FAM25 Conference

Attributes and Identifiers - what have they ever done for us?

Jon Agland

Technical Services Manager

Trust and Identity

Jisc / UK federation

2nd July 2025

The UK Access Management Federation

FOR EDUCATION AND RESEARCH

Attributes

- **SAML attributes** - typically describe a user in assertion
- **entity attributes** - describe a SAML "entity", often use with entity categories
- **LDAP attributes** - describe objects in a directory

```
<?xml version="1.0"?>
<saml:Assertion
 <saml:saml="urm:oasis:names:tt-SAML:2.0:assertion">
  ID="1234">
<saml:Issuer>issuer.example.com>
<saml:Subject>
 <saml:NameeID>-</user@example.com>
 <saml:AttributeStatement>
<saml:Attribute>
<saml:AttributVave"role">
 <"admin>
</saml Attribute>
```

Attributes

pieces of information about a user that are included in a SAML assertion, used by a service provider to make access decisions for a protected resource

some AI platform

Attributes - What do they do?

Typically in federations, they relate to a user..

- Identifiers
- Entitlements
- Affiliation
- Personal information / personal data `( ! )`

Attributes in R&E federations

Within SAML Research and Education federations..

- eduPerson- see eduPerson standards
  - Written with SAML federations in mind
- Other schemas in use `inetorgperson` etc..
- Other federations use `schac` SCHAC standards

eduPerson usage

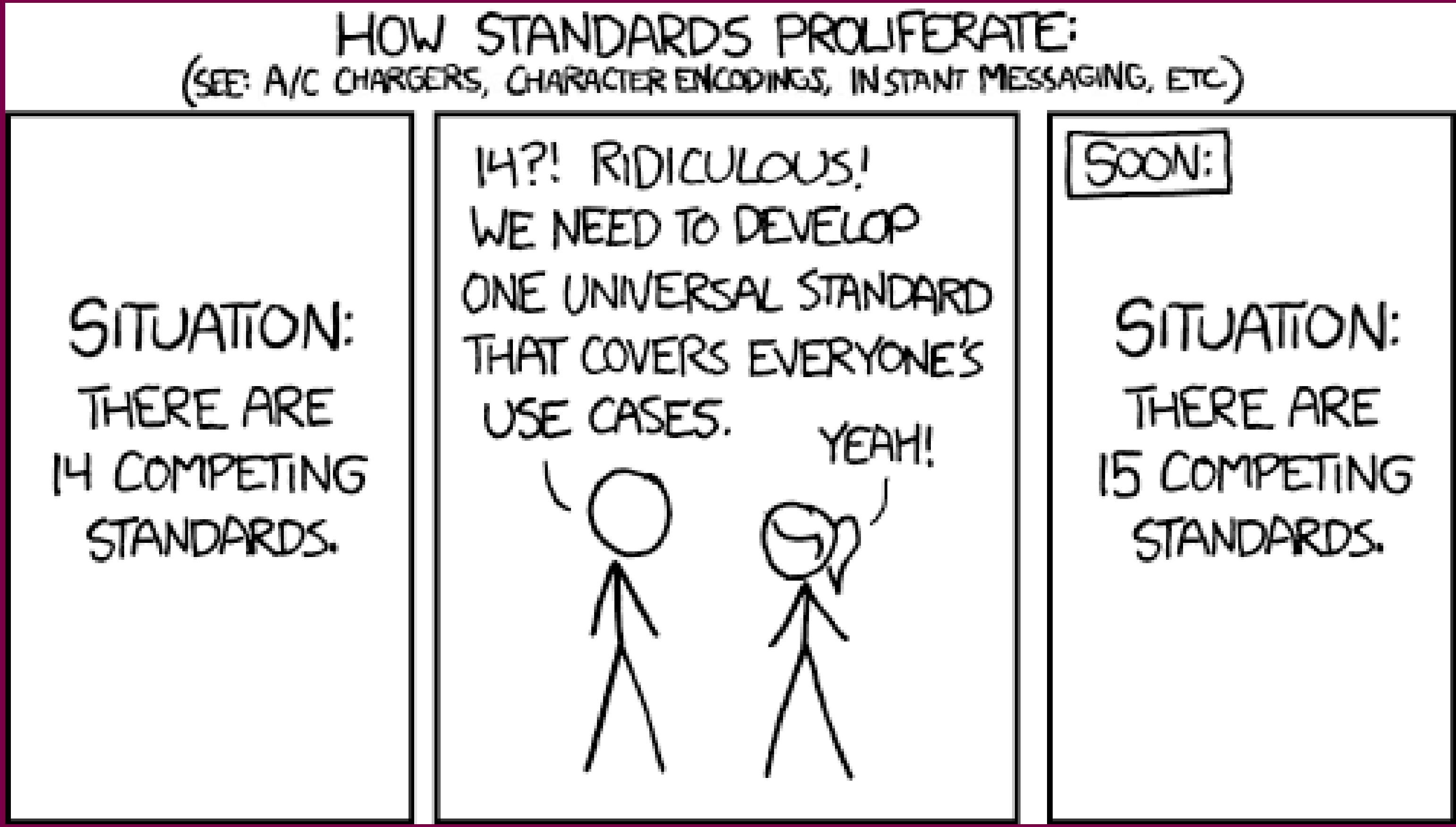
- UK federation attribute recommendations are;
  - `eduPersonTargetedID` (*used as identifier*)
  - `eduPersonScopedAffiliation`
  - `eduPersonPrincipalName` `(!)` (*used as identifier*)
  - `eduPersonEntitlement` `(!)`

eduPerson schema

- Within the schema
  - There are multiple versions (at least 9) of the schema
  - UK federation tech recommendations were defined based on `eduPerson12`
  - Likely that attributes defined in later standards are in-use
    - Example `eduPersonOrcid` - `urn:oid:1.3.6.1.4.1.5923.1.1.1.16` a
  - Conversly some attributes signalled
    - As of eduPerson 2020-01 `eduPersonTargetedID` - `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`

DON'T PANIC

There's another "new" standard...


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Technology can be slow to change

protocols

- `IPv4` `->` `IPv6`
  - [RFC1883] - When?
  - Are we nearly there yet?
- `RADIUS` -> `Diameter`
  - When?
- `SAML1/SAML1.1/Shibboleth` -> `SAML2.0`
  - When?
  - Are we nearly there yet?

Subject identifiers

- 2019 standard ratified
    - `pairwise-id` different format to eduPersonTargetedID.
    - `subject-id` same format as `eduPersonPrincipalName / eduPersonUniqueID`
- attributes in the metadata to signal what you want
    - `EntityAttribute` - `urn:oasis:names:tc:SAML:profiles:subject-id:req`
- do we have enough adoption?
- 2021 - UK federation - Subject Identifier webinar slides and - webinar recording
- OpenID SubjectIDTypes specification compatible with.

What does the future look like?

- existing: SAML federations
- new: OIDC federations - do we adopt?
- existing: eduPersonTargetedID as the identifier
- new: identifiers - do we adopt `pairwise-id` / `subject-id` ?

But what about the users?

- Scenario: Jon at the supermarket

What should we do for user experience?

as Identity Providers

- As identity providers
  - Maintain the old
  - Embrace the new
  - Start supporting `subject-id` / `pairwise-id`
  - Understand what attributes we are releasing to what service.

What should we do for user experience?

as Service Providers

- Support multiple attributes and identifiers
- Collect them
- Be agile and which can be used
- Don't rely on a single identifier
- Utilise attributes in metadata
  - Requested attributes
  - Signaling attributes
- Implement standards fully

What should we do for user experience?

as federations

this slide is blank, you tell us

Can't we just use email address?

Email Address as an Identifier;

- Not guaranteed unique to a subject
  - e.g. `service@ukfederation.org.uk`
- Maybe be re-assigned
  - e.g. `vc@camford.ac.uk` , `joe.bloggs@camford.ac.uk`
- Life events or affiliation may change it
- Not always assigned by institution
- May not be validated
- See InCommon/Internet2 - Why Email is not an appropriate user identifer?

Libraries

Libraries are a key use case for the UK federation

- They are why we exist.
- but are *for education and research*

Libraries, Privacy and Humans rights

- CILIP - "the Library and Information association" - Protecting the Individual's right to privacy

“Freedom of access to information and freedom of expression as expressed in Article 19 of the Universal Declaration of Human Rights, are essential concepts for the library and information profession. Privacy is integral to ensuring these.”

- UN - Universal Declaration of Humans Rights

Enabling attributes for research

sometimes we need more personal data and more assurance... so IdP operators

- Review REFEDS assurance framework
  - Whilst doing that see what level you can support now, and maybe what later?
- As an IdP support `eduPersonAssurance`
- Review Research and Scholarship entity category support and look to support it
- Support and adopt REFEDS MFA
- Support and adopt Sirtfi

Setting future directions

- Open ID federation spec - *no mention of attributes!*
- eduGAIN Technical Profiles Working Group - *Jisc/UK federation will be participating*

That's all folks!

- Jon Agland jon.agland@jisc.ac.uk
- Trust and Identity trustandidentity@jisc.ac.uk
- UK federation service@ukfederation.org.uk