Link to 2023 ACAMP Wiki

Advance CAMP Thu. Sept 21, 2023

Room - II

Session Title: Bridges and Proxies/OIDC Federation

CONVENER: David Groep

MAIN SCRIBE(S):
Niels Van Dijk, Jon Agland

ADDITIONAL CONTRIBUTORS:

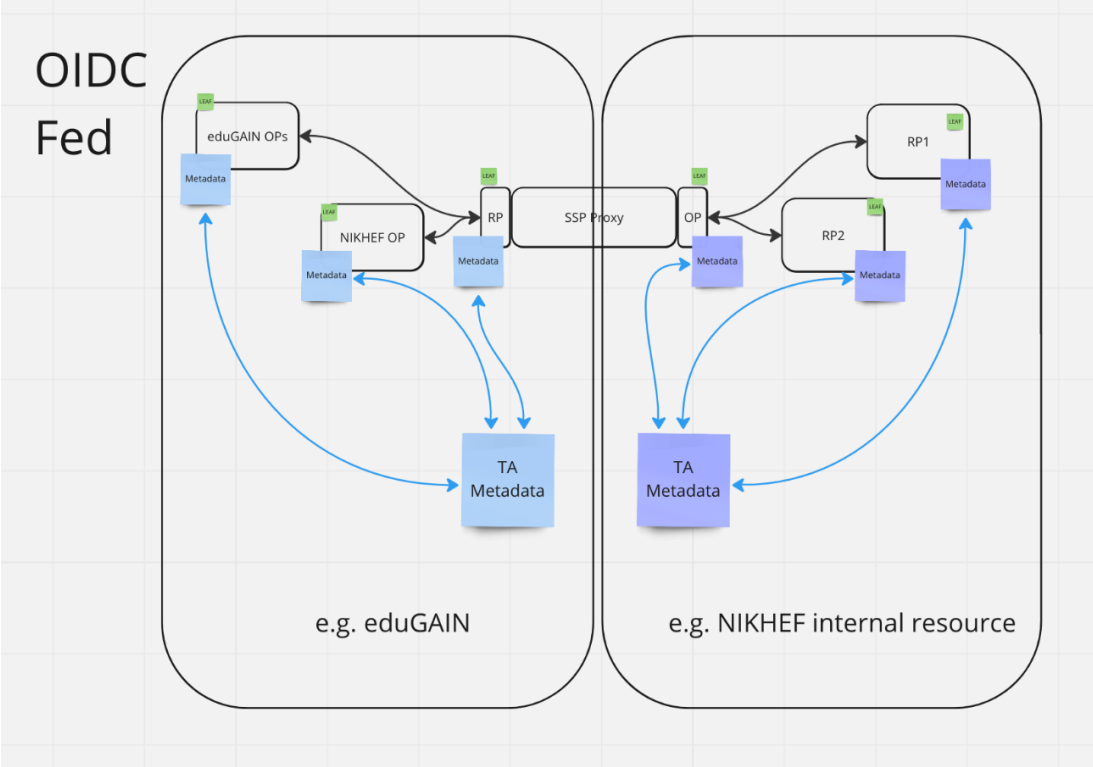
# of ATTENDEES: 20

DISCUSSION:

Introduction video into OIDCfederation:
https://wiki.geant.org/download/attachments/589070375/OIDCfed_mid-demo.mp4

Specs deepdive explained (slidedeck)
https://wiki.geant.org/download/attachments/607715591/Spec%20Overview.pdf?version=1&modificationDate=1678201337023&api=v2

OIDCfederation Specification: https://openid.net/specs/openid-connect-federation-1_0.html



David Groep:
Raise of hands
Who knows about

- Proxy: most in the room
- OIDCfederation: few in the room
- Bridge PKI (public key infra): 1

What was the problem that triggered this session?
Proxies are wonderful, they can be opaque and expose things to the outside world..
Proxy into eduGAIN using SAML, token translation, attribute transformation, augmentation
Membership services?

OIDC world, to amalgamate a set of RPs
Essentially overloading the proxy with two roles, technical role of translating one for format to another (+ augment of claims), but also bridging trust between both “domains”
In OIDC federation, you can chain metadata statements not by publishing to a list, but building hierarchies, trust anchors who can sign intermediates . multiple signatures on the same

OIDC federation based on a set of OPs, no technical reason why you couldn't expose all the other side of the proxy by cross-signing the metadata. Cross-signed set of trust anchors.
Re-doing Bridge PKI (which did not work in the first place, according to David)

Not just two trust anchors but two or three or four
While in many cases these are the same, both a technical proxy and policy bridge, can be separated.
Seperate the two concepts proxy and bridge
z
How do you build these sorts of federations?
simpleSAMLphp and Trust and Identity Incubator (GEANT)
Two different roles, what are immediate thoughts on cross-signing trust anchors

Niels Van Dijk: One comment, if you have OIDC federation, why would you need a proxy at all? Express on different sides, box of lego you can use for different purposes. Proxies will still be there, for instance for token translation scenarios e.g. for SSH, or another protocol on the other side of the proxy. Regardless of what is setup in OIDC federation and it's capability.

Other thing really wanted to do. In OIDC fed, you have three types of entities

- Trust anchor top-level e.g. edugain

Intermediate is pointing upwards, but same as above, but can have peers e.g. national federation [but does not have to be, could have 80 trust anchors let's say]

Finally, one or few entities SPs, typically institution one IdP, and number of SPs, different brand names for institutions and multiple IdPs do exist. In OIDC federation, not going to set the individual but have intermediate for the institution? Trust is inferred on the intermediate, and don't have to register each entity in the federation, but on the policy by which the institution intermediate can register in the federation. Even so flexible, and tested (almost completed) new SPs on the fly via another party in eduGAIN< with not action by other parties.

Christos Kanellopoulos: so flexible, that it will die by it's flexibility. If people are completely lost everyone is lost?
Tom barton: too many words of course we are lost :)
Christos Kanellopoulos: hasn't proved itself anywhere, production systems? [disagreement], unless we properly provide this, and simple, it will just die [agreement], it allows you to cut

yourself in many ways. Discussion that an OP federation and RP federation. Something that does not exist now or in the foreseeable future.

Niels Van Dijk: starting point from David that this is an early idea

Christos Kanellopoulos: discussion could be had at a different level, value of the proxies could happen, things are going in the direction. Simplify for universities who cannot handle the complex, but have nuclear scientists come play with us? Capacity to do that but hide it from the edges, where the is not capacity.

RP federations are not rocket science, new research services new are RPs, they are RPs without OPs, and that building OPs is more complex. RPs are teared

Pål Axelsson: OP and RP must share the same trust anchor? Per the design of this infra.

An OP cannot trust another trust anchor all the way down?
David Groep: You need at least one OP to make it useful.
Pal Axelsson : is that just a traditional proxy, in the bridge layer it's a totally different thing.
David Groep: Cross signing where you federate everything
Pal Axelsson: extremely context we don't start there
David Groep: profiling everything we want to do..
Pal Axelsson: Need to this in a good manner so it is useful
Tom Barton: More intermediates more policy process implements or organization functions who have that experience, so there is going to be a huge no technical complement following this and breaking new ground, training substantial aspect, so that they understand what they are agreeing to when they sign, but also verification, some degree when you delegate, i need to verify vs i don't some agreement. A lot to think through there…
David Groep: intermediates that mimic the old proxy scenario, as you don't control the RPs. Intermediate anchors. RPs will emerge and be torn down, dynamically created and are destroyed again. Are all signed by an intermediate trust anchor, OIDC federation could be created on
Pal Axelsson: agree, control RPs in that environment
Christos Kanellopoulos: AARC blueprint architecture [some know, some don't about this], proxied environment to transport identity and connect systems, working on a trust technical framework to use the proxies as a way to simplify the technical complex of OIDC. Number of

systems that can spin up at any moment, don't go to register themselves. Metadata publishes, RP doesn't need to know about this complexity
David Groep: Is it a proxy or RA that signs?
Christos Kanellopoulos: is the proxy, added value of that, complexity stays in proxy on wards to closed network of proxies, not sure if this is all viable, but to limit expansion of full understanding and tech capacity of a full OIDC federation. Using the proxies to hide the complexity from local parties. In order to consider the use case of short lived services, you don't need OIDC end to end?
David Groep: proxy as part of the trust
Pal Axelsson: single layer within the proxy, just use `.well-known` services
David Groep: hierarchical infrastructures will be see proxies, that import other infra proxies.
Christos Kanellopoulos: is there a way we can automate technically this whole co-signing technical trust establishment, assuming something we can all technical proxies. A way to get rid of the proxies without the complexity, all the signings imaging someone doing something
Davide Vaghetti: don't think the signing and distribution is complex if you do not use proxy. Metadata mgmt in a federation, OIDC flow is another thing. The main issue that they have to solve, that they wish to solve, that they have proxies anyway, vanilla OIDC connections are like vanilla saml that do not support multi-lateral federation or discovery. If you want to make them federated is to proxy, and that must understand OIDC federation. The federation is another component that can be put along to the proxy is the trust resolver and signing engine, and metadata distribution not embedded in the proxy, a lof complex that might be useless
Christos Kanellopoulos: imagines this has to happen at scale, and can this be automated?
Niels Van Dijk: entity needs to publish the anchors of which it is part, and to the trust anchor, intermediate via API. automatically cause it points upwards, it's now a member. Fully automatable in principal
Christos Kanellopoulos: offers open the floor
David Groep: who is lost *laughs_
Pål Axelsson: automatic signing can happen, happens in saml federation today.
Niels Van Dijk: Depends how you proxy behaves, metadata will need to propagate upwards, yet you services need to work in 5 minutes
Pål Axelsson: OIDC way might be the best way, but not as good as existing SAML, will this be an interesting journey?
Davide Vaghetti: If we can step back , what is exactly the problem of cross-signing? If I had an entity, what is the problem that an inter-federation service is trying to solve, the user of one of these entities would need a trust bridge, inter fed is doing this, is signing metadata from different federation and merging and republishing, could save the same problem without an inter

federation service? Having a common trust anchor between two intermediates between the two federations. Say you have edugain-a and edugain-b (or edugain and EGI) you could have intermediate bridges… with two different … the intermediate could remove having multiple trust anchors
David Groep: multiple not needed if trust can be established, you do need cross signing because RP/OP trust? Information between ultimate OP and RP can flow with out proxy
Davide Vaghetti: if that is the problem you want to solve, then metadata configuration is a problem, intermediate and trust anchor can establish policies, that can for example could use some type of algorithm that are not allowed in the federation? The metadata you are going to use for an RP is filtered through a metadata policy of a federation.
Niels Van Dijk: that's always the risk?
Davide Vaghetti: common trust anchor can define and apply common policies for all the entities that recognise the trust anchor
Niels Van Dijk: there could be no trust possible

Main reason for using a proxy?

David Kelsey (STFC): - OLD ARC proxy could not join the federation?
David (GEANT): agree and cross sign
David Kelsey (STFC):: different problem,
Niels Van Dijk: different protocol
David Kelsey (STFC): it's not just the attributes
Pål Axelsson: exist usage of proxies could still apply

David Groep: different roles of trust anchors and proxies, policy
Tom: drawing parallel with earlier session on "middlethings" by adopting this you are obliged to address those things
Davide Vaghetti: you will need high level of trust, you cannot apply same configuration to be both entities
David Groep: facilities in OIDC fed md, to constrain the trust.
Davide Vaghetti: you are to some extent by-passing those facilities
David Groep: in those cross signed facilities you could constrain

Christos Kanellopoulos: Who can do the cross signing?

Davide Vaghetti: not perse missing the cross signing not just missing this use.

Christos Kanellopoulos: asking just because you can do that, should you do that? ;-)
David Groep: referred to bridge PKI, that had a lot of interesting features - aimed for 25 years, gave up after 10.
Davide Vaghetti: second time the good one
Tom: community here, will try to
PKIs started at the top within countries…
Davide Vaghetti: need more than a 101 on a OIDC federation.

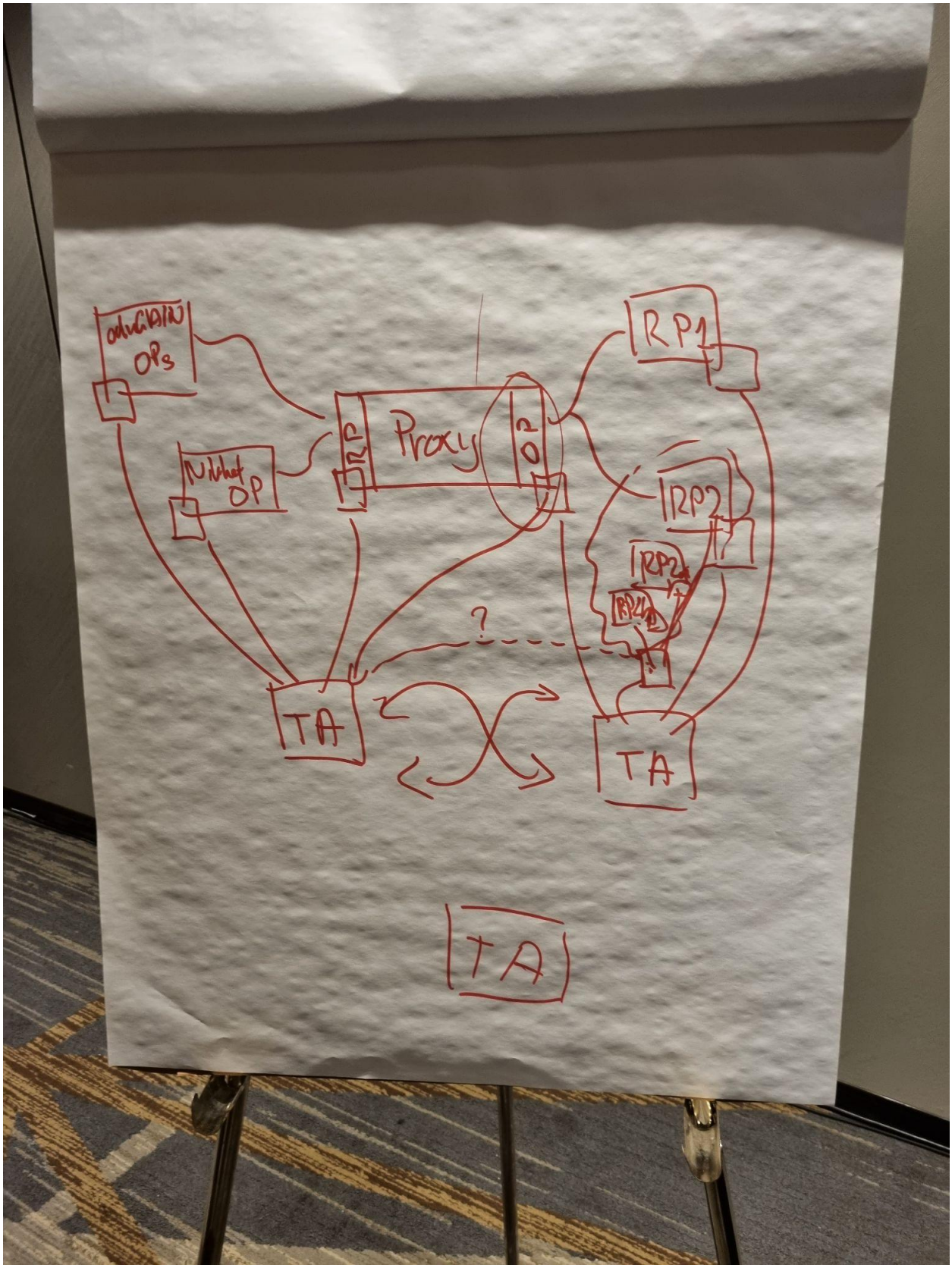
2023 specification on OIDC federation, asking all to review/may want to review.
Separating technicalities from policy, and what it means to trust.
Transparency: this could give you some.

Pal Axelsson: discussed in other groups OIDC federation, federation part is applicable to other parts of technology, federate way of thing in that space. Even the SAML boat left a long time ago. Trust federation and how to build it and that's good.

Pal Axelsson: OIDC much more about federation, is not multilateral protocol, assumes one IdP to rule them all.
Niels Van Dijk: Pondering whether we would get a wallet ecosystem on OIDC/OIDC federation and SAML, might be proficient, one protocol for all of these things, a lot rebuild SHibboleth IdP and SP, or some shim layer that takes care of the metadata handling? MDQ protocol has a lot of similarities. MIght be able to do this together.

Christos Kanellopoulos: Opportunity for metadata proxy?

David Groep: add comments and questions. End of day, pick things from the parking lot and put them in your favorite slot or new topic, 08:30 start in this timezone!


OPs
OP
Proxy
RP1
RP2
?
TA
TA
TA