Agency for Digital Government

9. februar 2026

Follow-up on the Market Dialogue regarding Trust Services – Winter 2026

1. Introduction

The Agency for Digital Government (DIGST) has conducted a market dialogue to assess the availability of generally available Hardware and Software components required to support the Agency's Trust Services. As part of the market dialogue, suppliers have been invited to answer a number of questions.

DIGST is looking for off-the-shelf hardware components with the required functionality and certifications to provide eIDAS2 compliant solutions.

This paper contains a summary of the responses that the Agency has received in connection with the market dialogue. DIGST has received responses from a total of three suppliers. These are Keyfactor, IN Groupe and Cryptomathic.

2. Trust Services currently provided

DIGST is currently providing the following Trust Services:

- Issuance of Qualified and Non-Qualified Certificates for Electronic Signatures and Seals
- Creation of Qualified Time Stamps
- Creation of electronic signatures or electronic seals
- Management of remote electronic signature creation devices and remote electronic seal creation devices
- Qualified Validation of Certificates, Electronic Signatures, Electronic Seals and Time Stamps

3. Services provided by DIGST using Trust Services

eID Services and eID brokers create electronic signatures based on certificates provided by the trust services and are using HSM modules to protect the private key.

4. Current setup

The current setup is placed in two separate data centres in a highly available configuration.

4.1 CA component

Appliance solution from KeyFactor ("EJBCA Hardware Appliance") with multiple Utimaco CP5 PCI plug-in cards. The root CA and Issuing CA are using separate appliances. The root CA is offline.

4.2 The Timestamp component

Appliance solution from KeyFactor using Utimaco CP5 PCI plug-in card.

4.3 The Signing component

Cryptomathic Signer 5 in standalone server with Utimaco eIDAS Compliant network HSM appliance. The HSM appliance are CC certified according to the eIDAS Protection Profile (PP) EN 419 221-5 “Cryptographic Module for Trust Services”. The SAM Module is supplied with Cryptomathic Signer 5 with the appropriate CC Certification.

5. Follow-up on the market dialogue

5.1 Remote Management

Today Appliances (CA, Time Stamp, Signing-QSCD) are all placed in a special cage in the data centres with dual access control, i.e. securing that no one can be alone in the cage. Configuration and operational procedures are carried out by personnel being physically present in the cage. DIGST aims to open for remote management, thus limiting the requirement of being physically present in the data centre.

The suppliers were asked how their solution can be remotely managed and still adhere to eIDAS2/ETSI requirements for trust services, including management of CC key material. In the market dialogue, one of the suppliers outlined that their solution is designed for secure remote administration while respecting the requirements in eIDAS and ETSI EN 319 401/411/421 regarding trusted roles, dual control and protection of cryptographic key material. Another supplier explained that their solution allows remote management through asociated client programs based on smart card authentication. The supplier explained that any Issuing CA(s) can be remotely managed from a secure console room, which has been established with the required measures, including dual access control. At the same time it would be recommended that the physical environment in which the HSMs backing the Issuing CA(s) are hosted allow for emergency procedures to be performed in-person, including all prerequisites required to perform the same operations as can be performed remotely from a secure console room. Another supplier explained that their solution can be fully operated remotely over encrypted channels with the use of Smart Card Authentication.

5.2 CA

The Agency wishes to continue the current Root CA and Issuing CA's, where the CA key is to be migrated to a new HSM without compromising the key's certification level.

This model for continuation is important, in order to avoid a large-scale certificate replacement across both the public and private sector in Denmark.

The suppliers were asked how such a continuation can be realized using their HSM product(s) and which HSM products the CA key will be transferable to. One of the suppliers recommended that in the proposed architecture, the CA private key is generated and stored inside a Utimaco general purpose HSM and never leaves the HSM in clear. Continuation of the CA key in case of HSM replacement or platform upgrade is achieved through vendor supported secure backup, restore and migration mechanisms. Another supplier outlined that keys on Hardware Appliances using the Utimaco CryptoServer CP5 can be migrated to a net-attached Utimaco CryptoServer CP5.

Furthermore, the suppliers were asked to describe their recommendation for CA Software and associated HSM's going forward. Here, one of the suppliers recommended a standards-based, extensible CA platform backed by certified general purpose HSMs, with clear separation between root, issuing and OCSP or other service keys. Another supplier recommends that DIGST continues to use Keyfactor EJBCA Enterprise Edition as CA software going forward.

5.3 Remote Signing solution

The Agency wishes to move from the existing solution based on current Cryptomathic (Signer 5) based solution to a Cloud Signatory Consortium (CSC) based solution. The suppliers were asked to describe their eIDAS 2 compliant CSC V2 based remote signing solution, including Signing Software, SAM Module and QSCD.

One supplier replied that they have a compliant remote qualified signature and seal solution.

Furthermore, the suppliers were asked to describe their roadmap for remote signing using the EUDI Wallet.

In relation to this, one of the suppliers replied that they support remote qualified remote signing with the EUDI Wallet by extending its existing remote signing platform so that the wallet acts as the primary identification and consent interface, while qualified signing keys remain under QTSP control in a certified server side QSCD.

5.4 Remote EUDI Wallet WSCD/WSCA

The suppliers were asked to describe their plans to support remote HSM based WSCD/WSCA implementation. In this regard, one of the suppliers replied that they are investing in support for Wallet Secure Cryptographic Application (WSCA) and Wallet Secure Cryptographic Device (WSCD) concepts based on remote HSMs.

5.5 Certification roadmap

The suppliers were asked to describe their roadmap for CC/EUCC certification of their products according to eIDAS2. Here, one of the suppliers replied that they do not have a roadmap for CC/EUCC certification of the mentioned products.

Another supplier replied that EJBCA 7.4.1.1 is common criteria certified, and EJBCA 9.3 has pending common criteria certification. The supplier added that they have completed all lab testing and that documentation has been sent to NIAP for review/approval. SignServer is not common criteria certified as, under common criteria, there should exist a defined “protection profile” for the product to be evaluated against. To the supplier’s knowledge, there does not exist a protection profile created for digital signature products. Utimaco CryptoServer CP5 and Thales Luna are both common criteria certified. Another supplier replied that they already operate key components of its remote signing solution under Common Criteria and has a roadmap to maintain and extend certification in line with eIDAS 2 and the future EUCC scheme.

Furthermore, the suppliers were asked to describe their plans to certify their products as CRA “Class I” Products. In relation to this, one of the suppliers replied that they expect all mentioned products to be certified by the deadline set by the implementing act for CRA "Class I" products (11th of December 2027). Another supplier replied that they intend to align the relevant components of their remote signing and trust services platform with the EU Cyber Resilience Act (CRA) as Class I products with digital elements, to the extent they fall within the CRA annex categories.

5.6 Support for development and test

The agency is using several environments to support development and test. The suppliers were asked to describe how this can be supported in a cost-effective manner. In relation to this, one of the suppliers replied that to ease development of new products there exist simulators or cloud-based services, which developers can quickly make use of.

Another supplier replied that the recommended setup is a test environment, an acceptance environment, and a production environment. They added that test

practice is to mirror the production environment on the acceptance environment and that a test environment can have reduced capacity.

Another supplier replied that they support cost-effective deployment by combining software based HSM simulators for all non-production work with flexible sharing and phased scaling of physical HSM appliances in production.

5.7 Network appliances vs PCI cards in servers

The suppliers were asked to explain the pros and cons of using network appliances vs PCI cards in (appliance) servers.

In relation to this, one of the suppliers replied that HSM network appliances allow for better utilization and hence may be more cost efficient than PCI cards, as they allow multiple applications using a shared appliance and there are no specific requirements to the hardware running the applications like available PCI slots. Further high availability and scalability may be easier to achieve since you do not need specific hardware management whenever an extra application client is added to the setup. Network appliances are, however, often more expensive than PCI cards – so for smaller and static deployments PCI cards may be a cheaper option. It is likely that both types of HSMs must be purchased to accommodate the CC requirements most cost-effectively, network appliance(s) for the PKI and PCI card(s) for the QSCD.

Another supplier replied that Built-in PCI cards, as installed into the Keyfactor Next Generation Hardware Appliance, do not require additional training, support contract, license, and maintenance. The supplier added that network attached HSMs requires dedicated training, support contract, license, and maintenance. However, multiple applications can use the same HSM, providing flexibility. Another supplier replied that their solution can operate with both network attached HSM appliances and PCI HSM cards. The supplier added that the choice affects capacity management, cost and operational complexity.