FINISHED COPY
APrIGF 2017
BANGKOK, THAILAND
27 JULY 2017
WORKSHOP 48
ENABLE INNOVATION AND TRUST IN
INTERNET ECONOMY: TOWARD AN
INTEROPERABLE ONLINE AUTHENTICATION
AND IDENTIFICATION INFRASTRUCTURE
2 P.M.

Services provided by:

Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.captionfirst.com

***

***

>> KAREN HSIN-LING CHANG: Good afternoon, everyone. I'm Karen. We are still waiting for one speaker until he is coming. Oh, he is coming.

>> Marina, can you speak again, please? Just last test.

>> MARINA KIROVA: Can you hear me?

>> There is an echo. Can you use the headset from your side unless there will be a lot of echo? Okay. We communicate. We chat later. We pass it on to the Moderator.

>> KAREN HSIN-LING CHANG: Good morning, everyone. I'm Karen. Good afternoon, everyone. Sorry for that. It is too hot outside. I'm Karen, Karen Hsin-Ling Chang and I'm your very close friend from Taiwan. And it is my honor to be here today. And this session is Enable Innovation and Trust in Internet Economy. It is a long topic. Toward an interoperable online authentication and identification infrastructure. And this session is also supported by Asia APKIC. And some of us especially are from APKIC and some of us are from enterprise and also Civil Society. And welcome all of you. And we

will have regional development of e-identification and e-authentication for the presentations.

There are five presentations, and the last will be the panel discussion through the view of Civil Society and also private sector or Government representatives later on.

And -- so here's me. I'm the deputy director on the board of science and technology and executive UN of Taiwan and also the chairperson of business case and application working group of APKIC. And later we will have Hwang. He is the deputy director of Industrial Technology Research Institute of Taiwan.

Next will be Jonghyun Baek. He is the leader of next generation digital signature and authentication team of Korea. Vijay Kumar who is the head of technology of eMudhra, enterprise of India. So why don't you have your handshake to everyone. Next will be Secretariat of Digital Economy and Society of Thailand, Wanawit Ahkuputra. And Min Hsuan Wu, yes, Mr. Wu is the deputy CEO of Open Culture Foundation. Also the Hackathon organizer of Gulf 0.-- Taiwan. Next will be Nantawan Wongkachonkitti, yes. Deputy manager of Student Loans Fund Office of Student Loans Fund of Thailand. I welcome all of them. Thank you. Thank you for coming. And we have the special guest. She will come in to join us from the video. And she is the -- Marina Kirova. Hello, Marina.

>> MARINA KIROVA: Hello.

>> KAREN HSIN-LING CHANG: Marina is the policy officer of DG CONNECT of eGovernment and Trust, EU. I welcome her. And let me introduce before the presentation, the APKIC to all of. APKIC actually was transferred by Asia PK Forum in 2007. Focused on Asia region. And also we have lots of members, like Thailand, Thailand, India, Hong Kong, Macao and China and Bangladesh. So we have nine principal members in APKIC. And mainly focus on promotion of applications of PKI e-commerce, eGovernment. And what we do is collaborate with the global community to deliver a comprehensive framework of e-authentication.

The first presentation will be by -- present by Dr. Jonghyun. The topic is development of electronic identification and authentication. It will include Asia region. Not only one country is Asia region. Welcome Dr. Hwang, APrIGF.

>> WEI-CHUNG HWANG: Good morning, everyone. Here I will introduce some status of e-identification and authentication. Here is some background why today -- why we are here to discuss this topic because and right now today e-identification and e-authentication is a very important fundamental technology for digital society. Right now there are a lot of solutions for e-identification and e-authentication. So we have -- right now we have a national e-identification system in many countries that we -- the country or the government issue identification cards to citizens. And besides that we also have some other solutions. We have PKI, that's for more

than 30 years is a very long history that we have with the PKI, public key infrastructure system. And other years we have e-identification solutions, try to make the e-identification more convenient, more convenience and more -- better user experience.

One of them is vital, vital. Try to use public key technology and in the same time it also combine the biometric technology, to provide secure and stronger e-authentication system. And in the same time we have mobile connect and solutions. So they are all about e-identification and e-authentication. There are so many solutions. And we also have a lot of applications that depends on such kind of e-identification solutions. And in the other way we also have some kind of legal regulation framework in every country or every region. For example, we have an electronic digital signature, legal framework in some country. And we also have some regulation for e-translation. And we also have some legal framework for other eGovernment or financial regulations. So I think the solution became more complicated today. We have many solutions. And we also have many regulations, many policy, and a lot of other considerations we have to face.

So here is some basic idea why PKI is so -- right now it is a fundamental infrastructure for many countries because in Asia-Pacific there are many countries that have PKI legal framework.

So here is a survey for members of Asia PKI Consortium. They are one similar, since that all of -- all members of Asia PKI Consortium have similar legal framework for digital signature. For example, Korea and in Korea we have a national PKI and also Government PKI and Korea also have electronic signature X, more than 20 years ago. And also China also has some similar regulation and also India and Taiwan, Thailand, Hong Kong and Macao. And that's why PKI is very important, fundamental and e-identification and authentication in Asia country. But however right now there are many solutions try to make the system more convenient and lessen PKI data too complicated. So there are many other systems. For example, in Korea, Korea is very aggressive in e-authentication and e-identification. So actually Korea is a very good practice for national PKI. But right now Korea has PKI vital system that addresses how the system can be ready, convenience to be deployed in the mobile environments.

So later on in the session we will discuss about the Korean experience. And also for China, China also try to have a national EID system and the industry of China, there are many big companies in China also try to join vital alliance and try to address how to deploy e-identification system with very good user experience. And also in India we also -- later on we will also have a session for -- from India that will talk about the national e-identification system and PKI in India.

Also have a PKI system in Macao and Hong Kong and also have similar e-identification system. Today we are here to share our experience

and try to discuss if we can have more better and comprehensive solutions for e-identification.

So here, first of all, I will just mention about Taiwan. So in Taiwan that we have e-identification system in financial sector and also with national PKI system, also in the Telecom industry also have an e-identification system. So here is some experience and practice how Taiwan deploy e-identification system. So first of all is Taiwan's public key infrastructure. To set up national public key infrastructure starting from year 2000. And since that in Taiwan we have two PKI systems. First one on the left PKI system, right size financial PKI system. So based on the two PKI system a lot of Government application and also financial applications depends on Government or financial PKI. And besides that we also have many B to B application, B to C applications and even enterprise have a lot of applications depends on Government PK and financial PK. And here is some example of the government PKI system. Among those applications the most popular one is the e-text filing system that many Taiwan citizens use system with PKI and able to download their yearly income ready convenience.

And starting from this year the Taiwan also try to set up -- set up a national Taiwan financial identification center. So this financial identification center try to address the problem that have so many tokens that can all be used for the financial transactions. So such kind of a TWID center try to aggregate all the tokens. So they work together with I.D. partners and try to provide some integrated solution that can use not only PKI system but also financial card. And even in Taiwan we have the health scale insurance card that can also be used in the financial transactions. And actually try to address the financial transaction is an application driven solution that for those sessions we can use a lot of e-identification solutions. But for high risk transactions that is mandatory for high risk transactions.

And the last one that is starting from this year in Taiwan the mobile application, starting to set up their I.D. identification system that work with mobile connect service that was read by social. So in Taiwan we have a company, five operators, they work together to set up the mobile connect service that try to aggregate all operators in Taiwan to provide a single, single solutions that every application can just use such kind of service to verify the users' real identification. So that's based on the mobile connect solutions.

So here is some experience from Taiwan, how Taiwan just try to use different solutions for different applications. So that's my presentation. Thank you.

(Applause).

>> KAREN HSIN-LING CHANG: Some kind of status of Taiwan or Thailand and India and also Korea, et cetera, Asian countries status. And he is not only working on this PKI and also open data and Big

Data in Taiwan.

Next we will welcome Mr. Baek from Korea. And he is in charge of the operation of Korea -- management of Korea's national PKI system and also the representative of APKIC. Welcome. Welcome Mr. Jonghyun Baek from Korea.

>> JONGHYUN BAEK: Thank you so much. Yeah, I tried to finish my presentation. Okay. Yeah, my name is Jonghyun Baek from Korea. I just have a presentation. Actually this time I would like interesting status of Korean PKI and then just -- we just -- nowadays we are using the PKI systems in Korea now. Interesting about the case of FIDO. Usually PKI certificate we don't take like that.

Actually just Dr. Hwang about PKI but more exactly we have two kinds of PKI system. One is national PKI and the other is the Government PKI. So maybe from 1999, which is establishing the Letter Signature Act and then from 2000 we operate this -- national PKI systems over 17 years. And the other is call the Government PKI because just only for the public servants issue this kind of PKI certificate and then use in their work. And currently the population of Korea is 50 million people. But our mPKI users is 36 million, over 36 million. So many people using this kind of system. But it is 17 years and also 36 million people using this kind of certificate. That's why we have lots of challenges. And sometimes argument. So complaint. Lots of things. But most major complaint is on convenience. So maybe we are just starting this kind of technology. We are using the FIDO technologies. That's why we just serve some problem on convenience for our national PKI certificate.

So -- also importance on -- with regard to provide online means that play the role of identification. In Korea we are just using their -- only this plastic card, like we call license card. So we need some signature, some kind of document. We are just using the sill or signing in the time. But usually online is totally different situation. We need electronic check or sometimes digital check. We need that kind of law. And also we are just using the identification and the digital signature with that kind of certificate.

So as we mentioned before we just have -- we enter certification, national PKI certificate because we just accredit -- we got the five accredited CAs and then the Government is making reservation and Government control this kind of system. So we just called accredited certificate. So this is for approving electronic documents and transaction on the cyber page. So I scroll down, the environment has changed to the mobile and Smart Cloud. So nowadays over 6% of users doing the certificate on the mobile phone which is called the Smartphone. And it is because more convenience and a little bit more secure and it is to the user create certificate. Nowadays many people are using the certificate in the mobile devices. So that's the reason we just started these technologies development.

FIDO alliance, this FIDO alliance certification at December 2014.

And then we are just preparing our -- a little bit different with -- which complies with the FIDO alliance certification but just try to keep their specification and also -- how can adopt our national PKI certificate with FIDO alliance specification. So we make some survey, sorry. From 2015 a survey and also developed a FIDO foundational PKI. And finally 2016 May we announced the guideline for the safe user of certificate in the Smartphone environment with the FIDO technology, FIDO authentication technologies. And also from May 2016 we just provided service Internet banking and online data exchange.

Currently in financial part, financial area they can use the national PKI certificate with FIDO authentication technologies. And also currently we are just ongoing, kind of environment working, association with Korean Microsoft and Microsoft in those platform by using the FIDO technology. It is not an ongoing project, not decided yet. So anyway we just try to make more convenience to the user of the national PKI certificates.

This is a test of user -- of the certification course. 131% of the economic active population in Korea. It means really lots of people using the national PKI certificate. So Internet banking and Smartphone banking and e-service and bidding and online stock. Lots of service we can use with this certificate. So this is shown how can we make FIDO and certification technology. Actually one -- as I mentioned before one of the reasons we prepare these technologies is the convenience to the user of the certificate. So one of the big problems today on convenience is memorizing the password because we just recommended 12 characters. And then using our -- number and using the special marks, something like that. So never memorize that kind of one password.

So it is one of the complaints to them, users complain. So we just prepare these technologies and also just -- so only using the fingerprint or iris, the kind of biometric information we use. So this is kind of the FIDO alliance specifications. Usually they are Smartphone environment. They care about the Smartphone environment. So when using mobile phone they can use this kind of print or iris to make that authentication, that kind of technology.

So the entries about how can we handle these FIDO technologies in the desktop environment. So first is just using the Smartphone inside here. So when using the PC or desktop and then using the mobile phone here. And then mention to the FIDO servers and then like this. So but nowadays from FIDO 2.0, maybe they can directly contact the FIDO server and using the FIDO technology desktop environment. So that's why we just have a cooperation with the above issues.

So this is some detailed technology. So they have three kinds of party. Like it is users and we needed DA system or they needed issuing a certificate in these times. And also when the user want to make some certificate with FIDO technologies. That time, FIDO certificate

with the PKI category, make SMP and sent to party and then party send this kind of information to the CAs and then issuing the certificate. And send to the users and they just store this. Actually we recommend in the Smartphone. Okay.

Okay. And this place -- we recommend using the (inaudible) to store these kind of informations. And this issue on how can we use the FIDO informations, biometric data without entering the password is like this. Usually PT data is inside here. We are using the PT and then just encrypted private key and when they need future, we need to encrypt to the private key, biometric data. So we can just take private key and then signing the document using this private key. Yeah. So I mentioned before we -- using the iris or the fingerprint with FIDO technologies. So we got the real application like this. With bank, can't use this kind of certificate with FIDO certification technologies. From last year we are just starting with this kind of user case. And also this is an issuing flow is like this. I think you understand about this, because you are experts of this kind of play. So I just shown that.

Client centered IP server to certificate and FIDO server back to recast for entry in FIDO and then user using the biometric information in here and send response. And then they can use the certificate for the signing like this. And this is user of certificate. And they needed some service which is needed, national PKI certificate. Can use this kind of process and then just signing the document with certificate.

Okay. Detailed block, but maybe for the developer can reference this kind of process. But I don't think we need to explain about this kind of deal process. First is JMP, IPR, yes. That's all my presentation. Thank you.

(Applause).

>> KAREN HSIN-LING CHANG: Thank you, Mr. Baek. Next is Vijay Kumar from India, is head of eMudhra. He is involved in technical architecture of insight from the start, with India information technology ministry and blah blah blah. Largest electronic signature program in the world enabling 1.45 billion to digitally sign using their national I.D., using their biometrics or one time passwords. Vijay is on behalf of APKIC, Asia PKI Consortium. Let's welcome Vijay Kumar.

>> VIJAY KUMAR: Thank you. Good afternoon, everyone. Thank you, Karen.

So I represent India here. I'm to provide a regional update as well as what's happening in online authentication and identification in our country. So this is what I intend to cover. Just a few minutes. Our national I.D. system and how the world works with identity and authentication. The authentication mechanisms, interoperatibility which is the topic of the panel now. And then a brief introduction on (Off microphone).

So here we go. We have our national I.D. system. You heard of this other. So this is -- this is just a national I.D. system across the world. We have 1.25 billion population. Out of it already 1.16 population is covered with national I.D. So it is 100% foolproof system what is there. Approximately 98% of adults are already covered in this system. So what national I.D. does it prevents identity to -- where it also empowers instant online authentication and it can be OTT based, fingerprint based. Authentication has open AP system for online applications. This is most important thing. That's why ecosystem can evolve.

Widely used by banking and Government and other financial applications for authentication as well as curiosity of users. That's the part of regional update.

How national I.D. has emerged in India. Very second slide how Internet world is evolving. So it was a closed room usage of computer where a person and a system was being used. From there it went online. Now in today's world things have changed to something where it is things to things authentication. It is not just a person, human and a server being interacting. So what we have in today's world, there are some identities sitting here which can be either user, either device or other thing. The thing is most spoken about IoT, Internet of Things. Then there is Internet where there are several applications what we to use, several applications. They do interact with open APIs, integration of services. And other side, once again we have users who has to recognize, validate the other person or other device. So similarly we have almost a cross-connecting picture where users are authenticated by users. It is not just servers. Users by users or devices by things.

Then what is happening with authentication? Today we have -- we have about 15 plus factors of authentication widely adopted over the Internet. So passwords, passwords have come more advanced. At least they are not short enough to be predicted. So advanced passwords. And then the important thing is PKI digital signature has emerged, HOTP and POP and there is other various forms of TOP. Mobile certificates and then smart cards, biometric is most popular, fingerprints and voice, green cards are there and knowledge base. If you see four of these are taking prominence and having more reliability when it comes to online authentication. Then there is time based OTP which is being used. Biometric is most popular now. Most of these authentications are used for two factor or multi-factor authentications. If there is something behavioral analytics going on and this is more risky transaction and there comes the knowledge based authentication and it puts forward some questions about some personal information and you are to authenticate with that information.

So these are the types of authentication which is being used. Coming to the topic of panel, more is on interoperable online

authentication and identity and how this has to be achieved. One is how the technology and legal framework has to evolve. Maybe like it has to have more open APIs for standardized identities. So if you have identity system, maybe a banking system or maybe a national I.D. system or any kind of identity system it has to come with some open APIs so the ecosystem can easily adopt.

The second is data protection and privacy laws. The country should have its own regulations for data protection. When you say authentication or identity you are revealing something to that person or entity. And then comes security and audit certifications. This is also more from the regulation standpoint. There should be some system. Because when we say ecosystem is evolving it is more a number of people using this data. So that's why security and audit certifications are very important in this technology and legal framework. Then comes recognition of identities. So whatever the recognized identities, maybe like Government issued I.D.s, digital signatures under national road PKI, social I.D.s, social I.D.s are being used for several reasonable assurances. Maybe a medium issuance case. This is very important if the world has to interact, right, to mutual recognition and also data sharing agreements between the countries and recognition of national PK. And this is more on the mutual recognition front. So this is more on the topic.

As eMudhra we are the largest certifying company in the country. We have about 18 million customers for digital signatures. 10 million online users who authenticate using our platforms in various banks and Governments. We have 100 plus large entities using our platform. And we have enabled 1.25 billion national I.D. holders of countries to electronically sign on any mobile or the computer.

So what we do as imploding the ecosystem we are the certifying authority. We have 20 million plus unique users. Short-term and long-term digital signatures are issued and also as part of the digital India program we are also the providers of electronic signature. We are the first time currently largest index space. Online electronic signature service we -- 200,000 users per day use this particular platform. Then we have an authentication platform which is used by banking and Government apps. It carries about 10 million authentication transactions. And then also we have a paperless platform, what empowers all types of Governments or businesses to go paperless any time anywhere.

So that's all from my side. Thank you.

(Applause).

>> KAREN HSIN-LING CHANG: Thank you so much, Vijay. And Mr. Baek of Korea, he told us the relationship between FIDO and PKI, the International Standards Organization and FIDO. And in Vijay's presentation he told us what eMudhra does for online identification and authentication.

Next is Mr. Wu. And he doesn't have any slides, but he could tell

us many things and share with us his experience. Welcome, Mr. Wu.

>> MIN HSUAN WU: Thank you. I don't believe you understand what FIDO is. I start my career with PKI in 1991. Some of you don't even -- even before PK, scriptographics or SEIS. That is the first CA in the world run by Ericsson under the name of AU system.

So I implement the Swedish system under host and then I come to Malaysia with the digi certificate run by remote. Take back in time. Welcome to the real world. And so optimistic. But the topic is about enabling innovation and trust in the Internet economies. Two key words, cross-border. So are there any PKI experts on cross-border? The closest thing in your hand is passports. Can you use your electronic passport here? How much I see -- okay. Identity ICAO in industry. Even the SIM card standardization coming from that. I.D. 01, I.D. 2. That is shaping up the whole thing. So what I would like to say is that if you talk about the cross-border Internet economy, welcome to the club. The physical world and digital world is not the same place. You only have physical identity. Actually for Thailand we have two. We have Thai local language and then you have English one, but there are no control welcome. So you get your names either from the teacher from Catholic school that are the nuns spelled family name this way and you go to the -- with another press and he spell different family name. I have one of the staff, four of them study in different schools and have different family names. He apply visa to go to UK and have to go to UK and prove they are the same family. Okay?

That is a physical world we face. Digital world, you can be anything. You can be Mickey Mouse. You can be anything. So and you know what, it is interoperability. You need to know the RC822 going back and read about that. That's the only way that the Internet works. Otherwise you go for user name and password. I think that nobody else in this room is talking about that. If you talk PKI, if you don't read RC822, fine. Everything is dreaming. The issue, there are a lot of discussion on I.D. and tomorrow I think that's the Government part. I remember Edmon Shu, he talk a lot about the international e-mails. I don't know what it is. Even though I work in PKI and then I start to study that the most important thing that I can deliver to the world to create interoperability on the domain parts, which means that you can have your local language I.D.

Now there RC talk about local parts. Local parts would be oneaweek@gmail.com. You never Thai, conduct Thai or any other language. The local part can be different. I don't want to go in to the details. But we see facing the problem of interoperability on because the coding under local parts is different with the UD F8 that have been standardization in the PKI world but in the domain industry they use this when we call -- encode. At least you remember to study about that. The world is not ready yet on that aspect. So digital I.D. you can have anything. One person can have 100.

Physical world you only have one. In Thailand where I live for 15 years legally I am only allowed to have one digital I.D. That is my first name dot family names (cutting out). That are the sponsor domain. I can deliver to UPU is the legitimate address for the digital I.D. for me.

And fourth, anything, I forget to pay the telephone bill. So they deduct the money directly from my account using that enforcement crew and start to talk about the legal aspect of it. Just keep in mind that digital identity is different than the physical world, and the digital always the case that people try to dream of a lot of problems and try to fix in the digital world. Not going to go anywhere. Going back to check what physical mess up you have. Leave it there. Don't try to fix things on digital environment.

Second issue when we talk on PKI we have been working with this. Long time ago. 20 years, 10 years PKI. The time has come. It is not -- it is enforcement. Coming to the regular tree capture agreement, there is 90 regional trade agreement in Asia-Pacific. 90. 50% of regional transaction talking about top 50%. Top key word is paperless.

Second, authentication and digitalization. For Thailand we are binding with TFA, trade facilitation agreement or talk about digital signatures, cross-border recognition frameworks. And so that means we enforce. We capture by all these trade agreements. Plus you can respond. If you are really interested in this, go back and search the MC law. This year published the most important document called legal. It shows on e-authentication. That respond to the cloud services. Trusted services like FIDO. You have to read that if you are interested in this. Under United Nations, big paper talking about claiming services, online party should do -- training with the bank and all of them getting. Because these are the issues that we need to tie up between legal aspects and technology aspect. You can talk -- we are understanding which direction you are going to go, biometrics, fingerprints and it is not about mechanism. It is about how you conduct the business.

That's the second, to get update of Thailand. We don't have one. We have a PKI. We have credit to CA and we use in domestic. Internet. Trade and Chair of commerce of the -- that one whole chapter. If you are interested you can search and you will find people talk about whether we go block chains and all that other stuff. No. The world is living with digital signature. Future recognitions because that proves and model law, plus the limits of APO this year is even confirmed that the world is the base ICA, legal frameworks because without the interoperable legal framework the interoperable technology doesn't exist. How I recognize credential issue by Taiwan to Thailand you need legal frameworks like this one, already lists out which country is the legal frameworks and legal frameworks is very old. It is based on 1996. Sorry for the innovation.

You have to go back in times and the playing field -- we always call it golden oldies. Somebody getting rich by covered the golden oldies. Catch up the new technology and then fundamental for you to go out, but if the new generation look back in time, make a cover base on golden oldies, I really appreciate FIDO alliance. And this is the cover that you made based on the existing technologies that are proven and stated in several agreements. But if we have a patch of the (inaudible) the new generation that they are fascinated about new technologies, and you have to look back, study very hard on whether we talk about key words in the last message for me. We talk about PKI. We talk about identity, digital signature. The key word is legally binding. Without the understanding of legal frameworks how the cross-border legal frameworks, why every country need to state that. We follow the law. So the technology cannot achieve the interoperability without looking back in time. So that's the message I want to convey with you. Thank you.

(Applause).

>> KAREN HSIN-LING CHANG: Thank you, Mr. Min Hsuan Wu. Cross-border, paperless, legal framework and trust services. Also we have to focus on. Later we will have a panel discussion. And sorry, we have Marina from Europe. Marina, are you there?

>> MARINA KIROVA: Yes.

>> KAREN HSIN-LING CHANG: Good. Marina is from EU actually. She is -- okay. Marina, can you start right now?

>> MARINA KIROVA: Yes. Hello, everyone. Thank you for having me.

>> KAREN HSIN-LING CHANG: Okay. You can start right now.

>> MARINA KIROVA: Can you hear me well actually?

>> KAREN HSIN-LING CHANG: I'm sorry again.

>> Marina?

>> MARINA KIROVA: Can you hear me well?

>> KAREN HSIN-LING CHANG: Yes, we can.

>> MARINA KIROVA: Okay. I want to talk about the eIDAS regulation and the mobile access for electronic identification and the services. But first of all, where it comes from and what is the rationale behind the framework. Well, we have interim mark, but we are also facing in the digital challenges. And the EU being an entity of 28 different Member States, these challenges require a common approach. And sometimes the rules that we have for the physical market are not -- they don't apply to the straightforward way in the digital domain. So in many areas we need to update our legislation to keep up with the upcoming trends in order to be able to face the opportunity, the digital area for all of us.

So we have worked for many years. And now we are trying to remove the digital barriers and borders where they exist. So how does eIDAS help in this? Storage. So what eIDAS tries to enable is the building of trust, convenience, more seamless digital transactions across

borders. And this is really important. These are really key principles for us. And eIDAS is trying to solve issues that are in this -- in this area. So we have a regulation that is based on the internal market principle now. And the internal market principle says products and services across the EU. EIDAS is one regulation for electronic identification and Internet services and it is directly applicable in the 28 Member States.

This is important because in the past it wasn't the case. We used to have a directive on electronic signatures. And directive -- the directive as a tool implies a position within each Member State. So it let -- it led to different national implementations in the area of electronic identification and e-signatures. In addition the e-signature could be used as a identification tool.

Now under the eIDAS regulation, electronic identification are completely separated in terms of rules that are applicable to them. Trust in principle are (cutting out). So electronic seals, timestamps, certificates for website authentication, electronic registered delivery of services. So services now completely separated from the electronic identification. We have applied the principle of normalization approves. In the area of electronic identification and because electronic identification is the right of each and every Member State to decide how they want to do it, we cannot apply the principle of normalization. There what we have is the principle of mutual recognition underpinned by interoperability.

So this is what the eIDAS regulation brings. And it is one regulation but we receive the opportunity to adopt up to 28 additional implementing acts and one delegated act to clarify further where necessary technical and other implementing rules. So far we have adopted four implementing acts in the area of electronic identification and four trusted services. I have a link with the references for those of you who are more interested to improve more decals at the end of my presentation.

So the key principles for electronic identification in the European Union are cooperation between Member States. Member States are obliged to cooperate in the process of having their electronic identification schemes recognized across the EU. There is also the principle of reciprocity which relies on defined levels of assurance. So if the Member State requires of a certain level assurance, for instance, say substantial and there are three levels like this that we talk about in the nature, the Member States cannot request a higher level for the citizens from other Member States when they decide to choose their own national EID to authenticate. There is a mandatory cross-border recognition only for public services. So the Member States whenever they require electronic identification for the services they provide nationally, they are also obliged to recognize other EID, notified EID. But this is not applicable to the private sector. The private sector is completely autonomous to choose

whether or not to rely on EID means to recognize by a Member State. So Member States are as I mentioned before are completely free. They are free to decide all kinds of EID needs to use, whether to use at all. And we have the interoperability framework. How do Member States cooperate under eIDAS. The cooperation is based on an implementing act which defines the rules for this. Member States are obliged to cooperate in order to ensure interoperability and security of this system.

They are points of single contacts from each Member State. Whenever a scheme is notified for cross-border use Member States initiate a peer review to be sure this complies with the level of assurance that it claims to have, with security. And all this is happening on voluntary participation in the peer review. But actually Member States cannot be denied the right to take part and to make sure that indeed this scheme can be accepted as a cross-border identification. There is a lot of exchange of information and experiences and good practices on a continuous basis. And this is happening largely in a mechanism that is set so-called operational network where Member States take big part. And this is convened by the European Commission. And this cooperation network adopts some things and guidance and helps in the process of achieving interoperability and security identifying network.

So for the interoperability framework the purpose of it is to reconcile the differences between the very diverse national schemes. I mean we have very different models. We have EID cards, mobile identification system. We have in some cases Member States recognizing the card. Really a variety to host. And all these tools need to be able to interoperate across borders.

So the interoperability framework we have been building in the EU need to keep technology neutral and high level of requirements. And we have open source technical specifications that are developed under the program. And they are available for each Member State to adopt.

So Member States shouldn't impose these proportional requirements from each other. And it really -- the part is to make sure that the information that is being exchanged by the -- by each Member State across borders. So there is a system of notes that is being established in each Member State. And there is an interconnection between the notes and they communicate based on established standards. The electronic identification schemes in Europe, certain levels of assurance and the eIDAS regulation defines three levels of assurance. Substantial and high, and these are very much outcome based levels of assurance. They are set -- they set their objectives to be achieved. And they are only applicable to schemes, interoperability cross-border. There is an implementing category which sets clear criteria for each level of assurance. And what is important to understand is that Member States have the obligation to recognize electronic identification means which are of the same or higher level

than the ones that they are requesting nationally.

But they have no obligation to recognize lower levels of assurance. And here they are just a few -- very high level description of the elements which different levels of assurance have to address in order to comply -- to comply with implementing acts. And as you can see in the level high there is the kind of presumption of equivalence to verification. So this is very -- in the interest of time I give very high level description of the system that we have related to electronic identification.

But what is the timeline for all of this? The implementing acts, all the implementing acts were adopted in early September 2015. And since then Member States have been able to recognize on a voluntary basis other Member States eIDAS tools. But as of the 29th of September 2018 all Member States will be obliged to recognize schemes. This is the date when the cross-border effects of eIDAS regulation will be getting in.

Where we stand in terms of implementation? The majority of the countries are well advanced in implementing the eIDAS note and which needs to be set up by the 29th of September of 2018 and be operational for the purposes of recognition. All the others are making a lot of effort and they still have time to meet the deadline. Most of the countries have one or more eIDAS schemes. Others are in the process of implementing someone or setting up legislation in view of having one in the future. We have already had one country that notified the scheme. And the eIDAS scheme went under this so-called peer review. And the cooperation network issued the positive opinion.

So the next step is the formal notification which will happen at the end of August. And afterwards I mean the process for Germany is finished. And we are actively encouraging other Member States to also step up their efforts and notify their schemes because this is a huge opportunity for their citizens and for the EU as a whole.

So this was in very brief terms a presentation of the EID framework. I am happy to answer any questions that you may have. And I would like to say just we believe this is a very unique approach, federated approach for cross-border ability and mutual recognition which would inspire other regions to adopt similar approaches on the original basis. Thank you very much. (Applause).

>> KAREN HSIN-LING CHANG: Thank you. Marina is from eIDAS. Thank her for sharing with us. Member States cooperation in EID and also interoperability framework and the level of assurance, et cetera. And she is the remote speaker. If there are any questions will you please ask her right now? Any questions to Marina or to the eIDAS of EU? If not, thank you, Marina.

Okay. Then we are going to have the panel discussion. We would like to invite people or speakers from the Civil Society and private sector, also the Government representatives. And we have some kind of topics that we would like to discuss. But not limited for those

four topics. I would refer you. The first one is what is the most important policy and technical consideration in the development of e-identification and authentication application. That is the first one.

The second one is there a single solution to provide and secure and convenience e-identification/authentication mechanism. Third one is how to accelerate international cooperation to develop interoperable e-identification or authentication framework. And the last one is anything else to have discussion.

And the first one I would like to invite is Nantawan Wongkachonkitti. The first electronic Government agencies head of innovation department, develop, integrate and communication technology systems to achieve, establish an e-government which is the country -- effectively leverage Government's capability of management and public service systems. Let's welcome Min Hsuan Wu. Sorry. Deputy manager of Student Loans Fund Office of Student loans funds. Let's welcome again Nantawan Wongkachonkitti.

>> NANTAWAN WONGKACHONKITTI: All right. Sounds good. Actually I work for student loan. Anybody know student loan? There you go. Same faces. I used to be electronic -- using -- doing a lot of computing and blah blah. But now I'm -- I'm looking at a different angle. More like user now. So this topic -- it was interesting when Karen talked to me and said hey look, are you interested for this topic. Sounds like it is something that we use or we want to use, right? Because in my office, let me talk about my office. It will be something in the first question, what is the most important policy and technical consideration in development of e-identification/authentication application is so long. Anyway, so in my office the loan applicant, I don't want to have a paper anymore. I want to have paperless. Ease of use. No paper. No warehouse to collect. No more. Right? We don't cut the tree anymore. What do I do? How do I know that the user from suburban somewhere in Thailand is saying who she is or who he is. Right? And that's the thing that I'm looking for is e-authentication or mobile authentication. I don't know, e-authentication is out. Maybe. In Thailand mobile is everything. If I don't have mobile, just like I am naked. Seriously. Everything is in my mobile. My calendars, my life. Everything. Her names, I can't spell her last name if I don't have my mobile. Everything is here in my life.

So in terms of it I want the student or my borrower to be ease of use. That means I need to come up with something to identify her or him. That means I have to have a policy in my office saying that all right, from now on, new semester, the policy goes, every borrower, the new borrower has to download my application, right, that authenticate who she is or who he is. Whatever it is. I might have to go to the service provider and say look, put the SIM with the PKI, blah blah, whatever, ISA1024, whatever it is. The encryption

algorithm that they can provide. I don't care. As long as I can say is legal first of all. The law is good for them and for me. I'm not doing something illegal. And the borrower is not something they are responsible for when they are digital signing, right? Because I will collect them if they default, if they become default. So that's the thing.

Policy comes first. I don't care what it is. But policy drive all of this application. Without policy you can, even you have innovation, blah blah blah. But the user needs to use from the policy. My office can distinguish from now on we use this. Then the application, the innovation will come now. Everyone will come to my office and say hey look, have this. Technical. Right? So this question is really from my office or from my point of view. Yes, policy has to come up with it. We need to make sure that policy come up and it is fair for everyone. It is ease of use. Making sure that it is applicable for them and for us as the user and owner of the system. Right? And that's the thing. And really anybody has followed the loan before, any loan, not student loan, any loan. Has anybody borrowed a loan? Man, everyone rich here.

>> Yeah. The chance we can speak long.

>> NANTAWAN WONGKACHONKITTI: Okay. You want to speak?

>> That is often for what they ask the question or you keep making the presentation?

>> NANTAWAN WONGKACHONKITTI: I don't know. I'm not sure either. Okay. Go ahead and ask I guess.

>> KAREN HSIN-LING CHANG: Yeah.

(Laughter).

>> NANTAWAN WONGKACHONKITTI: I'm not sure. Go ahead. Go ahead. She said go ahead.

>> Okay. I think you know this is API. We are talking about Internet Governance Forum. So in the Internet Governance Forum we are really concerned with the mechanism. I know that PKI we know -- I think we are in this area for 20 some years. We want to know how the policy development mechanism is. It is just developing by Government topdown? Or the people can have say? Or you implement the e-identify, identification? And somebody say and the people cannot say anything or just -- we just follow it. So we would like to know what is the mechanism there to let us know how we can participate.

>> NANTAWAN WONGKACHONKITTI: Okay.

>> I think that people here know that. In the Internet Governance we really care is a process. The technology this is not new. Everyone know. And we really like to know when you implement this technology in application what is mechanism you are going to use. And there that is the point I like to raise and ask you all tell us. And so let other people have a chance to give their opinions.

>> NANTAWAN WONGKACHONKITTI: Okay. Go ahead.

>> I think South Korea is one case on point on what Dr. Wong has

said, the risk of Government's topdown approach on e-authentication. South Korea passed a law that all online payments are underwritten by a Government issued electronic certificate, PKI based. And people are required to download these certificates issued to individuals from their hard drives, on their mobile phones but because it was issued by South Korean Government it was not recognized by, you know, timing on web browsers, Chrome, et cetera. So the users had to download all these plug-ins to make it work. And as luck would have it they had to do it through active X, which Microsoft had an addendum many years ago and stop servicing, which created a lot of security risk because that trained people in to accepting all these plug-ins that cause this -- there is this untrusted plug-in and all these Koreans are trained to accepting untrusted plug-ins which created really bad hygiene, bad security hygiene. And also because so many plug-ins were downloaded they became -- there were compatibility problems among the software and with the hardware.

I am from KS Park and Civil Society worked very hard for years to abolish the law that required online payments to be backed up with Government certificates. All the decision of creating the electronic Government certificates and making mandatory and online payments, they are all done topdown without talking with users. That I wanted to back up what Dr. Wong has said with a case study in Korea. Now even with a law abolished we still have a problem because the whole industry have lacked behind, have not really developed other secure authentication methods than this Government issued certificates. So although it is no longer mandatory the banks and all the financial institutions are not investing resources in developing new ones. So people are still suffering from all this plug-ins and computers crash. And -- so, you know, what you decide topdown will have consequences for decades. Thank you.

>> KAREN HSIN-LING CHANG: Thank you Hai from Japan or Korea.

>> Korea.

>> NANTAWAN WONGKACHONKITTI: I want to make sure that what I say even the formulation of the policy is not topdown automatically. It is when -- when you talk about policy formulation, that means you have to consider the people's voice as well, but when you formulate there is a process of formulation, not laughing matter. But really the formulation of policy is not just the hearing saying right now. When the process is actually here from the voice, from the citizens but then actual law policy come down. But the formulation process is from the citizen. We heard from the people. And that's -- that's the process itself. You have to understand the process first.

>> I agree. I think in your case maybe but not necessary in other countries. So don't use your case to improve -- to say other country is doing that.

>> NANTAWAN WONGKACHONKITTI: I said my case.

>> In Taiwan doesn't do that.

>> NANTAWAN WONGKACHONKITTI: I said my case.

>> KAREN HSIN-LING CHANG: Thank you, Mr. Wong. And since we are -- we negotiated an additional 15 minutes for this session. So we have another 15 minutes. We have -- let's see, the opinions from Civil Society. We have Mr. Min Hsuan Wu and data -- his opinions have some feedback from Mr. Baek from Korea and government. Mr. Wu is a well-known activist and companion of Civil Society in Taiwan and involved in the anti-nuclear and environmental issues. His expertise and the well-known communication design and programming.

>> MIN HSUAN WU: I come from Open Culture Foundation. We care about open data and open government. And I'm also a member of Taiwan Human Rights Association. So I'm here to speak on a certain topic or opinion from Civil Society. So I think regarding this topic I think the most important what Civil Society wants is to understand how this legal framework to protect your privacy, how the data security is stored, where. And also whether or not people have the right to choice if we want the old-fashioned way only. Or we can choose which solution we want. Or we can control how much risk, like if I want to go high risk but I only want two factors because it is convenience. Can I choose or not? Or the last one is which agency can access our data. As you know if we use the EID online, they will generate a lot of new data. You don't have that before. Like metadata. Like the -- when and where you use for what purpose. And this kind of data can actually make in your whole life what you are shaping your house record, but not the detail but which dot do you see and so on.

So what's the policy and regulation to restrict Government or private sector to assess this kind of data? We didn't hear too many from that. And the second part is open standard and open source for the platform. So third can review. Like Taiwan, we have kind of like EID but it is not. Right.

>> (Off microphone).

>> MIN HSUAN WU: Yeah. Yeah. Actually it is the PKI, right? Yeah. But the private key is generated by the Government. Not generated by user. Yeah. So that's a problem. And another problem is drive or is not open source. We can only use Windows and this can't be used on cell phone and Mac. So still there is a lot of things that have to go on. And the third question is a further discussion. Now we are talking today. But the further fear is about biometric, just biologic. Right. So -- right. I think I will leave my time to others. So that's basically all I have.

>> KAREN HSIN-LING CHANG: Thank you. We have the representative from the Government that is Mr. Baek from Korea. Do you have any feedback? And next will be Vijay.

>> JONGHYUN BAEK: I think it is a very difficult issue and every country is different. I don't care full control, who making the policy or legislation or technical consideration. But just some party for -- can make some regulation, policy. Must be Government. Yeah.

And it is not for person to -- persons to the citizen just making some policy and regulation and using for safety and secure something like that. Also every private sector's company can develop technical part. So maybe it is not -- I'm not sure. Even in Korea got some problem with that. Not problem. Just some argument or some problem is faced about this kind of issue from NGO and the Government part. Anyway, most important thing is just think about the user. How can make them easier, make them convenienced, make them secure. Secure is not -- their convenience is not -- it is a little bit difficult. Making more convenience. But if there is a mechanism, security is there. So I'm not sure how can we use that kind of system. So yeah. It is my just opinions.

>> KAREN HSIN-LING CHANG: Thank you, Mr. Baek. And Vijay, you are from the private sector. Do you have any solutions to face this kind of solution? What's your opinions?

>> VIJAY KUMAR: Yes, we work closely with the Government of India also. And I think this is the matter what comes from the public generally, what is the security, the data is there with Government or any agency. This was the solution revolves around the transparency. That's why if there are technical solutions that are talking, they should not stick to closed APIs. And the ecosystem should evolve and the privacy will increase. And the open platform should be in place. You have the right points, mentioning the right words in place. It is more about open platform and also not to single programming language. It should not be something like it was only on Windows and not in maybe Linux or Macs or the mobiles of the world. So that's why the technologies around this particular topic should be very much programming language agnostics and work with any solution. And also legally talking what I also covered in my slide Government should look in to some data protection laws and privacy laws so that people can rely on the data, what is submitted to the Government. Important to build the trust in the people.

>> KAREN HSIN-LING CHANG: Thank you. Any other opinions or suggestions from the floor? Mr. Wong.

>> Kenny Wong. Two questions. First question is based on the definition of public, basically the public key and infrastructure should be well-coordinated and should be interoperable among themselves, so-called infrastructure. But in reality all the countries that PKI system are not talking to each other. Let me -- application in reality, so actually how can we make kind of well coordination among the different PKI systems not only in different countries. Even in one country they probably have different -- isolate PKI system and don't talk to each other. My first question, what matter we need to apply to resolve that kind of conflict. The matter I call in here could be multi-stakeholder model or define the legal framework. So identify what sort of architectural review is required.

My second question is usually centralized identity system has a tendency to stimulate variety application. What do you think from your opinion could be -- has potential risk that violates personal data. Because usually personal data can only be collected for a specific and one purpose. Thank you.

>> I have a question. So what happens -- so I wanted to understand like if Thailand has an EID program, what happens in the case that this is not working? From the perspective of India, we have a system that is linked to a variety of welfare schemes. Sometimes the authentications do not work in the remote areas and the citizens do not get the minimums and those people are surviving on the bare minimums. So I -- so if there is a similar situation that happens in Thailand or what's the solution to the problem when it happens?

>> MIN HSUAN WU: I have to make it brief. Look in the trade agreement. Whether it is a go from multi-stakeholder, it is not a challenge. When we use the first time we go from multi-stakeholder partial model. We listen to Committees and we bring them in to the trade negotiation sessions. We work close with several Committees, since I am working in the e-commerce.

Secondly if you read the text, several key words mentioned about the business and having a regulation, that prohibits the business is the liberty, business to choose which technology you are going to use for this interim cross-border. If there is a cap out on government policy, legitimate public policy, that okay, Government can come up with local measure to regulate certain things. If you read on WTO, necessity tests that means even if you have the legitimate policy your Government, you haven't specified this mechanism to be used. Mobile only and when you propose this, the bureau might say this is not a necessity. Not every country has created discrimination. So then that measure cannot be used.

So that is the empowerment from trade agreement that recognize the problem of the difference. I talk about this only on a context of cross-border. So try to read and put yourself in to the trade agreements that carve out a lot of Government measure and that might cause capture of regulator or regulatory. They are not free anymore. When you talk about a cross-border the community is backing you up. The most important thing I see, a challenge with the business exactly know what they are going to do. The only cross-border I'm aware of is swift and based on the technology in 70.

What else cross-border in business? And that are the preparation part, that and the private sector need to work together what initiative you want, what technology you want. Satisfying, filling the legal framework, that empower you. I think community empowerment coming, wisdom. The collaboration works. You have a unified voice, cross-border. Which are the model we are going to work is not Government following up this Forum for the business sector. How the business coming together and coming out as a single void to the

Government and saying this is what we want. This is the way we want to have it. Then I think that might -- my response is. The Government you mention about and we have that case, too. The Government Open Office, 924 and then not to mention that is the denial of service in terms of system having a compromised problem. They even closed the system. After 4 o'clock in the afternoon it is not available anymore.

I think those lot issues that the community and business have to voice. Government has nothing to do with that. That's not the issue. The other service that might have, it is just an issue of service level agreement or information or commitment that the Government need to make to the private sector.

>> KAREN HSIN-LING CHANG: Thank you all. And time is up. So if there is any other further questions, you are more than welcome to go up to the speakers to have a chat or discussion more further. Thank you very much. Thank you all. Thank you.

(Applause)

***

***