The role of the Cloud Signature Consortium (CSC) API in the new European digital identity framework and beyond

CLOUD
SIGNATURE
CONSORTIUM

Executive summary

In this second paper in our two-part series, we explore the **benefits of deploying the CSC API within the European digital identity framework**. These benefits include interoperability between e-signing platforms and remote signature creation devices, enhanced security, ease of use, flexibility, and compliance with EU laws.

The CSC API's use extends beyond EU borders. It can provide the technical foundation needed to standardise remote digital signature creation and achieve the ultimate aim of a global, interoperable digital signature framework.

Background

Regulation (EU) 2024/1183 (**eIDAS Amendment**) entered into force on 20 May 2024. It amends Regulation (EU) No 910/2014 (**eIDAS Regulation**) to establish a groundbreaking "*European digital identity framework*".

At the heart of the new framework is the "*European digital identity wallet*" (**EUDI Wallet**). From late 2026, every EU member state will provide[1] at least 1 EUDI Wallet as a mobile app to citizens (and businesses[2]), built to the same technical standard. It will enable users to identify and authenticate themselves online or in-person[3], securely store and present digital documents, and sign documents with the digital signature[4] *gold standard* of a qualified electronic signature (**QES**).[5] The EUDI Wallet will help the European Commission fulfil the ambitious target set out in its Digital Decade Policy Programme of providing 100 per cent of EU citizens with access to a digital identity by 2030.

Any reference to "**eIDAS**" is a reference to the eIDAS Regulation as varied by the eIDAS Amendment.

This is the second paper in a two-part series. In our first paper, we put QES under the microscope and explained its advantages over other types of electronic and digital signatures. We made the case for the EUDI Wallet transforming *remote signing with QES*[6] and spurring adoption of QES as the primary method of document execution in the EU. And, finally, we looked at the critical role played by the Cloud Signature Consortium's API specification in the current, pre-EUDI Wallet landscape for remote signing with QES (**CSC API**).

---

[1] There are 3 permutations for providing an EUDI Wallet under Article 5a(2) of eIDAS. It may be provided directly by an EU member state, under a mandate from an EU member state, or independently but recognised by an EU member state.

[2] The EUDI Wallet will also be made available to EU businesses for identification, authentication and electronic sealing of documents. However, this paper concentrates solely on the use of the EUDI Wallet by EU citizens (and residents).

[3] The EUDI Wallet enables authentication in public **and** private sector use cases. A perceived shortcoming of the eIDAS Regulation was its narrow focus on the public sector and, consequentially, modest level of adoption by the private sector.

[4] An electronic signature produced using asymmetric or public key cryptography.

[5] A QES is a digital signature. It is defined by Article 3(12) of eIDAS as "*an advanced electronic signature (**AdES**) that is created by a qualified electronic signature creation device (**QSCD**), and which is based on a **qualified certificate** for electronic signatures.*" An AdES is defined in Article 26 as an electronic signature which is (a) uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using electronic signature creation data (i.e. a private cryptographic key) that the signatory can, with a high level of confidence, use under their sole control; and (d) linked to the signed document in such a way that any subsequent change to the document is detectable.

[6] *Remote signing with QES* is a highly secure method of signing documents digitally, ensuring both the authenticity of the signatory and the integrity of the signed document. The signatory's qualified certificate and cryptographic key pair are managed and stored by a qualified trust services provider (**QTSP**) in a remote QSCD (i.e. *in the cloud*). This architecture enables a signatory to sign their document via an e-signing platform from any device with internet access.

We now turn our attention to the myriad ways in which the European digital identity framework is set to benefit from the CSC API. We also assess the potential of the CSC API to standardise remote digital signature creation on the *global* stage.

Overview of the CSC

The Cloud Signature Consortium (**CSC**) is an international group of industry, government and academic organizations committed to driving standardization of highly secure, compliant and interoperable digital signatures (including QESs) *in the cloud*. The CSC was founded in 2016 and now comprises 78 members from 41 countries.

ETSI TS 119 432 is a technical specification developed by the European Telecommunications Standards Institute (**ETSI standard**) and defines protocols and interfaces for remote digital signature creation. The ETSI standard incorporates elements of the CSC API and underpins remote signing with QES on e-signing platforms in line with eIDAS requirements.

Figure #1 below shows how the CSC API acts as the interface between an e-signing platform and a qualified signature creation device (**QSCD**)[7] to enable remote signing of a document with QES.

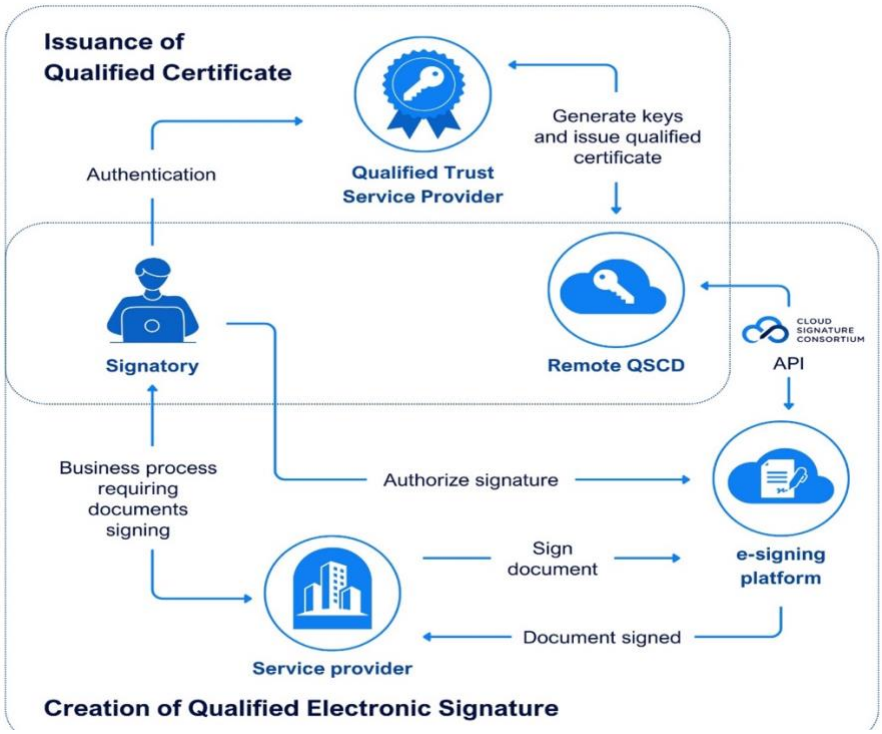

Figure #1

[7] The QSCD is a hardware security module which stores the signatory's qualified certificate (digital signing certificate) and their cryptographic key pair. The QSCD is managed *remotely* by the QTSP on behalf of the signatory.

How the European digital identity framework benefits from the CSC API

In our first paper, we highlighted the requirement under Article 5a(5)(a)(xi) of eIDAS for the EUDI Wallet to support "*common protocols and interfaces*" for the creation of QES by means of a QSCD. The CSC API already provides the interface between the e-signing platform and the QSCD for remote signing with QES, and it will continue to do so when the EUDI Wallet is made available to citizens. Moreover, the draft Implementing Regulation on the "*integrity and core functionalities*" of the EUDI Wallet published by the European Commission in August 2024 makes an explicit reference to the CSC API. Article 12(3) considers a scenario in which the "*signature creation application*" (**SCA**)[8] is integrated into the EUDI Wallet (and not provided externally by an e-signing platform). It states that if an SCA is integrated into the EUDI Wallet, it *must* support the CSC API.

The benefits that the CSC API brings to the European digital identity framework include:

- **Interoperability**. The CSC API provides a standardized interface that ensures compatibility across *different* e-signing platforms and QSCDs. This enhances user choice and counters the risk of vendor lock-in.

- **Security**. The CSC API has been implemented in the ETSI standard and incorporates robust security measures to protect the integrity of documents signed with QES.

- **Ease of use.** The CSC API is user-friendly, easy to deploy and has a proven track record for remote signing with QES.

- **Flexibility.** The CSC API supports various authentication methods for remote signing with QES including biometrics and national eIDs. The flexibility of the CSC API means it can support use of the EUDI Wallet as a new method of authenticating signatories.

- **Compliance.** The use of the CSC API for remote signing with QES is compliant with the strict legal and technical requirements set out in eIDAS.

- **Innovation and competition.** Qualified trust service providers (**QTSPs**) who enable the creation of QES (*see our first paper*) can innovate around the CSC

[8] Technical information about SCAs can be found in ETS TS 119 432.

API to differentiate their QES product(s), and foster competition in the EU marketplace.

The Data Act

Regulation (EU) 2023/2854 (**Data Act**) came into force in January 2024 and will be applicable in EU member states from September 2025. It is a key pillar of the European data strategy and aims to create a fair and innovative data economy in the EU.

The Data Act also includes measures to increase fairness and competition in the EU cloud market. Article 35 imposes a duty on providers of "*data processing services*"[9] (i.e. cloud service providers) to develop "*open interoperability specifications*".[10] The European Commission will also assess barriers to interoperability of data processing services and may ask European standardisation organisations to produce harmonised standards which comply with the interoperability requirements set out in Chapter VIII of the Data Act. This is intended to promote multi-vendor cloud environments and facilitate switching between public cloud services.

E-signing platforms and QTSPs provide data processing services within the scope of the Data Act. But conformity with Chapter VIII of the Data Act will be straightforward: the API CSC *already* fulfils the requirements for an open interoperability specification that enables remote signing with QES.

The role of the CSC API on the global stage

The EUDI Wallet is a catalyst for countries outside the EU (**Third Countries**) to develop their own digital wallet solutions. Increasingly, digital wallets are seen as a means of signing documents and not just a means of proving identity, storing credentials and making payments.

[9] Defined in Article 2(8) of the Data Act as "*a digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"
[10] Defined in Article 2(41) of the Data Act as "*a technical specification in the field of information and communication technologies which is performance oriented towards achieving interoperability between data processing services.*"

The CSC API is not confined to remote signing with QES in EU transactions.[11] It is a global, interoperable API which may be used in *any* digital wallet solution (or application) for remote digital signature creation.

Recital 47 of the eIDAS Amendment acknowledges the growing importance of QES and other *qualified* trust services for international trade and cooperation. The European Commission plans to adopt implementing acts which will set the conditions under which trust frameworks in Third Countries could be deemed *legally equivalent* to the eIDAS trust framework (*Article 14*, *eIDAS*). Article 14 also gives the European Commission the ability to agree mutual recognition of QES (and other qualified trust services) with Third Countries pursuant to Article 218 of the Treaty on the Functioning of the European Union.

Although the objective of Article 14 is to achieve mutual recognition of QES between the EU and Third Countries, the European Commission has also established a "Third Countries AdES List Of Trusted Lists" (**Third Countries AdES LOTL**). The Third Countries AdES LOTL is based on an "*advanced electronic signature*" (**AdES**) (*see footnote 5*) rather than QES. It contains information notified by a Third Country to the European Commission and enables a relying party to validate that electronic signatures created in that Third Country meet the requirements for an AdES under Article 26 of eIDAS.

At the time of writing, only Ukraine has been admitted to the Third Countries AdES LOTL. More Third Countries are expected to follow in Ukraine's footsteps. The European Commission has commented that inclusion in the Third Countries AdES LOTL "*can be seen as the stepping stone towards mutual recognition of qualified trust services following the conclusion of an International Agreement [pursuant to Article 14 of eIDAS].*"

Readers should note that the CSC API supports the creation of all types of digital signature including QES and AdES, and has been successfully adopted in nearly every geographical region.

[11] This is explicit in the Foreword to the CSC API, which states "*The Cloud Signature Consortium has developed the present specification to make these solutions interoperable and suitable for uniform adoption in the global market, in particular – but not exclusively – to meet the requirements of the European Union's Regulation 910/2014 on Electronic Identification and Trust Services (eIDAS).*"

Conclusions

International recognition of QES is the ultimate goal. Global electronic and digital signature laws remain inconsistent and fragmented. If the EU and Third Countries can settle on QES as the internationally recognised standard, it will dispel the legal uncertainties that have hindered digital transformation. As is so often the case, it is the law that lags behind technology, and not the other way round.

The CSC API provides the technical interoperability, which is needed to standardise remote digital signature creation *on a global scale*, including remote signing with QES. As emphasized in this paper, the CSC API's role extends beyond the European digital identity framework, supporting international cross-border recognition of QES, AdES, and other digital signatures.

CLOUD SIGNATURE CONSORTIUM

Cloud Signature Consortium VZW
Rue du Luxembourg 22-24
BE-1000 Brussels