Mathieu (00:23)
Okay. It looks like we're live first podcast on the video. So, that'll be cool to see how this turns out. We started a working group within the Trust Over IP last year to start looking a little bit more into detail around how different credential exchange protocols compare against one another. And we're obviously seeing.

If you look at the growth rates and stuff in the decentralized ID and digital wallet market, you're obviously seeing a lot of uptake of programs and investment in the programs that want to implement digital credentials, either as issuers, and we're seeing a lot of government agencies invest into that globally to start issuing citizen digital identities to their citizens. And there's also on the other side protocols to help consume or verify credentials from mobile wallets as relying parties or as verifiers. And the space is still very technical, I would say in nature today. A lot of the buyers and implementers are technical by nature. And what we were trying to do with this credential exchange protocol task force was really not dumb it down, but just create a framework that makes it a little bit easier to compare protocols one against another, against a common set of criteria, so that if implementers have certain business requirements or certain contextual aspects to what they're trying to do, that they could kind of more easily weigh different options one against another.

And so with that said, I would love to just hear from the two of you and either of you could jump in and we could kind of bounce off each other throughout this conversation, but maybe the good starting point would be to talk a little bit about some of the initial credential exchange protocols that we chose, which we chose because that's where we're seeing, I guess, market demand, but just to give maybe an overview of those if possible. And maybe the good starting point is just to talk at a high level or why these protocols exist for what types of objectives do they have and how may they differ in terms of architecture lay the ground of what we're seeing, at least as the main credential exchange protocols that seem to be gaining traction in the market today.

Hakan Yildiz (02:57)
Sure, yeah I mean when we started this task force we were looking into like you said which are the more predominant or relevant protocols that are out there. We identified to start with rolling with four of them. One of them was the ACDC which is strongly bound with the KERI protocol itself. The other one was the ISO 23 220-3.

I'm talking about all the issuance protocols right now by the way, which is about how to issue a mobile driver's license, the protocol itself about that. The other one is the Aries issue credential protocol v2, which is used by all the Aries frameworks and the final one that we were looking into is OpenID for verifiable credential issuance, which is gaining quite a few traction at least in the Europe so far through the European Digital Wallet Initiative and the large-scale pilot projects that are running at this point. And the reason, well, there are many more credential exchange protocols as well. We wanted to keep the scope a bit low at this point. Like there's also Credential Handler API. There is a VC API and there are some couple of others that we might also consider in the future to put it into the scope. But from the size of our working group and the task force, and from our own expertise, we decided to focus on these four first of all, and I think what we were trying to grasp around is to understand or like categorize them, like for a business owners to make a decision on which protocol to use. for their implementations.

And from a very, very high level point of view, I think what we were looking into is the architectural model, being whether a protocol is based on server client pattern, meaning there is a server that is serving multiple clients, or if it's a peer-to-peer model.

Hakan Yildiz (05:18)
where the communication is happening through also peer-to-peer protocols. Yeah, and from this, this is like more or less like one of the bigger distinctions in my opinion, at least of these different protocols to decide on which course you're going to take because they're also inherently not very compatible with each other. And one of them is being message-based, for example, the peer-to-peer model. Whereas the other one being session-based and you're relying on certain transport protocols such as HTTPS and TLS.

So one of them is relying on a request and response and the other does not have to have that. Like there's a state to the interaction that is happening, but you don't have to get a response back at that very moment when the request is being done. And I think these differences are also affecting what kind of use cases they might be more suitable for server clients or the session-based structure may be more suitable for digital identities for natural persons where the interaction is happening just on demand, on the go when the consent is also being given. Whereas when we're looking into the more the peer-to-peer based protocols, it might be more suitable for, for example, machine-to-machine communications or when there's like an offline or when a response cannot be made just on the fly.

But without just taking too much about this architectural model right now, like we had a couple of other categorizations there, like for example, what kind of security model that they're using? what is the performance scalability? what kind of privacy features that these protocols offer to the maturity of these protocols? how are they being deployed? maturity in terms of not only the protocol maturity itself, like the standards on what level they are, but also how many implementers are using these protocols and which projects are being used.

Vladimir Simjanoski (07:33)
Yeah, maybe just to follow up on that and take one step back, I think, at least for me, I'm always sounding like a broken record trying to repeat this. And I think I was the one always coming back to it during our meetings is the why, right? So why was a certain protocol invented in the first place? Like why, especially if it was not the first protocol around.

Why was there a need initially to implement a new protocol? And I think this is a great, in my opinion, a great basis in order to understand the design principles behind the protocol afterwards. And the architecture model, whether it's peer-to-peer or it's a server client, just logically answers, like logically flows through that thing once you have the background context set in.

So for example, if you look at Aries and what was the initial scope or goal to solve there. So we are solving digital identity, right, in the internet. The internet doesn't have a digital identity. Let's solve that. That's a very different scope, very different requirement than we have this big upgrade of EIDAS 2.0 coming in.

We think that we have a lot of infrastructure lying around, and we have a timeline. So within this timeline, we have to make sure that we can solve this thing. So we can issue these digital counterparts of governmentally issued documents. So these are totally different things. So if you think from that standpoint, and I think the creators, in order to understand the protocols well, you also have to to look and understand the background context as well.

Mathieu (09:31)
Yeah, that's a good point you made there. where I guess if you look at the open ID for verifiable credential spec, it is one very straightforward in what the use case is for it. Like it's really all about personal identity and it has very strong ties to identity and access management use cases versus some of the other protocols that are very open and the types of claims or the types of credentials that could be moved over these protocols are much broader in nature than something like OpenID4VC. And then you also have different, I guess, types of identifiers that would be able to interact with these protocols as well too, right?

We often talk about the decentralized identifier in the self-sovereign identity space, but if you're looking at like more like ISO based standards and having EIDs and MDLs and using ISO based credential exchange protocols. Or if you're looking at KERI or if you're looking at OpenID, there's maybe a difference in how identifiers are assigned and managed as well. Maybe worth talking a little bit into that too. And maybe fits into the whole server client or client to client type of model.

Vladimir Simjanoski (10:54)
Yeah, and it also answers the question like, especially for OpenID4VC, since you know that the government is behind or the governments are behind it, of course they will put a lot more emphasis on things like, you know, agnostic, credential format agnostic, you know, as a requirement or crypto agility as a requirement.

because they don't want to be locked in into a particular set of technology. They also have to think about how you can migrate to the next thing. This is nothing lasts forever, right? So you have to take this into account right from the start and hence the results. So yeah, I think the background context sheds a lot of light into the details of the protocol

Hakan Yildiz (11:51)
Yeah, but I totally agree with that. But I also think that the reason why maybe OpenID is seeing so much traction in the regulatory environment is because most of the participants in those regulatory environment are actually based on the authentication by OpenID Connect or OAuth 2.0. And what OID4VCI brings on the table is building on top of OAuth. So anybody who has

already have experience and knowledge in the traditional identity and access management space has an easier time to get into decentralized identities.

Whereas with Aries...

Vladimir Simjanoski (12:41)
There you go, blank canvas.

Hakan Yildiz (12:44)
Exactly. So coming with like whole new concepts of like decentralized public key infrastructure DIDComm and connections and whatnot.

Vladimir Simjanoski (12:54)
Yes, but then again, if you remember our discussions of how should we compare, or what is the most suitable format to compare these protocols? Because it's natural that you want to compare it, right? At some point, and the most natural thing is to have a table, right? So with different columns and just say, oh, how do they stack against each other? While I do think that this is a useful format for comparing it and checking it and learning about it, it doesn't give you all the insights because of that.

I think what we did with the long formats, all right, we have the long format, which is like 10, 15 pages long, textual description of all these categories that we put in place, and then we have the shortest, the distilled version where you can do this side-by-side comparison of different protocols.

yet I believe we can still say that we don't have the perfect format for comparing these protocols. So if a newbie comes into the place and wants just to pick some protocols, he knows maybe he has a fairly certain idea about the requirements that they might encounter. It's still hard. So in challenging to just go through the spreadsheet and just say, oh, clearly that's the winner for me.

Hakan Yildiz (14:18)
Absolutely, maybe to extend on what you were saying, Vlad, I think we had this conversation while comparing it on a bilateral basis, but comparing these protocols is like comparing apples with oranges, because when we're looking into OID4VCI, for example, it is a very long specification, and it covers many, many different topics, including the transport layer including how mutual authentication happens, how the credential is being issued. Whereas when we're looking into Aries IssueCred v2, it is solely focusing on the states of the holder and issuer and what kind of message is going to be sent in which state to complete the transaction of issuing a credential.

However, it has a lot of dependencies that are not necessarily mentioned in the protocol itself. For example, DIDComm being a hard dependency, you cannot have issue cred without DIDComm. And if you're talking about DIDComm, you have dependencies with the connection protocol, DID exchange protocol, I don't know, out of band protocol, many, many RFCs that are written in the Aries world.

Mathieu (15:35)
I like the point too that not locked in. I think that's what we've seen at least from national government bodies as well, is that they want to make sure that they're not using anything that isn't internationally accepted as well, not based on international standards. When you're talking at an international between countries, countries have requirements not to impact trade or impact the economy between countries and things like that with different implementations. So that's perhaps why we see a lot of interest and stuff from the ISO world come up as well because one, governments are directly involved within these ISO working groups and second of all, it's an internationally accepted or run standard body which reduces these risks of being locked into a specific technology or something proprietary or something that just isn't globally adopted or accepted.

And then another thing I think we saw, like you made the point about OpenID, Hakan and why there's a push for this as well. But I think that there are misconceptions that we saw as we were diving into this where the levels of maturity of these things, at least from an implementation standpoint, is not always as accurate as people think. Like I think you talk to people and they think, because, you know, it's based on OpenID or OAuth, that this thing all works, it's mature, it's ready to go. Whereas I think once you dig into stuff, not that it's not moving at a good pace, I think it definitely has a lot of momentum, that specific protocol in question. But looking at the implementations was an interesting exercise as well.

Vladimir Simjanoski (17:24)
Yeah, I can attest to that because we did the same exercise here on our side as well. Well, I think you have to understand that there are several activities going on, right? So the one thing is, and I think that's why we add this governance category in our comparison metrics. And that is obviously the state of the specification is one thing. Then you have also the state of the implementation as well.

And then on top of that, once the implementations are around and used, you also want to see, okay, is there some kind of an interoperability test suite or whatever, profiles, whatever, and this process, they're usually not the one-time things. You also want to see that there is a vibrant community around them, right? So it's not depending on two persons, rather it's a vibrant community that is extending, or at least it's not shrinking very fast.

So you also have to take into account all these things before deciding on a protocol, because the protocol might be the most used, but that doesn't mean a lot. Things can change very quickly within a year, so to speak. So all these things you have to juggle in order to find the most suitable protocol for your requirements.

Hakan Yildiz (18:48)
Yeah, absolutely agreed. And maybe to extend that statement is when we are looking into, for example, ID4VCI, we see a lot of traction. However, when it comes to testing, for example, is there is a lot of things that can be improved. And I also have to admit that we have another working group in the Open Wallet Foundation for OpenID for Verifiable Credential Protocol Family Due Diligence. And OpenID Foundation is actually working on the conformance tests to offer implementers a way to test their implementation, whether that is conformant or not.

However, the issue is though, and the OID side of the things is that there are new profiles popping out quite fast. So there is the HAIP profile, High Assurance Interoperability Profile that is supposed to be the one for the architectural reference framework, EIDAS 2.0. There's the Dutch international identity profile and some others as well. And making these tests, like the conformist tests with the profiles or like to achieve interoperability from an ecosystem point of view, these profiles are playing a very, very large role.

Both in probably ISO in ACDC, I would assume there as well, but like in Aries world, we do also have these two AIP 1.0, 2.0 as one of the two predominant ones. And I think what Aries did well in the past was also offering a test harness and the interop results of these different frameworks that are out there to prove that an AFJ can communicate with a cloud agent Python using a profile.

Mathieu (20:47)
Could you, just provide a little bit more context around the concept of profile? I think the word profile has been getting used quite frequently and being looked at across different vectors in this space, but you touched on it a bit, but what is exactly a profile and why is it important?

Hakan Yildiz (21:06)
So I think to that answer, there are two answers to that question. If you're looking into it from for example the OID point of view where there's like a very large specification that is saying what can be included, what are the *mays*, what are the *musts* and what are the different optional parameters that a query can have for example. In that case a profile is a specification of what are the *musts* that are involved in the interaction that's happening between these parties. It also includes things like credential format to ensure that both parties can actually receive or validate the credential for example.

But on top of it, yeah the IDs, for example, at which what kind of DID methods are being supported or what kind of key management, key resolution types are being supported like JSON web keys and et cetera. So this is the side from the, of the perspective from the OpenID4VCI. But when we're looking into the Aries side of the things, it becomes like coming back to the statement that we just did with the dependencies that are in the coming with the issue credential V2 protocol for example. In the Aries world, the AIP, Aries Interoperability Profile 1.0, 2.0 specifies which Aries RFCs has to be supported in order to have a communication between or exchange a credential between two parties.

because there are also multiple ways to exchange the IDs, for example, there's the connection management that you can use, but there's also DID exchange that you can use. There is this DIDComm v1, there is DIDComm v2. And these profiles make sure that there is a set of RFCs that are being used and tested against in the conformance tests.

Vladimir Simjanoski (23:18)
Yeah, I think you put it nicely because there are multiple even within one profile there are multiple combinations, right? So I think, especially as you said in the OpenID4VC space the different kind of DID methods that you have to support is just you have to make sure that within this Interoperability test you can support them all right, so it's not simple by any means.

It's not it's not straightforward or it's that one, that integration, that interoperability profile that I support, just run the tests, I can communicate with anyone else who is claiming to be that, to support that profile as well. So it takes quite a lot of effort, continuous effort to sustain, to develop and to sustain this kind of interoperability in place.

Mathieu (24:11)
And you would expect to see evolution in these over time as well as, as adoption happens, as more, more use cases and verticals come in, there'll probably be a lot more of these. So I guess it becomes important for implementers to stay up to speed with that.

Vladimir Simjanoski (24:26)
For sure, I think this is a must, right? So otherwise, the cost of just maintaining a solution and developing a solution will be too high. So I think we have to think of how we can lower down the cost of the whole thing, right? So the the building and the operating, maintaining, everything has to be affordable, right? It doesn't have to be too big of a price if you want to achieve the main goal, which is to be able to deploy multiple digital trust ecosystems out there in the wild.
It will take some time, like a maturation of the whole ecosystem that we have, but also always have in mind that we have to lower down, right, so the cost of everything that we are developing.

Hakan Yildiz (25:09)
Absolutely. And to that extent, we're also at the OWF in this working group, the Due Diligence Task Force, we're looking at creating a baseline profile for OID4VC protocol family, which is to help developers to get into the specification and the implementation without being very overwhelmed with certain features that might be harder to implement like for example some features in the HAIP profile yet to have a common ground between all these different profiles so that once the baseline profile is established even though it might not offer all the neat security features of the protocol itself that there is a base communication interaction and exchange of credentials that can happen if you support the baseline profile and any implementer who has worked on the HAIP or DIIP (Decentralized Identity Interop Profile) or other profiles would have a very, very easy time to tune down to this protocol to offer that as well.

Mathieu (26:23)
I have a vision and it would be interesting to gauge your thoughts on this, but when I think we're all used to the verifiable credential trust triangle or at least the decentralized model where an issuer signs a credential, issues it to a holder which is able to store it in their wallet and is able to present it to any relying party or verifier as they wish.

When we look at that model of the issuer holder verifier, which is impactful just because there's no call home, there's no central authority there, credentials don't lose their integrity as they move around within there. There's three parties that need to be thinking about credential exchange protocols. You have the issuer, you have the holder or let's just say the wallet providers or the technology solution providers for wallets. And then you have the verifiers, the relying parties.

I have a vision of the wallets in the middle being very key for interoperability and needing to support multiple protocols because you may be interacting with one specific issuer that wants to use an ISO protocol to issue a mobile driver's license because they want to use the ISO family, the ISO spec but you may be interacting with another one who may be wanting to issue a verifiable credential using an OpenID4VC or an Aries issue credential, RFC type of thing, or even ACDC from the KERI family. And then you may have similar types of things on the verification side of things.

Do you agree with my statement that the wallet is maybe going to need to be very flexible and supportive of these different protocols versus kind of the two other ones, or do you suggest that issuers issue similar credentials using different protocols? How do you look at interoperability from that standpoint of the digital or verifiable credential trust triangle?

Vladimir Simjanoski (28:28)
That's a great question. Hakan, if you allow me, maybe I can interject first. So you can look at it from different angles, right? So I will try to use the pragmatic cap now to answer this question. So if I look at it from the pragmatic standpoint, I think that the issuers, they would want to have the freedom, the flexibility to choose whatever protocol, verifiable credentials format, cryptography, whatever suits them in order to feel confident that they can go on with the issuance of these verifiable credentials. For them it will be up to them to decide what they want to use. And obviously once they commit to a particular infrastructure they will always lean towards the infrastructure.

On the verifier side I think we'll have to see something similar to what we have in the payment industry, right? So we have merchants today, they basically say, okay, we support credit cards coming from all these big players like Visa, MasterCard, whatever, American Express, whatever. So they will be the verifiers, they will commit to acceptance networks, if you will leave, I might use that terminology here, right? So I believe that there will be a development of these networks and on the verifier side, they will have to support multiple, right? So protocols which brings the question; Okay, this means that at the end, at the center of this dilemma, we have the holder and the wallet. So either the wallet needs to be flexible in order to support these multiple protocols, or which can definitely, I can see that not all the protocols under the sun, but maybe the most, you know, used ones, the most common ones. And at the same time, you would want, we also have to take into consideration that when all these components, they are part of a digital trust ecosystem, which means that they also should be in line with the governance framework behind.

So let's say for EIDAS 2.0, there might be some requirements when it comes down to the technical stuff that the wallet needs to support A, B, and C, right? So you have to take this into consideration. And at one point there might be some features or some constraints up to which you have to draw a line. Okay, this is what it should support at that point in time. We cannot support the rest of them. I'm not saying that such thing exists at the moment because it does not, according to my knowledge, but they might. I might say that there might be some constraints which are coming from the governance framework of that particular trust ecosystem.

Vladimir Simjanoski (31:20)
which kind of forces you to stop at one point and not think about, let's just extend that wallet, the universal wallet, whatever, call it what you want. But instead, just go out with your own. And vice versa, even if there is no constraint to do that, just the maintenance of that wallet, I would assume that there will be significant cost in order to support all of these things, especially if they are, you know, continuously developed.

Hakan Yildiz (31:50)
Yeah, so I totally agree with Vlad and don't want to repeat what he said. I think his view on this is like pretty accurate of like seeing like how interoperability can be achieved. It's based on the perspective. It can be on the wallet, it can be on the issuer, it can be on the verifier. But if you also take a look a bit into the value chain of identity and think about like who benefits the most from validating or having a credential information that is tamper-proof and accurate and etc. And that's a service provider.

Those are the ones who are relying on accurate identity data to grant access to goods and services. And in that case, what I also can think in terms of interoperability is the verifier side of the things being much more flexible than the holder side. Analog to the topic of payments, for example, we have VISA, MasterCard. People have two cards. Like it's basically inherited the different networks.

They do not have one unified card to go with it. But the service providers accepting cards or payments from both of these networks and then many more, like PayPal and direct payment and whatnot. So for that purpose, I think even though there is a strong emphasis on a universal wallet, I believe that the verifier side of the things are also quite interesting to take a look into to solve the interoperability problem so to speak so that the verifier can validate credentials using these four different credential exchange protocols agnostic of credential formats but depending on its own policy rules right because they need to trust these credentials.

So who the issuers are, authenticity of these credentials are, so that there's like a policy engine behind which credential I want to accept, disregarding the fact like from which protocol they are coming.

Mathieu (34:05)
And you could imagine then in that framework that there's a world where a credential is able to land in a holder's wallet using credential exchange protocol X, but is able to be presented into a verifier using credential exchange protocol Y. And that type of interoperability should be achievable, I would think, which makes the verifier not necessarily have to use the same credential exchange protocol family as the issuer, but there needs to be some mechanism not to lose the integrity or to be able to know that the data hasn't been altered and has been signed by the right party and all of the stuff that comes around.

Vladimir Simjanoski (34:50)
Yeah, I've seen some interesting initiatives there which are actually solving this on the verifier side, right? So, and this is for the same reasons that Hakan mentioned, right? Because it's in their interest, right? To recognize and to verify this credential because it saves them time and effort and money at the end which means that, you know, just support multiple protocols on the verifier side. And instead of placing that burden on the wallet, you just ask, you can also have this ask at the start of the negotiation, right, so with the holder, what is the language that you can speak, like what is the protocol that you can speak, and once you know, once you exchange this information, then you obviously have to keep these verification requests in some kind of an agnostic model, right, so we already have that with the DID presentation exchange up to a certain point and then you can do the translation on the verifier side. So depending on which language you understand, this is what I'm asking from you. So this means that you put the responsibility of interoperability on the verifier side instead of the wallet side. Then you hope that they will do this because of their interests, because the incentive structure will be in place.

Mathieu (36:17)
So we talked a bit about the verifiable credential or the digital credential trust triangle as a framework of looking from the different perspectives of different entities, what their role is in the ecosystem. And by the way, like a verifier in the use case could very easily be an issuer right away and in another use case type of thing as well. So that type of complexity comes into, but a verifier, if we assume, we often in the model assume organization issues to person, person presents to organization. That's just the easiest kind of model that we tend to always think about, but there's tons of other types of interaction models that are possible. Some of these credential exchange protocols are better suited for certain interaction models versus others. But if we start talking about interactions or credential exchanges between organizations and machines and starting to mix the different types of personas or entities, how do we better look at these credential exchange protocols?

Are there some that are better suited for certain types of interactions, like organizational data or organizational identities or even machine-to-machine transactions? It'd be great if we could just look at that lens and understand how the different credential exchange protocols, or at least choosing or looking at them, would come into play for these types of use cases.

Hakan Yildiz (37:45)
Yeah so since my current client also coming from the automotive data space, we're also having a similar dilemma here about the credential exchange protocols itself. so to your question, I think the answer is a clear yes. There is a distinction and there is a distinct differences between requirements from a human to machine or human to human interactions or human to business interactions and there is a distinction or a set of requirements that are different for machine to machine interactions. And what we're talking about the governmental eID stuff, this is a clear case for the human to business or human to human interactions.

And in that area, the OID4VCI and OID4VP, for example, are very, very suitable because the origins of those protocols like OIDC, for example, or OAuth being also very inherently suitable for human credentials and disclosing those human credentials.

And the protocol itself in the OpenID4VCI is very human centric. There is a part which plays a large role in the human consent. There's a conscious decision of making an agreement that you want to share a certain information from your wallet with the verifier for example.

And talking also with the spec authors about this topic, because we were also considering OpenID4VP for credential exchange for machine to machine, we came to realization that it's not necessarily very suitable for that purpose. Having said that, even though there are contenders here, like the Aries protocols being not a bad contender due to also mutual authentication that happens with the DIDAuth, with the DID communication as well as the automation of the credential exchange that is the possibility with these protocols. There is still a gap in the market I would say for machine to machine credential exchange protocols. There is nothing that we can say this is going to be it in the future so far. There are some developments happening in the automotive data space. There's a protocol called Verifiable Presentation Protocol. But that's a very, very early stage and we haven't seen any implementation of it so far. It's, it's really a blue waters for the time being.

Vladimir Simjanoski (40:30)
Yeah, that's a great insight. I would delve into the organizational identity space. And just in the last couple of days, there was this incident which supposedly happened in a, I believe it was a Hong Kong subsidiary of a financial institution. I suppose you've encountered this news because it was published by all mainstream media. It says that An employee within a company just wired 25 million worth of US dollars to these fraudsters who are actually using the deep fake AI technology, in order to convince them that it's actually this instruction is coming from the CFO of the compny. So I'm not sure whether it's real, not, but everyone translates. So to me, this opens a lot of questions, right?

The way that I understood it was that first there was this email which sounded a little bit fishy but then the follow-up to that was that they went on a video call like we have now and then this employee was you know talking to several employees on the other side the CFO and several other employees that he actually knew from the company and he verified them that these are actually you know the right guys actually sitting on the other side of the video call. So after that, he did the wiring of the money and obviously made this go away. So the problem, there are multiple problems there at stake, right? So the first problem is you need to have some kind of processes within your company.

So it's not just like, OK, let's go jump on a video call and I'll hand out an oral instruction and you just go run with it. So just wire this money to our offshore HQ in the Bahamas, whatever the case may be. So that is the first thing that's coming up to my mind. And I think some of these protocols, and If we are thinking about digital trust within organizational identity and what vLEI in particular is doing with the stuff that they have, I think authenticity is really a key there. Right? So first, we have to make sure that we are actually talking to the right parties on the other side. I don't want to talk to a robot. I don't want to talk to a bot. I don't want to talk to a deep fake. I have to make sure that this is authentic, the discussion that I'm having. That's for like number one. Let's set up the baseline there.

But then on top of that, I would want to set up some kind of processes which reflect the complexity of the hierarchy within the company. And this usually means that for different kind of goals, for different kind of actions, there has to be different kind of co-signing or multi-signature schemes, so to speak. And some protocols, KERI in particular, have this built in into their protocol.

So you can set these identifiers within the company and within the persons responsible within the company, and you can actually control the access to the signing key by setting up a respective multi-signature scheme. So you can argue that if these guys were using some protocols like KERI, this is only for the identifier, let alone the verifiable credentials. For sure, they will not have this problem.

Mathieu (44:10)
is looking at, and I know we did this in the comparison, but I guess you mentioned authenticity, but looking at security and looking at privacy, authenticity and confidentiality, I guess is a good lens as well, which could help like in the case of an organization like this, if authenticity is kind of the most important thing, maybe there'll be a preference of one over another.

Vladimir Simjanoski (45:35)
Yes, so I think that it's very easy to, just drive the direction towards one of these things towards privacy, especially when you're talking about personal identity, because that's what everyone wants, right? At least claims that they want, that I want my conversation in digital realm to be as private as possible. I don't want anyone to spy on me, big brother scenario, blah, blah.

But we also have to take into account, especially within the Trust over IP, the findings of the best practices that we need to the other task forces, especially the Trust Spanning Protocol. And I think, Matthew, you mentioned the secure privacy, authenticity and confidentiality. So this triangle and this theorem that you can only achieve two of them at the highest level at the same time. So, right, so you cannot achieve authenticity, confidentiality and privacy at the highest at the same time.

So if you look at the work of the Trust Spanning Protocol Task Force, we can clearly see that the prioritization is authenticity first, confidentiality second and the privacy is on the third. Doesn't mean that it's not important, right? So but with privacy there are certain different kind of infrastructure that you may use because at the end, it's always about correlation on the metadata. And this can become very complex, very fast. So the law of diminishing returns will also kick in very, very fast. You have to make the right balance in order to achieve the desire to privacy levels without raising the costs really heavily.

But as you said, I don't think that there is enough discussion and understanding of how these things are related out there in the wild. And I think there is a great communication challenge that needs to be done there in order to raise the awareness and understanding.

Hakan Yildiz (46:48)
Also, I think there is a differentiation that we have to make when we're talking about authenticity, integrity, confidentiality, non-reputation, privacy, etc. On one level, it's the communication. A communication, the message that we are sharing with each other right now can be end-to-end encrypted. It has certain characteristics like integrity of the message that has been sent, authenticity from who it is coming from, confidentiality that is only for the eyes of the one party and non-reputation for not being able to think that it has been sent to the person. But when people are talking about the privacy, I think the focus is also, at least in the decentralized identities, the focus is also on the credential itself, like what kind of privacy preserving features a credential brings on the table. Right. And the good thing I think about the whole credential exchange protocol comparison is that most of these protocols are actually credential agnostic. So you can use Anoncred with OpenID4VC, you can use it also with issue credential, you can use SD-JWT, you can use whichever credential format that you want to use.

I'm not very sure with the ACDC and ISO side of the things. ISO probably a bit more restrictive in mDL. But if we're talking about the privacy features of a protocol, exchange protocol itself, I think the most important factor that we have to weigh in is what kind of data is being required to have this exchange happening? do they want from you more than that you need to deliver to have that transaction?

Yeah. And in OpenID4VCI case, for example, it can go really, really quite off the roof. So like you can go on up to wallet identifiers and verifier identifiers that you know from which wallet, which credential is coming to which verifier it is going which might be a required thing on a regulatory use case like electronic identification. Whereas at least from my understanding the Aries protocols have been inherently more privacy focused more than enabling these additional identifiers to be had in the protocol.

Vladimir Simjanoski (49:29)
Privacy is a very interesting thing, right? It's very interesting to discuss because it might mean multiple things, right? So if you look at the interactions that we have with different counterparts, and especially in the regulated business, especially let's say the banking industry, whatnot, there is no privacy there between me and the bank, right? So they will ask for the data they don't need because they're regulated. So this is currently handled so they cannot I cannot send go to the bank and just give them a you know a zero knowledge proof that this is this is it and they will say oh that's not a problem you can run with it we don't need to know. So I think we have to distinguish this you know when we are trying to replicate the already existing rules of the physical world into the digital realm we have to take into account this but also then on top of that, have this other discussion that you also mentioned, because things can very easily go on the other side very, very wrongly. If I have to share all the metadata that I have, meaning the wallet identifier, crash letter, pretty much everything, then a correlation would be a very simple thing to do, right?

So we have to make sure that the correlation is there is a balance there. There has to be sufficient effort that one needs to do in order to do the correlation. If it's not, if let's say two banks, the three banks can just intermingle and just correlate everything very easily, we haven't solved quite a lot of things, even though we don't have the back to home in the first place. So we have to make sure that this correlation doesn't exist at the very far side, or it's hard to do, right?

Hakan Yildiz (51:21)
But on the other hand, like a bit more maybe philosophical question here, who decides which kind of data should be shared for which purpose? I mean, yes, the regulatory side, but on the other hand, for example, all this KYC is related to, for example, all this terrorist financing, or I don't know, drug money and money laundering, things like that. Which is corect, but like that is made for like a very small amount of transactions that are happening in the global scale of the things. We are willing to participate in it to ensure that we are covered for the edge cases, but that *Boogeyman* of edge cases can drive us also into a very surveillance method of authentication and verification using credentials.

Vladimir Simjanoski (52:19)
Yes. I think there is a clear danger there, right? So it's especially since you're moving towards digital realm more and more. And the more digitized the process in the data are, of course, the correlation will be easier to be done than in the physical world. So yeah, from the philosophical standpoint, you can argue that the number of devious transactions potentially, they can definitely be considered edge cases in comparison to the normal standard transactions.

And you can also argue that the bad actors they will definitely, I mean their core skill is how to you know circumvent procedures and things like that so for sure they will find a way how to circumvent this.

Mathieu (53:10)
Which is why I still think multi-protocol or having multiple profiles be able to be used by a wallet holder, whether they're interacting with issuers or verifiers is interesting. We often overlook, we talked about regulatory, but there's regulatory, there's non-regulatory I think I agree the bank for KYC and AML purposes needs to collect and store your data and they have processes around that. So you're not going to do a zero knowledge proof type of thing with them. Versus if I'm just looking to do an age proof online to, I don't know, access some websites, for example, I don't want to give the same amount of data, perhaps value my privacy more in that to use case, right? And so it takes us back to that, to start the conversation as well, like why we're talking about different purposes for these different exchange protocols, where you have some for high integrity personal identities or access management use cases, where perhaps the relying party is regulated and has regulatory requirements to collect data or just part of their policy versus just a widespread use of verifiable high integrity data on the internet, where perhaps you need mechanisms to have stronger privacy preserving types of interactions there.

And then there's also like how confidential or how private do you want your data to be anyways, right? It's like a, is it PII data or is it data about like some behaviors I have? Or if I'm an organization, go back to organizations, maybe it's just public data I have as credentials. It's verifiable, but I'm okay sharing it with, with whoever. Or maybe it's my, I don't know, more private information as an organization that I don't, so just the types of credentials, like we talked about too. I guess, play into what use case and then what type of exchange protocol we want to employ.

Vladimir Simjanoski (55:16)
Yeah, definitely. I think that we have to be cognizant of everything that you just mentioned. And you could expect that the more processes we have online, and hopefully when there are more verifiers online, the more these questions that Hakan asks will be questioned, will be asked.

Like, who gets to decide what kind of data do I need to pass this check? And if you say that there is a centralized entity that does that, you put a lot of control into the overall trust ecosystem, because you say in order to do this check, you have to, these are the *musts*. In order to do that check, these are the *musts*. So there has to be one central or hierarchical, whatever. someone who is setting up and then propagating these rules.

On the other hand, you have the Wild West, right? So everyone gets to say what do they want, and then it's up to the holder to make an educated decision based on the request. They don't have to accept, but they have to be educated well enough in order to understand, okay, so I'm going to the, I don't know, to my gym. And my gym is actually asking for some stuff that is absolutely not required for this. So you can say, I don't want to share this data with you.

But yeah, it's not a trivial thing to solve, right? So it gets complicated. You don't want to place the burden or too much burden on the side of the holder especially when you widely deployed everything. Because most of the people, they are not aware of these terms like authenticity, privacy, and confidentiality. It doesn't mean anything to them, right? So they just want to get the deal done as fast as possible and just move on with their life.

Hakan Yildiz (57:19)
And on the other hand, I think if we're going for like privacy as an option instead of like privacy by design, we're opening the route for again, the whole surveillance capitalism because in the end of the day, if I don't agree to share my data, I won't get the access to the service that I want to.

Vladimir Simjanoski (57:42)
Yes, and you're stuck. Yes, I think this was a positive, it's a positive movement, a positive step in the right direction that we are starting to think about privacy right from the get-go, right? When we are architecting the system. So privacy by design, definitely a thing, I think. This would stay. For sure, data minimization, I think this is definitely a best practice. You don't, the less data you share, the less problems you will have. So it's just a common thing, right?

So I think this will stay. It's harder to make the balance where the boundaries are. You always want to, in order for a thriving ecosystem, you really have to give a little bit of autonomy on the side of the players, so they get to decide and move with the market speed, not with the speed of the governance body, whoever it is, because this will usually be slower.

Mathieu (58:39)
Which is why I think it's probably important to keep these protocols as thin as possible, that you're able to do a lot of different things with it, but it really comes down to the implementations which are driven by the use cases, which are driven by the regulations or different policies or just more of the business requirements versus enforcing something within the protocol. Cause even when we talk about something like privacy, when you were talking about the, the deep fake earlier, so much of our, but well, as this video is going to go out to all of our biometric data will be available to take and someone will be able to use it and construct a deep fake with it. All of our voices out there on different presentations and podcasts. It's out there anyways.

So ever the more reason to say, let's maybe keep these things as thin as possible and make sure that we're not creating some unwanted like second or third factor situations that come out of it when like what problem are we really trying to solve?

Vladimir Simjanoski (59:44)
Yeah, we are definitely, I think this is the question, what are the problems that we are trying to solve? And in this community, I think the problems or the prioritization of the problems, they change frequently, right? Especially with the boom of the AI technology, deep fakes and whatnot. Today, you might not even be able to recognize whether something is coming, a song sung by you, whether you are on the other side or not, you can quickly reach to that point. So it can be very, very messy and very, very ugly, very quick.

Hakan Yildiz (01:00:15)
Yeah, absolutely. Well maybe a bit of off topic for the credential exchange per se, but nevertheless credentials and identity. So about these deep fake videos, we were also at extension with a colleague thinking about how to prevent this or like how can we use actual decentralized digital identities ourselves or identity as a part of fraud prevention to make sure that the origins of a video or a voice recording is actually authentic and not has been faked.

We were thinking about, yeah, what about like a user being able to sign with their device the video that is being created and made actually an analysis on what the internet video content is made of. And I think I'm its numbers right but like somewhere between 80 to 90 percent of all videos are coming from Android or Apple. Like two devices generating most of the internet video content in the world. And yet they still don't sign these videos for example. This is not a feature that is to my knowledge not there yet and Sony came with that with their one of their photographic machines, now they're capable of signing any video or picture that has been taken by a Sony camera to make sure that the picture that has been taken is authentic and it has not been tampered with and I thought this is perfect like something like this we really need in the future for any content that is coming into social media news outlets wherever?

Vladimir Simjanoski (01:01:58)
To me, we are lacking severely behind this, I think. Because we are, especially if you're working in the personal identity space, we have all these regulations we have to take into account while this giant dark wave is just looming over our heads and it's crashing the internet. And I think that the number of stories like this will just go on and on and then this is an organizational incident, but who knows how many incidents are there on the personal level that are not published out there. So to me, authenticity is definitely number one problem that we have to solve.

Mathieu (01:02:42)
Yeah, there's a big content authenticity problem arising. And luckily there's work happening in that space. You just mentioned one example of signing I think just having more signatures available solves a lot of problems to begin with, which is a core to the whole verifiable credential exchange stuff as well.

So for folks listening to this, we're rebooting this working group within the Trust Over IP, so the Credential Exchange Protocol Task Force. By the time this podcast is out, and you're listening to it, we've already rebooted it, but we will ask and we'll put it in the show notes if anyone is interested in joining and contributing there's also other protocols, like we talked about the VC APIs being another method of exchanging credentials we want to make sure that we have more coverage and we're really ultimately helping decision makers and implementers of this stuff have an easier time getting up to speed with what's available and spend less time on reading technical documentation and research before having a little bit more direction.

So we think it's very important work for all different types of credential exchange protocols. So we're rebooting this working group. It'll be going throughout 2024. So if you're interested in joining in the show notes, we'll have a link and instructions on how to do that, we would love to see you there. Before we wrap this up today, Hakan and Vlad, any final parting words that you would like to leave with our listeners?

Hakan Yildiz (01:04:21)
Yeah, so I mean, I'm happy that we started this working group. And I think we still have a way to go because the decision as this conversation shows and the result of our work so far shows that it is not as simple as choosing A over B because there's a clear distinction to go there.

So I think we still need to refine where we are heading to make business owners to make a concise decision on which credential exchange format they want to use. It's still quite technical, but we're getting there. And on the other hand, maybe one more important topic here is I think the interoperability. I think overall what we're doing is very interesting and these different credential exchange protocols, but there is no preference for me. Like I don't prefer OpenID over Aries issue credential protocol or something like that. The most important thing is that the whole SSI as a concept, as a identity and access management paradigm fosters and that we can achieve only through seeing these protocols being implemented all across the world, but having interoperability in some way like either through the holder perspective or from verify perspective that is I think still yet to come

Vladimir Simjanoski (01:05:50)
Yeah, from my side, definitely an exciting time to participate in this, because I believe that now, especially with the European large-scale pilots in progress and the whole EIDAS 2.0 thing being one of the most prominent deployments, hopefully out there for SSI, I hope that things will catch up with the rest of the world. And I can see that things are heating up in some places. And this will be very interesting, but also at the same time very challenging because each one of us know how much time we had to spend just to learn the jargon, let alone understand the fundamentals behind. So I think that we as community will be put to a test in order how to constantly improve the communication, the message that we have. So we always have to work on this in order to, to reduce the barrier to entry because currently it's too big.

Mathieu (01:06:55)
Yeah, and I'm hoping conversations like these will be helpful and we continue to progress along those lines. And guys, thank you so much for doing this. I would love to do this again at some point throughout the year. I think they continue to be important conversations and I'm hoping they're valuable for our listeners as well. So thanks again.