail (urn:oid:0.9.2342.19200300.100.1.3)

Examples	lukas.haemmerle@switch.ch john.doe@example.org
Unique	
Non-Reassignable	(some universities reassign e-mail addresses after a few days)
Opaque	
Persistent	⚠️ (unizh.ch ➔ uzh.ch, zhwin ➔ zhaw.ch, …)
Targeted	
Usage	International, very well supported and used world-wide
Comment	😲 Case-sensitive by definition 😒 Should not be used as identifier attribute!!!

eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)

Examples	johnd@example.org myloginname@university.edu
Unique	
Non-Reassignable	⚠️ (unspecified, some organization reassign it)
Opaque	(not generally, looks like an e-mail address)
Persistent	
Targeted	
Usage	Worldwide very well supported and widely used.
Comment	😎 In SWITCHaai: eduPersonPrincipalName = swissEduPersonUniqueID

eduPersonUniqueId (urn:oid:1.3.6.1.4.1.5923.1.1.1.13)

Examples	23489cd8u@example.org sdc32easdsaf@university.edu
Unique	
Non-Reassignable	
Opaque	
Persistent	
Targeted	
Usage	⚠️ Worldwide, not very well supported so far
Comment	😎 In SWITCHaai generally: eduPersonUniqueId = swissEduPersonUniqueID But localpart may only contain a-z, A-Z, 0-9!

eduPersonTargetedID (urn:oid:1.3.6.1.4.1.5923.1.1.1.10)

Examples	https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!yrVdvdAmohZY+c[...]/Dubc=
Unique	
Non-Reassignable	(might be reassigned/reused if identifier attribute that this depends on is reassigned)
Opaque	
Persistent	
Targeted	(different value for same user for different SPs)
Usage	⚠️ Worldwide, moderately well supported.
Comment	😟 Not a a string attribute value but a XML SAML NameID. 😨 Bad implementation support (almost only Shibboleth/SSP) 🤮 Ugly to display to user and very long to store 😮 Case-sensitive by definition

New identifiers: subject-id / pairwise-id

Why? – Because “identification of subjects in security protocols and applications has

- a fraught history of inconsistent syntax,
- bugs,
- terrible but deeply cemented practices such as misuse of email addresses,
- vertical market-specific approaches, and
- failure to precisely communicate intended semantics and constraints.”
- “use of the NameID feature is confusing”

➔ Clean-slate approach that abandons existing practice

How Should the New Identifiers be?

- As stable as possible
- Little or no risk of reassignment to different subjects
- Opaque
- Compact
- Simple to handle and manipulate (case-insensitive!)
- Clearly express the scope of an identifier’s uniqueness
- Ability for different parties to issue the same identifier

subject-id (urn:oasis:names:tc:SAML:attribute:subject-id)

NEW

Examples	idm-1234567xy@example-uni.com 23C8IODOI@uni-xy.edu
Unique	
Non-Reassignable	
Opaque	
Persistent	
Targeted	
Usage	Just being implemented by first IdPs
Comment	😀 Almost identical to eduPersonUniqueId but better defined 😀 Case-insensitive by definition

TO SUCCEED EDUPERSONUNIQUEID

pairwise-id (urn:oasis:names:tc:SAML:attribute:pairwise-id)

NEW

Examples	idm-8901ab@example-uni.com 8DOH4D9IDPU=@uni-xy.edu
Unique	
Non-Reassignable	
Opaque	
Persistent	
Targeted	(different value for same user for different SPs)
Usage	Just being implemented by first IdPs
Comment	😀 Case-insensitive by definition

TO SUCCEED EDUPERSONTARGETEDID

Outlook

- Guides on supporting subject-id/pairwise-id probably available in Q3 2019
  - Likely easy to support via configuration relying on existing identifiers
- Supporting them mostly relevant for IdPs whose users access international/eduGAIN services
- Unclear how fast other federations will adopt new identifiers

SWITCH

Working for a better digital world