EVIDEN

cryptovision SCinterface VSC

Virtual Smart Card with flexible back end

The use of a physical smart card is not always feasible. SCinterface VSC from Eviden Digital Identity makes it possible to use a Trusted Platform Module (TPM) like a smart card. The use without a TPM or in a hybrid mode is equally supported. SCinterface VSC, an extension of the proven smart card middleware cryptovision SCinterface, offers more than the discontinued Microsoft VSC and allows a smooth migration.

The TPM as a security anchor

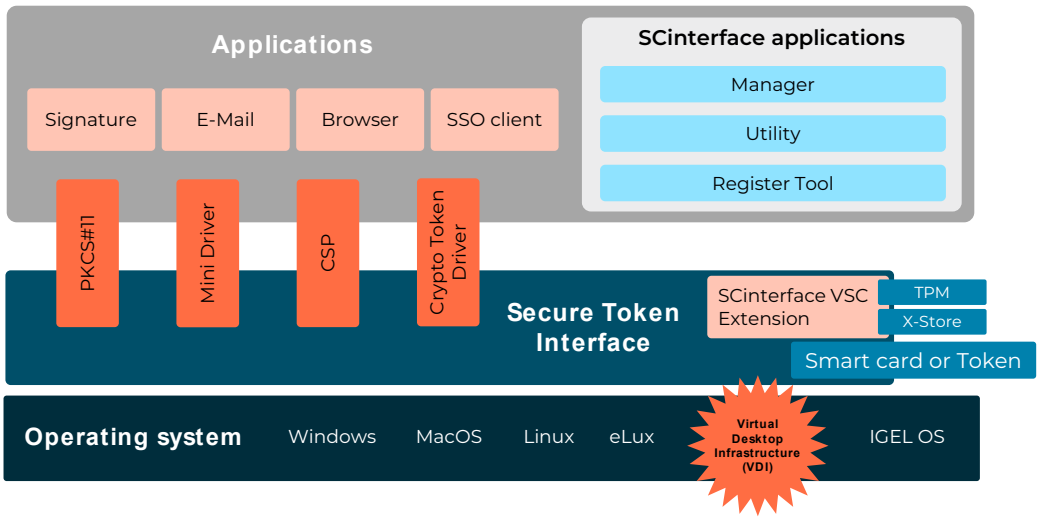
A Trusted Platform Module (TPM) is a security chip permanently integrated into commercially available PCs. It contains, among other things, a trusted root key. This hardware security anchor can be used to protect a virtual smart card against manipulation.

For a long time, the Microsoft Virtual Smart Card (MS VSC) was the leading solution for emulating a smart card using a TPM. Microsoft is currently focusing on certificate-less authentication techniques and has announced that it will no longer support the MS VSC in the future.

Cryptovision SCinterface VSC is an innovative VSC solution that was developed as an extension of the proven smart card middleware cryptovision SCinterface from Eviden Digital Identity. It can fully replace the Microsoft Virtual Smart Card.

SCinterface VSC not only offers all the functions of the Microsoft VSC, but also a number of additional powerful features, such as secure key injection. With the TPM-based version of the SCinterface VSC, operations with private key material take place exclusively on the TPM.

A smooth transition from the Microsoft VSC to the new solution is possible without any problems and without having to forego any of the familiar functions. SCinterface VSC is therefore the ideal choice for making certificate-based two-factor authentication solutions future-proof, secure and efficient.



SCinterface VSC enables a PC application to use a Trusted Platform Module (TPM) like a smart card.

EVIDEN

Flexible back end

Unlike the MS VSC, SCinterface VSC can be used in a hybrid mode with TPM protection, on Windows systems without TPM 2.0, and on Linux-based systems in addition to the TPM-only mode. This so-called X-Store functionality greatly expands the possible usage scenarios.

The hybrid mode enables the TPM-protected use of key material that is not natively supported by the existing TPM (e.g. RSA 4K). In this case, the key material is stored in the file system protected by the TPM root key and the user credentials, and is only decrypted briefly to carry out specific operations, thus making the private key usable.

If no TPM is used, the encrypted private key material is stored in the file system as well. In this mode of usage, private keys are secured by the user credentials (PIN/PUK). It is also possible to bind the key material to permanently installed hardware components using dedicated IDs in order to further increase the level of security.

Smooth migration

SCinterface VSC extends the functionality of the proven smart card middleware cryptovision SCinterface. Cryptovision SCinterface supports a wide range of cards and tokens on different platforms, using common interfaces such as PKCS#11, Microsoft CNG and Apple Crypto Token Driver.

Cryptovision SCinterface has been used by numerous companies and authorities for almost two decades and is also widely used as middleware for electronic identity cards.

What sets cryptovision SCinterface apart is the additional support of various extensions for secure PIN caching, the use of remote keys, and a dedicated virtual smart card in the form of SCinterface VSC. Not only do customers have the option of switching smoothly from the Microsoft VSC to the SCinterface VSC, but they can also easily switch from and to any other card or token or use them in parallel. The user experience remains identical regardless of the chosen form factor.

Key Features

TPM use as a smart card

SCinterface VSC enables the TPM of a device to be used like a smart card. All smart card functions are emulated.

Simple migration from Microsoft VSC

SCinterface VSC can be operated in parallel to Microsoft VSC with the same functionality, which enables a smooth migration.

Key formats

SCinterface VSC supports different key formats. The Microsoft VSC, on the other hand, requires a FIPS-186-4-compliant format, which can lead to incompatibilities, especially with older keys.

Additional functions through X-Store

Thanks to the X-Store, which enables the secure use of storage areas outside the TPM, SCinterface VSC supports numerous functions that the Microsoft VSC does not offer. This includes the storage of any number of crypto keys as well as the use of 3K and 4K RSA keys. In addition, elliptic curve (ECC) algorithms can also be used on the basis of brainpool curves, which Microsoft VSC does not support.

Crypto interfaces

SCinterface VSC uses the TPM via the crypto interfaces PKCS#11 and Microsoft CNG (including Smart Card Minidriver). Other platforms will also be supported in the future.

ISO/IEC 7816 and PKCS#15

SCinterface VSC supports the smart card file system defined in the ISO/IEC 7816 and PKCS#15 standards. Unlike the Microsoft VSC, all functions are available.

Compatible with other smart cards

The SCinterface smart card middleware supports over 100 smart cards and tokens. Parallel operation with the VSC is possible without any problems, which enables simple migration.

VDI integration

SCinterface VSC can be integrated into a Virtual Desktop Infrastructure (VDI).

EVIDEN

Who uses cryptovision SCinterface?

Cryptovision SCinterface is used by the following customers, among others:

Allianz

The market-leading German insurance company based in Munich uses cryptovision SCinterface to connect multi-application smart cards on different platforms to the respective application.

Energy Supplier

An energy supplier is active in the consolidating markets of Europe and growing globally. Cryptovision SCinterface is an important component for securing access to company data and is also used for digital signatures.

European Patent Office

The European Patent Office (EPO) uses cryptovision SCinterface to secure online patent applications. Cryptovision SCinterface replaced an existing proprietary solution that had led to a vendor lock.

Standards and technical spezifications

Operating systems

- Windows 10, 11
- Windows Server 2016, 2019, 2022
- Linux Ubuntu 24.04

Formats

- PKCS#15
- ISO/IEC 7816
- PC/SC
- ISO/IEC 19794-2
- PKCS#10
- PKCS#12

TPM

- TPM 2.0

Crypto interfaces

- PKCS#11
- Microsoft CryptoAPI
- Microsoft CNG

Crypto algorithms and key lengths

- 2K RSA on a TPM 2.0
- 3K/4K RSA per X-Store via the crypto library BOTAN
- Elliptic Curve Cryptography (ECC) with the NIST curves supported by the TPM
- ECC Brainpool curves per X-Store via the crypto library BOTAN

Find out more about us: www.cryptovision.com

Connect with us

eviden.com

20250129