Bridging the readiness gap for Free Qualified E-Signatures in the EUDI Wallet

Introduction

The European Union Digital Identity (EUDI) Wallet, mandated by the European Digital Identity Framework, represents a pivotal step toward fostering digital inclusion across Member States. Under Article 5a.13, by 28 November 2027, **all Member States must provide citizens with at least one EUDI Wallet that offers free qualified electronic signatures for non-professional use** to empower individuals with secure access to digital services.

However, based on our knowledge and data from the EU Trust List in February 2025, **most Member States have not made the decision on how to offer these free qualified e-signatures yet**. With the 2027 deadline fast approaching**, Member States face a tight timeframe to close this readiness gap** and must identify effective solutions quickly. The challenge is not only technical but also involves navigating logistical, financial, and regulatory hurdles to achieve a secure, accessible, and harmonized digital identity ecosystem.

This short paper presents the two implementation models to kick-start the discussion ahead of a time-sensitive deadline. It compares the **fully public infrastructure approach** and the **public–private partnership** model, to address the complexities of deploying free e-signatures while ensuring privacy, cybersecurity, and innovation and provides CSC recommendation based on its member expertise.

Fully public infrastructure model

In a fully public infrastructure model, governments assume complete responsibility for the design, development, management, and maintenance of the digital signature system. This centralized approach offers **governments unparalleled control over data and service delivery**. By directly managing the system**, governments can tailor solutions to national priorities and seamlessly integrate the digital signature service with other public services.**

However, this model also comes with significant challenges. **All the burden is on a single actor**. Relying exclusively on a fully public infrastructure for the European Digital Identity Wallet means that governments must assume complete responsibility for regulatory compliance, financial investments, technical oversight, and human resource management.

Public–Private Partnership model

Alternatively, a Public–Private Partnership model involves forming **strategic partnerships between government entities and private-sector organizations.** This collaborative model leverages the specialized expertise, innovation capacity, and technological agility of private companies while sharing development and operational costs with public institutions. For instance, **private partners can introduce agile software development methods and cutting-edge cybersecurity measures**, as well as services centred on seamless user

experience. Moreover, collaborative models can foster the establishment of common standards and protocols across Member States, as evidenced by the work of our industry consortia, the Cloud Signature Consortium[1] which helps ensure that remote signing processes and digital identity management remain aligned with the evolving requirements of the European Digital Identity Framework.

However, this model requires the establishment of **robust governance frameworks** to align incentives, manage data protection (in line with GDPR), and ensure clear roles, responsibilities and cost-sharing arrangement. Technological evolution in this field is progressing rapidly, which means continuous improvements in services and addressing cybersecurity threats come at a high cost, directly affecting the sustainability of these services.

Strategic recommendations

Member States now face the urgent task of closing their readiness gaps. In light of the short timeframe for deploying the EUDI Wallet, the **Cloud Signature Consortium (CSC) encourages public authorities to explore public–private partnerships as a beneficial strategy**. Selective outsourcing can help support governmental tasks and distribute responsibilities more effectively. By leveraging the specialized expertise and resources of private partners, governments can mitigate risks, ensure compliance, and meet critical deadlines. For instance, our CSC API[2] already enables interoperable e-signatures across Member States and is globally recognized in the eIDAS Implementing Act as a key resource for implementation standards.

Conclusion

Ultimately, the choice between a fully public infrastructure and a public–private partnership hinges on a careful evaluation of national priorities, budgetary constraints, technological readiness, and citizen trust. While a fully public model offers complete control and integration with governmental systems, its high resource demands and potential inflexibility may limit its long-term viability. Conversely, a public–private collaboration harnesses the innovation and efficiency of the private sector, offers a more scalable and cost-effective solution provided that robust governance and oversight are in place. **The Cloud Signature Consortium stands ready** to discuss this further with European government and support them to successfully implement the European Digital Identity Wallet.

About CSC

The Cloud Signature Consortium (CSC) is a global group of industry, government, and academic organizations committed to driving standardization of highly secure and compliant digital signatures in the cloud. The consortium is composed of more than 60 organisations from across the globe, who are leaders in the digital signatures sector. Drawing on the expertise of our members, the CSC has developed and regularly updates an API specification for Remote Electronic Signatures and Remote Electronic Seals. This solution allows users to seamlessly issue electronic signatures securely and is collaboratively developed by experts, who work closely with the ETSI team on Electronic Signatures, thus making it eIDAS compatible, while also meeting sole control requirements. At the EU level, CSC uses its expertise to help EU businesses and governments to successfully comply with the eIDAS Regulation by driving the standardisation of highly secure and compliant digital signatures in the cloud. Our vision for secure signatures is to achieve a single digital market across Europe and the globe.

[1] The EU digital identity wallet: a new tool for remote signing with qualified electronic signatures, Cloud Signature Consortium
[2] Protocols and API specifications, Cloud Signature Consortium