Mathieu (00:02.091)
Okay, we're live. I think Christina, we'll start with you and hopefully through this conversation, we could bounce off each other. And I actually don't think we'll have a big problem doing that. There's lots to cover, but a good first step maybe would be, although I do want to talk about technology and focus on interoperability when it comes to technology through this episode.

I would like us to maybe focus on the adoption lens beforehand because that really influences the technology discussions. And so it may be an interesting standpoint to just start from the perspective of the German government and what the German government is doing, how it fits into the ARF, how it fits into eIDAS, how it fits into what other nation states are doing, and then how it aligns with some of the technologies. I know there's a lot to discuss there and we could probably go on for the whole hour on that, but maybe it's a good starting point just to talk about from a practical standpoint in Germany.

Kristina Yasuda (01:02.)
Yeah, so the eIDAS 2.0 went into effect and it outlines what each country needs to do. So in the wallet project in SPRIN-D on German Federal Agency for Disruptive Innovation, our goal is the success of the entire world ecosystem in Germany. But at the same time, there are places where government can influence more, so we are starting with the focus on the wallet as the part that government has to provide the infrastructure for the country. And there are multiple deliverables we're working on. One is this entire picture, the architecture for the German wallet ecosystem. So it's not just the wallet, but how the wallet interacts with the issuers, with the verifiers, and it's work in progress, so that's mainly what we have now. But the goal is to also cover the trust aspects, the offline use cases, not just PIDs, but also PIAs. So not just national ID, digital national ID, but also other use cases. Second deliverable we're working on is this consultation process, where we are directly talking to the public, the civil society, the organizations.

We're explaining to them what we are doing, getting feedback from them, what are their expectations, what is their feedback, what not. And most recently we launched this innovation competition called Funke where the goal is really to learn through code, learn through implementing, because there are a lot of pieces in this architecture, in this consultation where with the places where we need to fill in and as opposed to just doing an exercise on the paper, we said, look, let's move our hands, let's get the code and learn from that and make decisions.

Kristina Yasuda (03:07.05)
So what this innovation competition does is we selected six teams, they compete with each other how much innovation they can achieve in this wallet space. So we had the jury, it was a really holistic process. We had a jury from different corners of society, public sector, private sector, experts of security, experts of UX, experts of open source, because the code will be open source in the end. And also, most importantly, experts from the civil society. And they selected these six teams that have already started working. And they will progress in three stages. First stage focuses on presentation and issuance of PIDs.

After that, only four teams will move to the stage two. So it's really a competition. Stage two, we'll focus on issues and presentation of EAAs. And after stage two, only two teams now will move on to the last stage, which will focus on advanced topics like pseudonymous login, payments, QES. So I think that's what's really unique about German approach.

So, but one important thing, like the wallets in that competition, have nothing to do with production level wallets in Germany. So each government has a choice either to build the wallet itself, either, you know, accredit the wallets, you know, delegated to private sector. And like that has not been decided yet, right? Like that is completely separate from this wallet competition. So these wallets are really prototypes for those who are trying to learn from them because again, as I said, without something running, it's really hard to learn. So just highlighting that very important point so people don't get confused. But yeah, that's how the German government is trying to approach this right now.

Mathieu (04:59.23)
Niels, from your perspective, that you're working on this project with the German government, I'd be interested to learn. And it sounds like a pretty cool initiative, because that's really how you're going to see a lot of innovation very quickly through different cycles with different types of vendors. And all of these components that become open source become composable. It could be reused in future phases. Like it's pretty cool. From your perspective, Niels, along those lines, like what are some of the pieces that are already existing that maybe Sperion and yourself have worked on that you're able to use here? And what are some of the new things, the new innovation pieces that you're looking to push forward on this wallet side of things?

Niels Klomp (05:44.00)
Yeah, yeah, indeed. And actually to begin indeed with the initiative of the German government, I think it's really a nice approach to getting indeed quality implementations, although, as Christina mentioned, it's at the POC level. Of course, there's quite a significant amount of parties that have experience in building SSI technology, decentralized identity technology and they're doing it in a completely different way than basically every other country out there and I think in the end that what this will bring to the open source community and as well as Germany itself, of course, to the government is actually a real innovation at a relatively low price, actually, if you ask me.

We have indeed been selected as one of the six parties in the funder track, And yeah, we are of course really excited about that. And to talk a little bit about the things that we hopefully will be contributing there is first of all the experience we have in the Netherlands with building this type of technology, the open source work that we have been doing for quite a significant time already, mainly around the OpenID4VC types of specifications and implementations, things like OpenID 4VCI, OpenID4VP, Sciopv2, also Presentation Exchange, for instance, in there and all types of other open source libraries we have available. And those are typically low level libraries where we don't make too many assumptions yet so that actual developers can integrate and implement those. And one of those examples is, for instance, integrations into Veramo. Others are integrations into the Open Wallet Foundation Credo framework which a lot of organizations are also using.

And the developers of those frameworks basically decide how to integrate those low-level libraries. So we don't make any assumptions about what type of keys you want to be using or whether you want to be using DIDs at all or not. So those are things that will also be used, of course, in this German project. And next to that, on top of that, we have our own software development kit in which we have modules that can be used basically to create issuers, relying parties and wallets, both cloud-based wallets as mobile wallets. And then specifically, for instance, React Native wallets. And those SDKs are being used by our own wallet as well, of course. And of course, in this project, we will be using as a basis our wallets and those are SDKs and low -level libraries. But at the same time, we will be adding some quite new innovations, I think - we would have probably never done some of the things that we proposed in our proposal otherwise. And that's, I think, yeah, I think that's a testament to sort of the innovation character of it because simply as an organization, you always have to be thinking about your customers first and foremost, but at the same time, you also have your development costs and we are in a market which is really young meaning we are not a self -funded organization, so there's no external money involved, which means that we really have to be looking at our budgets, of course, and making sure that we deliver value for our customers as soon as possible. And that does sometimes mean that we don't have an awful lot of time to really start experimenting. And in this project, we will be doing some of that.

Niels Klomp (09:36.03)
So one of the things that we will be adding, for instance, is anomaly detection. So one of the key things is you want to make sure that users using digital identity wallets are protected. And you always have parties that want to abuse the trust people typically have in internet transactions but also you have the really big 5,000lb Gorilla relying parties and if they ask for certain information people will typically be very inclined to just provide it. It's a bit similar to the cookie problem we have most people just click okay without really reading what will be shared.

And with this anomaly detection, for instance, we really want to make sure that we learn based on using AI and using models. First of all, we know already what type of personally identifiable information is available. We can classify certain types as personally identifiable information. And then whenever a relying party starts asking for information, we will basically assign a certain level of risk associated with it. And we do that then based on learning. So have you interacted with that relying party in the the past, for instance, or not. And the more you've interacted with it, the better the score basically will be in terms of trust. The more privacy involved in the information you will be sharing, the higher that score or the lower the score, depending on how you look at it, will be.

Niels Klomp (11:06.20)
Similarly, we will be adding things like speech to text, text to speech type of integrations, and even more like a chat-based type of integration, because we also really would like to see people with disabilities or maybe there are less technically inclined people to be able to use this type of technology as well. And well, there's many more things we will be integrating, for instance, the MooseDev library, which is an abstraction library for secure signature creation devices. And we will be experimenting with that library also, for instance, using eSIMs as secure signature

creation devices. So we'll be working together with mobile network operators on that, which will be, from our perspective, definitely an interesting approach. And yes, those are the things we would never have done without this project, to be honest.

Mathieu (11:56.09)
You mentioned Christina. So obviously that there's investment happening here in research and development and quick iterations in the wallet space. It's a very important space for governments. I guess in the traditional identity world, the government kind of process is just to generate the IDs and give them to the citizens so that they could be used downstream in different interactions. Obviously we're seeing tons of involvement from governments in the wallet space because that is a key piece of infrastructure. I'd be interested from your side, and we started talking about governance a bit here. It would be interesting to me, I don't know if your opinion or mindset has changed moving from kind of a, from Microsoft to a public sector entity on kind of the role of governments, maybe short -term or long -term with wallets, and then more from a control standpoint. And then on the flip side, how much does governance kind of play into protecting citizens in the wallet too? Like are there efforts or are they thinking about how to actually like enforce governance or push governance into the interactions between wallets and relying parties, for example? I know that's a loaded question, but would be interested to hear your opinion on that.

Kristina Yasuda (13:17.14)
It's a great question. So to tackle it, if we look at the entire wallet ecosystem, we already covered the wallet component, but there are also the entities who issue data into the wallet. And when we talk about those entities, actually, eIDAS regulation does mandate the public sector to provide specific authentic sources. So that data can flow into the wallet, right? So there's definitely, I think, this kind of kickstarting, kind of crossing the chasm role that the government can play in terms of providing certain data being available in the wallet. And also because in the end, it's the services, the relying parties, recognizing that using the wallet, the benefits are users, right? And if we look at the perspective of those relying parties, I think what we can see is them recognizing that this government-attested data is what they see really valuable, right? Like in the end, that alone, I think, is not enough in the very long term. You'll have to combine it with different kinds of private sector-provided data, like in a bank account information or your phone number information in a verifiable manner. But to kickstart, I think there's a certain role governments can play there. And From the relying party perspective, right? Obviously, it would be nice to have a beautiful end -to -end story where you can use the wallet to get digital government services. But here, again, that role becomes even smaller because you need to have this end -to -end stories for not just inside government relying parties, but you know, whole kind of sectors.

Kristina Yasuda (15:05.07)
I think here we're starting to get a bit more clarity in terms of this kind of governance trust layer. I think there are a lot of active discussions and investigations going on. And I think we are at least right now we're at the point where we're trying to take one step back, identify the requirements to make sure how much existing infrastructure like X5 or 9s with trust lists already fit versus how

much, you know, we have to push it to integrate with things like OpenID Federation or maybe even blockchain or you know, I distribute ledger kind of technologies. I think that part is still more actively, you know, is actually being discussed. So I can't really say like this feels our way to go. I think two other points where the government's our thing, we'll have a say. So one is this from a security perspective, Niels already touched upon, but how the keys are being managed, right? Different keys actually, because, If you look at it, this whole ecosystem is pretty much grounded in cryptography, in this protection of private keys and how do you discover these public keys, right? Not just for the users, but also for the issuers, for the verifiers, for the accreditation bodies. And not just that, now we also have keys for wallet providers, you know, who are testing the wallet. So figuring that out, Setting clear requirements with clear reasoning, like which keys should be hardware protected, which keys are okay to be not exactly hardware protected. I think that's one area. And second area is, again, I'm just touching upon it because I have to form an opinion a bit more, but probably the area where how much the wallet provider, from a privacy perspective, how is the wallet provider uses the user data.

Kristina Yasuda (17:07.084)
I think there's a room to add clarification to prevent abuse or reuse, whatnot, especially because the wallets…. How do I say this in the politically correct way? So there are platform providers who are interested in becoming the wallets, right? And who are not necessarily known for really good privacy practices. So how do we balance that getting help from the platformers while making sure we are achieving the spirit of eIDAS 2, which really, you know, hopes to break away from those data monetization based models.

Mathieu (17:57.07)
From your point of view, Niels, so Christina talks about the importance of the public key infrastructure, and it's maybe more complex than we think about it sometimes. And these large deployments, it would be interesting to start talking maybe a little bit about the concept of technical interoperability profiles, because there have been technology recommendations made by the architecture reference framework. But I think It's maybe a bit of a more complex discussion than that. So it'd be interesting to hear from your perspective. I know you've worked on different technical interoperability profiles.

What are the different pieces like PKI, I'm sure is a piece that needs to fit within a technical interoperability profile. I'm sure the credential exchange protocols need to be there. How does one go thinking about a technical interoperability profile from a vendor perspective from like just a private sector ecosystem and just looking at what the governments are doing at the same time. How do you look at that? How do we make that environment maybe a little less complex to understand for people?

Niels Klomp (19:05.08)
It's actually a really important problem and actually it's one of the key reasons why we started an NGI project in which we are creating an interoperability testbed as well. Because in the end, although of course, EIDAS 1 and also version 2 now has room for identity wallets and has room for certificates, actually the actual regulation is vendor and technology neutral or tries to be, of

course, it cannot fully be. But that does, of course, leave room for quite a significant amount of interpretation. The Architekt Reference Framework, of course, already helps out there, but at the same time also that one still leaves room for interpretation at this point in time. And what you see is that, there's multiple versions of specifications out there. They are mostly still in draft, which is, of course, totally something which is understandable given the significant amount of work that has gone into it and still is going into it. But that does mean, of course, that all of the vendors need to try to keep up. And that's One of the key things which we have been and to a certain extent are still afraid of as a vendor is, yes, we can make the nicest relying party solutions, issuer solutions, wallet solutions, But in the end, if the organizations and natural persons that will be using this technology, and let's take, for instance, just a natural person, if they will be using wallet technology, they will install a wallet that will then, of course, be allowed by their local country. And if that wallet then doesn't work one time, could be a glitch or the user would be okay with it. If that wallet doesn't interact with a reliant party or an issuer a second time, well, then they probably get annoyed and by the third time, probably they will discard the whole wallet altogether.

Niels Klomp (21:14.16)
And maybe you have a persistent user that then tries another wallet, but at the same time, of course, a lot of people will be involved in this or potentially involved with this. And that could, of course, mean that people will just have a negative connotation with this technology in the beginning. So that's actually one of the key things that we see as a risk for the adoption of this technology. And at the same time, the fact that we now have eIDAS 2 also means that a lot of parties are working on this and we all basically have the same goals. And so I am relatively sure that we will make sure that those implementations will become interoperable. But at the same time, we just have to realize that yes, the technology is complex and it's all to defend us to make sure that those solutions work together. And of course, there's multiple initiatives to do interoperability. Actually, we also have an initiative in the Netherlands, which is mainly around organizational identities, that's called Company Passport, in which we are also basically creating a profile which initially was focused on the Netherlands for onboarding of organizations. And those could be new organizations, could be existing organizations.

And for instance, in the Netherlands, what happens is that if you want to create a new organization, you first have to go to the Chamber of Commerce and then depending on the type of organization, a notary will be involved in making sure that you are basically identified and they basically will handle the process for you and do all the interactions also with the Chamber of Commerce. Then you go, or that's an automatic step, go to the tax office, then you want to open bank accounts and stuff like that. And what we are doing there is basically making a distinction between natural persons wallets and organizational wallets because there are different requirements for organizations and natural persons. And going from functional requirements to technical requirements and also basically creating an architecture, how different implementers would be able to implement that. And of course, the basis again are the technologies also mentioned in the architecture reference framework.

Niels Klomp (23:36.10)
We're seeing similar things happening also in the large scale pilots. So there's test beds in the different large scale pilots as well. You now have, of course, the reference implementation of the wallet. So we are now sort of seeing a focus on versions being used. And I think that's already a plus that more vendors start using the same versions of the specifications because in the past that really has been a problem, of course, that a vendor might have a nice solution but if they are using a different version of the specification then you still cannot talk with them and that has been one of the key issues and actually with our library we have been lucky enough to have virtual detection in there so that we typically could be interoperable with an awful lot of other vendors. At the same time that's also a drawback because of course we're still at draft versions of specifications so in a few months we will be dropping all of that old version support because of course that also brings with it the maintenance needs for it. So all of that to say that I do believe that we will solve that as a community of developers moving forward and I think that is definitely something that the eIDAS regulation now is helping us also to do actually.

Kristina Yasuda (24:54.22)
And maybe just add to that, I think Because of the problems you mentioned, not the problems, because of the challenges you mentioned in the beginning, at least to make something working in the next one to three years, we don't have the room to argue like one standard over the other anymore. I think, we're at the point where, you know, thankfully eIDAS, ARF, Upcoming Implementing Act is giving us, clarity on this initial tech stack and we should focus on to your point, bringing those standards to a final, that is very needed. Like absolutely agree. And instead of arguing like, can we replace this credential format or like, can we change this instead of arguing that starting to focus more on like, yeah, even for example, if there's some, you know, government employer who's guiding the user how to install and use the wallet. Is that employer doesn't know how the wallet uses or is that employer tells the citizen, yeah, the wallet doesn't work versus that employer being excited, being like, can you please install this wallet? Because if you install it, you're going to make my life easier as a public servant. You know, like I think those are the areas where we need to really start focusing on. But that is not to say that, you know, we don't have to keep challenging the choices ARF has made, but that is more kind of long -term conversation and we really need to distinguish those because, you know, in 10 years time frame, you know, what about DKPs? Maybe the blockchain is going to come up again. Like, we don't know, but those questions, we shouldn't forget about them. It's just that, again, I'm repeating myself, but really have to differentiate that for one to three years, We have to focus on building what we have now, focus on taking to the finish line while having a separate conversation, what does innovation look like in 10 years?

Niels Klomp (27:02.01)
Yeah, no, totally agree. One thing I would like to add though, and that's what we are doing now in the Netherlands with indeed organizations like Notaries, like the Chamber of Commerce, the Tax Office, the banks, the payments organizations and then all kinds of other organizations is indeed also the focus on organizational identities and organizational wallets. And I do believe that they need to happen in the next few years as well, because although I am confident about the technology being adopted by users, I actually do believe that the adoption will happen and

will be pushed mainly from the organizational perspective first. It's as simple as organizations being able to save money using digital identity technology in terms of risk involved with interactions with third parties and whether those are organizations or natural persons. Typically an organization is involved in receiving data from organizations or persons and then sharing data with organizations and persons and typically in a lot of processes you need to repeat certain data and information. And as soon as that data can become trustworthy, of course, you can minimize risks. You can save money in terms of processing time. And actually, we believe that the adoption will happen from the organization perspective and sort of will trickle down to natural persons.

Niels Klomp (28:27.00)
And there's not a lot of focus, actually, on that. So what you see in actually the eIDAS regulation, but more importantly in the architecture reference framework is the complete and utter focus on natural persons. And basically, well, organizations are mentioned every now and then, but there never has been a focus on that. And I think that's something that was missed. And we will now also be looking together with the Chamber of Commerce in the Netherlands at sort of creating a, how do you call it, to investigate sort of the things that were missed or potentially missed or that would even sort of prevent organizational wallets from happening. So that's also something that we are involved with in the Netherlands and I think is an important part.

Kristina Yasuda (29:18.06)
Maybe it's not a topic for now, but yeah, I would be very curious to sit down with you or anyone else to identify the requirements for organizational wallets to make sure that ideally the same tech stack would work for both use cases. And we already started having those conversations and I have a hypothesis, but we need to brush it up.

Niels Klomp (29:39.05)
Yeah, happy to do that. And that's also one of the reasons and actual goals of the company passport project that I mentioned. The name might be a bit odd, I guess, but it's really indeed to focus on these types of things that are really important to organizations.

Mathieu (29:55.04)
So just double clicking on the concept of a technical interoperability profile. Christina, you were one of the authors of the OpenID4VC, a high assurance interoperability profile with SDJOTVC. That's a mouthful. Could you give some background on this and kind of who is this written for? Does this kind of align with your statement before of “we need to make some hard choices to see adoption in the next one to three years and then...also have a longer term roadmap for five to 10.” Does that kind of fit within that conversation as well? And so basically, yeah, like what was the genesis of this? Who is it written for? Who's consuming it? Can you give a bit more background on that?

Kristina Yasuda (30:36.13)
Yeah. Again, thank you for asking. So high assurance interoperability profile for a stage of VC hype for short. The goal was to, yes, fill in the gap between high level requirements given in ARF and the actual technical specification that implementers can start implementing. So when the ARF came out, we were hoping that, you know, large scale pilots or implementers, like they would define something like this, in order to start building things. but it was happening, I guess, slower than they were expecting. So we just sat down and sat, you know, let's, let's provide a starting point on for that conversation. So yeah, like that profile is intended to target these government-centered use cases, so to say, that require higher security than maybe just more enterprise identity kind of use cases. So it does, for example, mandate center -constrained tokens, or it does mandate certain elements like that.

To clarify the reason why it focuses on the stage of the VC is because there's kind of a separation of responsibilities where for MDocs, MDoc credential format, we were trying to delegate it to ISO so that, you know, there's, hopefully less confusion for people if they want to know something about an MDocs, they go to ISO. If they want to learn something about the stage of the state VC, that would be in a pipe or on. So that's a thing in a nutshell.

And I don't think it has an official standing in terms of ARF or whatnot, but we do have a lot of implementers feedback that it has been extremely helpful as a starting point to start interoperating, start testing. So I think it served the original goal we were hoping it would serve. And now we would see what will be the next steps for it, whether it's going to be replaced by something else or it's going to keep evolving. Yeah, I think that's yet to be decided.

Mathieu (33:13.04)
you were involved on your side, Niels, on another interoperability profile in the Netherlands called the Dutch Decentralized Identity Interoperability Profile. They all have fantastic names. How does that differ from the one that Christina described and what is its place, I guess, within the ecosystem?

Niels Klomp (33:33.18)
Yeah, we actually ditched the word Dutch from there. Because, yeah, although we like to think that Dutch is the entire world, and maybe at one point in history we might have been, but that's for sure a long time ago, and it's a good thing. So DDIP, Decentralised Digital Identity Profile, is mainly focused on moving towards actually the architecture reference framework and maybe with some additional goodies. But the important bit is what we have been seeing mainly from vendors in the digital identity space, but as well organizations that now need to start working or start experimenting with the technology. Because over the next few years, we now have the regulation, the member states are basically making their local laws over the next few months. And then in two, three years time, we will have the actual implementations in place. And that means that a lot of organizations will start needing this technology. And they have a problem of, okay, it's complex technology for us. We have no real experience with it yet. How are we going to go about it? And the profile that we are creating is basically in a six month cadence, basically defining which specifications to use. So to be clear, the current version of the DDIP Profile isn't

using MDLM docs, for instance, it's also leaving out trust establishments altogether. And of course, those will be happening in the next versions. But basically what we are doing is creating a profile based on different versions of specifications, saying what needs to go in there, what doesn't need to go in there at this point in time, and then making sure that people and organizations know in advance what the next version will be, what needs to be in there, so that we all can go more or less in log step to the next versions of it. And at the same time, of course, leave room open for parties that have already implemented way more than that is in the profile itself.

But the important bit is that we basically have a common subset of technologies, versions, and specifications that needs to be implemented so that we can achieve interoperability. And then not only interoperability between vendors of the technology, but indeed also having parties on board that can actually start experimenting with the technology and know that, for instance, that if they want to set up a relying party, that they also have wallet software from different providers they can use to start interacting with it. And of course, similar for issuers or a party that wants to test a wallet, that they can actually use different issuers and different relying parties, for instance.

So that's the goal of the whole profile. It's not so much to create this big bang type of profile and say, okay, this is going to be the end result and you need to implement all of this. No, it's okay if you want to go in a steady cadence and want to have different other organizations working with you and ensuring that they are interoperable with your solutions, then you have a six month cadence basically.

Kristina Yasuda (37:02.09)
I don't know how much you want to dig deeper into this, Mathieu, but I think the future of intro profiles is interesting. Like initially, personally, I expected much more intro profiles to be emerging. But for whatever reason, they didn't. So I think what's happening is kind of people looking at these, you know, some intro profiles being public or the actual specification and they make choices that they need to make and they build it. And, you know, once the problem arises, they kind of start trying to align. I think that's what's actually happening in the reality. So we'll see whether it's going to be like a consolidated profile or, you know, but also to Neils point on that they don't have MDOT profile yet. That dynamic is very interesting because It relates to this online offline dynamic where one of the usual arguments to keep MDoc format is because to present the credential offline, meaning over Bluetooth without any HTTPS connection, you need MDoc. But I really question whether it has to be that way. Maybe that's one area where I really want to see innovation in the sense that, that's what we tried to do is OpenID4VC over, is open ID for Bluetooth specification where we try to define how you can take the syntax of OpenID4VC over HTTP over Bluetooth, right? To make sure, because the big strengths of OpenID4VC protocol is that it's credential format agnostic. It's agnostic to trust mechanisms. So take that over Bluetooth, right?

And the big goal was yeah, to achieve that you can do is DJOTVC over Bluetooth for offline use cases. So it's because if you talk to implement at least implementers I talked to, their first use

case is usually online, right? Because for this key resolution, what not, you need internet connectivity in the end. And then it would be so sad if they would build this whole tech stock and the moment they're like, But this one small thing we need offline and then they have to build a whole new tech stack. Like that doesn't make sense to me, right? So how do we, you know, make that transition smoother? it might not be the highest, highest priority in terms of, you know, crossing the chasm and driving adoption, but that's definitely something I would hope to see as a, you know, innovation coming up. So, sorry, sorry, no. So because of OpenID4VC over Bluetooth. We didn't see as much of the adoption as we were hoping to. So now my hope is maybe extending it to you know, 13 -5 to be able to transport this DJ3C. And I have a job. It's honestly not that complicated. It's pretty straightforward. Sorry, Nios, go ahead.

Niels Klomp (40:08.12)
Actually, I wanted to just comment on that, that as long as we make it to phase two of the Funke, then that's literally in our proposal as well. So we just have to make it to the final four of phase two, I guess. And indeed, Mosip also has been doing quite some work on that as well, of course. And I think it would indeed also be really good to see that happening with SDJOD credentials as well. Because indeed there's now sort of this logical divide between in-person presenting credentials versus online credentials. And then indeed parties having the different preferences for the credential type being used and specifications being used. And yeah, that would be good to be able to see SDJODs over Bluetooth as well, indeed. Yeah.

Kristina Yasuda (41:02.13)
One big news that came in yesterday was that the Japanese government became the second government in the world to issue a digital version of national ID into Apple Wallet. And here I'm mainly speaking of the Japanese citizen. I was pretty shocked in a sense that the governments need to realize the implications of that. Like I hear that the motivation was to drive adoption of that, my number card, which is essentially a digital ID of certain national ID of Japan. But the government's arguably, and this is a personal opinion, not affiliated, arguably have the largest say up to the point that they issue the credential, right? Once it's issued, Even if it's HMAC, what not, that's when there's a lot of negotiations possible. So the balance between adoption, good UX, and leaving this very important public infrastructure into the hands of one tech giant needs to be very thoroughly analyzed and maybe they analyzed but I doubt it.

Niels Klomp (42:35.03)
Yeah, it is something I think, if you look at eIDAS, of course Europe sort of is also in their current regulations and just also with the current political climates across the world is looking at, okay, let's, how do we become a bit more independent? And right now, of course, like any country and any citizen, you are very reliant on big tech, which is understandable. But you're really seeing sort of this approach in Europe to try to make that a bit more independent, whether we will succeed in that, that remains to be seen. I think it's going to take a long time in order to achieve something like that. But I do agree, that's totally different and something to applaud, I guess, than as a government's choosing for your citizens, indeed, to adopt for your national ID to adopt the solution of a big tech vendor. And yes, of course, the user experience is very important. And well, of course, they are very good at that. So that is a plus. But at the same time, just having

your national infrastructure basically and all of your citizens reliant on that. Yeah, that is something which is, you mentioned the word shocking. Yeah, it is a bit shocking, I guess. Yeah.

Kristina Yasuda (44:06.15)
And I think one strong message from my side is that, like when we're talking about these BigTech platformers, it should be differentiated them playing a role of mobile operating system provider and browser provider versus them being an actual product provider, right? Collaborating with Google or Apple or Samsung or Mozilla or Microsoft on how does the browser as the primitive as an infrastructure pretty much, or the mobile operating system as an infrastructure again, as a place where you potentially store the keys, for example, how that can be improved for the benefit of any other company building wallets on top of that, or any other relying party issue or using those is very different from allowing those two companies to actually provide the product, like a wallet, using those primitives. Because at that point, they can do whatever they want. They can optimize the mobile operating system. They can optimize the browser for the need of that one wallet that now they have a commercial interest to make the best. Right? And those two discussions really need to be differentiated because it's not like we shouldn't be working with Google and Apple. Like personally, I think, You know, if they can align to eIDAS, like that's an old cement going for European Union, as opposed to saying, Google app, but we don't have to talk to them at all. Right. Which is, which is emotional. Like I understand, but you know, there, there's this big difference.

Niels Klomp (45:51.03)
No, I agree. And then actually the Wallet API that's now emerging is actually a good example of that, I guess, because in the end, you have browsers and at least there's a bit more choice. Although if you just look at the sort of the engines behind it, there's not too much choice anyway. But still, there's a choice for the user there. And second of all, and what the browser API will solve is two things actually: is in terms of cross-device security as well as user experience for people. So I agree with you on that. And then, yeah, it would be very unwise indeed to sort of make the same sort of statements to be surprised about Big Tech sort of playing a role there. Although I do get that, of course, certain people might be worried that the browsers, they are typically indeed also coming from large organizations who have a lot of power and interest and from a user perspective, yeah, if they sit in between, yeah, that could be something that they would never expect. But at the same time, you have to be aware that basically browsers are already a part of daily life for everyone and you're submitting all kinds of information in your browsers anyway. So that's not too different actually.

Kristina Yasuda (47:14.03)
Maybe providing a bit of a backstory behind the browser API. So I don't think the battle is won, but I am personally very grateful for eIDAS 2.0 because when the browsers originally recognized an opportunity of building those browser API to present credentials, Their impulse was to build everything from scratch, everything proprietary, everything designed by Google and Apple. Like we know better kind of mentality. And arguably having eIDAS, setting certain requirements and being a blueprint for this wallet ecosystem did help a lot in these arguments, which resulted in a design where open ID for real file presentations protocols can be used on

top of the browser API. So OpenID4VC instead of using the browser primitives, like redirects now can, you know, like request does this can go through the browser API. And there are a lot of benefits, but the two biggest ones are one for vendors who already invested a lot of work and a pain for OpenID4VC for them, the transition is, you know, the smoothest, hopefully. And also, like, I personally don't think every single person has to go to browser API. I'm pretty sure the use cases where vanilla OpenID4VC would still be very useful would remain. So it kind of, you know, hopefully we are avoiding the situation where I need to build another stack just because I wanted to end dots. Like we are avoiding, I have to build a whole new stack just because they wanted the browser API.

But the second benefit is really the learnings we've been having for the trust frameworks and all these choices from the tech stack perspective, right? Because browsers' natural perspective is, browsers are going to provide you the origin. You're going to match it with the origin the relying party is claiming and that's it. What else do you need? You know, and maybe for some use cases, that's enough. But there is a reason why the strong gross indication of relying parties is required. Why there's a use case that requires the whole federation kind of trust chain behind the relying party. So just having them understand that, for example, eIDAS was very helpful. So yeah, I think that's one example where EUs intention is hopefully playing out well, but again, like, you know, the bad was not won. I'm not going to relax until that, that browser and face specifications like published, you know, which is, it's just, it's not going to happen right away again, or it's going to take a few years probably.

Mathieu (50:20.09)
You're both making my job as a podcast host very easy. It's a fantastic discussion. And I would love to, I would love to continue this in, in another podcast conversation. I think we could do a whole series type of thing. it's very interesting. I guess as we go into the last 10 minutes or so of this conversation, I was going to go into a OpenID4VC direction, but I think it's quite interesting now that we're talking about the dichotomy between the browsers and the platform providers and governments. We do have major reliance on these platforms today. Like every single interaction we do, like all three of us are on our computers all day on browsers doing stuff or on our phones doing stuff. And you are right, Niels, that the user experience is far better natively on these devices because they're able to control the experience much better than the application layer on top of it.

When we think about these platforms or channels like browsers, does there need to be something built on top of a regulation like eIDAS? And maybe that's for you, Christina, as kind of a starting point. Are there missing pieces there? Because there is a lot of reliance on them, and there is a lot of reliance on the existing trust infrastructure of certificate authorities, for example, that are involved there.

Are there examples from the past that we could look at that, hey, we don't want to go down that road? Is there maybe something that needs to be put on top of the eIDAS? Something additional to kind of promote what we're, the vision that we're trying to push towards.

Kristina Yasuda (51:59.16)
So yeah, I think there is a precedent where the EU is trying to say, we're trying to replace the cloud providers. We're trying to prevent using large tech, large big tech versus, like going towards an approach where maybe one thing that can be done is have an investigation committee or something that investigates the competitive practices of those companies. Like why are they so big in Europe, right? Because surprisingly, like I was surprised having moved to Europe, there is a certain market of software which provides a very similar functionality as GSuite, M365, whatnot.

Right? So why are those companies not growing faster? Why are those companies not winning? For example, I think that approach, for example, is much more constructive and effective than trying to target the regulation only as a bigtech. And it's my hypothesis. I'm not an expert on this, but I think what could happen is you make it harder for big companies, but if it's hard for them, it's even harder for smaller companies. Right?

So if those big companies manage to survive those tight regulations, they might be the only one who can survive. So that kind of investigative approach to trying to help other companies out-compete in a, you know, for good or for bad, for living capitalism, out-compete and that as opposed to, you know, just say that don't use big tax services is probably more constructive.

but also, again, I'm repeating myself, but clearly separating the primitives infrastructure those companies provide versus, the, product they monetize on. so that that's really, I mean, I don't think you are going to invest to create a third mobile operating system or, you know, fifth browser. but clearly making sure that If those companies are providing platform kind of services like browser, mobile operating system, they don't prioritize their own products. Because for example, it's a very small sentence, but on Apple's website, they have a sentence saying, if a third party wallet meets Apple's requirements, we're going to allow it to handle digital credentials.

And that partially supposed to address the fear that Apple wallets going to be the only wallets that can handle this digital credentials on iOS, which was a fear following what they did in payments. So again, it's just one sentence. It's not executed. We can't relax. But enforcing things like that, again, would be very helpful, I think, for equalizing the playground, right? Like, so, Sorry, I shut up after saying this, but if they win when they have a fair playground, I think that's market forces. I think that's okay. But so we should focus on having that, you know, equal playground as opposed to enabling a situation where these big tech companies are, you know, privileged from the very beginning just because they control those infrastructure.

Mathieu (55:45.17)
Fantastic. In closing in this podcast, we're talking about different interoperability profiles, different types of drafts that only become real once you start to get implementers working on it and implementers feedback. If we focus on the OpenID4VC and maybe on the presentation side of things, has there been any constructive feedback from implementers that has maybe resulted in.. So I'm thinking about how we're changing the specifications and maybe it's an interesting

point to talk a little bit about presentation exchange. Yeah, so I don't know, Niels, if you want to kind of introduce quickly presentation exchange and what's the current state of it within the OpenID for verifiable presentation world.

Niels Klomp (56:31.16)
Yeah, I think that last part is better suited for Christina to answer, but I can definitely tell you a little bit about the background of the presentation exchange first. So presentation exchange, of course, originated in the decentralized identity foundation. It has its original roots in DIDcomm and of course is a specification to be able to create definitions for relying parties to request certain credentials, request certain claim from credentials. So in order to support selected disclosure, you can create a definition. And basically it has been or trying to be protocol agnostic in terms of how you transfer these credentials and also agnostic to the credential types being used. Having said that, of course, You only know what you know at a certain point in time, meaning it has a background in DIDcomm. MDL, mdocs, of course, they have been created and specified, well, the last 10 years, I guess, but the adoption wasn't really already happening at the page that it's currently happening when the specification initially started out.

So, It was created to be neutral and basically as a query language. At the same time, we already noticed once we moved from version one into version two, we made quite a significant amount of simplifications. And when I say we, it's of course the editors of the specifications and we on the experience side have been involved in the specifications a bit as well, simply because we are one of the first implementers of an open source implementation of presentation exchange version one and two and actually we have I think still to date the most complete implementation out there basically supporting everything.

Niels Klomp (58:34:02.)
One of the key things that we identified was the complexity of it. And just to give you a little bit of an insight, in version one, when we received funding from the European essif Lab projects to create an implementation for it, it actually took us a few developers for almost nine months because of the constant changes and things that weren't clear. So it has been quite a struggle to get it implemented. So when creating version two, we said okay let's make sure that things will become simpler. That's also when features were introduced meaning that if you just look at the core specification and if you wouldn't implement all the features then it's actually not too complex to begin with.

But yeah, it still has its roots inDIDcomm. You still see that indeed in certain areas. So initially a choice was made to use JSON path in there with all kinds of potential security issues involved. Then I look at JSON pointer. We looked at using JSON pointer, but right now and more recently you're seeing basically from different vendors as well sort of the questions, okay, can we have more specific query languages for different types of credentials? So that's what you see emerging now. And I think Christina can elaborate more on that. And before handing it over to Christina, I think there's things to be said for both ways. Of course, I do get that if we would have looked at it right now and we wouldn't have a presentation exchange, we would immediately say, okay, yeah, that's the best approach.

At the same time, you also have to be aware that there's quite a significant user base already using presentation exchange and also using presentation exchange outside of OpenID4VC. So that's something which I think hasn't been discussed enough at this point. And it means that all of those parties have put money in it and have it working right now, then So sometimes indeed a lot of people are claiming, okay, it's too complex. That's certainly true. At the same time, there's quite a lot of implementations out there already that have succeeded in creating the implementation. And well, your former employer, Christina, is one example of having a large -scale implementation of it. But at the same time, indeed, I do get why people are saying, OK, we really would love to have a more credential-specific query language type. And well, lots of things are happening there. And I'm happy to give it over to you, Christina.

Kristina Yasuda (01:01:26.08)
To give a bit of a context why we decided to use presentation exchange in OpenID4VC in the very beginning was multiple reasons. First motivation. We wanted to focus on getting it right, the rest of the specification, including trust frameworks, including on how to make it agnostic with different credential formats and whatnot and using presentation exchange, which was rather complete by that point, really allowed us to do that. And I'm honestly very grateful that we could do that. I think that helped us to progress quickly to, you know, give people the specifications they were looking for, but also there wasn't a motivation to bridge two worlds because when we started, There was a divide between people who were saying the way authentication identification works right now is completely broken. We have to scratch everything. We have to build from scratch. We have to use blockchain. We have to use the IDs. And there was this world of people where we're saying, you say we're it's broken, but we are actually user centric. We just don't understand how authentication identification right now works.

And both are right and both are wrong. So we really had to bridge those two worlds to make sure we are building up on experiences and learnings of those to make something truly good. And presentation exchange combined with, you know, OAS based OpenID4VC really helped us to do that. It helped to build trust with the community that we are listening to them.

It also helped build trust with that second community that we are leveraging existing experience from all of us, what not. And when the recent move away from this partially stirs from the conversation with the platform vendors, because when this browser API is being built as a browser engine or as a mobile operating system, it depends on the platform.

Kristina Yasuda (01:03:36.04)
They need to understand this query language. What is Verify actually requesting? Because they have to render this wallet selection screen where they're asking the user, look, this party is requesting this credential. Do you actually want to open that wallet so that the rogue bad wallets don't get that request in itself, but also helping the user to make this intentional choice when there are multiple wallets that can handle the same credential. So they had to understand it.

And that's when this feedback started coming in from those developers of the platform saying, we don't understand PE. Like how did he build that? Like why? and honestly, knowing how much effort went into simplifying PE and making it work. I was very reluctant to like, just say, look, let's scrape it and design something new. Like even now, like it makes me very emotional.

but I think what made a difference for me, and it's a personal comment, was that talking to non-platform developers, I realized that maybe I have underestimated how hard building PE is. like we have libraries that, you know, Spurion, for example, build, but people still seem to be struggling. so that feedback combined kind of, I think, at least for me, like, from my perspective, I tried to resist until I could, until there was a point where it was like, okay, if we really want the OpenID4VP to be successful in the long term, you might as well listen and try simplify on the, the query language part of it. And we really approached it very holistically. We spent a lot of time gathering requirements to make sure people are aligned.

What is needed. And after that, only after that, after having a lot of discussions based on incorporating like three, two, three proposals, we have this current draft. So, yeah. And I think the next big question is how does this transition would look like, right? So we have PE its implemented. We have this new proposal. It's about to start to be implemented.

Do we have a transition period where we say both have to be supported or as an editor, we've been refusing to allow two options for query language because from my perspective, and I think many in the working group agree it's an interoperability nightmare. Now that you also have to specify what query language you use in the protocol, it might, it would be a nightmare.

Niels Klomp (01:06:26.04)
Christina, you know I have a solution for that, right? So if the whole world just follows the DDIP profile, then at one point in time, all have to implement it and then we drop presentation exchange altogether.

Kristina Yasuda (01:06:39.04)
Okay, okay, sure. Let's march towards that world domination.

Mathieu (01:06:40.17)
We have the solution. Ding, ding, ding.

Niels Klomp (01:06:44.19)
Yeah, exactly. We don't care about big tech as long as our profile achieves world domination.

Mathieu (01:06:54.10)
Christine and Niels, I very much enjoyed this conversation. I would love if you're open to doing another one at some point. I think we could go on for a long time. So thank you so much for doing this. I really appreciate it and look forward to more.

Kristina Yasuda (01:07:10.12)
Thank you for having us. That was fun.

Niels Klomp (01:07:10.12)
Happy to. Thanks for having us.