cryptoVision

sc/interface

Smart Credential Middleware with biometry and MS VSC support

sc/interface integrates credentials stored on smart cards and other security tokens into IT environments. sc/interface supports more than 90 smart cards, security tokens and profiles across all major operating systems. Many useful features, including fingerprint recognition and Microsoft Virtual Smart Card support, are available.

MANAGEMENT SUMMARY

The rising demand for electronic identity verification requires much more than simple user names and passwords. Two-factor authentication – especially based on a smart card (or another smart token) and a PIN – is therefore a must. As a very mature solution, smart cards have been widely deployed for years on bank cards and more recently on electronic ID cards.

With many different smart card options, the hardware typically is not an issue. In fact, successful projects depend much more on the middleware (smart credential middleware) used. Smart credential middleware is software connecting a smart token (including the credentials stored on it) to an application. In the current heterogeneous IT world, smart credential middleware should not depend on specific operating systems or devices. Instead, it should be platform independent and support a broad number of applications across differing devices. In addition, strong security demands smart credential middleware that utilizes standards based protocols and advanced cryptographic methods.

sc/interface is powerful smart credential middleware which connects applications (Outlook, Edge, Safari, Firefox, etc.) to the desired smart card or token. It supports all relevant cryptographic interfaces for every major operating system: Microsoft CSP and Minidriver (for Windows), PKCS#11 (for Linux derivatives, Windows, and macOS), and Apple Crypto Token Driver (for macOS). With hardware support for over 90 card/token types and profiles (including Microsoft Virtual Smart Card), sc/interface removes dependence on any single card vendor and provides unrivaled interoperability.

Supporting RSA and Elliptic Curve Cryptography (ECC), sc/interface meets the most demanding encryption standards recommended by security agencies worldwide. ECC support is especially important, as the security of some cards using RSA has recently been questioned. Other features, like platform independence, modular architecture, implementation of all major security standards (including PACE), support of Microsoft Virtual Smart Card (MS VSC), IBM Tivoli certification and optional full biometry support as well as optional PIN caching (across applications), make sc/interface one of the most innovative solutions of its kind on the worldwide market.

BACKGROUND

What is Smart Credential Middleware?

Operating system login, VPN access, encryption, digital signatures, and similar use cases need appropriate protection. Many enterprises still use passwords for this purpose, which is neither secure nor convenient. As a replacement for passwords, more and more enterprises currently deploy two-factor authentication based on smart cards (or smart tokens) and PINs (or biometric credentials). A smart card stores a secret key (credential) that replaces the password and can additionally be used for encryption and digital signatures.

In order to use a smart card on a PC, smart credential middleware is necessary. Smart credential middleware is a software component that connects a smart card (or a smart token) with one or several applications. The core of it is a driver that offers a high-level crypto interface to applications and that communicates with the smart card via a (proprietary) low-level interface. In addition, many smart credential middlewares comprise a management tool for formatting, personalization and similar tasks. As many users use the same card on different devices, several operating systems need to be supported. In addition, there are dozens of smart card types with proprietary card interfaces and different crypto interfaces.

THE BASICS

Crypto Interfaces Supported

The most common crypto interface is PKCS#11. It is supported, among others, by Firefox, IBM Notes, Adobe Reader and many Linux applications. Microsoft has created their own crypto interfaces: Cryptography API Next Generation (CNG) and its fore-runner Microsoft Cryptographic API (MS CAPI). CNG includes the concept of Smart Card Minidriver. A Minidriver is a module that allows organizations to easily deploy smart cards by automatically downloading necessary connectors from Microsoft. Finally, MacOS provides the CryptoTokenKit (CTK) framework for macOS, including the concept of Crypto Token Drivers.

sc/interface supports PKCS#11, MS-CAPI and CNG (it includes a Smart Card Minidriver), and provides a Crypto Token Driver.

sc/interface
sc/interface is advanced smart credential middleware ideal for customers demanding a high security level without compromising flexibility. The flexibility sc/interface delivers allows for a single token to become a multipurpose device. sc/interface makes it easy to consolidate physical access with payment applications, secure website access, and digital form signing.

eIDAS compliance
sc/interface supports „Siegel" tokens and signature cards compliant with the European digital signature regulation, eIDAS.

Platforms
sc/interface is available for Microsoft Windows, Linux, and macOS. A user can use the same smart card on different platforms.

Smart Card Types
sc/interface supports more than 90 card/token types and profiles, including the latest Java Card generations and cards supplied by Atos, Infineon, NXP, Gemalto, G&D, Siemens, and Austria Card. All common smart card form factors are supported.

Plug-ins
The functionality of sc/interface can be extended with a plug-in that informs the user about soon-to-expire certificates and with another plug-in that automatically imports root certificates stored on the smart card.

Convenience Kit
Via add-ons (available in a convenience kit), sc/interface supports match-on-Card fingerprint authentication (sc/interface biometric) as well as secure PIN caching (sc/interface cache).

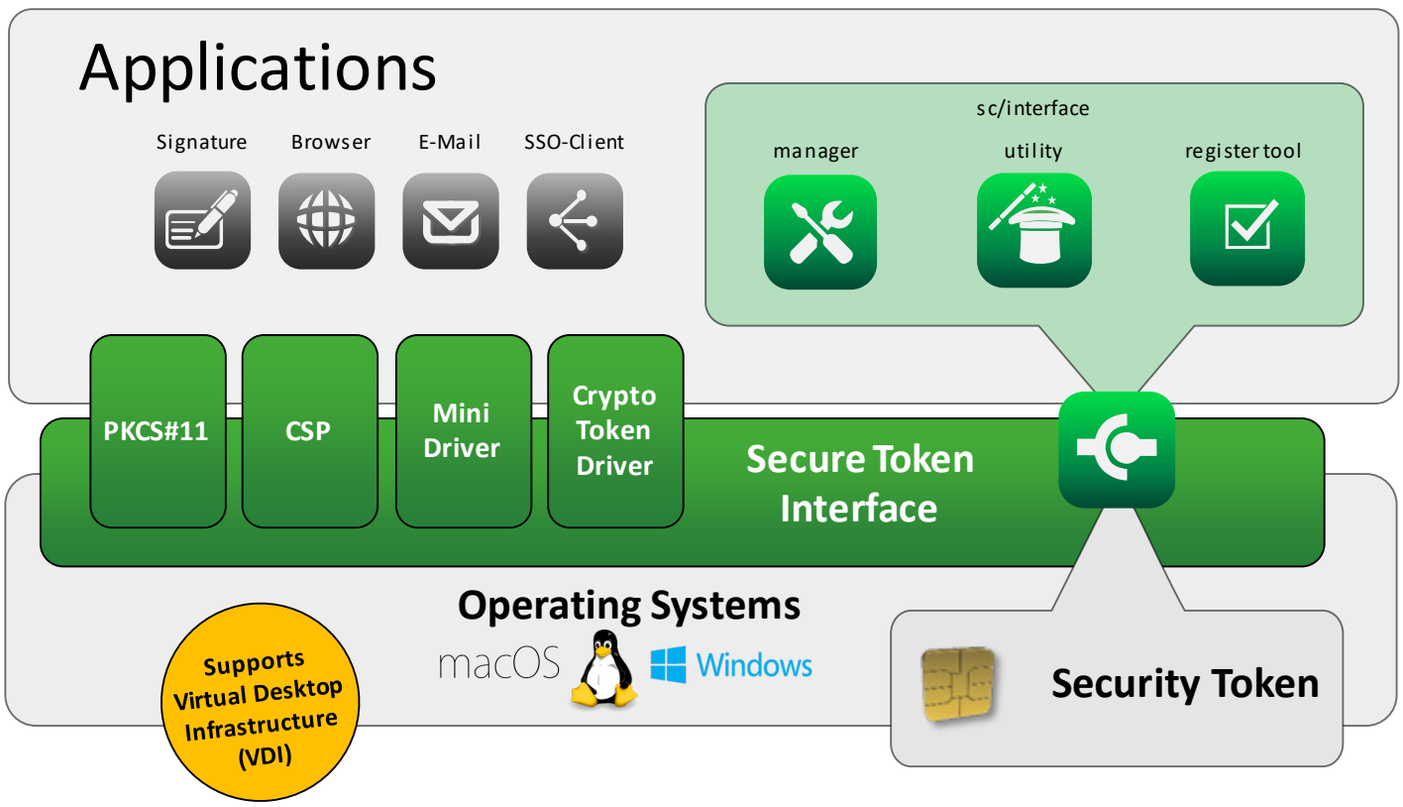
Microsoft Virtual Smart Card
sc/interface supports Microsoft Virtual Smart Card (MS VSC), including initialization and personalization processes. Thus, sc/interface enables the use of existing infrastructure in the case of a (partial) migration to MS VSC.

Crypto Interfaces
sc/interface interoperates with virtually every application program on the market (e.g. Edge, Firefox, Outlook), supporting all major crypto interfaces: PKCS#11, CSP, Minidriver, and CTK.

eID Documents
Government eID projects with millions of cards issued require coverage of all common platforms for broad user acceptance. sc/interface covers all major operating systems and supports modern security protocol standards like PACE.

THE TECHNICAL PART

sc/interface consists of several modules. The system components provide access interfaces (MS-CAPI, CNG, PKCS#11, CryptoTokenKit), while sc/interface manager and sc/interface utility are used for management tasks.



MODULES

sc/interface contains the following modules:

- **sc/interface manager:** Provides a complete range of card/ token management functions (e.g., initialization, profiling, PIN management, key generation, fingerprint enrollment).
- **sc/interface utility:** Provides card/token management functions typically needed by users (e.g., PIN change, fingerprint enrollment).
- **Register Tool:** Registers digital certificates stored on the card or token on the Windows operation system.
- **CSP Module:** Provides a Cryptographic Service Provider (CSP) to connect to the Microsoft Crypto API on Windows systems.
- **Smart Card Minidriver:** Connects to the Cryptographic API Next Generation on Windows systems.
- **PKCS#11 Module:** Connects to a PKCS#11 interface, e.g., for use with Linux derivatives, macOS, and many application programs. All major card management systems use PKCS#11 for card initialization and personalization.
- **Crypto Token Driver:** Connects to the CTK framework of macOS.

sc/interface and ePasslet Suite

sc/interface can be combined with cryptovision's ePasslet Suite. It supports the ePKI applet as well as the Common Criteria certified ePasslet Suite 3.0 with SSCD profile.

SUPPORTED SYSTEMS

Microsoft:
- Windows 7 SP1, 8.1, 10
- Windows Server 2008 SP2 / R2 SP1, 2012 R2, 2016

Linux:
- RHEL 6, 7
- Ubuntu 16.04 LTS / 18.04 LTS
- SLES 15

macOS:
- El Capitan (10.11.1)
- Sierra (10.12)
- High Sierra (10.13)

Success story

SwissSign, a leading provider of innovative identity solutions and subsidiary of Swiss Post uses cryptovision's smart credential middleware sc/interface for their product SuisseID.

SuisseID is a smart card, which stores certificates and private keys of its owner. SuisseID is accompanied by signature software (SwissSigner) and a solution for secure communication (IncaMail). The easy handling is granted by sc/interface, which is bundled with SuisseID software.

Thanks to sc/interface the SwissSign signature cards and tokens can be used on Windows, macOS and Linux computers. No matter if the user accesses protected websites, signs PDF documents digitally or performs other cryptographic operations, sc/interface always works transparently in the background and thus rises customer satisfaction.

Customers

sc/interface is used (among others) by the following customers:

- Government of Nigeria: Nigerian identity authority NIMC issues electronic identity cards to the 160 million inhabitants of the country. sc/interface is used to connect this card to its applications.
- Husky Energy: The Canadian energy supplier Husky Energy uses sc/interface for securing laptops.
- Minimax: The German fire protection supplier Minimax uses sc/interface for smart card authentication.

About cryptovision

cryptovision is a leading supplier of secure electronic identity solutions. Based on our two decades of market experience and broad background in modern cryptographic techniques, such as Elliptic Curve Cryptography, our products provide state-of-the-art and future-proof technologies. We produce innovative eID applications, security token interfaces, digital certificate infrastructures, and cryptographic development tools, which are key to securing identities, data, and communication worldwide.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 500 million people worldwide make use of cryptovision products every day in such diverse sectors as automotive, retail, industry, financial, government, law enforcement, and defense.

cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

T: +49 (209) 16724-90
F: +49 (209) 16724-61

cv cryptovision
100 Park Avenue / Suite 1600
New York, NY 10017, USA

T: +1 (212) 984 0750
F: +1 (212) 880 6499

info@ cryptovision.com
www.cryptovision.com