bitkom

Position Paper

2025 July

Risk management procedures for non-qualified trust service providers (QTSPs)

Summary

Bitkom emphasizes that substantial improvements are necessary to ensure the clear and proportionate implementation of the Implementing Act on Risk Management Procedures for Non-Qualified Trust Service Providers under eIDAS-Regulation (EU) No. 2024/1183. The draft regulation includes redundant provisions and lacks clarity regarding user risk communication, identity verification requirements, and secure data retention. Enhanced transparency obligations and harmonization with core security standards are essential to foster trust, regulatory coherence, and a risk-based approach. Furthermore, a sufficient transitional period is needed to enable smooth and effective adoption.

Specific comments on the implementing regulation

Nr.	Article	Action	Justification/Recommendation
1	**Recital 1**	Delete recital 1	The reference to the 'crucial role in the digital environment' conflicts with the notion of 'lower criticality'. Recital 2 already defines the role of non-QTSPs and their relevance under eIDAS, making Recital 1 redundant. Policies for TSPs should apply transversally, with adjustments reflecting a free and competitive market.

Nr.	Article	Action	Justification/Recommendation
2	**Article 2** Risk management policies	Amend article 2	**Add point 6)**: '*Non-qualified trust service providers shall inform end users about the risks, limits, of using their respective non-qualified services (e.g.: 'Warning: Using non-qualified services does not offer the same legal protections as qualified services').*' The idea behind this proposal is to ensure maximum trust and transparency of the trust services operated to facilitate their acceptance by users, particularly the less initiated.
3	**Article 4, par. 3 (a)** Risk treatment measures	Amend article 4, par. 3 (a)	We recommend to include the following statement: '*verify the identity of the users of the trust service directly or by means of a third party* ***and describe in detail within their Trust Service Practice Statement the identification methods used.***' The idea behind this amendment is to strengthen the provision by explicitly requiring non-qualified trust service providers to document and disclose the identity verification methods they apply. This promotes greater transparency, supports supervisory activities, and helps ensure consistency with the obligations imposed on TSPs. It also enhances users' and relying parties' ability to assess the reliability and robustness of the service, in line with a risk-based and proportionate approach.
4	**Article 4, par. 3 (b)** Risk treatment measures	Specifiy article 4, par. 3 (b)	We suggest **rephrasing this sentence for greater clarity** as the declared necessity to retain critical data until after closing without giving indications on how to ensure the security and availability of this data in the long term could generate arbitrary interpretations.
5	**Article 5** Entry into force	Amend article 5	We advocate for **extending the entry into force of this Implementing Regulation to at least 12 months from its publication**.

Nr.	Article	Action	Justification/Recommendation
6	**Annex** List of reference standards for non-qualified trust service providers	Amend the annex	**The points 7.3, 7.4, and 7.6 should be replaced with '*7. TSP Management and Operation*'.** The standard EN 319 401 establishes that the document addresses the general requirements for the security management and cybersecurity of trust services (both qualified and non-qualified). Therefore, **Chapter 7 should be fully applied to the risk management of non-qualified trust service providers (for example, essential paragraphs for the secure provision of a trust service, such as 7.2 Human resources, 7.8 Network security or 7.9 Vulnerabilities and Incident management, can be cited), except for those parts that can be demonstrated to be excessive in relation to the nature and level of risk of the services provided**. Such exclusions must be based on a duly justified and proportionate risk analysis, in accordance with the principle of proportionality. This revision also serves a broader objective: to harmonise the application of core security standards across all trust service providers, ensuring a coherent and balanced regulatory framework while preserving flexibility for differentiated risk exposure.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Lorène Slous | Policy Officer Trust Services & Digital Identities
P +49 30 27576-157 | l.slous@bitkom.org

Responsible Bitkom committee
WG Digital Identites