Nicole: We have put this initial draft together, starting point, requiring inputs from people. We captured things said so far. Some of them might be dropped or require change.

Let’s take a look at these problems statements.

We came up with a proposal based on the discussion we had.

For each recommendation we make, we reference it back to the problems statements and provide supporting evidence for why we want to solve these issues.

Today let’s check the problems statements first:

Prob.Statement 1:

1. With over 8000 entities included in eduGAIN, the number of different variables in the service experience between Identity Provider (IdP) and Service Provider (SP) has become extremely complex.

Everyone happy about this? Yes.

1. The inability to predict what information will be exchanged between IdP and SP makes it difficult for services to rely on eduGAIN mechanisms to offer services.

Slex Stuart: what is eduGAIN mechanisms: the service providers? Nicole: we might want a different wording there.

Therry Smith: What is in the “information meant there”? User attributes or Assurance, we have been broadly meaning information.

1. The very different processes adopted by Identity Federations in how they interact with eduGAIN causes confusion.

Are policies covered by processes?

OK to add “policy” there

Maarten: wouldn’t this overlap with 6? Nicole: it probably does it a bit

Alex Stuart: we would need one recommendation peer problem statement at least.

Nicole: we can refine later as we go along.

1. The different funding, staffing and service levels at Identity Federations makes the service offer variable across the eduGAIN environment.

Maarten: is this actually an eduGAIN problem? It affects eG but there is not much we can do

Nicole: there is little eG can doo here. But we wanted to highlight this. I would kind of agree with you.

Albert Wu: level of services are different, what is the variation we are talking about, could help

Nicole: we want to mention that for some federation is easy to do changes, have stuff to provide IdPs or SPs, whereas for some federation there is ½ an FTE in their spare time, so this is much more challenging.

Terry Smith: maturity and capability is the word to use here?

Capability and maturity of the Id Feed itself.

Alan Buxey: eG could provide IdP-a-a-S: there are indirect ways too deal with this.
Alex Stuart: it is really capacity building in these federations: terry you do a lot of stuff, woud be nicee to know how you onboard federations in APAN.

Terry: in APAN we have mature federations taking care of MFA stuff..It varies a lot.

Nicole; this is a problem that exists, people here agree on this.

We will cycle back on this.

1. Entities are slow to change and match changing security, regulatory and policy requirements (e.g. Sirtfi, CoCo, baseline).

Nicole: I think here also capabilities and maturities od entities could mnaake it here.

Alan Buxey: not directly in control of eG, sometimes is not the entities but the federations.

Nicole: I think eG can act here, raising the bar, changing the standards. We have some possible recommendations against this one. We wil;l get back to this.

1. Identity Federations have different processes and requirements to implement the security and policy standards.

Nicole: I think we could add this into #3. Any disagreement on the actual point or on integrating with #3 ?

No.

1. eduGAIN itself is slow to make decisions and necessary changes to its service model.

Any objections ? clarifications ?

Maarten: 7 and 8 could be combined, I think 7 is a result of 8.

We could combine, there is a correlation on this.

1. The mission and role of eduGAIN is unclear, leading to different expectations.

Comments ? No comments.

Nicole: these are the problems statement. Anyone thinks we did not capture something here ? Anything clearly missing here ?

Meshna Koren: we are mentioning the interaction between federatins and eduGAIN, and ldPs and SPs, but I think eG couyld do more perhaps helping institytions to join the federations. Even if the federations have different initial policies, this is not necessarily a problem for institutions in countries, but this could be a problem for the SPs:

Needs of SPs and eduGAIN itself: we miss a clear onboarding process.

This is part of it.

An SP needs to join a federation, but providing a Starting Point for SPs: why, where do you start, while joining a federation.

Nicole: any other comments on the problems statements ?

The document will stay open for comments of course.

If you see issues with the introduction or any other bit of the text.

Nicole: let’s move on with the recommendations now:

We have done recommendations in the same way we did the problems, relating to the observed issues.
Recommendation #1: enforce the use of security and tech contacts

Any objections?

Alex Stuart: what is management contacts here?

We have a process for catching delegates and deputy but sometimes we lost the entire team. This is reflecting the typical process: you need an authoritative mgmt contact.

Albert Wu: this might be part of problem 4.

Kevin Hickey: "enforce" what does it mean here?

How do you bring people along if you do not have much control?

Nicole: I think eG can only unblock access or suspend a federation. This refers to do this more regularly.

Alan Buxey: 33 or 37 members have security contacts - 33 or 37? maybe you’re considering the feds in Joining phase?

Nicole: I will double check these numbers.

Recommendation #2:

Upgrade the eduGAIN technical infrastructure and policy process to allow eduGAIN to filter individual entities as appropriate

Comments?

No comments here.

Recommendation #3:

Support the implementation of the eduGAIN CSIRT and develop robust security incident response practices in conjunction with Identity Federations

Nicole: This is already happening, this is reinforcing the support for this!

Questions here? None.

Recommendation #4

Define clear guidance as to the required standard for “authentic, accurate and interoperable metadata” for eduGAIN

One of the req of BE is to have authentic, accurate and interoperable MD in eduGAIN. What is it? currently compliance with SAML profile, but also we have the validator, or the JISK fed tool. So it is a bit unclear: it is a high level recommendation, we might detail this more.

Here Alex suggested to add about interoperability: this is very useful.

Alan Buxey: I don’t think it will really address problem 1, just help there.

Nicole: there is quite some work to do here.

Is there anything missing about our rec on BE?

No.

-----------

Goal 2 Recommendations: Service provision

Establish 3 consistent profiles to be met by Identity Providers with increasing levels of functionality (anon, pseudon, personalized)

Every SP should at least support one of these.

Albert Wu: mostly around about how both parties (IdPs and SPs do benefit form this. If every IdP supported this, (they do today, just do not declare) - how will SPs ans users benefit from these categories.

These are essentially attribute bundles definitions.

Nicole: the idea was that ATM about 3000 IdPs, when you connect to those, you have 3000 different experiences. So the idea is to have an idea about what my experience as an SP will look like.
Albert Wu: If I am an IdP supporting all of them (3), but because there is not explicit reqs on when I release those, the SPs experience will be nasty: I would not know which set I am getting unless I have another agreement in place, basd not n profile definition, but on other negotiations.

Alan: Don’t SPs have a tag on MD stating which ones of these profiles are required by them?

Albert: it is not a must, they cuually do not. Contracts have to be in place for this.

Alan Buxey: the idea of eG is to remove ned fr bilateral st ups.

But if every SP has to have bilateral conversation with 3000 IdPs

[ can’t all this be made dynamic ? mario ]

Meshna Koren: agreements and setting up fed access can be separated events. Often Much later in time after the agreement has been signed, the attribute releaswe is set up.

Albert Wu: at eG level, how does it work?

in order this to work, we need a component outside of eG.

I don’t know how we can turn this into asking in eG very IdP and every SP supports this.

Nicole: the idea is not to ask everyone to support, but everyone to state if they do: anonymous should not need any negotiation, normally.

Automatic attribute release should be supported.

Alan Buxey: those bundles are clearly defined: this helps avoiding SPs will ask for their weird version of attributes

Albert: I am not saying this is not useful, I say if we include them, we need to add additional information (talking about anonymous and personalized)

Nicole: anonymous and pseudonymous are under revision.

entitlement you cannot enforce it.

Albert: also organization ..

If you take away entitlement, is this still useful for an SP?

There is a bit of detail that ORG gives you.....

Nicole: consistency of vocabulary and of approach.

Nicole: I hear you Albert.

Albert: in InCommon we’re starting to look at the attributes bundles, and considering if including them in the InCommon baseline or not.

Nicole: we might have further conversation on this.

If we don’t have this, the question is: is there a way eG could solve this for the SPs?

Alan Buxey: what will happen to R&S ? Nicole: I don’t know the answer on this. We could include this in here too.

Meshna Koren: Visual Consent: w.r.t. attribute release, ask the users to choose the attributes they will pass on to the SPs or not, that will complicate the usage of the bundles.

Nicole: yes. consent is a problem here. yes, we need to think about how ot interact with it. I think the categories themselves reference this.

2.2

Create a roadmap to upgrade all entities to support Sirtfi, CoCo and Assurance and make a formal part of the eduGAIN policy requirements

Therry: I agree with Guy: is an international version of Co.co coming along now?

Nicole: we’re waiting for one person in the REFEDS SC to vote.

I think Alex’s point is about intermediate state.

Albert We: these 2 are “Baselinsh” - fit the baseline.
Alan Buxey: regulatory regions, local data compliance regulation:

you need a data compliance officer there.

There are a lot of out-of-bound issues to consider here.

Nicole: the doc is open, please take a look at it.
in the next meeting we will go through all of recommendations.
We could then focus more on the controversial one's.
Please take a look at what might be missing completely from the document!