PSD2 keys in Trident HSM

By storing cryptographic keys on Trident HSM, Information security is not an issue, even after PSD2

The new directive on payment services (PSD2) affects a great number of organizations, banks and service providers in the EU. According to the regulation, the financial service providers have to offer new opportunities for their customers and partners while maintaining the appropriate level of security for their customers' data and their transactions.

The purpose of this document is to explain how Trident HSM can help you meet the security-related conditions of PSD2. Storing your cryptographic keys on this eIDAS-approved device ensures that you fulfil the requirements while also enhancing the security of your systems.

PSD2 and the service providers

The regulation aims to enable the customer base of banks to manage their finances in a simpler and more transparent way. To achieve this, financial institutions need to introduce new services and capabilities. However, the new services might create new data security issues that need to be addressed.

One of these is that Account Servicing Payment Service Providers (ASPSP) must allow certain (previously approved) external organizations to connect to their systems and access certain data, with the permission of the customers. This enables the third-party providers to offer personalized services to customers based on the information accessed.

Authorized third party providers are the following:

- **Account Information Service Providers (AISP):** organizations that provide information services about the payment accounts
- **Payment Initiation Service Providers (PISP):** they provide the service to set up payments
- **Card Issuing Service Providers (CISP):** provide information about the funds availability on payment transactions based on the payment cards

All organizations that deal with PSD2 should set up their security levels in line with these categories.

HSM provides the safest way in order to meet the requirements and ensure the appropriate level of security, data and communication among the service providers have to be protected with cryptographic keys. Since these keys ensure the protection of the sensitive information, they need to be stored the safest way possible.

The most secure device the cryptographic keys can be stored on is a hardware security module (HSM), like Trident HSM. It is capable of safeguarding and managing the keys efficiently. The keys remain in your physical location and within your systems constantly, so you can be sure they cannot be copied, cloned or backed up without your knowledge and permission. Therefore, unauthorized parties cannot access your keys, nor the data they are protecting.

eIDAS certificates for greater security

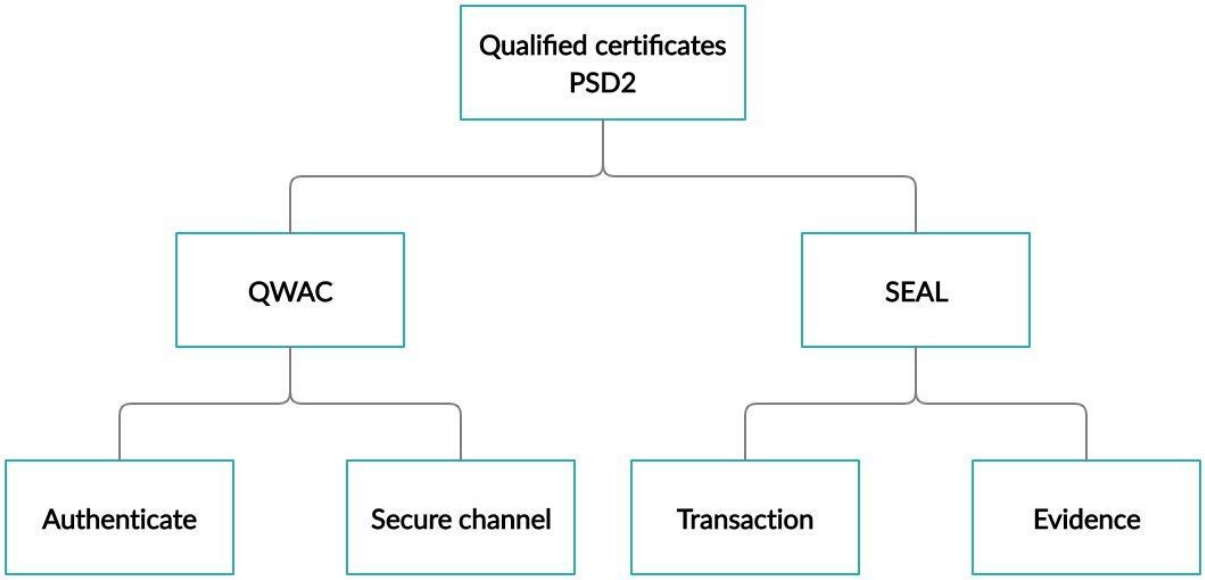
Cryptographic keys are essential in the protection of communication among the specific parties described in PSD2 as well. The financial institutions must ensure that they can communicate with AISP, PISP and CISP organizations in a secure, encrypted and authenticated manner. To do this, they must use certificates based on the Public Key Infrastructure (PKI), which is regulated by **eIDAS**, the EU's regulation on electronic identification and trust services for electronic transactions in the internal market.

The two types of eIDAS certificates for ensuring this type of secure communication:

- **Qualified Website Authentication Certificates (QWAC):** ensuring identification at the transport layer, namely the appropriate authentication and the secure channel
- **Qualified Certificate for Electronic Seals (QSEAL):** ensuring identification at the application level, confirming the authenticity of the transactions and messages and protecting them from potential attacks

A list of Qualifies Trust Service Providers offering QWAC and QSEAL certificates is available at the website of Open Banking Europe. The financial service providers have to use certain certificates individually or combined in different scenarios:

- **QWAC** certificates can be used individually in cases when the payment service providers have to identify themselves and communicate securely but no evidence is needed to confirm that the data submitted originates from the identified provider.
- **QSEAL** certificates enable payment service providers to identify themselves to each other but cannot ensure confidentiality during the communication.
- **QWAC and QSEAL certificates used parallelly** allow the payment service providers to identify themselves to each other, communicate securely and ensure that the data submitted originates from the previously identifies parties.



No matter how the providers use or combine QWAC and QSEAL, the qualified seals for these certificates must be created, and the related **private keys** are supposed to be stored in a safe place since they ensure the security of the communication and the processes. The keys need to be safeguarded by the owner of the certificates and cannot be accessed by unauthorized parties. In order to ensure the appropriate protection of the keys, the regulation orders organizations to store them on specific ways, namely HSM devices that have been previously verified and approved. **Trident HSM** is one of these products and moreover, it features a very unique secure multiparty computation capability that provides even greater security than its competitors.

The ideal solution

Service providers can access the list of the approved devices here, and i4p's Trident HSM (formerly known as distributed remote Qualified Signature Creation Device (drQSCD) v1.0), has recently been inspected, verified, approved and added to the list.

Trident HSM is not only one of the solutions capable of offering service providers the required secure connection to open banking platforms, but also the first in the world to feature the mentioned **multi-party cryptography capability**. This means that it can create, store and delete secret codes, cryptographic keys in a **distributed manner**, so no key data can be identified on any device independently. If this feature is in use, at least two device, two approval is necessary for the encrypted data to be useful.

Trident HSM features high availability and can easily be integrated into existing infrastructures. The solution also enables both local and remote users to use multi-factor authentication and allows local client applications (LCAs) to be installed into its protected environment. LCAs run in protected containers to ensure that they are isolated from other LCAs and from the HSM core.

As a result, the solution offers the highest level of protection required in business – not only for the financial industry but for other sectors as well.