How much PKI is in: PSD2; eIDAS; GDPR,

24.10.2018

DIPL. WIRTSCH.- ING. ARNO FIEDLER

NIMBUS TECHNOLOGIEBERATUNG GMBH

- Single Market of Goods
- Single Market for Services
- Stronger European Networks
- ....

SEPA
Single Euro Payments Area

Regulatory Technical Standards (RTS) of Directive (EU) No 2015/2366 (**PSD2**)

Article 29 Traceability

./. payment service providers shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following:
./. **timestamps** ./.

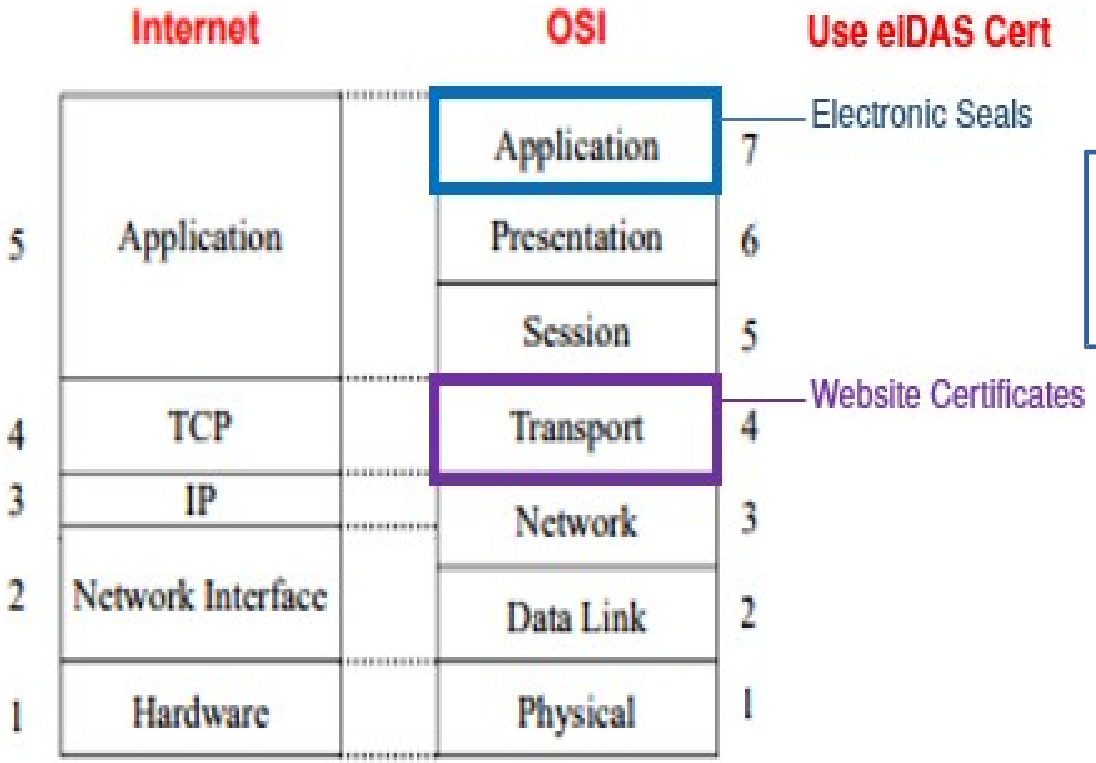
Article 34 Certificates

For the purpose of identification, ./. payment service providers shall rely on **qualified certificates for electronic seals** as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for **website authentication** as referred to in Article 3(39) Article 35

Security of communication session

1. ./. exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and **widely recognised encryption** techniques.

eIDAS meets PSD2 (Slide from ETSI Workshop Luigi Rizzo, InfoCert)



It's important to know that QWAC and QSEALC Certificates are used for different purposes and effects.

QSEALs provide:
- Identification
- Integrity

QWACs provide:
- Identification
- Confidentiality

Some of the key provisions of the GDPR require to:

Implement technical and organizational measures to ensure data security appropriate to the level of risk, including “**pseudonymisation and encryption** of personal data." (Article 32)

Have in place "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing." (Article 32)

Safeguard against the "unauthorized disclosure of, or **access to, personal data**." (Article 32)

GDPR Article 32 – Security of processing

./. the controller **and** the processor shall implement appropriate technical and organisational measures to ensure a level of security **appropriate to the risk,** including inter alia as appropriate:

- **the pseudonymisation (by PKI?)**
  and encryption (by PKI?)
  of personal data;
- the ability to ensure the ongoing
  confidentiality, (by PKI?)
  integrity, (by PKI ?)
  availability and resilience of processing systems and services;

GDPR Conclusion

Implementing PKI with Certificates/Credentials and Policies

seems to be a SHALL to cover the technical and organisational measures

eIDAS Requirements for every **public** TSP

05	13	15	16	19
Data processing and protection	Liability and burden of proof	Accessibility for persons with disabilities	Penalties	Security requirements

PrimeKey NIMBUS

Art. 5 – Data processing & protection

1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC. (*will be updated to GDPR)*

2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.

PrimeKey NIMBUS

Art. 13 – Liability & burden of proof

1. TSPs shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with obligations.

   The intention or negligence of a QTSP shall be presumed unless damage is proven to have occurred without intention or negligence.

2. Advanced notification about limits to use of service absolve liability for damages arising from uses exceeding those limits.
3. To be applied in accordance with national rules on liability.

PrimeKey NIMBUS

Art. 15 – Accessibility for persons with disabilities

1. Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

Art. 16 – Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive.

Art. 19 – Security requirements for TSPs

1. QTSPs and non-QTSPs shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the **latest technological developments**, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, **measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders** of the adverse effects of any such incidents.

PrimeKey NIMBUS

Art. 19 – Security requirements for TSPs

2. QTSPs and non-QTSPs shall, without undue delay but in any event **within 24 hours** after having become aware of it, **notify the supervisory body**… of any breach of security or loss of integrity that has a **significant impact on the trust service provided** or on the **personal data** maintained therein.

   Disclosures will be assessed concerning public interest.

PrimeKey NIMBUS

Art. 19 – Security requirements for TSPs

3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.

eIDAS and Distributed Ledger Tech:

eIDAS Preamble: (part of the applicable law)

(26) Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.

(27) This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met

Putting together eID and Trust Services in Europe can cause the “blue Wonder” for PKI

Or on global scale:

United Nations Commission on International Trade Law
Working Group IV
(Electronic Commerce)

Putting together eID and Trust Services in Europe can cause the “blue Wonder” for PKI

Many Thanks!

Arno Fiedler

www.nimbus.berlin