# Overview of practices and legal framework of eID in FInland

LL.D, Prof. Olli Norros

# Introduction

- The scope of the presentation
  - Which actors grant eID in Finland?
  - Which private and public services are available in Finland using eID?
  - How function of eID, and particularly the consequences of unauthorised use, are regulated in Finland?
  - Case examples regarding unauthorised use of eID

# Which actors grant eID in Finland?

- Banks
  - Lists of identification numbers on paper, which were needed to access online bank services, were used also for identification in other services
  - Lists on paper have been nowadays mostly replaced by mobile apps and separate electronical identification devices

- Telecom operators
  - Telecom ops grant ”mobile certificates” attached to SIM card to be used in mobile phones etc.

# Which actors grant eID in Finland?

- Others
  - Finnish Digital Agency (state authority) grants eID attached to official identification cards
  - Even other organizations such as employers may attach eID to their identification cards
  - Rare in practice → bank IDs and mobile certificates dominate

# Which private and public services are available in Finland using eID?

- About 60–75 % of all identifications concern public services
  - Proxy domain suomi.fi maintained by Finnish Transport and Communications Agency (state authority)
  - Tax authority, actors of public health care, welfare authorities etc.

# Which private and public services are available in Finland using eID?

- The rest of identifications concern services of private and third sector actors (associations etc)
  - Banking and investment services, online pharmacy, private health care, insurance companies, telecom services, electricity retail etc.
  - Electronical signing services for different organizations and their clients

# How function of eID is regulated in Finland?

- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market
  - No provisions on ID holder's liability of unauthorized use

- *Lag om stark autentisering och betrodda elektroniska tjänster* (7.8.2009/617, "Act on Strong Electronic Identification and Electronic Trust Services", hereinafter "FinEIDA")

# How function of eID is regulated in Finland?

- FinEIDA sec 27
  - Structure
    - The main rule: ID holder is not liable for unauthorized use
    - The requirements for liability (subsection 1)
      - “1) he or she has made the use of the identification means available to someone else;
      - 2) the loss of the means or unauthorized possession or use is the result of the holder’s ~~gross~~ [other than mild] negligence, or
      - 3) the holder has failed to notify the identification service provider or a designated party that the means has been lost, is in the unauthorized possession of another person or of any unauthorized use immediately upon detection of this fact.”

# How function of eID is regulated in Finland?

- Structure of FinEIDA sec 27 (cont)
  - Defences (Subsection 2)
    - “However, the identification means holder shall not be liable for unauthorized use:
    - 1) to the extent that the identification means has been used after the holder has reported to the identification service provider of the loss, unauthorized possession or use of the means;
    - 2) if the identification means holder has not been able to report the loss, unauthorized possession or use of the means without undue delay after detecting it, because the identification service provider has failed to perform its obligation referred to in section 25 subsection 2 to ensure that the holder can report at any time; or
    - 3) a service provider using identification services has failed to check the restrictions on use or prevention or blocking of the means as set out in section 18 subsection 4 or section 25 subsection 5.”

# How function of eID is regulated in Finland?

- FinEIDA sec 40
  - Special rule on liability for the unauthorized use of a signature or an electronic seal creation data [more strongly encrypted method than "normal" eID]
  - Main rule (sec 1):
    - "The signatory and the holder of an electronic seal is liable for the damage caused by unauthorized use of an advanced electronic signature and an electronic seal creation data certified by a qualified electronic certificate, until the certificate revocation request has arrived to the certification service provider as laid down in section 39 subsection 2."
  - Exception regarding consumers (sec 2):
    - "~~The user~~ [a consumer] shall only be responsible pursuant to subsection 1 if:
      1) he or she user has given out the creation data to others;
      2) the unauthorized use of the creation data is the result of the user's ~~gross~~ [other than mild] negligence; or
      3) he or she has lost control of the creation data in other ways than set out in paragraph 2, and has failed to request the revocation of the qualified certificate as provided in section 39 subsection 1."

# How function of eID is regulated in Finland?

- Observations
  - ID holder's liability of unauthorized use is based under Finnish law on explicit legal provisions
    - Cf the peculiar and illogical application of the non-satutory doctrine of *tillitsfullmakt*
  - FinEIDA sec 27 leaves open whether the liability of the ID holder is a) full liability of the unauthorised legal act or only b) liability of damages of the third party
    - FinEIDA sec 40: liability for damages (negative interest)
    - Finnish Supreme Court KKO 2016:73: sec 27 creates full liability (option a) above)
      - Criticized in legal literature by Prof. Mia Hoffrén

# How function of eID is regulated in Finland?

- Observations (cont)
  - Finnish law contains analogous rules on liability of unauthorized use of different electronical services
    - Consumer Protection Act (*konsumentsskyddslag* 20.1.1978/38) ch 7 sec 40 on unauthorized use of credit card
    - Payment Services Act (*betaltjänstlag* 30.4.2010/290) sec 62 on unauthorized use of instrument of payment
    - Act on Electronical Communication Services (*lag om tjänster inom elektronisk kommunikation* 7.11.2014/917) sec 125(2) on unauthorized use of a telecom service

# Case examples regarding unauthorised use of eID

- Finnish Supreme Court case KKO 2016:73
  - B had kept papers presenting their user name and password list in drawer shared with their spouse C. C had been aware of the papers and had had access to them. C had raised an instant credit in B's name using B's user name and password list. C was sentenced for a fraud. B was regarded as having stored the identification documents showing other than only mild negligence. Because of this, B was regarded as being responsible for the credit by virtue of FinEIDA sec 27.

# Case examples regarding unauthorised use of eID

- Finnish Supreme Court case KKO 2018:71
  - Attorney A had kept their credit card in their wallet and a paper presenting the PIN code relating to the card in a drawer in their office. A had left the office for 10 minutes the door being unlocked and the wallet on their desk. An unknown person U had entered the office and taken the wallet and paper presenting the PIN code. Thereafter U had drawn cash out of A's account on ATM. The Supreme Court held that A's conduct as regards storing of the wallet and the PIN code had been negligent but not grossly negligent. Because of this, A's liability of the unauthorized use was limited to 150 EUR by virtue of Payment Services Act sec 62 (vote 3–2; the minority regarded A as having shown gross negligence)

# Case examples regarding unauthorised use of eID

- FINE Banking Complaints Board case FINE-020522 (2020)
  - ID means to a bank A consisted of user name, a password created by the user and a list of passwords on a card. A's customer C had kept a paper presenting their user name in a plastic folder send by the bank and kept the folder in their backpack in a zip fastened pocket. C had kept the password card in their wallet. The self created password was only in her mind. C's then spouse S had succeeded in peeking the self created password when C used online bank. S had also found the paper presenting the user name paper and the password card. Using these and the password created by C S had raised instant credit from a bank B several times during 2016 and 2017.

# Case examples regarding unauthorised use of eID

- Case FINE-020522 (2020) (cont)
  - BCB compared the case to the Supreme Court case KKO 2016:73 and noted that the facts were mostly simililar with the exceptions that in the present case C had stored their username and password card separetely, and C also had a self created password only in their mind. BCB also noted that even though C could have noticed the earlier credits raised by S in their tax proposal recieved in spring 2017, ommission to notice them there does not reflect too severe negligence. All in all, BCB held that C could not be accused for anything but mild negligence, and because of this, was not responsible of the credits by virtue of FinEIDA sec 27.

# Case examples regarding unauthorised use of eID

- BCB case FINE-033198 (2021)
  - A fraudster F had called in A's phone and represented themselves as employees of Microsoft. According to F, they needed a remote access to A's computer to be able to remove hackers using the computer. In addition, A was requested to accept installation of anti-virus software using their eID and pay a charge of 5 EUR. A had complied with these requests and input their eID passwords to web pages which appeared as genuine web pages of Microsoft and A's online bank. In reality, F had performed several payment transactions on behalf of A using A's eID information. The contact between F and A had lasted about a hour and half.

# Case examples regarding unauthorised use of eID

- BCB case FINE-033198 (2021) (cont)
  - BCB held that F's conduct had been so well prepared and convincing to the victim that any detail in F's conduct as such had not given A a particular reason to doubt F's conduct. However, the event as a whole – F's self-motivated call, granting of the remote access and several confirmations using eID had given A a reason to understand the true nature of F's conduct and to interrupt it. BCB held that A had acted negligenty but clearly without gross negilgence. Thus, A's liability of the payment transactions was limited to 50 EUR by virtue of the Payment Services Act sec 62.

# Conclusions

- The legal status in Finland is based on domestic special rule FinEIDA sec 27, not on extensive application of the non-statutory doctrine of *tillitsfullmakt*
  - Application of FinEIDA sec 27 appears as neutral in case law, albeit one may ask should the threshold of user's liability be gross negligence instead of 'normal' negligence, cf Investment Services Act sec 62
  - In addition, one may ask should the legal consequence of user's liability be liability of the opposite party's costs instead of the unauthorized legal act, cf FinEIDA sec 40