CASE STUDY: QUALIFIED ELECTRONIC SIGNATURE WITH A SMARTPHONE – THE EASIEST WAY POSSIBLE

Trust service provider Microsec is one of the first to offer a highly accessible and easy-to-use qualified electronic signature with remote key management service thanks to the revolutionary solution of i4p.

Microsec e-Szignó Certification Authority has set the goal of launching a qualified remote signature service as soon as the related system of standards has been established.

The signing solution, based on remote key management, allows key owners to initiate a signing operation from any of their devices, including smartphones, tablets, notebooks, and desktops, in a much simpler and faster way than ever before. The process of a qualified electronic signature has so far required a qualified electronic key storage device, a reading device and a computer. And now, even a mobile phone and the qualified remote key management service are enough. By managing the key for qualified signatures in server-side qualified signature creation devices, Microsec is able to offer its customers more freedom than ever while at the same time meeting standards and security requirements.

About Microsec

The Budapest-based Microsec trust service provider offers outstandingly high-quality services in the field of electronically authentic and legally binding documents, as well as business solutions based on electronic signatures.

Year of foundation: 1984

Number of employees: 110+

Number of engineers: 50

Further information: https://www.microsec.hu/

The challenge: managing the keys

eIDAS

eIDAS is the regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions, including electronic signatures.

Since Microsec wanted to launch the service as quickly as possible, they decided not to start developing their own solution, which they would have had to certify as well. Instead, from the products available in Europe, they chose the ready-to-use **server-side qualified signature creation device** that best suits their needs – the Trident HSM solution of i4p. The most secure form of electronic signatures is the qualified electronic signature, which is based on a qualified certificate and requires a QSCD (Qualified Signature Creation Device) to create it. Server-side or remote signature creation is important because in this case, the signing key is not stored in the key holder’s own device (e.g. chip card), but in the trust service provider's QSCD device, i.e. in the Trident HSM supplied by i4p, and the signature is performed by the service provider on behalf of the key holder. This allows customers to initiate a signing operation from almost any devices.

Microsec took into consideration a total of 65 different aspects when evaluating the appropriate solutions in several rounds. They found only four software and hardware suppliers in the European market that had the appropriate tools for this purpose on offer. The evaluation criteria for the company included testability, supported cryptographic algorithms, the structure of architecture, remote and on-site support, as well as duration of integration, while certainly return on investment also played an important role. Furthermore, they also assessed what internal improvements are needed to operate each function and what support the candidates can provide this.

The quotation of i4p proved to be outstanding in terms of the aspects listed, in addition they offered a cost-effective solution that ultimately proved to be appropriate in all respects. Moreover, i4p is easily and quickly available, they can even provide on-site support and respond flexibly to requests and expectations. Therefore, after a very thorough selection process, i4p was chosen.

The solution: a qualified electronic signature anywhere, anytime

Thus, Microsec is one of the first companies in Europe to offer such an easy-to-use service in accordance with the regulations accessible from anywhere that enables the creation of a qualified signature with the legal effect of a private document representing conclusive evidence even through a mobile phone. In addition, all this can be done with as few tools as possible, in an extremely simple and user-friendly way.

Microsec stores the keys in its own data centres, in the highly secure devices of i4p. They use both their own and leased data centres, which operate under strict control. The solution of i4p, Trident HSM, ensures the secure storage of and controlled access to the keys in accordance with the new eIDAS standards. In this way, customers can be sure that the keys function at maximum security.

The Trident HSM is capable of creating not only qualified electronic signatures and seals, but also remote qualified electronic signatures and seals, so it acts as a kind of a 2-in-1 solution and has all the necessary certificates. It has obtained the strict Common Criteria EAL4+ certification, which means that both qualified signatures and QSEALs can be created using it.

i4p, an expert in the background

The Trident HSM has been developed by professionals who are fully aware of the needs and challenges facing trust service providers as formerly they also created, brought to success, and later sold a qualified certification service provider company. As a result, they have considerable expertise in both cryptography and product and service development, and know exactly what solutions can effectively serve the needs of trust service providers.

The device also includes a Signature Activation Module (SAM). In this way, it complies with the related requirements as it guarantees the provisions of eIDAS, i.e. it provides sole control for the key holder.

The device can be easily integrated into any signature creation user application. In addition, it can be combined with the Secure Multi-Party Computation capability of Trident HSM, which makes it possible to organize multiple HSM devices into a distributed cluster and even manage the cryptographic keys in this cluster separately. In this mode, key data cannot be identified in any individual device, thus if a device is compromised, the information that can be obtained is worthless. Consequently, Trident HSM offers the safest method currently available.

Remote qualified signature

Providers may only use certified devices to create remote qualified signatures that guarantee exclusive use at Sole Control Assurance Level 2 (SCAL2) according to the standard Common Criteria (CC) EN 419 241-2 “QSCD for Server Signing” Protection Profile (PP). The Trident HSM also complies with this strict regulation.

Based on the innovative solution of i4p, Microsec provides the opportunity for both domestic and international customers to use electronic signatures more easily than ever before. This will facilitate the proliferation of electronic signatures, thereby simplifying administrative processes and reducing associated costs, as well as further expanding paperless offices and home office.