The EU digital identity wallet:

a new tool for remote signing with qualified electronic signatures

CLOUD SIGNATURE CONSORTIUM

Executive summary

The Cloud Signature Consortium welcomes changes to the eIDAS Regulation that pave the way for a new and ambitious European digital identity framework. At its core is the European digital identity wallet. This will provide EU citizens and residents with a secure and convenient form of digital identification to access public and private sector services throughout the entire EU bloc. The wallet also enables users to sign documents with a qualified electronic signature.

In this briefing paper – the first of a two-part series - we lay out the benefits of using the wallet for remote signing of documents with the gold standard of a qualified electronic signature to advance the EU's digital strategy. We also illuminate the key role of the Cloud Signature Consortium's API specification in facilitating remote signing with the wallet. However, challenges persist. The revised eIDAS Regulation allows users to sign documents with a qualified electronic signature "free of charge" for "non-professional purposes"; but it does not define the meaning of "professional" and "non-professional". Additionally, EU member states lack official guidance on financing the qualified certificates necessary for such signatures.

This uncertainty risks undermining the eIDAS Regulation's goal of harmonising trust services and creating a level playing field for actors in the trust services ecosystem. Furthermore, a lack of legal clarity around what constitutes "professional" or "non-professional" purposes when using qualified electronic signatures, and the associated costs, risks hindering the widespread user adoption of remote signing via the EUDI Wallet. As an industry leader, the Cloud Signature Consortium encourages EU member states to recognise the importance of qualified electronic signatures, clarify the distinction between "professional" and "non-professional purposes", and allocate adequate funding for creating free-of-charge qualified electronic signatures with the wallet for non-professional purposes.

Background

Regulation (EU) No 910/2014 (**eIDAS Regulation**) was enacted in 2014 and came into effect between 2016 and 2018. Regulation (EU) 2024/1183 (**eIDAS Amendment**) came into force on 20 May 2024. It revises and expands the eIDAS Regulation to establish a new "*European digital identity framework*". A phased implementation of the European digital identity framework – requiring the European Commission to adopt 40+ implementing acts - should conclude by 2027.

In this briefing paper, a reference to "*eIDAS*" means the eIDAS Regulation as varied by the eIDAS Amendment.[1]

The European digital identity framework introduces the European digital identity wallet (**EUDI Wallet**). Each EU member state will issue an EUDI Wallet[2] to their citizens (and other residents). The EUDI Wallet is based on common technical standards[3], and ensures a high level of cybersecurity protection.[4] It will enable users to identify and authenticate themselves online or in-person, and to share a wealth of digital documents such as a mobile driving licence, education diploma and medical prescription.

Data privacy is paramount: using a "*common dashboard*" embedded in the design of the EUDI Wallet, a user will be able to track their transactions with service providers, request deletion of personal data (under Article 17 of Regulation (EU) 2016/679 (**GDPR**)) and even report a breach of GDPR to national data protection authorities.

The EU public sector must accept the EUDI Wallet for authentication when it becomes available in November 2026. From late 2027, it will become mandatory for service providers in the private sector such as banks and telecom networks to accept the EUDI Wallet where "*strong user authentication for online identification is required by Union or national law or by contractual obligation*".[5]

The EUDI Wallet will also enable the user to sign[6] documents remotely with a qualified electronic signature (**QES**). In this briefing paper, we explore the concept of

[1] The consolidated text of the eIDAS Regulation and the eIDAS Amendment is accessible here.
[2] The EUDI Wallet will be provided under national eID schemes which have been (or will be) notified to the European Commission under Article 9 of eIDAS. The identity proofing and verification will meet the standard for a "*high*" level of assurance set out in Article 8 of eIDAS.
[3] The Architecture and Reference Framework or "*ARF*" for the EUDI Wallet is being developed by the eIDAS Working Group. The latest version (1.4) is accessible here.
[4] Every EUDI Wallet must be independently certified against a new cybersecurity certification scheme for ICT products established under the EU Cybersecurity Act.
[5] Article 5f(2) of eIDAS.
[6] Article 5a(4)(e) of eIDAS.

remote signing with QES in the EU (and EEA[7]) and consider the impact of the EUDI Wallet.

Overview of QES

eIDAS has established a hierarchy of electronic signatures: (simple) electronic signatures, advanced electronic signatures and QESs. QES is the "*gold standard*". It provides a higher level of identity proofing, document integrity and more support for signatory non-repudiation[8] than other types of electronic signature.

Article 3(12) of eIDAS defines QES as "*an advanced electronic signature that is created by a qualified electronic signature creation device (**QSCD**), and which is based on a qualified certificate for electronic signatures.*"

QES relies on technology called "*public key infrastructure*" (**PKI**). PKI is a protocol enabling a trust service provider (**TSP**)[9] to verify the signatory's identity and issue a digital certificate. In the case of QES, the digital certificate is a "*qualified certificate*" which meets technical and security criteria set out in Annex I of eIDAS. The qualified certificate confirms the signatory's name and links their identity to a pair of cryptographic keys (**key pair**). The rigorous identity proofing provides greater assurance than other electronic signatures that the signatory is who they claim to be, and that the signed document is authentic. The use of the key pair (*see below*) also prevents any tampering with the document after signing.

Nowadays, qualified trust service providers (**QTSPs**) typically operate QSCDs that are made available to signatories remotely *in the cloud*.[10] The QSCD is a hardware security module which stores the signatory's qualified certificate and key pair. The QSCD is – in a majority of cases – connected to an e-signing platform using the Cloud Signature Consortium's API specification for remote signing (**CSC API**).

[7] eIDAS applies to the EEA countries too (Iceland, Liechtenstein and Norway).
[8] Protection against a signatory falsely denying that they signed the document.
[9] TSPs are also known as "*certificate authorities*" or "*CAs*". Note that only QTSPs may issue qualified certificates for QES.
[10] https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-the-cloud.

Creation and validation of QES

Figure #1[11] below illustrates how a signatory uses a hash algorithm and their *private key* to create the QES. The recipient of the signed document uses the signatory's *public key* to decrypt the QES and ensure that the document has not been modified after signature. The recipient also checks that the public key belongs to the signatory, their qualified certificate was issued by a QTSP and valid at the time of signing, and the QES was created by a QSCD (*Article 32, eIDAS).* In practice, this is less complex than it sounds. Any PDF document that is signed with QES on an e-signing platform can be validated *automatically* using a PDF reader such as Acrobat or Acrobat Reader, or the European Commission's validation tool.

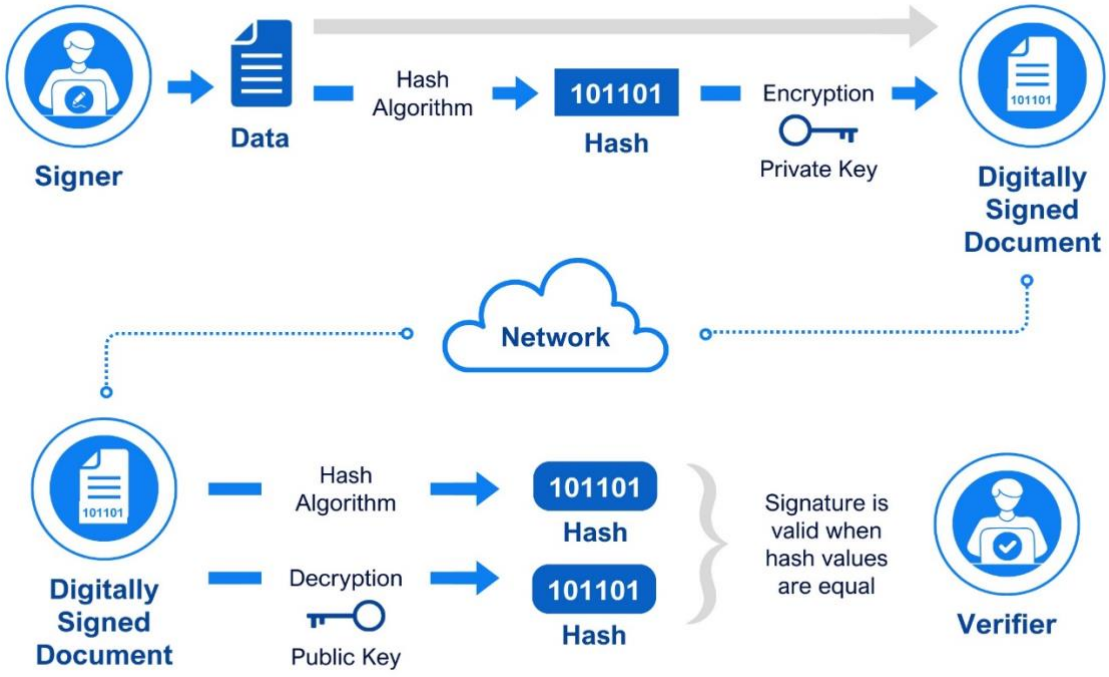

Figure #1

What sets QES apart from other types of electronic signature is not only more robust identity verification and cryptographic security, but its higher status in EU law:

- QES has the *equivalent legal effect* of a handwritten signature (*Article 25(2), eIDAS).*

[11] Figure #1 is adapted from the Interim Report on the Electronic Execution of Documents by the MoJ's Industry Working Group published on 1 February 2022.

- QES based on a qualified certificate issued in one EU member state is recognised as a QES in every other EU member state (*Article 24a(1), eIDAS)*.
- QSCDs certified in one EU member state are recognised as QSCDs in every other EU member state (*Article 24a(3), eIDAS)*.
- If any person suffers damage arising from the use of a QTSP's services, it is presumed that the QTSP has caused this damage "*intentionally or negligently*" (*Article 13(1), eIDAS*).[12]

The current EU market for QES

There are approximately 175 active QTSPs on the EU List of Trusted Lists who can issue qualified certificates for QES.

The QTSP must verify a signatory's identity in accordance with the requirements of Article 24 of eIDAS. This traditionally required the signatory to attend a face-to-face meeting. The process was slow, inconvenient and expensive. But the emergence of remote identity proofing techniques now enable QTSPs to offer video verification, or facial biometric verification (often using NFC technology)[13] to *enrol* a signatory and issue their qualified certificate for QES.

Today, remote signing with QES on e-signing platforms has largely displaced local signing (using qualified certificates and key pairs stored on USB tokens and smartcards). Many QTSPs on the EU List of Trusted Lists have API[14] integrations with commercial e-signing platforms. QES is widely available in the EU; yet despite its myriad advantages, QES is a far less popular method of document execution than using a simple electronic signature with a one-time password (**OTP**).[15]

---

[12] Conversely, if a person claims damage arising from the use of a non-qualified TSP's services, the burden of proof is on the claimant to produce evidence that the damage was caused intentionally or negligently. Article 13(2) does allow (Q)TSPs to limit their liability under contract law.

[13] The user typically downloads the QTSP's mobile app and uploads a copy of their passport. The QTSP's mobile app uses Near Field Communication or *"NFC"* technology to read the chip in the passport and extract the user's photo. The user then uploads a (video) selfie. The mobile app deploys AI algorithms to match the selfie with the passport photo and validate the user's identity. It also uses liveness detection to protect against biometric presentation and injection attacks. Once complete, the QTSP issues the qualified certificate to the user.

[14] An application programming interface or "*API*" is an interface that allows software applications to communicate and interact with each other. APIs typically provide a set of tools, documents, protocols and specifications. A majority of e-signing platforms (as a "*signature creation application")* use the Cloud Signature Consortium V 2.0 API to connect with QTSPs and enable remote signing with QES.

[15] A one-time password or "*OTP*" is sent to the signatory's mobile phone as a second authentication factor. This provides an extra layer of security but – unlike a qualified certificate – it does not actually verify the identity of the signatory.

Remote signing with the EUDI Wallet

The eIDAS Amendment is a harbinger of change.

Recital 20 provides that "*The use of a qualified electronic signature should be free of charge to all natural persons for non-professional purposes. It should be possible for Member States to provide for measures to prevent the use of qualified electronic signatures for professional purposes by natural persons free-of-charge, while ensuring that any such measures are proportionate to identified risks and are justified.*"

The eIDAS Expert Group has observed that this will "*enhance the use of the EUDI Wallet for signing, in a natural and convenient way.*"[16]

Article 24(1a)(a) of eIDAS enables a QTSP to rely on the EUDI Wallet for identity verification. This is because the EUDI Wallet meets the requirements for assurance level "*high*" in relation to identity proofing, verification and authentication (*Article 5a(5)(d), eIDAS*). The net effect will be to simplify and speed up the procedure for verifying a signatory's identity and issuing their qualified certificate for QES *on the fly* (*see figure #2*).

This means that the EUDI Wallet will enable remote signing with QES as part of a *remote* QSCD managed by a QTSP. It has the potential to transform remote signing on e-signing platforms and lay the foundation for *mass adoption* of QES in consumer, commercial, employment, corporate, real estate, government and financial transactions.

[16] Section 3.8 of the ARF.

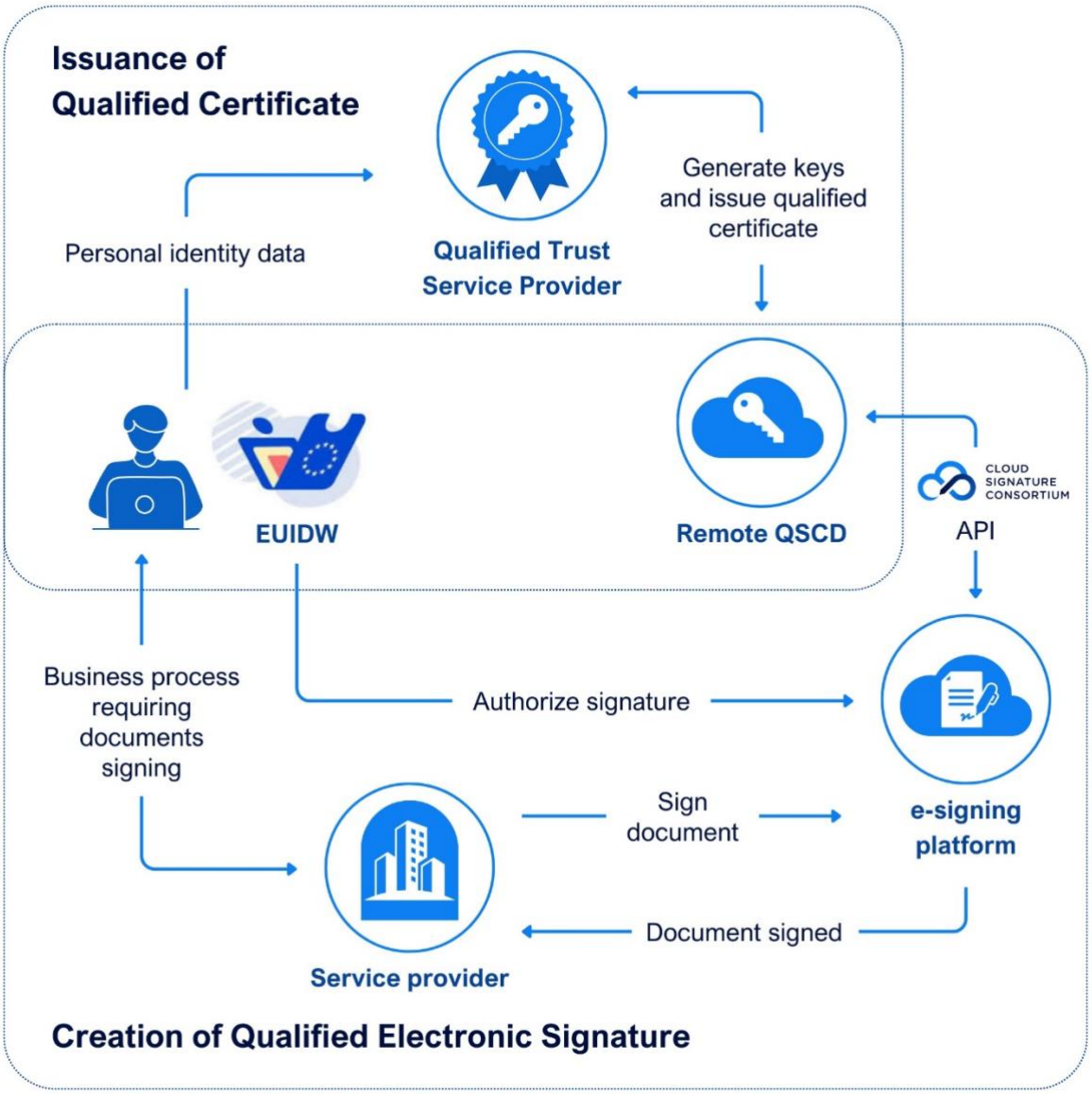

Figure #2

The role of the Cloud Signature Consortium (CSC) API

The CSC API is intrinsic to remote signing with QES. An e-signing platform sends a hash of the document to the QTSP via the CSC API. The hash is signed within the QSCD using the signatory's private key and returned to the e-signing platform. The signed hash is incorporated into a PDF document. The PDF document is now signed with QES and – as discussed above – the QES can be validated using a PDF reader or the European Commission's own validation tool.

Article 5a(5)(a)(xi) of eIDAS requires the EUDI Wallet to "*support common protocols and interfaces"* for creating QES by means of a QSCD. The CSC API will provide the technical interface between the EUDI Wallet, the e-signing platform and the QSCD to enable remote signing with QES (*see figure #2).* Article 12 of the draft Implementing Regulation on the "*integrity and core functionalities*" of the EUDI Wallet published by the European Commission in August 2024, also references the CSC API. It states in Article 12(3) that where "*signature creation applications are integrated into wallet instances, they shall support [the CSC API].*"

Remote signing with the EUDI Wallet for non-professional purposes

Article 5a(5)(g) of eIDAS provides that the EUDI Wallet offers "*all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.*"

This, however, is subject to an important caveat: EU member states may take "*proportionate measures"* to restrict free-of-charge usage of QES to "*non-professional purposes".*

The text of eIDAS does not define *professional* and *non-professional* purposes. In the absence of a clear definition, EU member states may interpret the meaning of *non-professional purposes*, and provide free usage of QES, in different ways. This may cause legal uncertainty and market fragmentation. It also risks undermining a primary aim of the European digital identity framework which is to harmonise the provision of qualified trust services in the EU bloc.

The EUDI Wallet is revolutionary. It will make digital transactions more efficient and secure. It will foster innovation and underpin the targets and objectives of the Digital Decade policy programme 2030. It is vitally important that EU member states recognise the benefits of remote signing with the EUDI Wallet and align on the meaning of *non-professional purposes.*

Non-professional purposes could, for example, encompass:

- personal, recreational, voluntary and non-commercial activities, but outside the scope of professional or business-related activities;

- interactions and transactions between a citizen and an EU public sector body; and

- interactions and transactions between a user and an EU academic institution such as schools and universities.

Funding remote signing with the EUDI Wallet for non-professional purposes

EU member states must carefully consider the funding model for qualified electronic signatures where the user signs documents remotely with the EUDI Wallet for *non-professional purposes*.

eIDAS does not specify how QTSPs will be remunerated for the provision and free usage of their qualified certificates. Remuneration must be offered on a fair, reasonable and non-discriminatory basis. We believe this is necessary to ensure that the activities of QTSPs are economically viable, and to sustain innovation, competition and a high level of trust in the QTSP ecosystem.

Every EU member state should ring-fence an annual budget for funding the provision and use of qualified certificates for *non-professional purposes*. This is an essential requirement for compliance with the EU member states' duties under eIDAS.

Conclusions

The EUDI Wallet – in conjunction with the CSC API – will accelerate digital transformation in the EU public and private sector, and contribute to the EU strategic agenda 2024-2029. The EUDI Wallet offers an easy and convenient way for users to obtain and sign documents remotely with a qualified certificate. This will be the catalyst for moving away from less secure, simple electronic signatures on e-signing platforms in favour of higher grade QESs. QES offers a higher level of identity assurance and cryptographic security. It is also the only type of electronic signature with the equivalent legal standing of a handwritten signature under eIDAS. This provides more certainty that the signed document will be valid and enforceable.

Nevertheless, more needs to be done to successfully promote the signature functionality built into the EUDI Wallet, facilitate user uptake, and harness the transformative potential of remote signing on e-signing platforms. If the EUDI Wallet is to achieve its full potential, EU member states should align on when a user is deemed to be signing for *professional* and *non-professional purposes*. They must also fund qualified certificates for the provision of free QES for *non-professional purposes*, and scale this funding as EUDI wallet adoption increases.

CLOUD SIGNATURE CONSORTIUM

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