Mathieu (00:02.222)
I wanted to go a little bit into the direction of exploring OpenID Federation with you today, Dima, but maybe a good starting point to getting there is just understanding how the OpenID Federation spec came about. It seems like it has some momentum now and there are various use cases that are looking to employ it, but with your background within the OpenID Foundation, it may be a good starting point to just take a step back and understand how it came about from the IM world, from the open banking world. And even if there's any intersections between what's happening in the verifiable credential space, which recently has been a subject of importance, I guess, within the OpenID world. So we'd love to get like a lay of the and maybe before we go deeper into OpenID Federation.

Dima Postnikov (00:51.12)
yeah, happy to cover that. I'll probably take a further step back and have a look at, how the trust management kind of evolved in my view, over the last few years. and a lot of it comes, a lot of comes from my experience of people, experience of people that I talked to about this topic. And I think you've been part of some conversations where people are trying to solve this problem in many places. the problem of trust management and trust discovery.

If you look at open banking ecosystem, which is where I spent quite a bit of my time in the past, they typically have a governing body that determines who is supposed to be participating in each ecosystem, who is allowed to do and what they allow to do within the ecosystem. So usually they create a trust registry of sorts that allows them to manage those participants.

If you look at any digital identity ecosystem that's been built or has been built, they tend to manage it in a similar way. So there is a governing body, could be a commercial entity or government that determines who is allowed to ask for what data and what type of levels of assurance they provide over this data as well. That's a problem that right now exists in eIDAS 2, as well.

where they build an ecosystem that needs to be managed. That's where the trust management fits in. So any digital identity ecosystem, any open banking ecosystem is in the same place. And if you look at verifiable credentials ecosystems, they have a similar problem. There are issues that would like to trust wallets and there are verifiers that would like to trust wallets and would like to trust the issues.

They need a trust anchor that describes to them what they're allowed to do, who they can trust and how they can authenticate. If you look at OpenID Connect based ecosystems, it's a similar problem. You've got data providers and data recipients, and they all need to trust each other. So data recipients within a typical open banking ecosystem, OpenID Connect ecosystem, need to discover identity providers or data providers, and there needs to be a mechanism to discover it. And then there needs to be a mechanism, who do I trust? The same thing from our One ID Connect provider, from identity provider, when a reliant party or FinTech, for example, is asking for a certain type of data on behalf of a customer, they need to understand if it can be trusted.

And if it's the right software representing that organization that can be trusted and has been endorsed by the government.

So all of those ecosystems are looking at the same problem in my view and trying to solve it at the moment in different ways.

Mathieu (03:48.22)
You mentioned open banking. There's been a lot of conversations in digital identity around trust registries, obviously in trust establishment, trust management type of things. Are there learnings that could go into the digital ID ecosystem that could be taken from areas like open banking? It would be interesting thing to hear kind of on the trust side of things, how far things have gone in that space today, maybe go a bit deeper there.

Dima Postnikov (04:19.23)
Most of the open banking, it's a good question, most of the open banking ecosystems sold it, they built a trust registry. Some of them have a fairly large number of participants. For example, open banking in Brazil has 800 participants. So that's a large number to manage and they need to be discoverable. They need to find a way to trust each participant to make sure that they are credited and that the right entities are requesting the right credit data.

Similar problems existed in the UK, in Australia and in other jurisdictions. They all solved it differently. There was no standard before. Each ecosystem ended up building their own type of a trust registry, whether it's a vendor product or custom build product. And there are some vendors that are starting to evolve in this space as well. But they're all non-standard based.

That's what we've seen in the open banking ecosystem to date. And there is a lot of conversation right now that we look at all these implementations of the same thing. They tend to use similar security profile. FAPI tend to use OpenID Connect for any identity interactions on top and some of the other specifications, but in a trust management space, they all do their own custom thing. This is why people started talking about using standards.

And there are a couple of conversations in this space that could potentially fit in the trust management space. It's not the only area, open banking is not the only area where this problem is being discussed. Like we said, in verifiable credentials in the eIDAS world, the same problem is being solved as well. Recently in the last few years, GAIN initiative and specifically the technical POC. looking at gain within OpenID Foundation, looked at the trust management space as well from slightly different angle. How do we trust entities from different jurisdictions? And different methods have been analyzed, different specifications have been analyzed. And that's probably the first time I seriously looked at OpenID Federation at the time.

Dima Postnikov (06:30.07)
And OpenID Federation came out as a clear winner for the GAIN working group to give us that trust discovery and trust management. How do I trust the entity from Canada, for example, that's requesting data from or identity data, for example, from the identity provider in Australia? So the

idea is always to encapsulate the accreditation of those entities within each of the jurisdictions and find a way to expose it through the trust chain walk. And that's where OpenID Federation fits nicely.

Mathieu (07:09.01)
You mentioned a few different acronyms too. So if you could just explain what GAIN is, go a little bit more into FAPI and then would also like afterwards to understand, and maybe in the context of using these things, how a trust chain would look like in a federated model.

Dima Postnikov (07:29.03)
So FAPI is a security profile. It's a secure version of OAuth and OpenID Connect that is designed to enable API consumption. And it is used by most of the open banking ecosystem became de facto standard in this space. Very quickly, as you look at different ecosystems being built in parallel, we realized, we started to realize that it's not enough security profile of what is not enough for you to build an ecosystem. It's the same thing as, you know, DIDs and verifiable credentials, data model, and even interaction patterns. It's not enough for you to build ecosystem. So there are additional building blocks required to build an ecosystem. And slowly there is a family of specifications being developed within the FAPI working group or being pulled from different places rather than developed where those specifications can be assembled together to build a functioning ecosystem.

So the way I look at it, in a few years time, potentially maybe in a year's time, in a FAPI Working Group and OpenID Foundation, we might have a full set of specifications required to implement a typical open banking ecosystem. At the moment, there are still building blocks that are missing and how OpenID Federation will fit into this space, it's still evolving discussion.

But a lot more momentum around the discussions of using OpenID Federation for an open banking ecosystem, it just fits in nicely. If you look at the API specification that comes from OpenID Federation spec, and if you look at the APIs, typical API specification from the register, from a typical open banking register, they almost match one to one. There are some differences that needs to be addressed one way or another. But I think that work will be happening in the next couple of years.

Dima Postnikov (09:21.10)
So this is part of my role with OpenID Foundation that I see my role as vice chairman is a way to help ecosystems to adopt different specifications together. Because at the moment as a community, we produce multiple specifications and we do it well. But when as an ecosystem builder, you need to assemble those specs together. And that's where I see FAPI evolving going further.

So GAIN is a global, assured identity network that was born few years ago as a concept based on a white paper written by 150 collaborators globally, most of them identity geeks and identity practitioners. And the idea was to connect the trusted islands and connect identity ecosystems across borders.

There has been a couple of efforts within the GAIN movement. OIX has looked at the rules and policy required to enable that. And OpenID Foundation had a technical working group, community working group, looking at technical POC. And the interesting part from trust management perspective, it took us probably six months to do the data exchange part of the POC, which turned out to be the easiest part.

And we spend another year and a half looking at the trust management. How do we trust entities across the border? And this is where OpenID Federation and other trust mechanisms were discussed. So that's a significant piece, especially it's important. So to take a step back, why do I think standards are important in this space? One is because every ecosystem tends to reinvent the wheel and redo it again and you don't benefit from vendor solution, open source solution in a space that you could sort of utilize and simplify the adoption or the creation of the ecosystem.

And second part is it definitely helps you to connect multiple ecosystems together. Whether it's connecting open banking in Australia with open banking in Canada or UK or connecting digital identity ecosystems in Singapore, Australia and Germany for example.

Dima Postnikov (11:34.03)
So that's where it becomes really important. That's what GAIN has tested over the period of time. Now GAIN technical working group has evolved into testing how do we plug in verifiable credentials, issues and verifies into the same trust framework. So there is a little bit of work happening there as well.

Mathieu (11:54.12)
We often hear when people describe like what digital credentials are and how they could be used. There's a lot of the times that use cases come from an identity and access management standpoint. And sometimes you'll hear people explain it like, you know, if you're logging into a website, maybe the, the relying party, the website has a username and password that they're managing for you or they're able to map that these, these match and they're able to authenticate you that way. And then there was kind of an evolution of things where, relying parties delegated that, authentication to third parties and people often use the login with Facebook login with Google, whatever login with, with Apple, which are very prevalent today all over the place. and then when people start to talk about verifiable credentials, they say like, you don't have to rely on, well, first of all, you don't need to ensure that your personal information or your username password, the knowledge-based stuff is shared with relying parties. You don't have to make sure it's all centralized. And so you move to this decentralized model.

When you think about trust establishment, if we're talking now about a federation and having trust chains, how does that either complement or conflict the vision of decentralized identity and decentralized claims and being able to do this interoperably on the internet and kind of achieve digital trust. Is there a conflict or do they complement each other?

Dima Postnikov (13:29.00)
It's probably both. And I think it comes down, for me, it comes down to separation of concerns. So there is data exchange level and data exchange can be direct between the participants. And that's quite a simple exercise. But if you look at the real life use cases, real life use cases need a lot more to be conveyed on top of the data exchange.

How do I trust that this credential comes from a reliable entity in Germany that governs the banks there? So there's the whole trust chain that needs to be walked through. At the moment, it's peer-to-peer. Entities tend to do it themselves. So you, for example, have a relation. One bank has a relationship with another bank overseas. They already have contacts. They establish peer -to -peer connectivity. They trust each other. They talk to each other. That works well for small one -to -one interactions, but for the larger ecosystems where entities don't control themselves who is in, they need to understand the context. A lot of times how a particular identity has been verified, how has it been authenticated? If you look at the wallets, for example, space, the wallets themselves could carry different level of authentication assurance, whether it's a similar, how do I trust that it's the right person sharing the credential with me, even if it was provisioned correctly at the time of provisioning?

So there is a lot more context required by the entities that need to trust this credential, whatever type credential is being used. It's always easy if you have a simple trust list of government authorities, but if you have a different variety of different institutions in different jurisdictions, it's much harder to make that decision. So only a German bank regulator would know what that means to be a bank in Germany and they can attest to that. Everyone else outside of Germany would struggle probably to figure out if it's a real bank and the entity on behalf of representing a specific software client or software representing that entity is the one that's linked to it.

Dima Postnikov (15:41.19)
To summarize, in order for someone to make a decision that I trust this interaction, there needs to be context communicated. And the way context is communicated a lot of times is that it's done through the regulator or the Federation Trust anchor or another entity that tells both you guys can trust each other. In the open banking ecosystem, it's actually, it's sort of much simpler because most of them force banks to participate. So for example, in Australia, all banks have to be part of open banking ecosystem which is called CDI here. They don't have a choice. And then specific software is being accredited for each of the bank. The Fintechs are admitted based on their choice, on their submission, but then the banks need to understand that they need to trust those Fintechs, that they have been accredited properly. They can be trusted with customer data and so on.

And at the same time, there are some explicit information that comes through the interaction and metadata, additional attributes that can describe the context of customer authorization, customer authentication, customer provisioning and onboarding. And there are some implicit controls that come through the ecosystem. A lot of times, levels of assurance are prescripted by the ecosystem. For example, whether it's LOA2 or gold, silver and bronze, something that

comes through ecosystem admission. There could be a minimum level set, for example, for driver's license ecosystems, the minimum level has to be NIST level XYZ.

Mathieu (17:23.12)
So when we talk about now, like looking at standards for these ecosystems when it comes to trust management, something that maybe wasn't there in a standardized way. And if we call it version 1.0 of open banking, what does version 2.0 look like with standards in place? So we're talking about OpenID Federation as being kind of a tool here that could be used. So maybe if we think about it in the context of an open banking ecosystem that wants to adopt this.

What are the different roles in that trust chain? And then what do each of them have to do according to the specification? Does everyone need to adhere to this new standard? What does that whole architecture look like within an ecosystem like an open banking one?

Dima Postnikov (18:11.05)
OpenID Federation is designed to cover many different use cases in different ways. If you would like to apply OpenID Federation to open backend or new versions of open banking, I see it personally, I see it as a profile of OpenID Federation that simplifies things a little bit because the trust chains seem to be much simpler in open banking because usually there is a government authority and then there is a flat structure underneath. So I provision all of those data recipients and I provision all of those data providers as a governing authority of open banking ecosystem. There doesn't need to be a significant trust chain work as you would do for inter-federations trust.

So it's more of an intra -federation trust, but there is a list of standardized APIs that can be easily supported by vendors and SDKs. This is where I see the benefits of using a standard, any standard for that matter. But to be honest, there are not too many of them at the moment. So far, there are two developments in the trust management space that we've seen recently apart from all the DNS-based trust lists. One is trust registry from trust over IP, which seems to kind of a from scratch development of trust management framework. Mostly it's deep based ecosystems. That's what it feels right now, but nothing stops it from developing further and become more generic going in the future. But there has been a lot of work done on requirements and I actually quite enjoyed observing requirements and specifications for trust registry APIs, which gave me a lot of ideas in the past.

And then the other one is OpenID Federation. It has been adopted in some of the ecosystem worldwide as well. So Italian digital identity ecosystems, two of them run OpenID Federation and they connect to each other via Federation Trust Anchor as well. There is the most important one and probably the large one, the large instance of OpenID Federation is AduGain, which is a network, a worldwide network connecting different universities and research facilities. So students, university staff and university related research researchers can access each other's assets worldwide. So as a student of an Australian university, I can walk into an Italian university and be able to provision some level of access to some level of materials, research materials and that's quite successful and it's been running probably four or five years at least, maybe more.

So there are existing implementations that use OpenID Federation which gives a lot of confidence. It also evolved. So early on it used to be called OpenID Connect Federation and you could see a lot of OpenID Connect related items but it evolved as a more generic framework for trust management, which is open ID Federation now and can be used for anything else and potentially will be used for issuers, boards and verifiers as well.

Mathieu (21:38.06)
So you mentioned in the Edgigain example that university assets could be accessed, I guess, would it be across different federations? Like would each university be their own kind of trust anchor or route within their own federation and have their own?

They use the term like the leaf node and then there's the term intermediaries within the specification as well. So within this example, like what would be the different roles and you actually have different federations or would they just be sitting inside of one or is it like an inter federation trust?

Dima Postnikov (22:13.09)
It's the Inter-Federation Trust. And I'm not too familiar with the actual implementation. I think they have about 80 countries participating right now. 80 countries, each of them have their own federation, and EduGain connects them. So the Australian Access Federation runs Australian Federation, Australian Leaf Node. That is linked via EduGain Trust Chain to the other federations.

Mathieu (22:45.17)
You also mentioned, so there's an access use case there when you're talking about the open banking example, it was also kind of an access, like could this organization or whatever access my API if I'm a Bank, what are the types of claims? Like is the specification specific to the types of claims that could be made? And maybe also understanding according to the specification or the standardized way how different entities in a trust chain are making claims about one another.

Dima Postnikov (23:20.22)
It depends on a specific protocol being used for the interactions between the parties. But for example, for OpenID Connect based ecosystems, there is a standard way of discovering in OpenID Connect protocol, outside of OpenID federation, there is standard way of discovering what claims each IDP supports and what claims each relying party can request. So the governing entity would need to sign a statement or sign an assertion for each of those entity statements or assertion for each of those parties to endorse it. So IDP can support five different claims, but when they participate in an open banking ecosystem, they are only allowed to share three. So there is always a place for the governing authority to stamp in a cryptographic way an assertion that allows the other entities to understand.

Yep.. This regulator told us that the bank can provide identity data, transaction data, and payments functionality, whether this bank or this institution is not allowed to do that. The same

thing from relying parties. And we use it, for example, with ConnectID. We have relying parties that are allowed to ask for data birth. And we have relying parties that are not allowed to ask for data birth. They can only ask for assertions over 18, over X, and so on.

And this is a way for us to work with each of the reliant parties towards data minimization, trying to ask them to reduce the amount of data that they receive, because we see it as important. And that certainly works well. And you need controls for the ecosystem to be able to enforce that. So a reliant party that's not allowed to ask for data birth will not be able to successfully execute that request.

Mathieu (25:16.09)
It's interesting to know that. So I guess like the, the trust anchor could start setting some governance of, I don't know, based on the role or even types of data you could request. So it could be pretty dynamic, I guess, downwards do. So if we look in, in a trust chain, then maybe we could take a simple one, like in the open banking. So the regulator would kind of make some, some claims or some statements as, as a trust anchor, for example at the top.

And the whole idea is that there is legislation in the respective country that says the banks need to start exposing some APIs to the ecosystem of innovators and Fintechs and whatever. And so I start to have different roles now. Like we have the regulator, whatever body that is, or could delegate the Federation trust anchor within the country in question. You would have the banks in there. You would start to have, which would be, I guess, relying parties in this case, you would have Fintechs that would need to ask for access to API type of thing.

Do all the parties need to make claims about each other? Like, do all of them need to be running on this federation standard to be part of that chain? Or could the whole thing kind of be bootstrapped from the top down by the trust anchor? Like, how much involvement needs to happen from each party within a trust chain under the OpenID federation model?

Dima Postnikov (26:44.03)
So that depends how you use it, because every ecosystem would need to create their own profile of OpenID Federation. OpenID Federation is quite a complicated spec. I see the typical Open Banking profile being a simplified version of that. And my personal idea would be definitely to simplify what Reliant Party, what FinTech would need to do. So the majority of the work is done by the trust anchor, and should be done by the trust anchor in this space, to endorse it and relying parties or small Fintechs, they shouldn't be doing too much.

Because this is where the way I see Federation evolving is potentially some of the entity statements not being hosted by each of the parties, but being hosted centrally. Essentially replicating the trust registry as it is right now. Because what you do right now is you actually call a central registry with give me the list of participants or give me the information about this participant. That's how it works right now. Changing those interfaces to open ID federation and that's a current assumption that I'm making which might evolve will require, will potentially be simpler if, will potentially be simpler especially for inter federation communications to be hosted

by the central entity. As far as everyone else concerned, it's still a URL -based interaction, whether it points to a URL hosted by the relying party or a URL hosted by the registry. That's a smaller point.

Mathieu (28:24.19)
So the way I'm imagining it in my head is OpenID Federation has different elements to it, which just allow you to form a trust chain within a specific Federation or ecosystem. And then, even make some claims like cross Federations or cross ecosystems as well. And the, the trust anchor plays a key role, just like when we think about trust lists or trust registries in the digital ID space if it's for authorized credential issuers or authorized types of proof requests or whatever the list is about.

There is a trust anchor, which is kind of the governance body, which is managing this list and is making some claims about their list or their registrants within here. So the federation model, the way I'm imagining it just seems like a framework of doing things in a standardized way for a federation and opens up the door for trust cross federations as well. And then you would be able to still use some other specifications like the Trust Over IPs trust registry protocol to actually interact with these, these federated architectures, I guess. Is that a good representation of what we've been describing so far?

Dima Postnikov (29:48.09)
So maybe a bit of background would also help. So, and I agree with what you said, just a slightly different angle on the topic. So a regional OpenID Federation, the way I read it, was developed for open ecosystems. So where the entities like for example, universities could come together and plug into the global framework or global ecosystem of ecosystems.

And it's kind of voluntary. And then there are some controlled ecosystems, whether it's a digital identity ecosystem that a governing body wants to control who's in, who's out, a central authority comes in, or it's an open banking ecosystem where there is a strict control as well, usually. They have slightly different requirements. So if you look at the OpenID Federation spec, it needs to cater for both use cases, but it needs to be adapted, it needs to be profiled for open banking to simplify. There are some parts of the specification that actually won't be used in open banking ecosystems. And there might be additional features will be developed in OpenID Federation. So it needs to evolve. The same thing goes if there is another protocol that becomes the de facto standard in the space of connecting different ecosystems. So OpenID Federation might need to have a bridge developed for that as well.

So there is definitely a possibility. So we used OpenID Federation and GAIN in a little bit different way, in exactly that way. Actually, we used it for bridging between different trust networks. So we had yes.com in Germany, we had a net work in Japan, we had a net work in Italy, and the way we've connected it, they all use their own trust mechanisms internally. Only one of them, Italian based, was OpenID Federation native. Everyone else used their own protocols to do the trust management, but we used OpenID Federation to bridge them. So we

used that as a bridging mechanism. So in order for you to participate in the GAIN network, you needed to support a few interfaces. What happens behind the interfaces is up to you.

Dima Postnikov (38:08.02)
But these other standard interfaces, how you list the trusted participants, how you fetch the statement, how you figure out who you're talking to. So we use OpenID federation as a bridging interface as opposed to everything within GAIN. But in general, we can all mix and match some of those protocols and it depends on the circumstances on a specific network or specific network of networks that you build in.

Mathieu (32:35.18)
So the claims that are made within a OpenID Federation trust chain are signed JSON web tokens according to the spec is what I saw. It kind of made me think about verifiable credentials, not too far off from kind of just assigned payload like that from an authority. We've also been thinking a lot about this too in the context of a trust registry. Like a trust registry operator is making certain claims about their ecosystem or about the list. So it's like, where does the line happen between just a type of claim like this, even in the OpenID Federation, if it's a JSON web token versus could a claim be made using a verifiable credential as well? I don't know if that question makes sense to you.

Dima Postnikov (33:29.01)
I think you're absolutely right. There are different ways \ to convey the assertion from a trusted entity to a party that's asking for that assertion, as long as it's cryptographically verifiable. I think that's what we all care, whether it's a verifiable credential, whether it's a JOT, OpenID Federation traditionally from OpenID Connect world. So it does natively supports JOT type of assertions. But it doesn't mean it cannot support other assertions in the future as well. It's just the way they present it might not be specifically suitable for different protocols because it's usually a back channel conversation between an entity that wants to know something and the trust anchor. So there is no hold in the middle but it is a type of verifiable credential.

Mathieu (34:25.03)
Yeah, and then people will just argue whether or not it fits a specific model or not, but it's just to sign the attestation at the end of the day. And then you get back to the same trust management question with any signed attestation is how do I go back to the root or how do I go back somewhere just to get some confidence about the validity or the authenticity or the authority of the claim in question that was made.

I guess in the OpenID Federation model, there's just a standardized way to do that. I guess in the open banking space before standard-based trust management was considered, there were kind of trust lists in place, I guess, just to manage and bootstrap the ecosystem. So, could we take learnings from that too, where there's maybe some non-standard based things that could be put into place and we could still see adoption of certain innovations and then kind of in the future migrate to that? Is it a good idea? Is it a bad idea? And from your perspective, are existing open banking ecosystems that were up and running for a while, like in the UK or Brazil

or Australia, perhaps that was not based on standards having a tough time kind of migrating to a standard based approach or is it just kind of a logical evolution?

Dima Postnikov (35:53.05)
I think we definitely see the evolution of open banking. Every new ecosystem that's being rolled out is better than the previous ones and learning on the previous ecosystems experience. That's clearly been reflected even through the standards that are being developed as we go. There is definitely a desire in some of those communities to evolve towards standards and there are reasons for it too, especially if you start interconnecting it with other open banking ecosystems globally.

The change on the other hand is always hard within the existing ecosystems. But what I'm hoping the standards on the new standards, so evolving standards going to address is probably the needs of the new ecosystems coming in. So we still have a lot of countries that haven't rolled out open banking and the hope is that they will be able to benefit from all the previous experience and from new standards evolving in this space. It doesn't mean that they haven't used standards at all. So there's still, a level of standards being used for trust management. For example, open banking Australia, open banking UK, open banking Brazil, they all use dynamic client registration, which is a mechanism for, a reliant party or a FinTech to receive that assertion about what they can do or how they are supposed to interact with the ecosystem from the central register.

So there is a way how they receive it might be a custom way, but the way they present it to an OpenID Connect provider is a typical dynamic line registration or profile of that. And so that's a standard way, but it does what we've learned over the years is that particular way, and it's also allowed in OpenID Federation as one of the methods for registration, dynamic line registration, which is called explicit registration. What we've learned over the years that it's puts a lot of requirements on the relying party side. They need to keep track who they registered with what version of software statement and a large ecosystem. It can become a nightmare for relying parties. And if they lose that registration, that will create problems for them to recover. That's why I tend to evolve. My thinking is that for an open banking ecosystem, it needs to evolve towards the automatic registration, which is another method that OpenID Federation allows.

And that's what I see being an Open Banking Profile of Federation automatic registration, where the entity just presents itself to an OP, and OP decides based on the assertion directly from the register that this entity can be trusted. Then the Relying Party doesn't need to worry about the registration, doesn't need to do, even if there are some standards that can be used in that space, but it's all about the amount of effort that each party needs to do and what can be automated, what can be done by the vendors versus the smaller entities themselves.

So that's a typical example of how the thinking has been involved in this space. So new ecosystems, I see them using, whether they use Federation or not, but they would be using some sort of automatic registration way, which should really be based on OpenID Federation

because it just gives you those tools. And that's a typical example of how we would profile OpenID Federation for Open Banking.

It's specifically to your question around the payload within the entity statement, within the assertion that represents that entity. That's largely ecosystem specific, depending on what you use it for. There are some common elements there, but a lot of it has to be still designed by each of the ecosystems. And where I see open banking profile developing is probably standardizing it as much as possible for the typical open banking ecosystem, but allowing for local nuances.

Mathieu (39:48.20)
Do you see the creation of profiles outside? So I think the answer is clearly going to be a yes. But when we think about some of the digital identity use cases happening, and maybe if we just focus on public sector led initiatives, and if we think about what's happening in Europe, for example, under eIDAS 2.0, do you see the opportunity to create some eIDAS 2.0 specific profiles of OpenID Federation suited exactly for some of the use cases that? large -scale pilots or just eIDAS 2.0 in general is pursuing.

Dima Postnikov (40:24.00)
I think so. I think some, and there are some people in the EU that believe that that should be the way. And it's worthwhile considering it from, you know, from the point of building a brand new ecosystem. So there are other options being considered as well. And, you know, typical trust lists, they work well for basic trust, but they don't necessarily work well for the discovery bit, because one of the functions of trust management, one of the important functions of trust management for me,

is a discovery capability. How do I discover what features, what claims, what capabilities each of the participants have, what certifications they have, what assurance levels they provide? So there is a lot of metadata that's required by verifiers and reliant parties to understand and to make decisions, especially the sophisticated ones. So the sophisticated reliant parties, they need to understand how that particular identity came about, how it's been transmitted, how it's been authenticated at the time of the issuance, at the time of the presentation. A lot of it can be transmitted through the protocol. Some of it can be transmitted through the rules governing the ecosystem.

But trying to automate it as much as possible would mean that it has to be a some part of a registrar, some part of a trust management. Unless it's a simple uniform rule that across eIDAS 2, these are the two simple rules that we all follow and nothing else to be discovered.

But what we found out for many use cases, you do need that variability. Different use cases require different permissions, different parties participating as issuers or identity providers in each ecosystem. They have different capabilities. This particular one has payments as a capability. This one doesn't. For example, this one can do a bank account assertion because it happens to be a bank. And this one is a government acting as an issuer as well. But they can't

do that assertion and most of the cases would require discovery by the wallet providers to discover the list of issues or list of credentials available, and by the verifiers to see the list of credentials and wallets available that satisfy their specific requirement.

Mathieu (42:33.08)
When you talked about like the dynamic or automatic client registration, it also makes me wonder too, like, and I often have, concerns maybe in the digital identity space that there's so many, so many certifications and trust marks you're going to have to get and, and these different audits you have to go through and then get proofs for them before you're able to have equal competition or equal opportunities to other bigger players in the space. And I think a lot of the genesis behind open finance, open banking is really to spur innovation, right? New technology providers, new products that are able to leverage existing data that should be owned by the consumer that they could then offer them all sorts of different products and services.

What are some, because I read about the kind of trust marks within the OpenID Federation specification. And obviously under the eIDAS 2 stuff, there's a lot of talk about that as well, which I always think that if you're in the business of doing technical consulting or audits and stuff like that, it's all good for you.

But How do we ensure that we're not creating further barriers to innovation? Because it seems like having these trust registries, if I call it like that, in place, whether it's for discovery or whatever, just gives a lot of opportunities for innovation and new products and services and could be quite important to a country or to an ecosystem altogether.

How do we avoid putting too many barriers, but at the same time, we need to have assurance that the organizations or whoever is participating in the ecosystem complies to certain rules or governance.

Dima Postnikov (44:32.18)
So it's a really good question. It is a complicated problem. How do we make it simpler for verifiers and reliant parties to jump on the ecosystem and adopt it? On one side, you're trying to make it as simple as possible. On the other side, you still need to make sure that customer data is looked after. And there are some basic rules of play that need to be satisfied.

I think the simple answer, the first answer I'd probably say is, from my perspective, is a tiered accreditation that might need to be applied here. If you're asking for simple data over 18 flag or something like that, you probably have very basic things that you need to attest to in order to participate. But if you're trying to do payments, it's a different story. If you're trying to initiate payments, you need to be accredited to a much higher level. And some of those trust marks potentially can help to reuse your existing accreditation in a better way, rather than re-accredit you by each of the ecosystem.

For example, ecosystem might, instead of verifying that you can be payment services provider, if you are a bank and there is a trust mark that comes from a banking authority in this jurisdiction

in this country that says, yep, that's a bank that's linked together, then you might have a simplified accreditation rules for significant number of functions within the ecosystem. Or if you're accredited by a specific digital identity framework, in different jurisdictions there are different accreditations available. If you are accredited by some of them, you're actually allowed to participate in some use cases. For example, at the moment in Australia, in order for you to participate in interactions with the government, there is a government trusted digital identity framework that you would need to comply with.

So that trust mark can come from a right authority and allows the ecosystem governor to reuse it, to plug it in, that you exist in accreditation, as opposed to the additional burden of ecosystem governing authority, re-qualifying you, re-meeting it, re-accrediting you. The same thing goes with ISO certifications and any other ones. I see them as complementary, just a way to reduce it. But in terms of defining the requirements for each role, I think that has to be tiered and has to be simplified as much as possible from a technical perspective.

The ecosystems that I participated in, like ConnectID in Australia, one of the key requirements or sort of principles for us that we follow is simplify Reliant Party accreditation, simplify Reliant Party integration and standards that they need to follow. In the past, early versions of some of the open banking standards have been quite difficult to implement by reliant parties. Now it can be some of those standards evolve to be much simpler. For example, 5P2 is so much simpler to be adopted by reliant party than 5P1. It's just much simpler and much cleaner. And that's where evolution takes us. And I think this is the same goal to simplify it, especially for the smaller entities, smaller end of town.

Mathieu (47:43.07)
So Canada has finally written down the need for a trust registry to enable open banking. It's actually written in the legislation, but I don't know if there's necessarily a clear path to launch one. Being in the Canadian market and knowing that we have a good amount of listeners in Canada as well that are in different positions of influence, whether in public or private sector.

What would your recommendation be to the leadership in Canada that is behind the open banking space as they move towards adoption? You mentioned every ecosystem or country that enters just takes it a step further or does something better or these things evolve. Where can you see Canada evolving open banking and helping the rest of the world kind of go in that direction?

And I think there should be a case to be made around having a Trust anchor, trust registry, that type of thing. What recommendations would you give to the Canadian leadership based on your expertise and your learnings and maybe what they should really be thinking about, which is strategic to them and the rest of the world, and then maybe some things not to do if you have those suggestions too.

Dima Postnikov (49:02.07)
The most important one is don't do it alone. There has been a lot of work done in this space. Find people to collaborate with, engage with communities like the OpenID Foundation community. And I think most of those open banking regulators are already engaged and should be working with them. There is a lot of expertise that can be shared.

Another obvious one is use standard based approaches where you can. If you think that standard doesn't satisfy you, discuss it with the standard bodies, how it can be evolved to your needs. It's a way to test your requirements, whether they are understood correctly and whether they can be satisfied or should be satisfied by the standards. And it's also a way to evolve the standards as well. The benefit from using standard-based approaches they come in different ways.

So for one is you might have a set of vendors in the market in your market already that support those standards, especially in the open banking space. Most of the large IAM vendors support open banking standards by now and that's why your ecosystem can benefit significantly. But it also comes with additional tools available, whether it's SDKs for reliant parties, open source tools for both data providers and data recipients, or certification test suite that's available, for example, from OpenID Foundation that tests the full profile for Open Banking participants.

You can automate the at least technical part of the admission to Open Banking ecosystem almost 100%. And that simplifies everyone's efforts significantly, especially in security and interoperability space. So 5P2 and 5P1, they do come with certification tests available that allows you to run through the full large test suite that allows you to test all the positive and negative scenarios to make sure that each party in the ecosystem performs their duties to make sure that the profile is secure. That the security profile is followed up to the dot. And that's one of the significant advantages. Use those tools. Otherwise, you're on your own and you're going to have a problem in secure and not interoperable ecosystem where FinTech connects to one bank, they receive one result, they connect to a different bank, they receive a different result. And once again, they have a lot of work to do to reconcile it.

Dima Postnikov (51:38.09)
You want it to have as consistent as possible from a data perspective, but most importantly, from a security and interoperability, how you connect, how you interact with parties, what identity providers accept and what do they reject. So I think there is a big benefit of using conformance testing in some of those spaces, which is already available. So to summarize, use the standards, don't do it alone, engage with standard communities and use available testing tools.

Mathieu (52:11.17)
Would you recommend not overlooking standard based trust establishment systems? Like, are there good reasons to not overlook that, at least in the first iteration?

Dima Postnikov (52:23.16)
Absolutely. You need to look at what's available and you need to help the community to evolve it. If it's not where you want it to be, it needs to evolve. And that's every new ecosystem brought something new to a family of specifications. And I think OpenID Federation is next to be plugged in and profiled. And I think every ecosystem like open banking ecosystem, open banking Canada can benefit from leading that as well.

Mathieu (52:52.00)
I think that's a good spot to end the conversation. Dima, I really appreciate you doing this with me. I learned a lot today and it's an area I want to keep exploring. So thank you so much for doing this.

Dima Postnikov (53:03.11)
Awesome. That's been a pleasure talking to you, as always. Thanks, Matthew.