European Signature Dialog

Don't fragment the Digital Single Market!

Make eIDAS 2 even more powerful by deleting recital 31a

On 9th February ITRE has voted on eIDAS[1] that establishes a framework for a European Digital Identity. The European Signature Dialog[2] would like to support the upcoming trialogue and draw the attention to an important point that can make eIDAS even **more powerful and coherent.**

ITRE has, *unlike* the Council and the Commission, introduced recital 31a. This recital is built on top of recital 49 of the current version of eIDAS, adding: "*In determining the legal effects of signatures Member States should take into account the principle of proportionality between the judicial value of a document to be signed and level of security and cost that an electronic signature requires. To increase the accessibility and use of electronic signatures Member States are encouraged to consider the use of advanced electronic signatures in the day to day transactions for which they provide a sufficient level of security and confidence. The use of qualified electronic signatures should be mandated only when the highest level of security and confidence is required.*"

Although this is a recital, it offers information on **how the Regulation shall be read and understood**.

eIDAS was created to establish a common foundation for secure electronic interactions, a harmonized framework for the delivery of services recognized across Europe. As a result, Trust Lists and Trust mark exist and are highly used, and currently 254 qualified trust services providers offer qualified certificates for electronic signature, recognized across all member states.

Recital 31a is encouraging member states to consider other types of electronic signatures with legal effect and to establish national enclaves. The result of such approach can only be the **fragmentation of the digital single market** and returning to the situation that existed while Directive 1999/93/EC was in force.

Recital 31a is also not coherent with and contradicts the current legal framework, ENISA Guidelines[3] and also the future legal framework, that is under preparation.

---

[1] Regulation (EU) No 910/2014.

[2] The European Signature Dialog (ESD) represents the leading Trust Service Providers (TSPs) that enable secure digital interactions across Europe every day.

[3] ENISA Security guidelines on the appropriate use of qualified electronic signatures, https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures

From the **current** legal framework and guidelines, Recital 31a contradicts

⇒ **eIDAS principles** regarding:

- trust of SMEs and consumers in the internal market – recital 28.
- Level playing field for the security and accountability of operations and services of QTSP – recital 36.
- Building trust across market operators and confidence and convenience of on-line services – trust mark and easy recognition of QTSP (recitals 46 and 47).
- Cross border interoperability – recital 54.
- Qualified electronic signature validation shall be easy and convenient for all parties at Union level – recital 57.
- Reducing the cross border legal effect of Qualified Electronic Sigantures established in accordance with Article 25.2 of the eIDAS Regulation.

⇒ **NIS2 directive** - Article 24 Use of European cybersecurity certification schemes:

> In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. **Furthermore, Member States shall encourage essential and important entities to use qualified trust services.**

⇒ **ENISA Security guidelines** on the appropriate use of qualified electronic signatures:

> "***dependability*** *[of advanced electronic signatures]* ***is still lower than that of a QES because the signatory may be required to prove the security of the technology being used if the validity of the signature is disputed before a court.*** *This requires* ***significant costs and efforts*** *that could be avoided with relative ease by opting for the more* ***established and standardised*** *advanced and qualified signature solutions. It may also be the case that* ***the relying parties have no applications or tools to validate such signature, when not based on standards;*** *in such a scenario, the signature may be legally valid and technologically robust****, but of limited use.***"

From a **future** legal framework, the recital contradicts:

⇒ eIDAS 2.0 itself, as the new version of the Regulation is about harmonization and services recognized across EU, including the availability of Qualified Electronic Signature Services through the wallet.

⇒ Cyber Resilience Act[4] that asks for the usage of certified products.

[4] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020