Mathieu (00:01.15)
So I guess I would like to start the conversation with just maybe some learnings that you've had over the past years.

Daniel Hardman (00:07.20)
It's interesting because I've been through several different kind of aspects of learning in my SSI adventure. I've learned a lot of things about technicalities, learned some things about cryptography that I didn't even imagine before, and I'm still only a journeyman about cryptographic stuff, but I know a lot more about it than I used to. And I've learned some things about cybersecurity and technical topics like that. But I think the more interesting part of the learning journey for me has been more related to the way that all this technology has to interface to humans.

Daniel Hardman (01:09.12)
And that's partly related to governance maybe, but it's not just about governance. And as a matter of fact, in some ways I don't really love the term governance because it's a top-down word. It says that there exists some function or entity that is taking actions to govern and I think one of the deep truths about human beings is that certainly we can be governed, but that's not always the best way to think about what's happening And in many cases trying to govern people's behavior in an artificial way changes the dynamics of how people interact in ways that you don't want or don't intend.

Daniel Hardman (02:02.14)
So anyway, I guess I'd just say that the whole identity space is fascinating. The technology is interesting. But I think the part of it that has really kind of captivated my attention is more how the technology changes human behaviors or how human behaviors need to change the technology.

Mathieu (02:27.16)
We often talk about the technology and then we talk about the governance or human trust side of things. So if you're saying that maybe governance isn't the right framing for it, you obviously need something outside of the technology in parallel to make sure things are working, whether it's to make sure human behaviors are able to be supported by the tech or that our behaviors are changed, like you said, but how would you reframe the whole concept of governance or human trust then?

Daniel Hardman (02:55.23)
I guess I'd say another way to frame it might be to use the word empower or empowerment. There are certainly constraints or limitations on behavior that need to be part of our interactions, but framing the way that we achieve trust as a governance problem, although it's true and in many ways it's deeply true.

But I think there's an even deeper truth than that. And I think empowerment kind of gets at that a little bit. Part of the reason why we're not very self-sovereign today is because we as human

beings are not effectively empowered. And that's a statement about technology, but it's also a statement about governance. And it's also a statement about our own knowledge or lack thereof. And about circumstances in general. So really self sovereignty, you could say that an important essence of self sovereignty relates to the notion that this sovereign has the ability to act and act with effectiveness and confidence and so forth. And so if we're not making people confident, then maybe we're not achieving, confident and empowered, maybe we're not achieving self sovereignty no matter what other check boxes we're ticking off.

Mathieu (04:39.20)
And would that apply just as well to like a personal identity use case, just like an organizational use case as well. And I know you've been spending a lot of time in recent years on the whole concept of organizational identity, but with that same empowerment piece be needed there.

Daniel Hardman (05:03.20)
Yes, I think that Identity, you could compartmentalize it into personal identity or individual identity on one side and organizational identity on the other. But I actually think that that subdivision of ideas invites us to get comfortable with the mental model that's flawed.

I don't think it's wrong to talk about organizational identity or personal identity. But the fact is that organizational identity is actually composed of or highly intertangled with, at a minimum, individual identity. They're not really totally discrete things. If you think about the identity of Microsoft Corporation, for example, a big company.

How separable is the identity of Microsoft Corporation as an organization from the identity of its people? Well, it is separable to some extent. The legal system guarantees that's actually what a corporation means is that from a legal standpoint, it has responsibilities and duties and rights and whatever other things that legal entities have separate from its constituent employees. But if I said, you know what, all of the people who currently work for Microsoft are going to drop dead in 10 seconds, would Microsoft, the organization, still mean the same thing 11 seconds later? I don't think so.

Daniel Hardman (06:57.04)
Let me give you a less extreme example. What if every person who worked for Microsoft suddenly lost all recollection? They retain all their technical skills, but they lost all recollection of any of their colleagues.

Would Microsoft Corporation still mean the same thing after that event? No, because a big part of what it means to be Microsoft Corporation is to have people who have responsibilities to each other, to the world, people who know who the other people in the organization are, who have expectations of those other people, and so forth. And so that's an individual identity problem, but it's very much tangled up in organizational identity.

Mathieu (07:52.15)
And I guess if aliens landed here and they walked into a Microsoft headquarter, they wouldn't know that there's this Microsoft legal entity type of thing. They would just see a bunch of people doing a bunch of things. And so it's kind of… Doesn't exist in the physical world. It's a human concept. And so that is interesting to think about that a little bit differently. So from, from that perspective, how, how do you look at empowerment within an organization to empower the individuals to have more abilities or efficiencies or do stuff that they're not able to do today through identifiers and claims, credentials, stuff like that. One of the areas that we've been spending a lot of time is just thinking from an ecosystem perspective on how do we enable roots of trusts to be built? So where does it start then within that?

We could call it a legal entity or company, or we could just start using a different framing for it. But how does that root of trust start within an organization?

Daniel Hardman (08:58.18)
what you said at the end right before, how do or how does, is relevant to your question. You were saying we could call it a legal entity or we could call it something else. I want to call it something else because I think that legal entity prejudices our thinking a little bit.

Imagine something that's not a legal entity but is nonetheless an organization. So let's take a string quartet.

Okay, you've got, you are a great musician, you play the cello and you've got three friends and the four of you get together and you form a string quartet. Now that is an organization, but it's absolutely not a legal entity. And I like to talk about organizations like that because I think it gets at some primitive things that are true that we lose sight of when we only frame organizations as something that the legal system gives us.

Organizations, you asked how do you start a root of trust? Well, you know, humans are social creatures and organizations are not created in a vacuum. And when we think about legal entities, we say, well, the root of trust is the legal system in a sense. You know, you go out and you fill out some paperwork and submit it to the right legal office and they stamp it and take your money and register you in some giant registry in the sky, and now your organization exists, and that's the root of trust.

Daniel Hardman (10:39.15)
But that's actually not really true. The deep root of trust in all organizations is actually human relationships. The reason that the legal system feels like a root of trust to us is because we have trust in one another and a legal system.

And it's fine as a simplification to say that the root of trust in our modern society is the legal system for legal entities, but the deeper truth here remains, and it will always be that way. So these four friends that form a string quartet, the root of trust there is some shared context that makes them friends.

And you use that trust to build a scaffolding of other things on top of. And building is something that unfolds over time. And so the time dimension of trust is relevant as well. We tend to talk about roots of trust as if they were instantaneous or like static, but in fact, your friendship evolves over time. Your ability to play the cello evolves over time. Your shared experiences evolve over time. You go to three really stressful concerts and knock it out of the park and have a wonderful experience. And you drop your notes in the middle of one of the performances and your buddy who's playing the violin figures out a clever way to lift it up with his toe and put it back on your seat and you trust him more. Things happen and your trust grows. And that's really organic trust, I would say. It's the basis of all the other ones. And sometimes I think in the SSI community, we lose sight of that.

Daniel Hardman (12:43.19)
We think that we can just designate a route of trust like the what is it, ICAO is the international consortium that sets standards for airline tickets or whatever. And we say, well, that's the root of trust. And it is a good simplification to say that. But the deeper truth is other than that. It's actually the willingness of society to trust ICAO based on many factors like legal things, treaties, shared history, shared incentives, what we hear on the news and don't hear on the news about plane crashes. There's all kinds of things that are really the basis of trust.

Mathieu (13:34.20)
So within a group of people or an organization, you would still need these types of mechanisms available, right? And I would imagine, and it would be interesting to hear some of your learnings from the organization side of things, but it seems like you need a lot more. You started introducing things like roles, you start introducing things like delegation, the environment gets a little bit more complex than if we're just imagining a mental model of yourself or myself getting a driver's license or a passport credential type of thing. Where do the complexities come within the organizational context?

Daniel Hardman (14:12.05)
A simple way to say it might be that the number of relationships that we have to manage and the rules or constraints or expectations around those relationships become more complex and that is the source of a lot of the complexity in organizational identity. You know, it's really interesting. I haven't heard people talk about this very much.

But credentials, which we talk about all the time, have a very strong affinity for a particular facet of a person's identity. So let's suppose that you are an employee of Acme Corporation. And on the day that you arrive at Acme Corporation, you go to their headquarters, and you have to bring in your passport and whatever else to prove who you are.

After you go through a bunch of hoops and fill out some paperwork and this gets stamped and that gets delivered, they hand you a badge, an employee badge. And that badge is going to let you into the building and into your own private workspace and whatnot. Well, that badge is

associated with a newly minted facet of your identity your identity facet that concerns itself with being an employee of Acme Corporation.

Now, you could think of that badge as a credential. And you could say that it's not an accident that if you cease to be an employee of Acme Corporation, you probably have to turn in the credential.

Daniel Hardman (16:03.16)
So a driver's license is associated with a facet of your identity. Most crisply, it's associated with you as a driver on public roads. It turns out that that particular credential has been used for so many other things that it's a little bit fuzzier bound to a facet of your identity than many. But I think that roles are a good way to kind of encapsulate many different considerations. And what an organization requires us to do is think carefully about our roles.

If we're, let's say, acting as a parent and a spouse in a nuclear family, we may not think constantly about whether we're preparing the dinner in our role as a spouse or our role as parent, or maybe just in our role as an individual, we have those different facets of our identity, but the need to delineate them clearly may be a little bit lower. But now let's say that we're the CEO of a company and we're going to go to the bank and sign on the dotted line to take out a loan.

When we do that, we have to know which facet of our identity we're acting in. Are we acting as the CEO of the company when we sign that paperwork, or are we acting as a private individual? And the legal system actually demands that precision from us. Our creditors want it, and we ourselves want it, too. If we're signing on behalf of the company, we don't want to be held permanent or personally responsible for the company's loan and vice versa. So I would say that the complexity emerges as a natural consequence of the fact that our relationships proliferate and the facets of our identity proliferate and the stakes for being crisp about the distinctions between the facets of our identity go up.

Mathieu (18:31.10)
is being able to interoperate or at least have portability between organizations. Cause you would assume within an organization, and this would be interesting to get your thoughts on like, can there be a foundation of facets or roles or rules that apply regardless of the type of organization so that if you're having interactions with people that maybe are part of one organization or one ecosystem and they want to work with their supplier on the other side, could they talk the same language? Like, how do you start thinking about semantics in this? Is that something that's at all important to discuss?

Daniel Hardman (19:21.06)
Yeah, it is important. So let's go back to you being an employee at Acme. If your job at Acme is to be, let's say, a purchasing manager, then there will be people outside of Acme who need to know that you have that responsibility because you will be negotiating contracts with them, maybe you'll be signing bills of lading and other kinds of things for your company. But on the

other hand, if you have a new aspect of your identity, you join the company's ping pong team and you're going to a ping pong tournament, does everybody in the supply chain need to know that there's this other aspect of your identity? that you are captain of the ping pong team. No, they don't need to know that. So understanding the audience for a particular role is quite important.

Mathieu (20:24.21)
Should we be trying to codify all of this? Does it add value or does it become important to be able to codify this or is it something that is an impossibility to do?

Daniel Hardman (20:34.18)
Yes, I think we should be trying to codify it, but I don't think that the way we should do it should be... When I say we, it shouldn't be that humans have to think about this. We should build software that helps people codify it. So, let's just take my example of the supply chain thing. If you have a bunch of supply chain tools, when you act in your capacity as a supply chain manager, a purchasing manager, the tools should expect from you manifestations of an identity that are related to supply chain problems.

And if you accidentally gave them an identifier for yourself that didn't have anything to do with supply chain problems, the tools should say, this isn't the right kind of you. You're showing up as captain of the ping pong team to sign off on this paperwork. I don't want that. And we tended to think in SSI land that the way that we express what you want and so forth is by talking about credential schemas, credential manifests and all that stuff, that's fine, but not everything is credential oriented.

Daniel Hardman (22:04.06)
And so the solution, the problem has to be thought of as broader than credentials and the solution's broader than credentials too. And so I now want to kind of say something a little controversial. Decentralized identifiers and all of the variations thereof, I work a lot on, AIDs, which are the version of identifiers that it's kind of a specialized form of DID that is used in KERI land. Decentralized identifiers of any kind have these wonderful characteristics that we like to talk about that you can prove cryptographic control and all these things. And they are the basis for using credentials and the basis for the very facets of your identity management that I've been talking about. But if what we've done is proliferated a bunch of identifiers that humans can't recognize and understand when they look at them, I don't think we've really helped a human very much. So the quick answer that I think the community would give is, oh, this is why we've got wallets.

No, I don't think so. I'm not satisfied with that response because if you look at any wallet today and you say, okay, great, give me an inventory of all the identifiers and help and tell me what they mean. I think you'll get a very, very unimpressive experience. What wallets do today is they'll give you an inventory of all the credentials that you have. And that may imply something about identifiers, but it is not the same thing as managing all your identifiers.

So if I simply want, let me go back to the thing of you're going to sign a loan. When I sign a loan, forget the fact that in the end there's going to be some kind of cryptographic evidence of the signing, if it's digital. Just concentrate on the action of signing and the question that I'm about to ask, how do you express the fact that you want to sign in the capacity of CEO of the company?

Daniel Hardman (24:32.13)
I'm not talking about how you prove you're the CEO of the company with credentials later. I'm just saying, if software wants to ask you, or if a human wants to ask you, in what facet of your identity are you acting as you sit down to sign this paperwork? How do you select an answer as a human?

Answer, no technology that I know of today gives you a good answer to that question. The closest you can get is you can go onto the .SSH folder on your Linux box and enumerate all the SSH keys you have and hopefully you named them something intelligent, you can select one. Or similarly, you can open up a password manager and you can scroll through all 500 items that you have in your password manager and you can say, well, I'm going to pick the login that goes with this website because the password manager stored the URL of the website, and it's going to help me match the website I'm currently on to something in there. That's a beginning of sort of answering this question, but it's really not an ending. It's a very poor answer, in my opinion, because my relationship to, let's say, Acme Corporation is more than my ability to log into Acme Corporation's website. But my password manager doesn't know that. It doesn't know anything about aspects of my identity, except as they relate to logging into companies' websites.

Daniel Hardman (26:02.08)
So I believe an unsolved user experience problem in SSI today, one that I'm quite passionate about, is simply helping people attribute meaning to the opaque things they have to manage. Whether it be keys or whether it be DIDs. Here I have a key ring. And I can tell these two keys apart because they look visually different. One's the key to a building that I have some duties to, and one is the key to my apartment. And as a human, I can actually look at those things, tell them apart, and select the one that I want before I use it.

There is no equivalent functionality in SSI land for identifiers. If I have 100 opaque identifiers that represent 100 facets of my identity, and I think that's a low estimate, most humans that are actively participating in the internet world today and that are adults probably have 500 aspects of their identity or more.

But how do I tell those apart? I'm just looking at identifiers. Here's my long list of 500. How do I select the one that I want? Answer? There ain't any answer. So I have been working on this concept. I call it aliases, where you name an identifier. I want the identifier for me acting as the cellist in my string quartet. As a human, I should be able to ask a question like that and get back the one item out of my list of 500 that's relevant.

Daniel Hardman (28:05.15)
And I can, as a human, just provide friendly names. So I could decide, I will associate for every item in my list of 500 opaque identifiers, I will associate a friendly alias that I made up. I could call one of my items: string quartet cellist. The problem is that humans, are not very good at being methodical. And we can't anticipate all the different contexts where the names of identifiers might be confusing to us because maybe I was a cellist in my high school orchestra and now I'm a cellist in my string quartet. And oh, that's right. I was a cellist in my string quartet in high school too, but that's not the string quartet I'm talking about now. We forget that there's all these other pieces of data.

So I know this is taking a long time, but what I'm working my way around to is, you said, should we try to solve this problem of helping users? And I think the answer is yes. And this is one very concrete example of a problem I think is being completely neglected that we should solve. Humans shouldn't have to solve it. We should solve it. And humans shouldn't have to think about it. When they create a new identifier, the software should know what context they created it in because it already probably had that context. As soon as you set up a chat group on WhatsApp for your new string quartet, probably the software would know that if you've used the software to set up the chat group. And therefore, when it creates an AID for you or a DID for you there, it should know that context. And it should name your identifier as something that goes with that context appropriately. If it had a method for doing that, it would even be able to tell you, hey, you're using the wrong identifier in this context.

Mathieu (30:11.19)
I guess you would need some sort of like templates or at least standardization around these templates and the types of aliases that you could assign to identifiers based on domain specific context, right? Like you could think about assigning aliases or, um, like in, in the world of domain names, we've made it a bit easier because you're able to put a human readable domain name. It's for a specific namespace. It's able to map to an IP address, but in the context of what we're talking about here, many different contexts, many different namespaces, is it possible to achieve alignment on this? And would there need to be some template mechanism that people, at least operating in similar enough environments, would be able to reuse these so that there could be some sort of understanding between two different groupings?

Daniel Hardman (31:10.01)
Yes. So I think that the template that we need and the convention that would help us all is really defined by three important questions. The questions could be called the who question, the role question and the context question. If you answer these three questions, I believe that 99% of the time, you will generate enough information to easily help a human make good decisions. So this might be the equivalent of me saying that with my physical keys, if I can have the characteristic of the color of the key, the characteristic of the shape of the key, and the characteristic of the style. These three things will be enough for me to always pick the right key.

So with identifiers, the who question is, which identity are you trying to manage? Is it your own identity or the identity of your group? If you are, let's say you're back to being an ACME

employee, when you ask for a bid, are you trying to do that in your capacity as a representative of the company or are you trying to do something as a private individual? It's the who question. And then the second question, the context would be, or I'm sorry, the second question is the role. So remember Acme as a corporation is a general context, but your capacity as a purchasing manager and your role as a member of the ping pong team are pretty different. And that's what that second question about role is getting at.

Daniel Hardman (33:22.02)
And then the third question context really gets at whether you intend for this to have a public audience, a more limited audience or a very private audience. So you can imagine a person, instead of you and me, let's suppose that the CEO of Acme Corporation is Cecilia. And she has all these different facets of her identity. So let's suppose that she has an AID or a DID, and the name of it is Cecilia as President or CEO of Acme.

If she were looking through her list of identifiers and she was asked the question, do you intend to sign this paperwork as Cecilia a person or as the representative of your company, and she saw that item in the list, do you think she could naturally make good decisions? Sure. That's a, that's an intuitive thing, Cecilia is going to say, oh, I need to pick the AID that is Cecilia as CEO at Acme for my signing.

And when she goes to, you know, book a performance venue for the fall concert for her string quartet, and she's looking through the list, and she sees Cecilia as a cellist at, you know, My Four Strings, she knows exactly that that is the right AID to use in that conext.

Daniel Hardman (35:16.12)
It's because she's answering these three questions. If Cecilia wants to post on social media on behalf of the company, maybe the first part of the alias isn't Cecilia at all. Now she's acting, projecting the company's identity, not her own as Cecilia. So this is Cecilia saying, in her identifier list, okay, I want the identifier of ACME Corporation on social media. So answering these three questions, the who question, the role question, and the audience or context question, I think would always lead to making wise choices. And that's the template I think you're asking.

Mathieu (36:03.09)
When we think about like trusting an identifier, whether it's an AID or a DID, like the foundational concept of an identifier like that is they begin as trustless and they get built up over time with different things. But if you start adding aliases and like when a DID is being used, it's known to the other party that an alias was used. Let's say just for example, um, or even if, if identifiers are within an organizational standpoint, you would think that some scenarios require identifiers to be controlled by more than one controller and perhaps assigned at times by one group or one entity to, to another entity. And in like just a real world, world example, if, um, a new employee joins Northern Block, we assign them an email address.

And that's an identifier that they have, and they could use it to do different things. Is that similar in the concept of AIDs and organizations that, and just trying to understand the complexity of these identifiers and having multiple controllers, and perhaps you start being able to build things into the identifier itself, which gives you more trust into an identifier and there's a lot of things you could do if you trust an identifier and you maybe don't require other trust tasks like credentials to be presented and such.

So is there more complexity in how identifiers are assigned, managed, controlled, and even how trust gets built into them within the context of a grouping of people or an organization?

Daniel Hardman (37:46.14)
I think that it's actually a very good thing that identifiers and cryptographic keys are opaque. I know that a number of people have accomplished a number of cool things using DIDweb, which is not a totally opaque identifier. You can see the domain name in the identifier and so forth. But generally speaking, when an identifier is not opaque, it invites human guesses about its trustworthiness that can be manipulated. So I think that the identifiers, whether they're DIDS or SCIDS or AIDs or whatever, those kinds of identifiers that have the properties that we have talked about in SSI land as being important cryptographic agility and the ability to resolve them and the ability to do multi-sig kinds of things with them, control them in sophisticated ways. All of those things, I think, need to be at a layer that doesn't allow you to make direct human judgments based only on the identifier itself, meaning the value of the identifier.

Now, if you said, the history of the identifier, that's a totally different thing. If you know that this identifier has done the following things, you can observe its behavior patterns. That's not what I'm talking about. Of course you should do that. But I'm saying, if you just look at the string content of an identifier, at its representation, it's probably a very good thing that you not be invited to make any judgments about what its trustworthiness is, because then you know that you're starting from scratch. And it is true what you said, you are really starting from scratch with every identifier. Now, I was talking about aliases. What if your alias actually encoded in it some kind of notation about what you believe is its trustworthiness?

Daniel Hardman (40:11.06)
So for example, Cecilia with all of her AIDs and DIDs for herself. Her aliases, she can say, look, I have a high reputation as a world-class cellist, and I think it's important or whatever. But what I'm talking more about is when Cecilia receives an identifier from a remote party, she should get that identifier, and maybe she says, oh, yeah. I got this identifier and I'm going to give it the name Matthew.

But should she be allowed to give it the name Matthew if she hasn't proved yet that the controller of that identifier is in fact Matthew? Maybe her software should insist on putting a question mark at the end of her identifier until she's actually proved the identity, the human and legal identity of the party she's talking to. And then once she's proved it, it takes the question mark off without asking her because now it knows that the trust in that identifier is justified.

Daniel Hardman (41:23.09)
This is the kind of thing that I think gets at your question. I think software ought to help people do that. The classic problem that we have in all kinds of identity oriented interactions is man in the middle.

Why doesn't our software say, can I prove yet that there exists no man in the middle between this identifier that I have imputed a human identity to and the actual human that owns that identity? If you could drive it out of the system, then maybe your alias that you keep for it ought to change.

Another way you could do it is instead of using question marks, you could say I have bronze, silver, and gold level identifiers for all my contacts. And I trust this identifier at the gold level versus the silver level versus the bronze level. I don't know how to do it, but I'm saying the notion of trust and identifiers ought to be managed in a really thoughtful way. Instead of today, assuming that humans magically decide stuff or credentials magically take us from zero to full trust. Neither of those is a good assumption.

Mathieu (42:52.19)
So is your vision to keep any authentication or authorization processes outside of the confines of an identifier? Like those sit outside of them. You don't want to make any trust judgments just based on an identifier.

Daniel Hardman (43:08.00)
Yeah, I think that it's helpful to maintain a crisp distinction between the low layers of stuff where identifiers live and the higher layers of stuff where humans live. I got this insight when a few years ago, there was somebody who used DIDcomm to build a cool thing and they made a poster and invited people to scan a QR code on the poster so that they could do this thing with DIDcomm. And people scanned the thing on the poster and some interesting work got done, but a hacker came along and looked at that poster and said, hey, All I need to do is stick a QR code sticker over the top of the main QR code on the poster, and I will have a great way of stealing this relationship. I can pretend that I am the party that put up the poster, and I won't actually be that, but nobody will know. And then this hacker who worked for, not worked is the wrong word, who's associated with, I think a German hacker collective, wrote an article and said, see, DIDcomm has a man in the middle vulnerability, which is silly because there was a man in the middle vulnerability in that scenario, but it wasn't an attribute of the low-level cryptography at all.

Daniel Hardman (44:56.11)
What it was was a way of tricking people about the assumptions they made to bind a cryptographic identity to a human one. And so if you can untrain people from the assumption, the leaping to conclusions that we do so easily that binds the cryptography and the human layer together, and simply say, of course you can get to confidence, but until you have actually jumped through the hoops, you shouldn't be acting with confidence.

I think you're doing users a service. And I think anything that keeps human judgments about trust out of identifiers is good for that reason.

Mathieu (45:47.10)
It seems like the versioning of identifiers or metadata associated with identifiers is quite an important one when it comes to organizational context. If you change certain related information to your identifiers over time, you may want to keep track of that. Is that a true statement? And did you feel like that's an important business feature that maybe needs to be thought about more?

Daniel Hardman (46:14.20)
Yeah. Versioning is the where I would go with that question is You know everything that we do unfolds over time and We evolve our state over time For lots of reasons my laptop died and I bought a new laptop and I had to create new SSH keys on my new laptop And now Github has another SSH key for me, etc, etc. I mean, there's a hundred reasons why we do this but the point is that There's been, in my opinion, an overemphasis on the assumption in SSI Land that everything happens now.

And in fact, that's totally not true. Think about your Slack history for just a minute. If you had some kind of a chat feature that was secured, it was bound to a DID, and you were signing everything that you said in the chat. Okay, so now you're looking at a history. What did I say? What did Fred say or whatever? And If the only thing you can verify is your chat partner's current key state, that's almost a useless feature. You need to be able to go back and say, well, was this really Fred when he posted this on February 1st? And you need to be able to answer that question with confidence.

Daniel Hardman (47:51.14)
If you can't, then all of these great things that we think we're accomplishing with SSI actually break down a lot because the only moment in time you can ever analyze trust is in the present. But a lot of things that we have to trust are actually based on actions that occurred in the past.

So what if the signer of a credential rotates their keys? Should that invalidate every credential they ever signed? I mean, at a human level, that wouldn't be their intention, probably. They probably would say, we want to invalidate all the keys that have been signed in the last hour, maybe. Or sorry, invalidate all the keys. We want to invalidate all the credentials that were signed in the last hour. But that gets into a challenge because can they selectively go back and point to a point in time that was an hour ago and say everything from this point forward? Does there exist something in their history that lets them designate that point forward? That's the versioning you're talking about. We need to be able to point at what we're doing and say, that point. That's what I'm talking about right there.

Daniel Hardman (49:07.12)
So there are a bunches of DID methods in SSILand that do not support the version ID feature. And in my opinion, that doesn't mean that they're useless, but it means that their use for a lot of kind of hardcore SSI -oriented interactions is severely curtailed.

And you could say, well, the only thing we're ever going to evaluate is whether everything is true in the present. And you can tell relatively interesting stories. Oh, we were able to unlock a turnstile and go into a concert using this credential. And we were able to cross a national border using this credential. But in fact, my contention is when push comes to shove, analyzing everything in the present is really not going to be good enough. I think it's a toy unless you can talk about things in the past.

Mathieu (50:09.16)
Seems at least that's when it really matters, right? Like you do stuff in the moment, but whenever something matters and you need to go back and look at the result of something, it's always looking past at what happened, not necessarily in the moment. Like you're not, you're never identifying fraud in the moment type of thing. It's always like you're going, you're analyzing something and you want to see what happened in the past.

Daniel Hardman (50:32.22)
Yeah, if you told an auditor, well, yeah, you can hold me responsible for everything I'm doing right now, but if I did it a month ago, I get off the hook free because I can just say that my keys have been rotated since then and there's no way to analyze whether that was really me. That's a pretty lousy story.

Mathieu (50:51.04)
Do things like versioning or anything else you feel need to be at the core of these standards or specifications? From personal experience, I often feel when we're looking at stuff, it makes the implementation of standards or specifications difficult from an implementer's perspective because you need to create a lot on top of it that maybe will impact its ability to be interoperable or usable by others. But are there things like versioning or anything else that you think are missing from core identifier specifications?

Daniel Hardman (51:22.19)
Well, I think our specifications have done a pretty good job of this. There is a version ID attribute that you can put on a DID URL. And so it's possible to talk about the right semantics, but it's not required of all DID methods. And maybe it shouldn't be required of all DID methods, but I'm feeling like it's being undervalued in certain places. But from the spec perspective, I think it's described well.

It might be nice to have a notation that would allow us to formally talk about some of these issues. We use words and we say the thing that, you know, that point in time that happened on February 1st, but we don't have any kind of formal notation. And so every time we talk about this

kind of a thing, we have to kind of rebuild the conceptual framework in our words and conversations to get to the point where we all know about this phenomenon we're talking about.

It might be nice to actually have a notation for versions, a notation that actually lets us compare the semantics that are expressible with respect to versions, or any other thing, like maybe a convention about naming aliases, or maybe some other thing. Any of these that have a formal notation would allow us to compare and say, does this way of managing identifiers, or this way of describing points in time, or whatever. Does it have a direct equivalent in this other system? That would be helpful.

Mathieu (53:05.00)
Daniel, I know we're up on time. I want to let you go, but thank you very much for doing this again with me. I always really enjoy our conversations and it gets me thinking a bunch, which is just, I love. So thank you very much again.

Daniel Hardman (55:49.092)
Thank you, fun to talk to you.