



Hackhofergasse 5/16

A-1190 Vienna

phone: +43 676 9409309

office@european-signature-dialog.eu

ESD comment on the Commission Draft Implementing Regulation¹ based on the Cyber Resilience Act (CRA)

The European Signature Dialog (ESD) stands as the pinnacle consortium of leading European Qualified Trust Service Providers (QTSPs), facilitating secure digital interactions across Europe every day. ESD has successfully collaborated with all institutions leading up to the adoption of eIDAS 2.

We would like to take the opportunity to comment on the draft of the implementing act based on the Cyber Resilience Act (CRA). We welcome the European Union's efforts to strengthen the cybersecurity of digital products.

However, we would like to point out a potential overlap and inconsistency that could arise from the application of the CRA to Qualified Trust Service Providers whose services and associated software components are already subject to comprehensive regulatory requirements and conformity assessments.

Qualified Trust Service Providers provide qualified and non-qualified trust services in accordance with Regulation (EU) No 910/2014 (eIDAS Regulation) and 2024/1183. This includes a variety of services such as electronic signatures, electronic seals, time stamps, and website authentication and other services. The provision of these services requires the use of complex systems, including background services, authentication applications, and signature release apps.

¹ Commission Implementing Regulation on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council

These systems and the associated processes are already subject to strict requirements regarding security and operational reliability in accordance with the eIDAS Regulation and the standards and regulations based thereon. In particular, as a QTSP, we must take appropriate technical and organizational measures to manage the risks to our services and report incidents. This also includes the physical security of our services.

Qualified Trust Service Providers must also undergo conformity assessments to demonstrate compliance with the requirements of the eIDAS Regulation. These assessments are carried out by accredited conformity assessment bodies.

Furthermore, we adhere to relevant ISO certifications (e.g. ISO/IEC 27001), as well as to relevant European standards such as ETSI EN 319 401, which sets out general requirements for the policy of Qualified Trust Service Providers, including cybersecurity requirements based on NIS2, thus ensuring robust, proven cyber defense practices. The ETSI EN 319 411 series of standards also lays down specific policy and security requirements for Qualified Trust Service Providers issuing certificates. The ETSI EN 119 461 probably part of the upcoming implementing act for Art. 24 of eIDAS regulation will regulate in detail the identity systems and applications used for the registration to a qualified trust service.

We note that the CRA introduces horizontal cybersecurity requirements for products with digital elements (Article 3 (1) CRA regulation). In the draft implementing act the "9. Public key infrastructure and digital certificate issuance software", core of any QTSP system, is explicitly mentioned as an important and critical product. While we understand the need for such requirements for a wide range of products, we see a **significant overlap** with the regulatory frameworks already applicable to us. Our entire background services, as well as specific applications such as authentication and signature apps, are integral components of our regulated qualified trust services and are already subject to comprehensive security audits and conformity assessments. This includes the whole qualified trust service and by this also the "remote data processing" related to these apps as mentioned in Article 3 (2) CRA.

A potential inconsistency arises from the fact that third-party signature applications that interact with our regulated services could potentially fall under the scope of the CRA, while the core components of our already regulated services would also be subject to the requirements of the CRA. This could lead to **duplication of requirements and unnecessary administrative burden without generating significant added value for cybersecurity**.

We believe that the cybersecurity of qualified trust services and their associated components is already adequately addressed by the specific requirements of the eIDAS Regulation and the associated implementing provisions and standards including NIS2 directive and implementing acts.

The eIDAS Regulation was specifically developed for electronic identification and trust services and takes into account the specific risks and requirements of this sector. Qualified trust service providers, by definition, must meet "qualified" levels of security and reliability, often **exceeding baseline standards found in generic cybersecurity frameworks**. To our view, the CRA aims to address widespread cybersecurity deficiencies in mass-market products or generic digital services.

By contrast, QTSPs operate in a narrowly defined, high-assurance segment, delivering cryptographically secured trust services. Including them in broad, horizontal legislation might be disproportionate, given we have a specialized, more rigorous regime already.

Exempting QTSPs from CRA coverage will maintain clarity in the EU's regulatory architecture: the eIDAS framework will remain the primary framework for trust service providers, while the CRA will apply to other products or services not covered by specialized legislation. This will avoid contradictory reporting lines, compliance duplications, or potential fragmentation in how TSPs are supervised.

Including QTSPs in the scope of the CRA and subjecting us to its requirements, in addition to the eIDAS requirements already imposed on us, would create redundant compliance demands, forcing QTSPs to meet overlapping or potentially conflicting rules. This could inflate costs, lead to confusion about which framework applies first, and spark never-ending discussions among industry stakeholders, partners, and clients.

Ultimately, such duplication will not only slow innovation in trust services without improving security but will also undermine the credibility of the EU's legislative actions.

Against this background, we respectfully request the European Commission to explicitly exclude Qualified Trust Service Providers and the software components necessary for the provision of their services including all smart cards or similar devices including secure elements according Annex II No. 3 eIDAS Regulation from the scope of the Cyber Resilience Act in the implementing regulation for CRA.

Such an exclusion would avoid regulatory duplication and ensure that the cybersecurity of qualified trust services continues to be guaranteed by the sector-specific and already established framework of the eIDAS Regulation.

We are available for further clarification and a constructive dialogue.

Our members are ready to assist decision makers and regulatory bodies in answering questions and concerns.

In case you wish more information please write or call us: European Signature Dialog

Mail to office@european-signature-dialog.eu