Mathieu (00:25.12)
Yeah, so I'm excited for this conversation, Sylvia, because I feel like often we're very stuck in the technical weeds in the whole space of digital identity. And I'm excited to talk to you today because although you go into the technical weeds, you're very much involved on the business and strategy side of things and digital identity and are always thinking about new commercial models and how to make this stuff actually work practically.

Um, maybe a good point to start since you're based in the US, um, and do a lot of work around standards and implementations of mobile drivers licenses, would be interesting just for kind of some setting to just understand what the US market looks like versus perhaps the Canadian market, the European market as it comes to mDL, or if we just want to go even more broad with digital identity altogether, just understanding, kind of from your point of view, what the different landscapes look like.

Sylvia Arndt (01:28.04)
Yeah, absolutely. Well, US market is big. We all know that. It's complex. The US doesn't really have a national ID system. Obviously, there are passports, but when it comes to driver's licenses, just like in Canada, those are issued by the individual states. So we have 50 of them.

And, you know, it's what I would call a complex ID system, even in the physical world. So, you know, what has happened here is that there is a whole industry that has built around verifying reliably or as reliably as possible these different credentials issued by different states with different security features based on template databases, et cetera, et cetera. And then, of course, adding layers of other verification on top of that based on the risk profile. So it's already a complex setup. And so now we are adding digital identities to that.

So in the US, in that space, the automotive departments, the DMVs, as we often call them, together with NIST, are really rallying around the ISO mDL standard. So we see a lot of activity, and we anticipate that to continue through the next year or two. Multiple states have fully launched programs. Some states like my own California, we have pilots, so you can obtain your mDL through the state wallet and they're just testing it, but it's restricted to a certain number of users, but as far as you can tell it's active, it updates, etc.

Sylvia Arndt (03:43.2)
And then there are some jurisdictions that are still working on putting legislation in place to support the efforts. So that's where we see the most activity in the digital space. We have some government agencies like USCIS, the immigration agency, that is scrawling around the other standard, the W3C Verified Credentials standard, but that is in planning stages right now. But so we expect both versions of credentials supported by both standards to exist here as well.

But back to mobile driver's license, it's quite possible that ultimately mobile driver's license will be the most verified form of identity in the US. So all the signals point to that.

Mathieu (04:47.02)
That's an interesting last comment. Before getting into the kind of the marketplace and the consumption of mobile drivers licenses, you did touch upon NIST and the Department of Motor Vehicles kind of having to make sure the right legislation is in place. Since there are many states in the US, are different states on different roadmaps there? what is some of that type of legislation that needs to be in place to support the digital form of a driver's license?

Sylvia Arndt (05:17.02)
Well, basic things like law enforcement is able to accept a digital form of identity, or a digital form of identity, you know, can be utilized for verification purposes. Most states have, who have already passed this legislation,passed it in such a way that the digital credential is a companion to the physical card. So it's still required to carry your physical card, which makes sense, digital is emerging. But we have one state that is already paving the way for the digital credential to be accepted as a standalone. And that's the state of Georgia.

So you could, the way they are preparing this is that either form of identification of state issued mobile driver's license will be accepted. And so Georgia surprised us a little bit in how quickly they are pursuing this. I don't think it has passed yet, but it's definitely in the chain of legislation to be passed. So I think it's a start of a trend. As more usage opportunities are for digital credentials, they're going to become prevalent and people will not want to carry their physical wallets with them anymore.

Mathieu (06:56.06)
Yeah, actually, just traveling right now, I realized that I have to have my passport on me most times because actually, even if I had a mobile driver's license, I don't know how these things get accepted or will get accepted more broadly outside of a state or the US or internationally. I guess, why the ISO standard?

Obviously mobile drivers license is in the name. It's a standard that's built around the use case of drivers licenses. But you mentioned USCIS is looking more at W3C verifiable credentials and decentralized identifiers. What is the decision pattern for a DMV or perhaps non-motor vehicle entities that are kind of looking at that ISO standard for digital credentials?

Sylvia Arndt (07:51.08)
I wasn't obviously privy to the decision making at the time when AAMVA and others settled on that. But if you look at ISO being international, ISO being interoperable, ISO being supported by NIST and ISO being released, and ISO supporting a concept whereby this can be implemented from a central system of records, which all the motor vehicle departments have. It's kind of a logical conclusion that it's not a bad fit.

And so, whereas so far we've only seen implementations that support the first version of the standard for in-person transactions. The second part of the standard for web-based transactions is highly anticipated. Obviously, because everyone believes that's where the biggest value is going to be generated, being able to reliably identify yourself on the internet and for companies and government organizations to leverage those benefits.

So why USCIS is moving down the path of verifiable credential, I'm not sure. There may be someone who knows, but I'm not sure why that path. But I mean, clearly there are pros and cons for either but it seems ISO, even its early days, it seems ISO is here to stay at least for a while.

Mathieu (09:48.15)
And we're at least seeing the interest for that in the Canadian market too. And obviously there's the interest in the European market and the fact that standard has been kind of made a must by the, uh, EU's architectural reference framework as being one to support for high integrity credentials. You, mentioned AAMVA. Could you maybe provide a little bit more clarity on AAMVA for the listeners? And I think it's an interesting discussion that gets us into kind of the root of trust for this whole system, and then maybe also shedding some light on is AAMVA global and how does a root of trust within mobile driver's licenses apply globally?

Sylvia Arndt (10:29.08)
Yeah, so AAMVA is the American Association of Motor Vehicle Administrators. So it is the group, the industry group that represents the state motor vehicle departments like the California DMV. Not all states participate in this organization to the same level.

But the majority of states do and AAMVA already has, or for several years, many years has been running a service that enables basic identity verification based on a card, a driver's license card number. So it verifies that this is an active credential for the participating states.

So AAMVA is obviously in these new digital efforts, providing guidance to the state DMVs, providing recommendations. So on top of the ISO standard, AAMVA has its own set of recommendations. Some of them, well, recommendations and standards, because some of them are mandatory, some of them are optional.

Sylvia Arndt (11:44.06)
Just designed to enhance the system of mobile IDs, the privacy and the transparency to the users and to the stakeholders. So AAMVA has been quite heavily involved with that and it is the organization that a lot of the state DMVs look to for direction in these efforts.

And they have a large background in facilitating the verification of physical identities. And they're also in this new digital world, they are setting up what is called the Digital Trust Service. The Digital Trust Service is one of the components of the trust framework and essentially they will be providing the keys, the public keys that are necessary to read an mDL. The service has just launched and I don't think there are any participants yet, so it's also emerging, but that will be one of the enablers for transversal verifications, meaning from, you know, across verifications across states. And then, you know, in behalf, TALIS also has deployment in Australia, for example. So similarly there, you have organizations that are very actively involved with ISO.

very actively involved with international interoperability sessions. It's really designed to be a global standard and, you know, with the efforts that we see in various regions in the world and the participants, right? It is not just the standard organizations. You have a lot of state governments heavily involved and you have a lot of the big tech companies heavily involved in these interoperability sessions.

Sylvia Arndt (14:05.09)
It's a good group of stakeholders that are moving the standard along and they have certainly helped to mature it and will continue to do so.

Mathieu (14:18.09)
Is AAMVA just a root of trust for the North American market, Canada, U.S. or how does it work outside of the U.S.?

Sylvia Arndt (14:30.05)
That's a good question. I believe AAMVA its members are spread across North America. So how this is going to be worked internationally I am not sure. I'm not sure it's been determined.

Mathieu (14:50.10)
So when you're talking to governments who are, I guess, Department of Motor Vehicles, who want to become issuers of mobile drivers licenses, what is their value proposition for doing this on behalf of citizens? It would be interesting to understand kind of what the motivation is from them to get engaged in this and then maybe if they have any broader future visions of growth that make that initial investment kind of worth it.

Sylvia Arndt (15:18.20)
Yeah, this is a hot topic. And in fact, we just ran a customer survey last year where we where we reinvestigated, you know, what are what the main drivers are now that we are we've started this journey. Somehave, you know, already ventured quite far down the road in a digital ID journey. So governments, have probably a handful of goals that drive them. One is to improve the quality of service to their citizens. Pandemic has shown us that we need to be more mobile, we need to be able to access government services, ideally out of hours on the internet.

And so, the mDL, the ability to reliably identify yourself when you request or apply for government services in any form or shape is key to making that happen. So that's one of the key drivers. The other equally, if not more important driver is the fight against fraud. The fight against fraud for government benefits but also anyone else who relies on the quality of a verification.

And so we, you know, we, all of us in this industry look at these increasing fraud patterns and trends. And so this digital identity and state issued digital identity, will be a major factor in combating fraud. It's not gonna be a single solution. Everyone is aware we still need to layer protective mechanisms based on the risk profile, but the ability to identify someone and know that this credential, this person is showing was issued by the appropriate issuing authority.

Sylvia Arndt (17:43.07)
And to know this because you can decrypt the cryptographic signature and the ability to know that this credential has not been cloned and it has not been altered, it's huge. And when you combine that with facial recognition on the internet, then you have so much more knowledge than you do today, when you have people in a very cumbersome way scan their credentials and upload them. Even if there's a facial match conducted against an image on an ID, it's not the same match, it's not the same quality of an image that you match against. So fraud, huge.

The other bit is the actual process of identity verification. Not only is it more reliable with much higher trust levels, it's also much easier, a lot less friction. B2B is going to really, really like this. When you as a bank or as a retailer with a high value transaction, you can have a simple process over a few seconds, you know, give you higher assurance levels than a two minute process, then you know, your risk of abandonment, cart abandonment or transaction abandonment is going to be a lot lower.

And then also when you look at maybe as a last point, when you look at the maintenance of ID systems. With traditional systems you rely on people providing you updated information or you have updates for law enforcement. To roll that out and to have that reflected in the credential is a laborious process. With digital credentials you're still going to rely on people updating information.

Sylvia Arndt (19:58.01)
But if you can make that easier the updates are released within whatever the update cycle is, within 24 hours. If someone has lost a phone or the phone got stolen, to retract that credential is a matter of seconds. So from an updateability and maintenance point of view, that's also progress that the government sees.

Mathieu (20:30.21)
So it seems like there's some good self-serving reasons for governments to do this. And then there's all these secondary benefits downstream in the market, which we'll get to throughout this conversation.

What does the wallet strategy look like for DMVs or issuers of mobile drivers licenses? Are you seeing a trend of the issuers want to own the wallet and the wallet experience? And is that decision based on a potential business model or does it really come down to risk mitigation?

Sylvia Arndt (21:04.09)
Wallets… there's quite a few question marks around wallets right now. There are of course a lot of push for inclusion of government credentials into the OEM wallets, Apple, Google, Samsung.

Several jurisdictions have proactively moved forward with that and users embrace it. There is the other philosophy from governments that says, okay, I don't just want to deliver a credential to my citizens. I also want to utilize my application or wallet to provide service access and communication.

And so the governments behind that, you know, they are saying I'm not going to stop at the credential alone. You know, I'm going to use this as to use my state wallet as a communication platform. For push notifications, possibly for fee collections and then service access.

Sylvia Arndt (22:27.13)
What is going to win in the end and how is it going to look like? That's a big question. You know, we all don't want to have 10 wallets in our phones, for sure. On the other hand, there are also, you know, when it comes to business models, I think there's concerns over who will control what in the end. I mean, in, you know, the credential clearly is in the possession of the holder. But the demonetization of that is, the monetization of the value that's being created. That's one of the big question marks right now.

Mathieu (23:14.19)
Is there an environment of tension between governments and the OEMs? Because I know they're kind of all part of similar working groups. They're all part of ISO. A lot of them are just working together. It also, like, just from my own perspective, I actually saw a demo last week from both Google and Apple at the Internet Identity Workshop, showcased how just through the native camera on each phone, they can just scan a QR code on a browser and share credential directly from the phone itself. And like, I do this, I'm sure you do this as well. Like when I travel, I have my boarding pass on my Apple wallets, different cards and benefits things on there. Like it's just by far like the easiest or most friendly user experience than just having a third party wallet out there.

So I wonder if it just comes to like… Will you have some governments just enforce that only their wallet is able to support this for either reasons of sovereignty or want to avoid vendor lock-in or just maybe own the user experience and have other value ads on top of it?

Or eventually is it just going to become like, Hey, like if the ultimate value is in the consumption of these things, it's going to be so much easier to to have third parties or relying parties consume these credentials if it's just directly on the device itself. And then you also think like any third party wallet application kind of has no chance here.

Sylvia Arndt (24:49.14)
You know, I too am a big Apple wallet fan. It's very convenient, personally. So yes, like you, I have everything in there and it's convenient. So I see from a user point of view, from a consumer point of view, I definitely see the benefits for that. There is the concern of the use of data, not the PII itself, but still there are data privacy concerns. Some individuals do not feel as comfortable having their whole lives in their OEM digital wallet. But I think from what we see currently, I think the biggest driver is how government, what government perceives their role to

be in providing convenient access to services. And if they choose an app form, then it makes sense to have everything within one place. And we see examples of that. Multiple states are providing various services or service access through their apps.

And so there is value for the users to have a consolidated place and maybe also use that application for updates, address updates or anything like that. So I would suspect there's going to be a mix of and the strategy would ultimately drive it. And no, in answer to your question, is there tension between governments and the states? I don't really see that. I think there is an understanding that OEM wallets are popular with people and they are playing an important part in fostering adoption.

But then, you know, the question is what's going to be next? And so I think that's where governments have a play.

Mathieu (27:32.20)
Yeah, and ultimately they're the authorities for this type of credential and making service access easier for sure is a value add to citizens.

You said, do you think the ultimate value is going to happen on the consumption of these credentials, the verification side of things? I would tend to agree with you. I'm curious to hear your thoughts specifically around mobile drivers license of where things are going. Um, there's only so many of these credentials, only so many of these government authorities, they issue these credentials, but for every one credential that gets issued, they could get verified X amount of times.

And It's interesting as you're able to start to selectively disclose certain information from these types of credentials that opens up new use cases. You mentioned the whole online world opening up and being able to share proofs of different mobile drivers license attributes online is going to open up tons of opportunities. And I don't necessarily think we have precedence, whether we're talking about mDL or any type of digital credential, of actually doing a digital transformation of existing physical type of credential digital world and just seeing what the uptake is going to be.

And we're not even getting into like, what if I start combining different credentials together or different attributes from different credentials together? What is, I guess, your outlook looking at the verifier market? Where do you see the opportunities in the short term in that market to really start taking advantage of these high integrity credentials that are coming from governments?

Sylvia Arndt (29:07.20)
Well, it's like any emerging market. Right now, I think people are seeking more application, more usage cases. The one effort that I think is making a real difference here in the US is the fact that governments have been actively working with the TSA, Transport Security Administration, and it is what we call the hero use case. So, the TSA is accepting mobile driver's licenses in various airports from various states. And so here in the US, that's a huge milestone, because not only

does it bring value to travelers to go through expedited lines of processing, but also it brings trust to the credential, because the general opinion is that if this credential is good enough for TSA to accept it, then everyone else will.

And so a lot of efforts, everyone has been putting in a lot of effort into working with TSA to get that up and running. And then there are several other initiatives on the verification side. In fact, with our customer in Florida, we have actually expanded the credentials in the Florida wallet.

So it is not just a driver's license, a mobile driver's license, but also car registration and insurance. So if you need to validate one or two or three, they are all right there at your fingertips in the Florida Wallet.

And so just side note, that is sort of one of the options for governments again to make documents and services more accessible. It can also help for car rentals etc. when you can easily demonstrate both documents and you have them with you on your phone and you don't have to run back to your car because you forgot one of your documents.

Sylvia Arndt (31:57.20)
There are industries that are established online or recently established online that are currently going through a very heavy identity verification process. The banking industry obviously, you know, for anyone if you for remote account openings, loan applications, and of course banking is highly regulated and there's many tools in place, but it is a process to onboard just because of the risks involved.

Another industry that we've been working with is the notary industry. So notary publics that are operating online also a newer development popular with people because again, available outside of regular office hours, whenever it's convenient, but they still go through credential upload, credential analysis, which can take a couple of minutes. And then of course they have video sessions, then the notary has to compare the images of the person in front of the camera and the image on the credential. So, you know, this industry is eagerly looking towards the second part of the ISO standards to be released to facilitate identity verification much more smoothly, much quicker some of the states like Florida already have legislation in place to facilitate that. So there has actually been quite a few initiatives to enable digital means of verification.

Mathieu (34:08.19)
Yeah, it seems like most of what you described is just being able to, it's almost like using, there's existing identity verification processes in place. You're just using this as a new input to either reduce costs, reduce frauds that happens due to existing verification processes. Being able to lower risk through these types of verifications could allow for more seamless user experiences. You mentioned the B2B earlier. So being able to do a verification on a potential high risk transaction allows you to do it a lot more seamlessly perhaps than how it would be done today.

Are there any new type of business models that you think become available because of this or new products or new businesses other than obviously there's going to be massive innovation around the digital transformation around existing verification processes. But are there new things that are able to get unlocked here just by having the ability to verify these high integrity credentials, maybe online where you can't do it today.

Sylvia Arndt (35:16.07)
Market signals show, you know, as you said, these type of verifications are going to fit into existing verification processes or platforms. The one change or the one advancement I would say that we are seeing and Talas particularly is highlighting that the use of biometrics, facial match, liveness detection and facial match is going to become a lot more prevalent and really needs to be paired with digital ID verification online and then also for access management, be it physical or be it digital. So we think, we're going to see a lot more ID verification with the biometrics check to make the verification as reliable as possible. Because unless you can match the face, you still don't know if someone has managed to obtain someone's phone. So it's a prudent check for anything that's not a trivial use case.

Mathieu (36:42.20)
So I wonder if we're going to see a lot more verifications, like combination of showing a credential and a credential proof and doing a biometrics against that kind of, kind of locally almost, and then being able to pass the results downstream. And then if it's for an access use case or whatever, do you see that trend of more computing and decisioning happening locally?

Sylvia Arndt (37:06.00)
Um, well, it depends. We'd like to see that happening on the phone. The analysis may not be happening on the phone.

Mathieu (37:14.13)
due to technical restrictions of perhaps?

Sylvia Arndt (37:18.13)
Yeah, I mean, just the processing. Yeah. But the beauty is, you know, and I think it will really help the adoption. The beauty is that if I now take this on the phone, so I am as a holder, I have my credential, I am the one who is authorizing information to be provided. I see you know what information I am providing to whom. And so it's much more in my control, you know, and the biometrics check as well. I mean, I know there are sensitivities around people's biometrics. On the other hand, we all have grown very familiar with using biometrics on our personal phones. So I think there's a little bit of education to be done as to why access to certain services is safer for the user, right?

With biometrics, but performing this on your phone and having control of the data from your credential. It's a world of difference from a privacy point of view for individuals as well. Because right now, you're handing over our card to anyone with everything that's on there. And so, you know, today we've talked a lot about governments and benefits, but there's also real benefits to the users and to the holders in terms of privacy and security.

Mathieu (38:53.22)
I think for me personally, understanding all of these benefits, sometimes when you don't see who you're interacting with, like if something's digital, you kind of, you have less trust inherently in the whole thing versus if I hand my ID to someone, you're kind of standing there with them and like you maybe have some rapport or you know what's happening because you're looking at them. But I wonder if you see any kind of challenges in adoption or people pushing back on at least In the US seems like a country that cares very much about these things compared to other places in the world, perhaps.

But did you see adoption challenges on the biometric side of things? And if we're talking about matching that with credentials, so we're talking about high integrity credentials being issued, kind of offered as a public service from the government, but biometrics side of things. To my knowledge, there are government databases for specific documents, but I don't know necessarily that we're talking about interacting with those. Those are more kind of biometric libraries and cross-verifications happening, right?

Sylvia Arndt (40:01.08)
Exactly. So it's a match, right? It's two things. You're detecting that the person who's identifying themselves is really life, is not a picture or a video. But we passively, I mean, that's the most advanced detection method, passive lifeness detection, you're checking that and then you're matching that person's facial features to the image that's associated with the identity document. So that's all that's been done. I believe there is probably some education needed as to why it's being done and what is being done to convince some people and you know, there will always be people who say, you know, I don't feel comfortable doing that. I'm going to go into the branch or I'm going to go into the office and that needs to remain a path.

But for everyone else who wants to take advantage of the conveniences of performing business online, it's a fabulous option. And you know, I think I really hope that as an industry we can help with that educational effort. Because yes, I understand there are concerns. But in the end, you know, these checks are being conducted. So your identity is safe to ensure that, you know, it is you and just you is getting access to your bank account or to you know, anything else that you're trying to access. So it's really all, you know, having the same aim of keeping data and people's identities secure.

Mathieu (41:58.04)
To expand on that, that is a priority for governments, that's a priority for the industry, for yourself and myself. How far reaching does the governance or recommendations or control need to be on the verification side of things, from an issuer or from whoever?

Just because we're sharing a higher integrity piece of data doesn't necessarily mean that the person on the other side of that is an nefarious actor, just like they could be today. What's the thinking around putting controls in place on the verification side of things, either from a government's perspective or from an industry perspective? I would be interested on what you're seeing.

Sylvia Arndt (42:43.15)
I think it's the one area that requires more thought and more initiatives around that as an industry. I think we've all been very focused on issuance, on the secure credentials, on interoperability, all of which are really, really important to get this started.

But the onboarding process for verifiers, I personally believe there are gaps. Of course, anyone will be subject to, any verifier will be subject to applicable data privacy laws in wherever they're based, wherever they are conducting business for sure.

But as fraudsters advance, particularly online, I really wish there was some form of registration process. Not necessarily a universal, you know, but some method of… Let me rephrase that. As a user, as a consumer, particularly when I'm online, I would like to know if I am about, you know, I found a new source, a new company that I'm contemplating purchasing something from or licensing something from. I would love to have assurance that this is in some form or shape a company that was vetted by someone or has gone through some type of registration process.

So, you know, there are, I mean, it's a legitimate business. How that can be done? That's the big question mark, I think, right now. So it's actually a thought I keep throwing out there as we are in the industry, you know, talking about advancing these programs. So I really think this subject needs some thought leadership and possibly some of the big stakeholders to get behind and lead the way in addressing this topic. Otherwise I fear it could be a little bit of wild west.

Mathieu (44:42.01)
Does it pose a risk for like, there's obviously, if like assurance kind of is something you want to get if there is risk in a certain interaction or transaction and so where, I'd be curious, like where does the risk lie in this whole model of a driver, a digital driver's license being issued to a holder, whether it's an Apple wallet, Google wallet, Samsung wallet, or if it's in the government wallet, then it gets presented. It's going, actually there's different fraud vectors. I guess the wrong person could get the fraud, like the wrong license. It could be an identity theft there. And then there could be different risks or attack vectors, I guess, on the verification side of things. Is that a challenge in the industry right now? Or how do you look at risk in this whole model? Does it differ from how things are conducted today? Or are we opening up more risk vectors?

Sylvia Arndt (46:40.17)
I don’t think that, in fact, you know be one of the one of the principles in setting up these ID systems and protecting you know the source data through multiple layers of security you know is that when you as a holder transact it's one credential that gets exposed so in that particular case, you know, the risk would be identity fraud. But that risk already exists, currently. In fact, you know, the fact that we have much more control over what we can pass on to someone gives

us as a consumer or as a private individual more control. So by no means would I want to imply that there are greater risks with digital systems. I think these digital systems are overall reducing the risks. What we are talking about is an advancement, right? An evolution in e-admin and e-commerce and so I would like to look at it is how can we make it safer. We already know there is exposure. So you know how can we use the means that we have available now to make it safer. That's you know that's what I would like to look at it. I don't really see additional risks particularly with all the safeguards that are built into these ID systems.

Mathieu (48:37.21)
Are there rules or agreements across state, like just talking about the US, so like there's legislation passed at the state level to allow for these to be consumed in the same way that maybe a physical representation of it could be consumed? Are there agreements or things from state to state so that one state could accept the other state's mobile driver's license in the same way that they can locally? And then How is that going to apply in the digital world?

Sylvia Arndt (49:10.10)
I'm not a legal expert, but the key part of legislation that needs to be in place is the ability to accept a digital form of state-issued identity. As it relates to accepting a digital form of state-issued identity from another state, that should still you know, that should still hold. But don't quote me on that. I'm not a lawyer. But, you know, the listening to our government customers, obviously, they're very keen on accepting out of state IDs. And so it's more the focus here is more about the key exchange assuming that this is an ISO supportive credential that follows that standard and is in fact fully readable. So I think the key exchange is the challenge that AAMVA is seeking to address with the digital trust service.

Mathieu (50:32.17)
So if everyone agrees that the value really comes down to the verifications, that's where the business value happens. A credential is issued once there's a cost to a government to having the infrastructure to be able to do that and manage the life cycle of that credential and so forth. And if the value is happening on the verification side of things, is there, other than saying like, yeah, like as the government, access government services, we'll do a better job, we'll reduce fraud, we'll, you know, offer better service overall if our citizens are able to present their credentials to access things or to make requests. But are there thoughts from the issuer's perspective of like, hey, maybe there's a business model in monetizing the verification side of things outside of the government walls? Are those discussions that you've heard happen or Is that even a possibility?

Sylvia Arndt (51:32.16)
I think most of the governments that are quite advanced with us, you know, they, they've all invested in these ID programs, because they understood in order to get them started. You have to, you know, they have to be available. And, and so it requires initial government investment. And, you know, once these ID systems are more mature and there are usage opportunities and so forth. I think there are some governments that say, you know, particularly since right now

pretty much everyone, I think with one exception, are issuing these digital credentials without additional fees in the US. They would like to see a return on investment in some form or shape.

Now, is that going to be through their own internal savings, that ultimately materialize through the process improvements on their end, or is this going to be by saying, we as an issuing authority, we would like to have a share in whatever the monetary value of these verifications is. It's a bit of a stretch, but it has popped up. Yes, it's definitely a consideration. I think because we have already an established identity verification market here in the US with traditional credentials, this new form of ID really is just another input into these services. And companies who are conducting verification, they are buying these services because they need them. So here in the US, we anticipate that mDL verification integrates into these type of solution stacks as another input. And ultimately, it will be likely a dominant input. So like with all SAS models that are completely new, the ramp up time could be extensive.

So I think that's one of the challenges for a lot of companies. You know, to get this rolling does quite a bit of investment, but there's not a lot of people yet leveraging these credentials. So critical mass has not been reached yet, but it will come. Question is how long it will take and then, you know, ultimately, what's the value split? How is that going to happen?

Mathieu (54:47.22)
Typically information technology, like software, is very deflationary in nature. Like costs go down over time. For companies that are providing verification services, if this becomes a new input, do you foresee costs of verifications going down over time and these cost savings being passed on to the relying parties that are purchasing these verification services? Like, is this disruptive at all to the verification business?

Sylvia Arndt (55:16.20)
disruptive I wouldn't say not in the sense of efficiencies so yes I would absolutely expect that efficiencies need to be achieved particularly because the volume of transactions is expected to go up. I think once that ISO standard is going to be released, we're going to see a lot more activity. And we're going to see identity verification in many more places than we've seen it. I mentioned access management. This is one of the areas that a lot of companies are looking at.

So what we and the analysts are expecting to see is that overall there will be a significant increase in volume of verification transactions. Unit costs will come down like they should, you know, in this type of operation once you have scale and you are able to fine tune. But for any business, you know, that obtains or utilizes verification, mDL is not going to make it go away. It is something that will just be enhanced with mDL and budgets should be maintained and may have to be increased if the volumes are going up.

But then on the other hand, if I have less cart abandonment, less friction, less service abandonment, you know, the bottom line should come out positive after all.

Mathieu (57:13:11)
It's a good vision and a good way to end. Thank you very much Sylvia for doing this with me today. Really appreciate you sharing your knowledge and experience with our listeners.

Sylvia Arndt (01:00:13.07)
My pleasure. Thanks very much, Mathieu.