Structured Attributes

TF-OpenSpace – Session 1, room green. 12 February 2014.

Lead by: ?? ()

Attendees:

Notes:

Problem:

1. ...

Structured Attributes

- Attribute Aggregation -> Structured (Maarten)
- Structured Attributes - More than just strings (Thomas L)

NOTES

The scope of the discussion is about SAML attributes and how to transfer more complex attributes. Whether the attributes are transferred from the IdP to the SP or from an AP to an SP is not very relevant.

Several aspects were considered:

- the value attached to the attributes a possible architecture to aggregate attributes from different sources
- a possible architecture to aggregat attributes from different sources

Clearly if attributes become more complex, applications would need to adapt their APIs to process them. Do we have use-cases for more structured attributes? Do SPs need structured attributes?

Olivier mentioned that some use-cases for more structure attributes appeared in the e-Learning sector.

One way would be to provide both the simple value as well as the structured value. Those applications that cannot process the structured value would just ignore it.

We should be careful not to ship too much information for each authN. Maybe AP should be shipping the structured attributes.

It was agreed to decouple the problem in:

1. Define the structured attribute
2. Define who wants structured attributes and how to make them consumable for SPs. A couple of use-cases were presented (Roland, Clarin, Olivier).
3. How do you present the aggregate attributes from different source?

Action: for those attending this section, to provide use-cases that would benefit from structured attributes. Ideally the use-case should be presented with:

- describe the authorisation decision in words
- list potential attributes to support this
- identify the sources of these attributes

Use case: **e-learning**

- User is subscribed to multiple courses and has different roles in the different courses
- In most courses the user is participant, but in one course the user is teacher and in other the user is assistant
- The course management system where teachers publish their courses, assign assistants to courses and students subscribe to courses

NOTES

Licia - can we work to provide people who come to us for help with some solutions?

We tend to provide overwhelming amounts of information/problems?

Are our AAI solutions not easy to sell?

TW: We can see how their requirements are difficult, where they can't.

Also, focus on VOs etc. hides some of the simple, basic answers that are not obvious to non AAI experts.

Christos: TF-STorage who do have knowledge were still confused. Even worse for those outside.

GÉANT Cloud providers - difficult to even work out the first step.

Trying to find information - info targeting is all mixed between federations, SPs, NRENs etc.

Need a more customer based approach that does not cover unneeded complexity.

KW: Supporting users is something that happens on a per country basis.

This group has 2 goals - educate people AND advanced topics and this can clash.

Christos:

eduGAIN has been evangelized in many different ways - expectations are very wide.

SPs - I want to provide across europe, what do I do? What if I don't want to join a federation in one country? Looks complicated

Things don't make sense at a pan-euro scale to users.

Ann: Explaining things in a too complicated manner.

Christos: 'publish information' got translated to 'join edugain'…misunderstandings.

KW: Should TF-EMC2 produce a document on what needs to be done for a pan european service?

Ann: GEANT should document edugain properly but TF-EMC2 can have a role working out techs and options that prevent SPs being confused by differences locally.

Stefan: Why should I have to join any federation?

KW: Is the model too complex?

SW: Some services don't need much.

TW: eduroam CAT does have a complex AuthZ but user is protected from it.

ANn: what to non experts need to be able to replicate CAT's success.

SW: Tiered approach with simple entry point.

KW: Every SP should be allowed join any federation as long as they have certain minimal reqs.

RH: AuthN as the default minimum function.

KW: eduGAIN as a potential entry point? SPs not exactly in federations.

LF: REEP as a potential solution? Not finished.

Ann: Id federations then more purely for identities.

KW: Users then have to be enticed to share more info.

Wholesale/retail interaction difficulty. NRENS/Federations operate at wholesale.

Ann: finance influences what is possible. IdPs are not paid to release attributes for example. Nobody pays.

Journals can handle this. Harder for EFSRI etc.

TL: Once AuthZ comes into play, difficulties arrive.

eduperson targeted ID as basic service.

CLARIN: that's a 2nd class attribute. More advanced use cases are more likely.

Ann; Who then is responsible for supplying the needed info?

KW: advanced info has consequences - could take the task themselves e.g. own e-mail verification system or outsource it to a service.

Christos: Commercial SPs are often happy to collect info themselves. Problem is how to authN the user in a consistent manner.

SW: If AuthN is the base service for free. We then potentially go into competition with ourselves. Need to make sure any value added attribute services we have are cost-effective.

Action point: can people ask in their organizations on the feasibility of the basis authN based on targeted id. service and SPs not in federations but via eduGAIN direct?

TL: In principle is achievable with caveats about support contacts etc.

KW: Hard for mesh federations.

SW: SP submits a web form on edugain, get a report on which IdPs support *now*. Could have layered reporting e.g. per country.

Roadmap for eduGAIN:

Step 1. IdPs in eduGAIN

Step 2: and support targeted ID

Step 3: and actually release the attribute and consume which SPs metadata

[**ACTION**]