Regulatory framework for the digital society: legal requirements for authentication and signing

Dr. Katrin Nyman-Metcalf

Senior Legal Expert

eGA.ee

The key legal message

- There should not be too many specialised laws
- Laws should be technology/neutral
- The legal issues are largely horizontal
  - *Digital Identity*
  - *Data protection*

eGA.ee

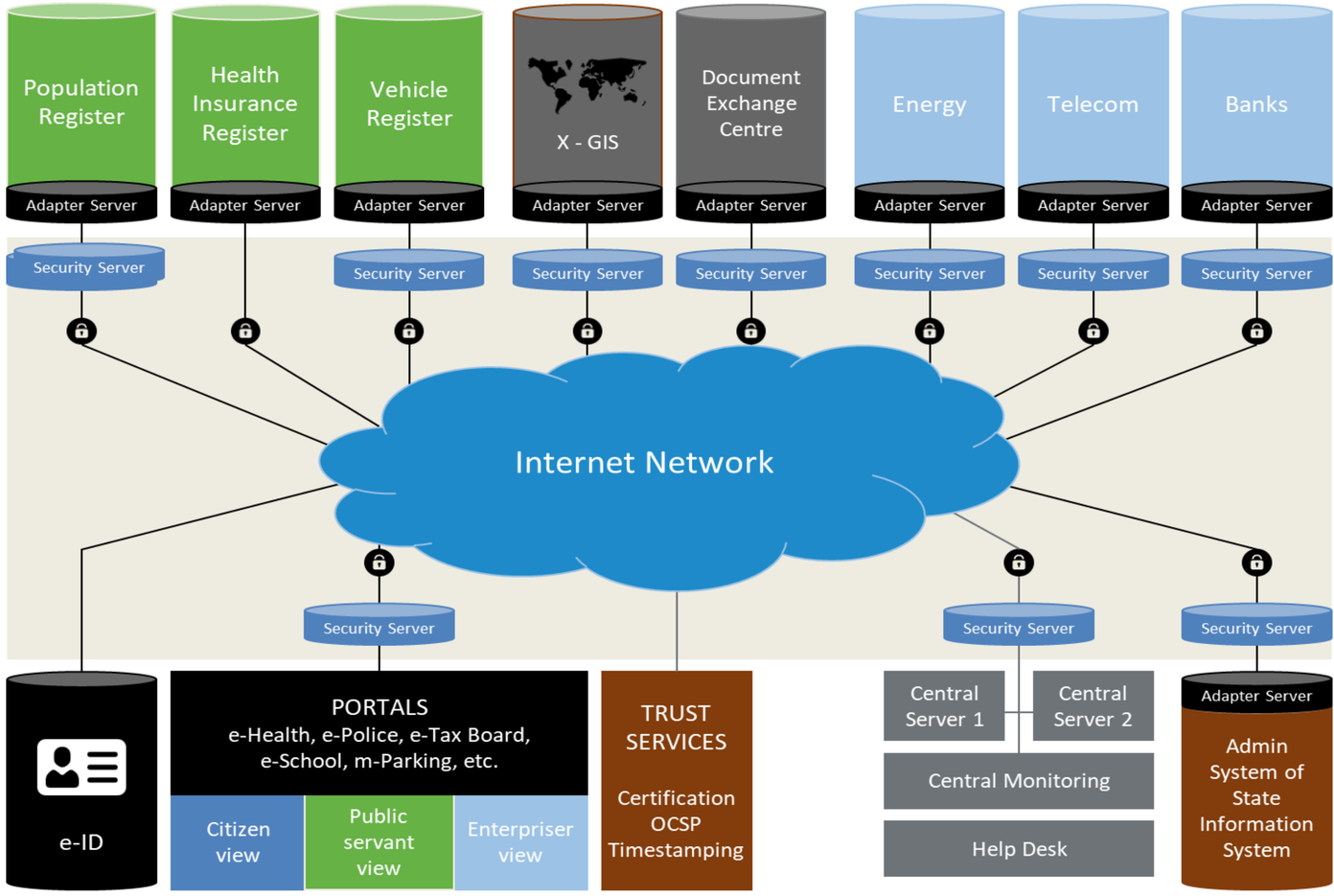
What is different without paper?

- The need for technology including access to internet for use of services
- Easier to have access to (public) information
- The necessity to accept digital data in all contexts (until as evidence in court)
- Move away from concepts like original and copy – the data and not its representation holds the value
- The possibility to identify oneself digitally

So not much work for lawyers…?

- Analysis of existing legislation: are there any obstacles?
  - Requirements of form, obstacles to interoperability, etc.
- Specific legislation on horizontal issues
  - Digital identities/signatures
  - Data Protection
- Organisational issues: legal competence to require what is needed for interoperability
- One of the key aims if to create trust!

- Once only. Citizens never have to provide the same information twice. No duplicated data
- Not greater access to data than what is needed – strict requirements for access
- Access to any personal data only after identification – footprint of data access
- Not one centralized database
- Sufficient rules for interoperability of databases
- Conditions for joining (agreements)



“The Brussels Effect”

- Influence of EU tech regulation (eIDAS, GDPR):
  - Global companies adopt EU (strict) rules for all their products and markets to avoid having to comply with multiple regimes.
  - EU rules as “gold standard”
- For the EU all rules have as a principal aim to facilitate intra-EU relations (mutual recognition, etc.) – for non-EU members this aspect is not relevant but rules serve as standards
- Proposed regulation on Artificial Intelligence (21 April 2021)
  - Focus on greatest risk (subliminal techniques banned, strict rules for facial recognition etc.)
  - Anchor in fundamental law that algorithms are transparent, verifiable, and fair and that essential decisions remain with humans

One of the key legal issues,
a prerequisite for
e-governance

Digital identity/ signature

- What is the (legal) role of a signature (identification)?
  - Different roles in different contexts: When this is understood, it can be recreated electronically

Signatures are expressions of identity

- What are the key elements that need to be created?
  - Ensure that the person is who he/she claims
  - Possibility to identify one individual (only)
  - Durability of identification
  - Ease of use

eIDAS

- *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market*
- Signatures are expressions of the identity, a way to express consent – not an authentication as such (as previously in EU eSignature Directive)
- Enhancing trust in electronic transactions through common rules, easy of cross-border transactions – reference to data protection rules
- Different assurance levels (STORK, ISO 29115) – low, substantial, high
- Trust service providers: entities that ensure the reliability of the identification scheme
- Agreements can be made with trust service providers outside of the EU

Identification and signature

- Technology neutrality: achieve the different levels with different technology
- Electronic signatures should not be denied legal effect because of their electronic nature
- Law can stipulate specific requirements for the signatures
- Remote electronic signatures or signatures where the device is controlled by the signer
- Electronic seals (also for legal persons)
- Authentication mechanisms: how persons use the electronic ID to confirm identity

Data protection

- The digital society must not undermine people’s sense of security or the protection of their fundamental rights. (Perceptions!)
- The law should focus on content of data rather than its form.
- Some data protection issues are the same regardless of traditional hard copy or electronic form. There are different risks involved with electronic data as well as ways to use technology for better protection.
- Data protection is a key issue in a modern information society - Human right to privacy (Article 7-8 EU Charter, Article 8 ECHR, etc.)
- GDPR – General Data Protection Regulation, in force May 2018. Global relevance.
- Importance of implementing structures (Data Protection Authority or similar).