Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

eIDAS Article 45: Behind the Scenes

Robin Wilton - Internet Society: Look at eIDAS, Article 45, a topic which I'm sure is in the front and center of everyone's minds. if you haven't heard of Article 45, don't worry about it. We'll get to that very shortly.

We have 50 minutes for this session, which is not going to seem long enough, so I'm not going to spend time giving you mini bios of all the speakers. Suffice to say, it is well worth you looking up their bios online because we've managed to assemble an amazing set of subject matter experts for this.

Very briefly, they are Alexis Hancock from the EFF CertBot project, where she is the director of engineering. Dennis Jackson from Mozilla, where he's in the crypto engineering team. and by that encryption, not cryptocurrency. And Thomas Lohninger, who is the executive director at Epicenter. So welcome to my panel.

Welcome to you in the audience. And we look forward to a fascinating session. to set the scene just at a very high level. Article 45 defines part of a general European Union strategy with regard to digital identification as part of a broader initiative called eIDAS. The primary focus of eIDAS is really historically a digital identity for the citizen, and it has evolved to include wallet like functionality or in principle, trustworthy assertions.

of, individual attributes, such as identity, age, professional qualifications, and so on. what we're here to talk about today is a very specific part of that, Article 55 of the IDS

regulations. And, I think, Thomas, I'm going to turn to you first, if I may, to just flesh out that very bare bones picture that I gave with A little explanation of what Article 45 is, if you can, and then perhaps we'll carry on to some of the broader, characteristics of the eIDAS as a scheme.

Thomas Lohninger - epicenter.works: Very happy to. Thank you, Robin. I hope everyone can hear me well. yeah, The eIDAS regulation is actually a very old piece of law. It was adopted for the first time in 2014. And the primary mission of this European law is to establish a harmonized platform for digital identity. this, 2014 law, never fully came to fruition because, there were, reasons why national member states, EU member states, did not want to basically acknowledge all of the different digital identity systems from other countries. And so in June of 2021, the European Union started to reform this eIDAS regulation, and it basically contained two big projects. One was the so called European Digital Identity Wallet, which should really establish one harmonized system for identifying natural and legal persons, so like people and companies, vis a vis the public and private sector, online and offline and physical proximity, and to also allow the verification of attributes about these persons. online and offline. And this importantly is also meant to be a general purpose universal system.

So it should really span from driver licenses, digital euros, border controls, all different types of society, even doctor visits. will be happening based on this European digital identity wallet. And the second, part of this reform was Quox, Article 45, which brings us here today, where this idea of we want to have everyone identified, is also extending towards websites.

And, it, as we'll soon, explain further, established this idea of having the owners, the people behind a website being authenticated towards the users who are using or visiting a website. And so this idea of having domain ownership identified with a certificate that then browser vendors are also obliged to Display to their users is in a way an old idea, but an idea that the European Union wants to bring back to the table, maybe to go into some of the arguments that we've heard around the debate, why some of the member states think it's a good idea.

We, as Epicenter Works, were working on this reform from day one. I have to say, our main focus was the wallet, because as a privacy NGO, that was something where we see a drastic attack on anonymity online, on our identity data cryptographically verified in government, certified, being proliferated to areas where it really shouldn't be, like big tech, or credit scoring agencies, but we were equally concerned also about Article 45 and, this attack on the trust architecture of the World Wide Web. And I think I'm going to leave it there.

Robin Wilton - Internet Society: Thank you. that 5 euro note I gave you for the perfect segue was well spent. because I think where you left it there was, yes, there are these potential privacy implications in having, what may in practice be a central government issued identity that is used as the basis for all of these attribute level assertions and I

think we'll come back to that in due course. But there where you left it was, There's this, idea of identifying websites to the end user as well. and so Alexis, I think I'd like to come to you next, if I can. I, the idea of identifying websites to the user, this sounds familiar because we've had the little padlock in the browser for a while, and then we've had the URL bar going green to tell you that this website really is, really, is the one that you thought you were going to. Are we reinventing that?

Alexis Hancock - EFF: Yes, this was a repeat. There's no other eloquent way to say that, where we had extended validation certificates and we approached this idea of verifying your identity through TLS, which was an approach we already took before.

And it did not live up to the promises that it once held about being able to pull in the, end user on a website to be able to feel, not only secure, but be able to know that the person or the entity behind the website is who they say they are and using TLS to do that through extended validation certificates.

When extended validation certificates were proposed, we were in a different time. The web wasn't as encrypted. The web was less secure and we had an ecosystem where domain validation certificates weren't as automated and they weren't as extended to the everyday, web user and enterprise system that we have today.

Being able to automate these things and be able to automate security for web service, services out there. So we have EV certificates. And we went through that cycle and around 2018, I think the browsers largely decided to deprecate the UI for the green padlock because it wasn't accomplishing what it set out to do.

Originally, it was a large effort. And I do want to point out. Put out there that EV certificates aren't cheap. They are expensive in comparison to domain validation certificates. And it was really the issuance of domain validation certificates that helped the web become more encrypted. More so than more expensive, more onerous certificates like extended validation.

So we went through this cycle. And so when I saw this, I saw a repeat of a solution to a problem that didn't live up to its standards that it set out to do.

Robin Wilton - Internet Society: Interesting. Okay. So the themes that I think we're getting there is, as you said, there's TLS, transport layer security, which provides confidentiality.

for, browser sessions, provided you have a secure means of key exchange between the server and the browser, but that secure means of key exchange itself means that you need to identify the server correctly, otherwise I might be getting a secure session from my browser, but it might not be to the correct web server.

so as you say, the TLS kind of solves that problem technically. But then you've got that procedural step of, is that the public key for the website owned by the organization that says it owns the website? and I think it's that procedural step. So, Dennis, can I come to you for this bit?

Because. and you've, been involved both in, the, technology of, encrypting sessions between browsers and websites, but I think you and, colleagues have also worked on this idea of certificate transparency. So how do you detect bad behavior amongst the owners of website certificates?

I guess the question I want to try and sum that up in is if you want to tell someone that. This website is using a fake certificate to claim that it's not who it is. Is the end user the right person to tell?

Dennis Jackson - Mozilla: Thanks, Robin. Yeah, I think that's a really interesting question. So from the perspective of the end user in the browser, as a user agent, we have to make a decision about whether the keys that we see, the certificate that we see is a trusted one, is the trustworthy one for that particular website.

And I think as you alluded to, whilst we can make some technical decisions around that, ultimately, the user will never be in a position to be fully informed about that website and its particular practices and policies, and be able to understand whether that website is the right, piece of authenticating information for this particular connection.

Back in the sort of the days of EV, as Alexis mentioned, we thought that maybe adding more information to that certificate might be a way to help users make this decision, and as Alexis mentioned, it really wasn't successful as an approach. So what's happened instead is that we've moved more towards a system of public transparency.

And now when certificate authorities issue the certificates that are used in TLS, they have to be logged publicly with a number of different transparency log operators. And the value of this is that these logs are now publicly accessible. And in particular, the website owner or security researcher or anybody else can inspect these logs and look at the certificates that have been issued.

And particularly in the case of the website owner, They're able to say, I recognize this certificate and this public key because it's mine. I generated it, I asked for it, and therefore it's secure. But they may, if they see something that they didn't request for, something that it doesn't belong to them, but is being used to endorse a connection for their website, they can report that as a serious issue and ultimately take action on that basis to secure connections to their website.

Robin Wilton - Internet Society: Whereas that, would be, that's something that the individual really can't do. so yeah, telling them that it's wrong when they don't have the

means to do anything about that. It may end up frustrating people. Having said that, I wonder how many people in the audience have seen a certificate warning pop up in their browser that says, Oh, this website certificate may be invalid.

And how many people actually. either back out or try and do something about that as opposed to just clicking through it and saying, ah, I wanted to get there anyway. and I suspect the vast majority would probably fall into that latter category. Thomas, I want to come back to you here because, Dennis mentioned Website practices and policies.

In other words, what is it apart from technology that you need in order to have some level assurance that the certificate for a given website really belongs to that organization? and Alexis talked a little bit earlier about EV certs, which involved, for example, someone from the organization providing much stronger proof of identity and proof of their role at the organization in order to get that certificate.

But, so the specific bit I wanted to ask you about is, and this comes really much closer to Article 45 here, is what's the difference between the certificates envisaged by Article 45, so these so called QOCS, Qualified Web Authentication Certificates, what's the difference between those and the TLS certificates that Alexis mentioned, which after all are the basis for that encrypted session with, between your browser and the website?

Thomas Lohninger - epicenter.works: Thank you, Robin. That's a great question and actually one that we ex discussed at length in the three and a half years since this law was proposed. And, you would hear different things from the legislators and also the trust service providers, which are the companies that stand to gain economically from Article 45.

And some of them would say, this is really two different things. quarks are really just another word for. Extended Validation EV Certificates that are meant to identify a website owner being displayed for the users and it follows this European idea that everything should be identified. We have a strong push in various sectoral legislation like the Digital Services Act where age verification is a thing.

European health data space, you see it pop up everywhere these days that, the EU seems to be quite, set in stone that you really want to eradicate anonymity online, which we see as a huge problem. And by the way, we also have a right to pseudonymity in eIDAS in Article 5 that tries to mitigate that risk.

And Article 45, of course, has, dual function. So some people, and we could convince the majority in the European Parliament to follow that reading, that QUOX are not TLS certificates. QUOX should be separate. QUOX should be just doing the identification bit and separating the end-to-end encryption via TLS from the QUOX certificate would be the right way to go.

in council, so when the 27 new member states, had to come to an agreement on this law, this distinction wasn't that clear. And, the trust service providers are usually quite close with their government, these are national organizations. there was a push to have trust service providers being, recognized by all browser vendors.

And you would sometimes hear arguments like, yeah, but it's so burdensome to get into the list of Apple or Google or whichever browser vendor and their root certificate store. And if the government says it's secure and it's secure enough for the state, then it also must be secure enough for these big tech companies.

That's an argument that we heard a lot in the negotiations. and to maybe also come back to where we are legally. so in May of this year, the European, Union approved the eIDAS regulation and is already in force. but there are so called implementing acts that are detailing the obligations in the law.

And there's also one implementing act on Article 45, but we haven't seen that. In total, there are around 28. at least 28 Implementing Acts, sometimes you could see several for one legal provision and only five have been up for consultation so far. The consultation ended early September and actually tomorrow will be the vote on those five that are all only concerning the wallet.

We've been actually working on that quite closely and it looks like they might fail. You can read in political Amlaks and German media that there is a big frenzy between member states on whether those five implementing acts will even make it. and that's to say that we will wait for quite some time until we get the technical details on how quarks are actually implemented and, Etsy, which is a standard organization that is also working in part around surveillance.

standards and lawful interception also has a seat at the table and these technical specifications. So the final word is definitely not here, but so it's really good that we can have this discussion.

Robin Wilton - Internet Society: I think you've given us a really important glimpse behind the curtain there because I'm sure it's no coincidence that you mentioned 28 implementing, different implementing acts for this.

And that, number seems. Coincidentally, close to the number of EU member states, within one or two, regrettably speaking. they've got it, I think, because you also said, you've heard the argument, if this is secure enough for the government to satisfy the government, then it should be fine for the citizen.

And yet across those 20 plus member states, we see governments of extremely different and very political complexions. and, so what you're really saying is on the one hand, we've got this global set of rules about how TLS certificates get into the trust list

of the major browsers. And on the other hand, we want possibly up to 27 different national rules about how these certificates get into the same list.

And that seems to me to be the absolute. kernel of this problem. so with that, Alexis, can I come to you for a bit here? We've hinted at the idea that there's a set of rules through which TLS certificates get into the browsers. And as, as Dennis said, those in turn rely on policies and procedures about how certificate authorities, allocate and attest to those certificates.

Are these the same rules for the QOX certificates, because it doesn't sound like it.

Alexis Hancock - EFF: So no, and I want to look at this from a security incident lens with a, let's say, badly issued or nefariously issued certificate. So some years back, Kazakhstan, the government had been basically putting a certificate into Snoop on traffic onto their citizens.

And they did this with, the browser, at the browser level, because they were previously trusted. And once Mozilla found out, once Chrome found out, they were distrusted because They were acting out of not only, not out of the realm of civil rights in general, but acting badly as a CA. That is not something you're supposed to do as a certificate authority.

And a part of that is being able to act quickly. So once people were aware of what was going on from the monitoring level, Kazakhstan's CA and certificate was removed and they were distrusted. When you put law into that process without consulting the parties involved with that process, it slows that security incident response down significantly because now the browsers would have to gone through a legal process just to get a CA or a QTSP removed if they were acting out of bounds.

Now let's talk about those bounds, right? So you have Rootstore programs. Now every major browser has one. That wasn't always the case. I always like to bring this up because in this conversation in the past three years, approach TLS and approach G, approach the ecosystem as if it was the same ecosystem we had 10 years ago, and it's simply not the case.

We have root store programs now. We have root store programs that communicate with each other. You have baselines, guidelines. We have certificate transparency. We have stronger account controls. There's a whole bunch of things that's going on that are more helpful than they were before. So you have root store programs and their rules and their auditing process now.

And not just root stores, just, whoever decides a CA can go in there, but an actual process of being able to monitor, audit, And transparent process of kicking that CA out if needed. So there is a standing process behind that already. The QTSP with Quox and

Article 45 would be able to completely bypass that process and automatically get trusted in the root stores of the browser.

So you can see now where the overlap would be in terms of democracy, transparency, and what that looks like when you have a, a Essentially, a state sponsored CA, in this case, be able to bypass those kinds of rules, and also not only bypass the rules, but now legally bound to be required in these browsers.

And when the browsers take a stance that a CA is not up to their standards, We now have a whole new legal process to adhere to, just to get that CA distrusted if something was misissued, mishandled, or nefariously input.

Robin Wilton - Internet Society: And so that, yeah, and part of your fear is that legal process would take time to unroll, and it, and actually for an operational security point of view, you need it to happen much quicker than that, on a faster timescale.

Thomas, I'll come to you and then Dennis, I have a question for you as

Thomas Lohninger - epicenter.works: well. Thank you, Alexis, for touching on this and you're absolutely right. There are some additional hurdles that are created by this, but I also want to make an important distinction that, when you look at the recitals and the legal debate, What, would be seen as like a reason to exclude a trust service provider from the root CA store is much more something like DIGI Notar, so security breach at the CA, but if there were a case of lawful intercept and a trust service provider of a country, let's take a country with the weak rule of law, like Hungary, where to issue certificate, totally legal for intelligence agency purposes, for example, then I'm not even sure how that would classify, we wanted to have stronger language around legal intercept because that's a main concern for us.

But sadly, that is not something where we see strong language in the law.

Robin Wilton - Internet Society: Yeah, it's, you paint a worrying picture and I was going to come back to you, Alexis, for this, just before we move on to Dennis's point. Really, it strikes me that. By including these government mandated certificate authorities in the same list as if they were the equivalents of the ones that get in there via the certificate authority and browser process, the Not only does it open the door to, as you gave the example of Kazakhstan, and they're not the only ones think, Mauritius tried the same thing, of a government taking steps to install a root certificate that would allow it to, to, to decrypt and intercept all the traffic going in and out of that country.

But there's another kind of harm as well, isn't there? Which is that, if certificate authorities are in the browser trusted root list that manifestly aren't to be trusted. What does that do to the trustworthiness of the other certificate authorities, which, as far as the user knows, got in there by the same process?

So what's the impact on things like TLS there?

Alexis Hancock - EFF: I am of the very strong belief that you need to create Internet policy and tech policy around the issues of tomorrow rather than the issues of just today. all EU members are not operating the same way as Thomas said. being, one of the entities that may be acting, maybe not in line with the same democratic principles as other EU member states.

So you have to look at it from that standpoint in that view of being able to create tech policy that doesn't think of just, along geopolitical lines. You have to think about how the Internet actually is. And it's a global thing. It's a global citizen membership party, on the Internet.

And I would like to think that in any time I have heard governments say anything along the lines of sovereignty and, creating fences on the Internet around geopolitical borders, I've never really rested well after hearing such terms and nomenclature around the Internet. Because if, once you start creating policy Around that aspect and not thinking of a more global citizen aspect of the Internet and who's interacting with it and not creating policy that protects people tomorrow and not just today.

You don't know who's going to be in power tomorrow. So you should need, you need to make tech policy for who is in power tomorrow and create those safeguards. Article 45 would have endangered that safeguard of trust. Definitely, especially if you had different parties acting differently within the EU member states.

What would happen to a user if, you had a QTSP from Hungary versus a different country? Where would they be able to even assess that? And I'm of the belief that we shouldn't put that burden on everyday users to assess that. It's up to us as experts and politicians and educators on this subject to come to terms on what that looks like rather than leaving the burden on users to figure out what this trust look like on the web.

Robin Wilton - Internet Society: Yeah. And we're definitely going to need to come back to the, privacy, pseudonymity and, fundamental rights impacts of this. but I want to bring Dennis in again. Sorry, Dennis, you've been on waiting patiently. So a couple of things I would love you to pick on, pick up on if you can. and the first one follows quite nicely on from what Alexis just said.

So one of the, one of, one of the pieces of pushback I got, a couple of years ago when I was, doing some research on trust factors and the Internet here, was that, this objection to, the implementation to deployment, of Article 45, objecting to it was undemocratic in the sense that here you had regulation, which had been produced through the democratic process, the European Union.

And on the other hand, you had a relatively small handful of certificate authority specialists who were saying, no, this is a bad idea. We're not going to let you do it. Is this actually an undemocratic thing, or is there a justification to be seen?

Dennis Jackson - Mozilla: I think, to answer that, we really have to unpack how Article 45 came about.

And back, as Thomas mentioned, in 21, there was a public process around crafting this law and identifying what it might need to do. And the main outcome of that was a suggestion that, a requirement that browsers would recognize these quacks and use it to display this kind of additional identity information.

And Mozilla and Edry and many other groups engaged in this issue and talked about the merits of EV certificates versus DV certificates and so on. And towards, the middle of 20, sorry, early 23, this law went towards its finalization. And in the EU process that means entering Trilog, which is a closed door series of final negotiations to produce the final text.

And it was only really at this point that, Article 45 began to metastasize and take on a new character entirely. And it was during these private negotiations, which is when new text was introduced to place these requirements on browser providers, to recognize EU QTSPs, EU CAs, and to not remove them unless EU governments agreed.

in terms of democratic principles, this very text was introduced in private, and was agreed in private, and nearly made it into the law essentially through a private lobbying process that wasn't transparent to the public, and that cyber security experts and academics were simply not aware of and not able to participate in.

What then happened as a result of that, as a reaction to that, It was that these NGOs, the browser makers, cybersecurity academics and experts came together to say that, this is wrong, this isn't something that should be done, this isn't something that's going to deliver value for European citizens, and essentially called on the European Parliament to oppose it.

And ultimately, the European Parliament chose to take up that call. and did choose to push for that text to be amended and change that at the very, last minute, literally days before it was due to be, published, to change that text to introduce new safeguards that would mean that the law would be restricted in its impact and wouldn't require browser makers to trust these CAs on the basis of government diktat.

Robin Wilton - Internet Society: Joe's put a question in the Q and A, saying the, amendments to this to Article 25, that allow taking urgent security actions, allowing adherence to best security user, experience. Do those take the pressure off some of the

issues here? If not, would you want to see more? Dennis, I want to give you a chance to give that one first, and I think Alexis, you might have some thoughts on that.

Also, Thomas, put your hand up If you want to come in on that one. So Dennis, you carry on for

Dennis Jackson - Mozilla: a second. Yeah, so the primary outcome of these last minute changes was to introduce a new exception to say that no obligation to recognize quacks would contradict the rights of browser manufacturers and distributors to authenticate websites in a manner and means according to their discretion.

And that is fundamentally the essential safeguard, which. protects against abuse from much of this. Although browser browsers are still going to recognize quacks and display this identity information to users this doesn't extend to the cryptographic keys carried within those quacks and browser vendors are still able to use their own security procedures for this.

So I think this is a you know an essential and a powerful safeguard but much like with the wallet This now has to be implemented in Implementing Act and realized in a technical standard. And part of my work at Mozilla has been working with Etsy on what those technical standards are going to look like.

And a central focus of this has been splitting the atom, if you will. So to take the existing QAC standards, where identity information and TLS information is contained within the same certificate, and splitting this in two so that then we have A TLS certificate, which is purely within the browser's controls and uses the existing transparent practices that we've used for the last 20 years.

And then the QAC itself, which will contain information about the website domain name, and information about the website legal identity, but not otherwise be used to establish these encrypted connections. And this has been a very long process, agreeing these standards, and it's still not done, and it has Thomas mentioned it might not be done for another six months yet, as different parts of technical and legal wrangling continue, but it has largely taken the pressure off, and I think the very worst case here has been avoided.

Robin Wilton - Internet Society: Thomas, we seem to be through, just through a step by step process of describing what the regulation says and what that means and what its implications are. We seem to be a very long way from the EI DAS type goals that we described at the outset in terms of things like wallet functions, improved user trust, because goodness me, I haven't I've got a great feeling about that from this discussion.

it, but put it bluntly, is Article 45 fit for purpose?

Thomas Lohninger - epicenter.works: No, not really. But the question is, which purpose does it serve? And if the purpose is to really create trust in the World Wide Web, then I think it was flawed to begin with. If the goal was to undermine the web security architecture, then The verdict is still out, but ultimately want to go back as we are now going through the timeline, what happened when, and, I can confirm that the Trilog negotiations were really a disastrous moment in time.

It's not my first EU law, I've been doing this for 10 years, which is why I have gray hair. And, It was quite a hopeful moment when we organized this 400 academics and NGOs letter that really managed to get this issue finally to the public's attention because the IDAS is super nerdy. It is a very technical, complicated law that was mostly negotiated without much public scrutiny.

I think we were the only NGO constantly providing analysis of every version of the law, including the non public versions that were discussed in trial law. to give some, allow for some public debate and scrutiny for what's actually happening. But it was with this big letter that we could really scare the MEPs and the council presidency to come back to the table to give us concessions that allow us a fighting chance now in the enforcement.

And, we could, at least get a few of the core privacy provisions in the legal text and your law is really moving very slowly. So once you have something like this, it usually lasts for a decade. So that means the real effect in practice. on people's browsers, on people's smartphones, on when you go to the doctor, to the dentist, or to the supermarket, or across the border.

Give us two or three more years and then you'll actually see it because then member states will have to offer the full suite of these new technologies and to ball it and everything that might impact our daily lives. The one argument that is our success metric and that funny enough is also the strongest political arguments with lawmakers is that A big project like the eIDAS is ultimately judged by the trust that citizens place in it.

The trustworthiness of the ecosystem that we create, how resilient it is against bad or fraudulent actors that are trying to abuse or undermine the system. And this is still something where We have to be very mindful. We have to pay close attention. That's why I'm actually sitting on course, how the vote goes tomorrow.

And I actually hope it fails. I hope we get more time and the commission has to go back to the drawing board with a few of these things. The eIDAS Implementing Act will only be proposed, I think it was around May of next year, so there's still time. And the particular question that was asked by Joseph, concerns Recital 65.

And yes, there is good enough language, as I mentioned earlier, to have something like a security breach of a just service provider being handled. with precautionary measures by the browser vendor. They have to notify the commission, national authorities, but

they can act. When it is lawful intercept, maybe with a gag order, depending on the country and national laws, I'm not sure.

And I'm not at ease that Recital 65 is actually a meaningful enough safeguard to actually prevent that type of abuse.

Robin Wilton - Internet Society: Yeah, fantastic. One of my favorite questions when I'm shown something like this and told how wonderful it would be, is to say, show me what in this system actually prevents abuse of the functionality that you're describing.

and yeah, I think that's a fruitful question to ask in this case, but I want to, come to 10 minutes left to go, and I want to use part of that, Alexis, with you, if I may. so there you had Thomas, who works for, a, an organization specializing in understanding and commenting and trying to influence this kind of EU legislation.

and it's hard enough inside the EU. What is it like when you start to look at the cross border implications of this? how do you, Alexis, explain to policymakers outside the US? what a trilogue is for a start. What kind of issues have you encountered there?

Alexis Hancock - EFF: Yeah, so this was my first round with, learning the key differences of the committees, the commission, parliaments, trilogues.

And Since I, this is my first round, the gray hair hasn't hit just yet. but I'm pretty sure in a few rounds it will. trying to get this in the context of what does this look like, not just in the U. S., but abroad, broadly, the Internet. And what does this look like for the web of trust? As someone that works.

Kind of like in a more neutral line of being able to boast the gains of automated TLS security, which is where this most of this caught my attention, was this inhibits, this hinders actually the being able to automate TLS certificates, wholesale, and different structures, especially structures that definitely need it, like in EIDIS, where you have digital wallets, you need to be able to act fast, you need to be able to stay on top of security in a way, like never before, if you truly want to implement wide scale digital identity for someone, you need to be able to have a trust system that makes sense.

And rolling back a trust system to more archaic points of view didn't make sense to me, and translating that outside the U. S. and seeing what that could look like, not the U. S., not the U. S., the E. U., but also looking at it in the U. S. where they're also looking at digital identity, in many different ways.

It's not, federally on our, national level just yet, but different states have already implemented mobile drivers licenses. I want to say about a little over 20 states have implemented mobile drivers licenses and have implemented wallets or have contracted

with Apple and Google to use their wallet in their native systems and iOS and Android respectively.

So what you have here is possible influence. The U. S. looks to GPR for a lot of the data privacy gains around. Legislation and policy, and I was afraid if this went through as is, that people would look at that as an example in the EU, saying okay, look, the EU has accomplished this with Article 45, maybe we should adopt similar language and enforce this.

I don't even really know what this looks like if someone from a different country. Visited a website that was backed by QTSP and they were defrauded potentially if this system was abused. What are the means of, being able to challenge that or get some sort of compensation or retribution out of being frauded?

What was that? What would that look like for someone? And there's plenty of people outside of the EU using EU based sites. it wouldn't have just been contained to that one ecosystem of just being an EU citizen. So I'm not really quite sure what that would have looked like, but being able to explain that as, and, implore my, the, politicians within the EU saying that you're setting the example, you set the example with GDPR, so we really need you to get this right in this sense, or at least be able to guarantee basic security gains here, that we have gotten in the past 10 years and not roll that back to a time where TLS was expensive, onerous, you.

And honestly, not as tight as it used to be, or as it is right now in being able to support automation and support being able to, actually automate security in a way that makes sense for everyone and being able to have participants in the ecosystem make the decisions as they are now, because they're, it's, a transparent process.

It's a process that's outside the EU, even though we have EU members in different standards bodies, they're making those decisions together. It's not just in a silo. So making this decision in a silo didn't quite make sense to me. And that's what I was trying to explain to audiences outside the EU to not necessarily follow that particular path if it happened.

Robin Wilton - Internet Society: Yeah, and I think, we, can see this by analogy with, other products and services that, the last thing you want is like a browser that only works in the EU. That's just not how these networks or browser manufacturers having to develop different, different product, but with different geographic market that, that really, it starts to erode some of the fundamental, benefits of having a global Internet.

Okay, so we have just a few minutes left. I just want to, as it were, go around the table again for some last thoughts. Dennis, are you optimistic at this point, from a technical point of view, and then if the answer to that is yes or no, what about the non technical optimism?

Dennis Jackson - Mozilla: I think, I describe myself as an optimist, but I do struggle to be optimistic about the process at which this has been arrived at and the way that these regulations and technical standards are currently being written.

I think, you know So there is

Robin Wilton - Internet Society: a bit of it that is open and transparent and in the democratic process. You mentioned, for example, the European Parliament taking up the case against this, but in the Before it got to that point, there was also, there were also the more problematic kind of closed door sessions.

Dennis Jackson - Mozilla: Yeah, and I think not only before that point, but also now after that point, where the Commission will ultimately write an Implementing Act to realise this, based on a technical standard, and that technical standard will be developed behind closed doors at ETSI, which requires an extensive kind of commercial agreement to contribute to.

It won't be a standard that anybody can weigh in, or like at the ITF, where you have this more participatory norm, and that Implementing Act won't be supervised by Parliament, Fundamentally, it will be down to the European Council, the member states, to decide whether they consider it suitable.

And that limits the opportunity for scrutiny and control over these processes, and makes it much harder for the average European citizen to engage in this process in any meaningful way. And that European

Robin Wilton - Internet Society: Council, of course, is populated by National politicians. Yeah. so Thomas, perhaps you can close this off for us with some thoughts about the, wider impact of this on things like anonymity and pseudonymity and other fundamental rights and the technology that supports them.

Thomas Lohninger - epicenter.works: Yeah, sure. so I agree with Dennis. I always say I'm an optimist by profession. And in a way, it is quite hard to see the hands of our governments laid out here in front of us with the devastating consequences. At the same time, there is a reason to be hopeful because we could get meaningful changes into the process, into the negotiations with public pressure.

as long as We as an informed public, as experts of civil society, include to insert ourselves in these processes. We can make a difference. We have actually in the implementing acts that will be voted tomorrow, a quarter of our amendments were taken on board by the commission. So there is, opportunity to actually influence these decisions if we pay attention.

That public scrutiny is key. And we are at a watershed moment. Alexis mentioned how digital identity systems are already proliferating in many American states. I'm part of a UN project around digital public infrastructure that builds on the Indian ATAR system and the many other regions, why these systems, where these systems pop up.

So I think it is exactly the time now to pay close attention and to use these experiences from other countries to learn and to maybe not repeat the same mistakes. And when it comes to the concrete eIDAS process, there is a legal obligation to have a four week consultation period after implementing acts of Article 45.

So there is a way to have an official record of all the contributions around that. That's a great opportunity for a campaign. And, as someone who has like I'm not sure how the vote will go tomorrow and council is harder than parliament, but we are at least in, in, reach of blocking these implementing acts.

So there is definitely a chance and there's a reason to be hopeful if we all do our jobs and continue to pay close attention to these very technical issues. I still have hope that we can come to a good outcome and have these big technical systems respect our fundamental rights.

Robin Wilton - Internet Society: Wonderful. look, I think we've packed our 50 minutes with just the most amazing discussion.

I've got some thank yous. I'd love to, thank Seema Karaman and the team at Mozilla for assembling this workshop and this panel, Thomas Loeninger, Dennis Jackson, Alexis Hancock. What, as I promised, what a fantastic lineup of subject matter experts. Thank you so much for taking part today, as part of Global Encryption Day.

And, thank you to all those who've dialed in to, to listen and participate and submit their questions. Thank you so much. I hope to speak to you next time as well.

Alexis Hancock - EFF: Thank you.

Robin Wilton - Internet Society: Thank you. Goodbye. Thank you.