



Comments of the European Signature Dialog (ESD) on the Draft of NIS2 Implementing Regulation

European Signature Dialog

Title: Comments of ESD concerning Draft NIS2 Implementing Regulation

Subject: Draft Commission Implementing Regulation (NIS2)

Address:

Hackhofergasse 5/16
A-1190 Vienna

Email: Office@european-signature-dialog.eu

Date: 17.07.2025

European Transparency Registernumber: 994150833943-81

1 Introduction

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 experts possess decades of practical experience and have effectively collaborated with the European Institutions in the adoption of key digital legislation such as NIS2 and eIDAS 2.

This document focuses on our insights into the **Draft NIS2 implementing Regulation**.

As we approach the implementation of the NIS2 Directive and its impact on Trust Service Providers (TSPs), particularly Qualified Trust Service Providers (QTSPs), it is crucial to address several key areas to ensure a robust, harmonized, and effective regulatory framework across the European Union. The objectives we present aim to balance the need for enhanced cybersecurity with the practical realities of operating trust services in a complex, multi-party digital ecosystem.

A critical concern is the current **lack of differentiation** between **various trust services** in the draft regulation. These services, including electronic registered delivery, archiving, signatures, seals, time stamps, certificates for authentication, attribute attestation, management of remote signature and seal creation devices, and qualified electronic ledgers, each have **distinct levels of criticality and typically operate under different Service Level Agreements**.

The **one-size-fits-all approach in the current draft** makes it practically **impossible for Trust Services to meet the outlined requirements uniformly**. This is exacerbated by the **lack of precise specifications**, leaving room for diverse interpretations by Supervisory Bodies, courts, other authorities, affected parties, and the Trust Services themselves. Such ambiguity not only risks unequal treatment of Trust Services across EU countries but also significantly increases the operational risks for Trust Service providers, especially in light of the penalties defined in NIS2. To achieve this goal, it is essential that **established international standards are referenced** instead of differentiating our own requirements.

As Qualified Trust Service Provider are subject to strict audit regulations under various ETSI standards with different criticality, information security in the area of Qualified Trust Services shall be only based on the requirements of **ETSI EN 319 401**. For Non-Qualified Trust Services that are not subject to these strict audit requirements, the **ISO 27001 standard should additionally be referenced for harmonization**.

Our recommendations focus on:

- Enhancing **legal clarity** and **precision in terminology by creating legal definitions for every essential term used**
- Establishing realistic and **context-sensitive** incident reporting thresholds
- Aligning requirements with **existing industry standards, Service Level Agreements and best practices**

- Recognizing the **nuanced nature** of modern trust services
- Ensuring **flexibility** to accommodate **various types functions and components of trust services**
- Promoting **EU-wide harmonization by referencing established technical standards (in particular ETSI EN 319 401)**, to support a thriving cross-border market

These objectives are designed to address potential gaps in the current draft, prevent unintended consequences, and create a regulatory environment that enhances security while fostering innovation and growth in the trust services sector. By considering these points, EU Commission can craft an implementing act that not only meets the cybersecurity goals of NIS2 but also supports the continued development of a robust digital single market in the EU, while acknowledging the diverse nature and criticality of different trust services.

ESD respectfully submits the following detailed objectives and recommendations for your consideration.

2 Detailed Objectives and Recommendations as Comments

We respectfully submit the following objectives for the Commission's consideration:

N o	Article	Text from implementing act	Comments
1.	3.1.f	An incident shall be considered to be significant for the purposes of Article 23(3) of Directive 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled: (a) the incident has caused or is capable of causing financial loss for the relevant entity that exceeds EUR 100 000 or 5 % of the relevant entity's annual turnover, whichever is lower; (b) the incident has caused or is capable of causing considerable reputational damage to the relevant entity in accordance with paragraph 2. (...) (e) the incident has caused or is	Legal Clarity: Undefined legal terms such as "considerable," "media," or "material" are frequently used in the draft. We propose the creation of precise legal definitions for these terms within the implementing act. This would establish uniform, harmonized, and clearer reporting obligations for all entities subject to the regulation. E.g., the term "suspectedly malicious case" should not include successful penetration tests as incident. • Clear definition of all legal terms. Specificity in Causality and Liability: In Paragraph 1, sections d) and e), we recommend specifying mechanisms for assessing the causality and liability of actions. This specification would create uniform, harmonized, and clearer reporting

	capable of causing considerable damage to a natural person's health; (f) a successful, suspectedly malicious and unauthorised access to network and information systems occurred;	obligations for the obligated parties. For example, consider the following scenario: A physician is unable to issue an electronic prescription due to a temporary disruption in the signature service. Consequently, the physician must spend additional time issuing a paper prescription, resulting in a patient experiencing severe pain for an extra 10 minutes. It is unclear whether this event triggers a reporting obligation under Article 3, Paragraph 1, section e). Clear guidelines on such scenarios would be beneficial. Financial Loss We would like to draw the EU Commission's attention to an important consideration regarding the proposed threshold of 100,000 EUR for "financial loss" in the draft law. This uniform figure across all EU Member States does not account for the significant variations in purchasing power among different countries within the European Union. To illustrate this point: The purchasing power across EU countries varies considerably. For example: • Greece has a purchasing power of approximately 68% compared to the EU average. • Luxembourg, on the other hand, has a purchasing power of about 143% compared to the EU average. This disparity in purchasing power means that a financial loss of 100,000 EUR would have a different impact in different Member States. As a result, the likelihood of reaching this 100,000 EUR threshold is higher in countries with greater purchasing power, such as Luxembourg, compared to countries with lower purchasing power, even if the severity of the incident is identical.
--	--	---

			This situation could lead to unequal reporting and enforcement across the EU, potentially undermining the law's intended uniformity and fairness. We propose: To stay only with the percentage value in this case.
2.	3.2.b	For the purposes of determining the existence of a considerable reputational damage of an incident in accordance with paragraph 1, point (b) the relevant entities shall take into account whether one or more of the following criteria are met: (a) the incident has been reported in the media; (b) the incident has resulted in complaints from different users or critical business relationships; (...) (d) the entity is likely to lose customers with a material impact on its business as a result of the incident.	Guidance on Impact Measurement: The current draft lacks clear guidance on how to measure the impact size of an incident. - We propose as one option that detailed impact measurement criteria should be included in practice statements rather than in the legal document itself. Important time is often lost when determining the relevant factors and calculating the threshold values. It therefore makes sense to make these binding for the duration of a certification period. For Trust Services, the typical practice statements are Certificate Policies (CP) and Certification Practice Statements (CPS). These could be enhanced to include impact assessments aligned with NIS2 requirements. - It should also be clarified that the values determined by the obliged entity are decisive for the valuation and that this also applies if third parties report other values and parameters to the obliged entity. Specificity in User Complaint Thresholds: The phrase "Complaints from different users" requires more specific measurement criteria to avoid misunderstandings and potential over-reporting. As it stands, this could trigger a flood of minor incident reports, especially considering that all signatories, for example, are "users" due to the terms of use they accept. It is even not clear what is the difference between a

			"customer" and a person, since a trust service has very often a B2C nature due to the "terms of use" which must be accepted by all users. We propose clarifying: • Whether to count only active customers who are online when trying to use the service (e.g., submitting an electronic signature). • Or to count all potential customers registered in the service. • Clearly defining what constitutes a "user"(e.g., active user vs. registered but inactive user which could be even a potential user in the future). • A creation of a legal definition for "media." Furthermore "reliable" should be included as an additional criterion in order to prevent disinformation, unfounded, untrue or dubious reports from triggering a reporting obligation. • Establishing a specific threshold for the number or percentage of user complaints that would trigger a reporting obligation. Material Impact Size Clarification: The draft should provide clear guidelines on how to estimate the material impact size of an incident. We suggest including specific thresholds, such as: • A percentage of revenue (e.g., 5% of annual revenue) • A percentage of lost active customers over a specified period (e.g., 5% of active customers lost within a month)
3.	4	Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where	Legal Clarity: "Same apparent root cause" is also an undefined legal term and should therefore also be legally defined Example: Does a recurring "typing error" - caused by two

		they meet all of the following criteria: (a) they have occurred at least twice within 6 months; (b) they have the same apparent root cause.	different employees from two different departments with regard to different trust services – fulfil the criterion of "same apparent root cause"?
4.	14	General	Differentiation of Services and Components: The current draft significantly tightens resilience requirements compared to previously applicable guidelines. We propose that the requirements for trust services should be more nuanced, taking into account the differences between individual services, functionalities, and components. For instance: • Ultra-high availability should only be required for components necessary for validation, such as OCSP responders. • Lower availability thresholds should be applied to signing or archiving services and comparable trust services, aligning with industry standards and practical necessities. • A distinction should also be made between qualified and non-qualified trust services. They each have different requirements and areas of application. Non-qualified trust services usually have far lower availability on the market.
5	14.a/ b	a trust service, or a part of it, is completely unavailable for more than 10 minutes; a trust service, or a part of it, is unavailable to users, or relying parties, for more than one hour calculated on a calendar week basis;	Realistic Availability Thresholds: The current thresholds for reportable incidents are unrealistically strict • Even compliance with an annual availability of 99.3% (or above 99.99% in some cases), which is considered standard market practice, would regularly trigger reportable incidents under the current thresholds. Alignment with Service Level Agreements (SLAs)

			When determining reportable incidents, contractually agreed SLAs should be taken into account. It is contradictory if temporary service failures do not breach customer contracts but still constitute reportable incidents. We suggest: • Including an additional requirement that service outages must exceed contractual or other statutory availability requirements to trigger a reportable incident. Best practice would be to consider the deviation to the Service Level Agreements to be found in the Certificate Policy and Certificate Practise Statement (CP/CPS) which is mandatory for a trust service under eIDAS or equivalent legal documents issued by the trust service as contractual base. • Aligning incident reporting thresholds with commonly accepted SLAs in the trust services industry. • Instead of using the term "a part of" it should solely reflect to the SLAs independent which part was involved or not to meet the SLA's requirement. "A part of" is not defined and not clearly definable. Clarification of Roles and Responsibilities: The current framework does not adequately address the multi-party nature of electronic signature services. Up to now for the signature service a trust service could only manage the remote signing infrastructure and even if it provides signatures it takes the responsibility for receiving a hash of the document and provision of a signed hash. Signature workflow applications e.g. like DocuSign, Adobe Sign or others will build up a signed document based on the signed hash and the cryptological algorithms behind it. We
--	--	--	---

			propose: - Clearly defining the roles and responsibilities of each entity in the signature delivery chain, including trust service providers, signature workflow application providers, and internet service providers. - Establishing guidelines for determining accountability in cases of service disruptions or delays. - Providing a clear definition of "customer" in the context of electronic signature services. - Considering a tiered approach that recognizes both end-users and intermediary service providers as customers, with appropriate distinctions in reporting requirements - Establishing guidelines for distinguishing between delays caused by different components of the service (e.g., internet connectivity, application processing, trust service response) Allowing for a case-by-case evaluation of incidents rather than relying solely on rigid numerical thresholds.
5.	14.c	more than 1 % of the customers of the trust service in the Union are impacted by large delays in response time of the trust service	Exception for Planned Maintenance Windows: The current draft does not distinguish between unplanned outages and planned maintenance windows. (see Article 3.3) We propose: Explicitly excluding pre-announced maintenance windows from the definition of reportable incidents. This exclusion should be incorporated into the main text of the regulation, not just in the

			recitals, as recitals have no direct legal effect according to ECJ jurisprudence. • Providing clear guidelines on how and when maintenance windows should be announced to qualify for this exception. Refined Threshold for Customer Impact: The current 1% threshold related to the respective trust service can be quickly reached for specialized services with few customers. Furthermore, the current draft does not specify how to count customers for the purpose of assessing impact. We propose clarifying: • Whether to count only active customers who are online when trying to use the service (e.g., submitting an electronic signature). • Or to count all potential customers registered in the service. • Providing a clear definition of "customer" - specifying whether it refers to end-users, clients, subjects, or subscribers. • Basing the 1% threshold on the total number of all customers of the Trust Service Provider (TSP), rather than on individual services. • Alternatively, creating differentiated, interest-based assessment factors and thresholds that take into account the nature and scale of different trust services. Considering both the percentage and absolute number of affected customers to provide a more balanced assessment of impact. Definition of "Large Delays": The term "large delays" is currently undefined, leading to potential inconsistencies in interpretation. We
--	--	--	---

			recommend: • Relating the definition of large delays to the declared Service Level Agreement (SLA) in the service policy or CP/CPS, with appropriate limitations based on industry standards. • Incorporating references to relevant industry standards to provide context for definitions and thresholds.
6.	14.d	physical access to one or more of the areas where network and information systems are located and to which access is restricted to trusted personnel of the trust service provider, or the protection of such physical access, is compromised;	Clarification of Physical Access in Relation to Security Zones: The current draft should clarify that physical access refers specifically to security zones associated with network and information systems. Physical access alone should not automatically be treated as a significant incident. We propose: • Explicitly defining "physical access" in the context of trust services and their security infrastructure. • Specifying that security zones are areas where critical network and information systems are located or accessed. • Establishing that a reportable incident occurs only when physical access is combined with actions leading to a breach of integrity, confidentiality, or authenticity of the trust service. • Providing clear criteria for assessing when physical access becomes a serious threat to the service. Clarifying that routine access by authorized personnel (e.g., cleaning services) does not constitute a significant incident. Alignment with Existing Security Practices: The regulation should align with established security practices in the trust

			services industry: • Referencing relevant industry standards for physical security in data centres and sensitive areas. • Ensuring consistency with existing best practices for managing and reporting physical security incidents.
7.	Annex (and Art.2)		EU-wide Harmonization: We want to • emphasize the critical need for consistent implementation of NIS2 requirements across all EU member states for QTSPs. • highlight that this harmonization is essential to maintain and further develop the cross-border market for trust services, which was a key goal of the 2014 eIDAS Regulation. Addressing Potential Legislative Gaps: We suggest to ... • acknowledge the risk of new gaps in national legislation arising from the shift from eIDAS to NIS2 for IT and information security requirements and incident reporting. • stress the importance of preventing potential discrimination against national entities by varying national implementations of NIS2. Referencing Existing Standards: We strongly recommend to • reference established standards for information security, particularly ETSI EN 319 401 for QTSP and additionally ISO 27001 for TSP, in the implementing act. • consider that ETSI EN 319 401 has been recently updated to meet NIS2 requirements and is already widely used in QTSP conformity assessments.

			Continuity and Auditability: We want to - Stress the importance of maintaining continuity with current industry practices to facilitate easier compliance and auditing. - Emphasize that referencing established standards would enhance cross-border harmonization of enforcement and supervision. Preventing Divergent Interpretations: We want to - Highlight the risk of different national interpretations if specific standards are not explicitly referenced. - Advocate for clear, standard-based requirements to ensure uniform implementation across member states. Alignment with eIDAS Revision: We strongly recommend to - Emphasize the need for the implementing act to align with the ongoing eIDAS revision to ensure a coherent regulatory framework for trust services. Facilitating eIDAS-compliant Conformity Assessments. - Stress that clear and mandatory reference to established standards would simplify the work of conformity assessment bodies and lead to more consistent evaluations across the EU. Supporting Market Development: - Highlight that a harmonized approach based on well-established standards would support the continued development
--	--	--	--

			and innovation in the trust services market.
--	--	--	--

3. Harmonizing Trust: Empowering a secure, innovative and consistent EU Framework

By incorporating these objectives into the implementing act, the EU commission can create a regulatory framework that:

- Enhances **security and reliability** of trust services
- Promotes **consistent implementation and enforcement** across the EU
- Reduces **unnecessary administrative burdens** on Trust Service Providers
- Supports **innovation and growth** in the trust services market
- Aligns with **the broader goals of the eIDAS regulation** and its ongoing revision