

Implementing Regulation concerning QWACs

Please find below the comments of the European Signature Dialog (ESD). ESD stands as the pinnacle consortium of leading European Qualified Trust Service Providers (QTSPs). We are pleased to provide our contribution in relation to the implementing regulations of eIDAS 2 Regulation, in the spirit of supporting a clear, effective, and future-proof framework.

	Legislative reference	Article	Comment	Proposed solution
QWAC 1	Annex	ANNEX [...]	In the Annex, under the section “For qualified certificates for website authentication that are issued for use in transport layer security authentication outside the context of a web-browser:” we recommend explicitly adding the following standard: ETSI TS 119 495 V1.7.1 (2024-07) This addition is necessary to ensure that PSD2 certificates are duly included, as they fully qualify as QWACs not used by browsers. Without this explicit reference, PSD2 QWACs would no longer be issuable within the framework of Open Banking with a two-year validity, and their lifetime would instead be constrained by CA Browser Forum rules, which foresee progressive reductions to 200 days, 100 days, and ultimately 47 days. Such a development would dismantle a well-functioning and widely adopted framework, as recognised by the European Banking Authority and by the requirements embedded in the EPC payment scheme rulebooks. Failing to incorporate ETSI TS 119 495 would therefore not only undermine legal certainty and operational stability but would also <u>harm the resilience of EU payment systems</u>, exposing providers and users to unjustified operational risks and threatening continuity in a sector where trust and stability are essential.	We recommend adding the following standard ETSI TS 119 495 V1.7.1 (2024-07) under the section “For qualified certificates for website authentication that are issued for use in transport layer security authentication outside the context of a web-browser”.

	Legislative reference	Article	Comment	Proposed solution
2	Annex	ANNEX	Amend the section as follows: “For other qualified certificates for website authentication than those referred to in paragraph 1: – EN ETSI TS 119 411-5 V2.1.1 (2025-02), <u>with the provision that the qualified trust service providers shall not have to be part of the dedicated browser root store program.</u>”	This is to help clarifying that the web-browsers are – apart from the ability of taking precautionary measures that are both necessary and proportionate in reaction to substantiated concerns regarding security breaches or the loss of integrity of an identified certificate or set of certificates – not allowed, according to Art. 45a eIDAS, to “take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication”. The inclusion of a qualified trust service provider in a browser root store and thus participation in a browser root store program is based on individual and non-transparent decisions with no possibility of objection and legal review. A dependency on inclusion in a browser root store program should therefore not be established.

QWAC 3	General	Art 1-2	Certificate Transparency (CT) is an established industry standard that has proven effective in increasing trust in the issuance of publicly trusted certificates. Academic research, including analyses by Johannes Sedlmeir (University of Münster) and Pol Hölzmer (University of Luxembourg), has highlighted CT as an important instrument to strengthen confidence in Qualified Website Authentication Certificates (QWACs). The introduction of CT for QWACs is required for several reasons: It ensures consistency with the global WebPKI, where CT is mandatory for all major browsers. It enables early detection of mis-issuance or compromise of a qualified trust service provider (QTSP). The recent incident involving the Croatian CA Fina RDC 2020, operated by the QTSP Financijska Agencija, illustrates how problematic certificates can be identified quickly and reliably through CT logging. https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/SgwC1QsEpsc/m/eiPm9bL3AgAJ? It strengthens supervisory oversight, providing transparency to national authorities and supporting the objectives of eIDAS to enhance cross-border trust. It increases market confidence, as relying parties such as governments, banks and enterprises can verify that QWACs are issued and managed according to the highest standards. It contributes to the overall resilience and integrity of the European trust service ecosystem by creating a verifiable and publicly auditable record of QWAC issuance. For these reasons, it is appropriate to require CT logging of QWACs once a European CT infrastructure and related standards are available. An ETSI standard is currently being developed here. An appropriate transitional period should therefore be set (e.g. 01.01.2027) until the obligation for	In addition, another article should be established stipulating that once a European Certificate Transparency infrastructure and related standards are available, qualified certificates for website authentication referred in the Annex shall be logged in accordance with those standards.
-------------------	---------	---------	---	---

	Legislative reference	Article	Comment	Proposed solution
			CT logging takes effect and the standard and the required infrastructure are available.	

We 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

Hackhofergasse 5/16 - A 1190 Vienna – phone: 0043 676 9409309 – office@european-signature-dialog.eu

European Transparency Number: 994150833943-81

