WORKSHOP 4: SYNERGIES OF THE COPYRIGHT INFRASTRUCTURE
16 February, 2021

Laura Kolinen, Ministry of Transport and Communications: Means of electronic authentication
(translation of transcription to English)

> *"…it can also be possible that we have some other reliable electronic authentication, but not necessarily strong [authentication], … For example, in anonymity cases where the person does not want it or where it's not necessary to transfer any data concerning the person's identity, I could see it would be linked in some cases with copyrights – for example, the author wants to remain anonymous, yet there is a wish to convey the information that they hold the copyright for a certain work."*

So I'm Laura Kolinen from the Ministry of Transport and Communications, from the data department and safety unit. Issues pertaining to strong electronic authentication, and especially matters related to legislation are on my responsibility. So look at what "strong electronic authentication" actually means. To put it very simply, it means authentication of one's identity electronically. So it's kind of similar to how we may use an identity card or a driving licence or anything that proves our identity to prove who we are when we're performing face-to-face transactions – in strong electronic authentication, you do that in the electronic realm. From the user's point of view, I can prove who I am to the service that I wish to use, but the electronic transaction services can also – through strong electronic authentication – identify their own users and those who log in to the electric services and stuff like that. Strong electronic authentication is done by electronic identification tools – the most used ones in Finland are bank IDs as well as mobile certificates used by telecom operators. In addition, we have the state-granted citizen certificate on our identity cards. But what happens in practice is that you undergo a strong electronic authentication when you, for example, log in to Kela (social services) or Tax Administration with your bank ID, or with your mobile certificate, or something like that. So that's what strong electronic authentication practically is. Then we could move on and discuss what makes electronic authentication strong. Strong is kind of the same thing as **secure, information-secure, reliable, but in the law, strong is the term used.** Technically speaking, authentication can be based on different methods, so there has not been any technical standardisation, nor has it been ruled that it must be based on certain technical things; however, there must be certain elements in order for it to be strong authentication. At least two of these three should be included in the technical system in order for it to meet the standards of strong authentication. The first factor or element is that the person **must know a certain thing**. For example, a password, a PIN code, or some other thing that the person knows with regard to the system. The second element may be something **that is possessed by the person**, so for example, that you have a PIN entry device, or your phone has an application in which you enter the PIN code, or something similar that you separately possess, which is also different from something that you know. The second element can also be an intrinsic factor, such as something based on a person's physical feature – for example,

fingerprint authentication, which is available in many phones these days. If two out of these three elements are included in the system, one can speak of strong authentication. These factors contribute to the security and reliability of the authentication method.

So what are the benefits of strong electronic authentication? Why would we use such methods that are sometimes technically demanding just to authenticate one's identity? Our society is in the process of digitalisation, and services are becoming more and more electronic instead of physical, and the range of those is getting wider and wider. At the same time, when those services in the physical world that have demanded authentication of identity also in the past become electronic, reliable authentication in electronic form is a prerequisite – or at least it should be a prerequisite. If there's one thing that one should keep in mind regarding strong electronic authentication, it is that security and reliability are in key position – in other words, the user can securely transmit their identity or personal data to the electronic service provider, and the transaction service or the electronic service to which the person's data is securely transmitted can trust that the data is correct. If we were to compare this to so-called weak authentication methods which can be, say, based on the username plus password mechanism.

We just discussed the technical demands, so at least in my view, the personal data is more secure through strong authentication than through a username plus password login, for I think it is easier to crack and modify a username and a password for someone to whom one wouldn't necessarily want to give the personal data. Next, we could quickly discuss how this is regulated in the law. Well, the Act on Strong Electronic Identification and Electronic Trust Services belongs to our administration, and the legislation is, indeed… one could even describe it market regulation in some respects, but in addition, the regulation includes requirements concerning information security and other rights and duties that users have. But I think that it in a nutshell – perhaps the one thing that one has to keep in mind regarding legislation is that, in Finland, the legislation and electronic authentication services have been for a long time in a market-based manner, which is not necessarily the case in all EU countries; in some member countries, the state may play a bigger role.

And then I'll quickly mention that **national regulation is consistent with the EU eIDAS** regulation concerning cross-border electronic authentication in the internal market. The reform work will begin in 2021, so this spring. But that's it for the legislation. Perhaps the reason I'm here to talk to you is, first of all, that we get an understanding on strong electronic authentication but also on future trends. One trend is that strong authentication will become more commonplace. The more services become electronic, the bigger the risk of infringements on data protection and data security. That's why strong authentication and requiring it in transaction services can prevent identity thefts, for example, and if personal data has been accessed through an infringement on data security or a data protection breach, strong electronic authentication secures the use of personal data in other contexts.

However, in the future, it can also be possible that we have some other reliable electronic authentication, but not necessarily strong, so we may encounter situations that don't necessarily require the data on identity, so that it is not necessary to in order to give information as to who you are to use the transaction service. For example, in anonymity cases where the person does not want it or where it's not necessary to transfer any data concerning the person's identity, I could see it would be linked in some cases with copyrights – for example, the author wants to remain anonymous, yet there is a wish to convey the information that they hold the copyright for a certain work. So this can be a need in the future, and this is also related to that they may want only to convey some of the information, say, convey the copyright information through reliable authentication. There are several such discussions on a national level and also on the EU level, so as I said, since the reform work around the eIDAS regulation is about to start, they're discussing on the EU level as well that it should be possible to transmit only a portion of the information so that the identity should be kept secret in some cases, or that the information wouldn't be necessary to transmit. But maybe that concludes my presentation, and I'm glad to hear any questions you may have. Thank you.