Juha Mitrunen, Ministry of Finance: Digital identity as a support of creative individuals
(translation of transcription to English)

> *"Both private and public operators can issue data into the wallet, and then the person themselves submit them to the transaction service. This also drastically changes the business model of our entire ecosystem…, because …there are dozens of issuers and hundreds of transaction services, and the person in the middle controls the traffic in between – choosing which transaction service they give certain data from their wallet."*

Thank you. Right, so brief introduction – Ministry of Finance, public-sector ICT. I'm very closely involved with a government programme project where we're trying to improve or **reform our digital identity**. This is a fitting continuation from Laura's presentation, because Laura kind of presented what we currently have, whereas I will try and present the direction to which we are trying to develop or take this. Since I'll be speaking about something that does not exist yet – you'll have to use your imagination a lot – I think it's good to start by examining it as a process: what we have now.

So how digital identity is built in Finland is that… in most people's cases, it is built already when they are born. So it is basically already in the labour ward that the identity comes into being and a person's electric identity is created into the population information system. When we create the social security number and enter the basic information on the population information system, a core identity is born. From now on, when I'm talking about core identity, I'm talking precisely about the little ball in the middle of the population information system that contains the core information on the identity. It does not change very often. You've heard that, in the Vastaamo case (serious data leak case), they're even trying to change people's social security numbers, but in principle, it usually remains unchanged. Name does not change, sex does not change; such things do not usually change. There are exceptions, but generally speaking, this is the core identity. When we make some progress from the left, an electronic identity must be linked with a natural person – in other words, they must match: this identity, this person. That's when we're usually dealing with the police, in that we're trying to create some kind of a proof for the person, with the help of which they can prove their own identity, which is in the population information system. The police usually look at a photograph and the person's face; in a physical space, they may take their fingerprints, and then they link the natural person to the core identity found in the population information system, creating a proof of it – for example, passport or identity card. With these proofs, credentials, the person will prove their identity in transaction situations from there on. Then, progressing from left to right, we're already in the penultimate section, at which point the person probably has a passport or an identity card or both, and with these the person can prove their identity. At this point, one must take note that the police are not involved anymore. The population information system is not involved anymore. One does not ask the police nor the population information

system any more questions electronically, rather the person proves their identity wherever they please. This is the basic idea of core identity. The state creates a core identity that can be proved wherever, whenever. There already exists an electronic proof, credential, it is the certificate on the chip of the identity card. In principle, a person could prove their identity in electronic situations with the help of the state-produced core identity proof. In which case, there wouldn't be any service providers in between. Unfortunately, the identity card is so difficult to use, because one should have a card reader and a laptop, and we live in such a mobile and fast-paced world right now that the mechanism is outdated – it's usability is outdated. In fact, the data security is excellent, but the usability is a bit tricky. That is precisely what we're going to develop in this project.

We have basically done the exact same thing as before, but now we're trying to come up, in addition to the physical proof, identity card or passport that is, with a third method which would be enabling the citizen to prove their core identity in both physical and electronic transactions, and it would be easier to use than the chip on the identity card. Then, from the end user's point of view, it is possible to show on one's phone, for example, one's identity card, proving one's identity, when one is retrieving a package from the mail, for example – in case one's left their wallet at home, for example. Or electronically, when one tries to, say, authenticate themselves in a public administration transaction service in a transaction situation. The only difference in… as Laura presented the method of strong electronic authentication, of which there are several: there are bank authentication method, there are mobile operators' authentication method, and as Laura said, the technology hasn't even been defined, rather they are audited, and then they examine whether it's good or not. Basically, one could conceive that competition will arise from this: there will be a new method in addition to all the other methods. But this method has a slightly different role: the idea behind is that the person themself proves their information with the method to the transaction service – and there is no operator between. There is no authentication service or mediation service in between: the transactions truly take place between the person and the transaction service. This also creates difficulties: the transaction service itself must build such technical functionalities that enable it to verify and check the digital proof, whether it's still valid, whether it's authentic, whether it's actually good. Presumably most transaction services don't bother doing that themselves. Some of the big ones may do that themselves, but most still request verification and validation from an authentication service or a mediation service or some other service provider. As a result, authentication services remain in the picture, but one can say that, if a transaction service wants to do that from beginning to end themselves, it is possible. That's the idea behind core identity.

Now if we think about what it is that actually has to be executed in the government programme project, what are the new things that we seek to create here, the very first thing is that the state should, first of all, be able to produce electronic methods. If we cannot produce them, we cannot make such a solution. Then if we move on, we come to things we cannot do in our current strong electronic authentication. For example, it

is not possible to authenticate foreigners, because they have no Finnish bank IDs or a SIM card from a Finnish mobile phone operator. Foreigners also tend not to have their information on the [Finnish] population information service, so we are forced to do some homework, in addition to which we have to think about how one goes about registering a foreigner – they don't necessarily go to the police either; there are many cases where foreigners have no intention to come to Finland: they do the transactions abroad, in their home country, with Finnish services for whatever reason but don't even plan on visiting Finland or working in Finland or something like that.

In these cases, we have to think about how such a person can be registered remotely. How can we authenticate the person's identity in order to create the method of identification – when they're never present? In those cases, we may have to resort to a take-a-picture-of-your-face, take-a-picture-of-your-passport type of solution. We also have to think about what to do with minors, because in principle, things are analogous with passport and identity card: minors also get passports and identity cards. As to what to do with minors, for we have no possibility… for example, banks enable a sort of liability agreement: the bank gives their client the method, but the client signs a liability agreement, stating that they are responsible for it and that they will take good care of the method, and in case they don't do that, the bank has no liability. The state cannot make such an agreement with a citizen.

Instead, we actually have to create the method or instrument of authentication in a way that requires no liability agreement – or we cannot request for one. Currently, there is also an in-between group or an incomplete part of our extremely fine system of strong electronic authentication: there are some cases – it may be a question of cognitive disorder, some kind of an impairment, or alternatively, the person simply does not own a smartphone. In those cases, we have to consider an alternative method, because our primary idea is to make a mobile application, but depending on the results of our studies as to how many people incapable of using a smartphone with a data connection remain, we also really have to assess whether we have to make an alternative method – a USB stick or something similar – for those people who, for whatever reason, are incapable of using the primary method.

This leads us to cross-border authentication. When you authenticate yourself across borders: say, a Finnish person uses a German public-administration service, digitally. There are three things: the German public-administration service does not know our Trust Network, nor is it integrated with it in any technical way. Nor does it know whether it can be trusted or not. Nor does it really know how to pay – there is no agreement between the German public-administration service and the provider, say, a bank. All those things are missing. In that case, authentication must be transmitted from Finland to an EU country – in other words, you do cross-border authentication. It is a task that intrinsically belongs to states, but it leads to problems: the state guarantees a method of authentication, the state pays for the authentication, and the state takes care of the integration points for the German public-administration service so they can do it. That's why it would be very natural for it to also be a state-produced method with which the

authentication is done. You end up with a lot of trouble if you try to integrate all Finnish banks and mobile phone operators with a mediation service, and there are also trust issues, for the German would like to audit all banks and mobile phone operators before they approve of the method of authentication. That's why it would be more natural to do with the state-produced method.

The final section is about **the wallets, into which they collect data concerning identity.** But the collected data is verified. That means it's not just whatever data, it's not MyData, it's not a personal claim – what it is it's an attribute that some party has verified. Then they make a proof of that which is put into the wallet. In our case, it's mostly about, for example, right to drive or firearms permit or permit to fly or, say, fishing permit. They are permits, rights or data verified by someone in public administration. It is already common today that it gives the person some sort of a proof of it: a document or a card of some kind. But with wallets, all the different digital proofs granted to people can be kept in the same wallet. And one must be careful: we will not get very far while the project is on, until 2022. So I'm sure it will not include everything as of yet. For example, there is much discussion on corona vaccination certificate and whether it should be in the wallet, in which case one could prove that they are vaccinated or that they have had corona, wherever they are. Things like that. But you have to be very… you must not let your imagination run wild; I'm sure that the wallet we'll have made by 2022 will be very simple, and a fancier version will be developed at a later point. If I still have time, I'll discuss the wallet for a bit.

Laura mentioned that eIDAS will be undergoing a reform. The European Union is going to reform their eIDAS specification, in which identification is specified, along with electronic signature practices. According to foreknowledge… note, this is not conclusive, for this is only a rumour. According to foreknowledge, the EU is at least trying to enable such wallets, which would practically mean that the concept of authentication would get broader from what it is currently, i.e. authentication for us means identification. It's mostly just one's name and social security number that we verify and forward to the transaction service. Here, they have clearly broadened the concept in a way that there is the core identity in the wallet, in addition to which there are verified claims: for example, vaccination certificate or certificate of the person's right to drive a passenger car.

The person collects these certificates in their wallet – from different issuers. So there are several issuers. It is not just a bank or a mobile phone operator, rather there are several issuers. Both private and public operators can issue data into the wallet, and then the person themselves submit them to the transaction service. This also drastically changes the business model of our entire ecosystem, because there is not just a single authentication service to take care of everything, with transaction services being only connected to it. Rather there are dozens of issuers and hundreds of transaction services, and the person in the middle controls the traffic in between – choosing which transaction service they give certain data from their wallet. This is all in the future – I am not saying that this will be completed by 2022. What I am saying is that something like this is

upcoming, and a poor man's version might be completed by 2022. That's it actually. Thanks.