

EVIDENZ

cryptovision SCinterface

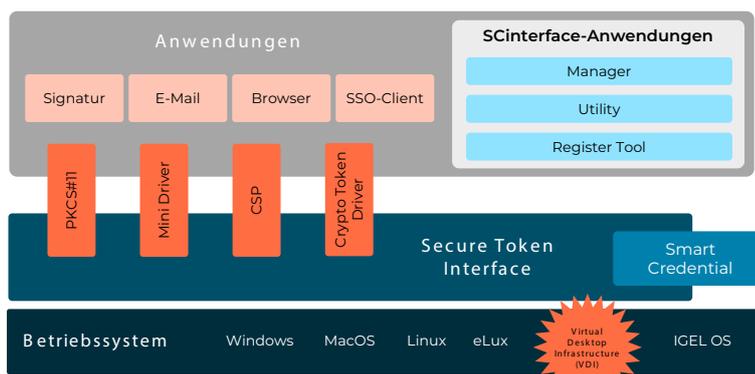
Integration von Smartcards und anderen Security-Token

Cryptovision SCinterface integriert Smartcards und andere Token in IT-Umgebungen. Cryptovision SCinterface unterstützt über 100 Smartcards, Security Token und Profile auf allen gängigen Betriebssystemen. Es gibt zahlreiche nützliche Features, einschließlich Biometrie und Unterstützung von Microsoft Virtual Smart Card.

Eine leistungsfähige Middleware

Ein Benutzer, der sich an einem IT-System anmeldet, nutzt dazu normalerweise ein Passwort – dies ist jedoch eine unsichere Methode. Als Alternative kann eine Zwei-Faktoren Authentifizierung verwendet werden, zum Beispiel in Form eines Schlüssels auf einer Smartcard oder auf einem Sicherheits-Token zusammen mit einer PIN. Diese Technik hat sich seit Jahrzehnten bewährt – unter anderem für Bankkarten, elektronische Personalausweise oder Speicher für Berechtigungsnachweise.

Der Erfolg einer solchen Lösung hängt weitgehend von der Software ab, mit der die Karte angesprochen wird – der Middleware.



Cryptovision SCinterface besteht aus mehreren Modulen. Einige davon sprechen Kryptoschnittstellen wie MS-CAPI, CNG, PKCS#11, CryptoTokenKit an, andere dienen der Administration.

Eine Middleware sollte nicht auf einen bestimmten Chiptyp oder ein bestimmtes Betriebssystem beschränkt sein. Stattdessen sollte sie plattformunabhängig arbeiten und so viele Anwendungen wie möglich unterstützen. Darüber hinaus sollten standardisierte Protokolle und moderne kryptografische Verfahren verwendet werden.

Cryptovision SCinterface ist eine leistungsfähige Middleware, die den Einsatz von Karten und Token in einer Vielzahl von Sicherheitssystemen ermöglicht. Sie unterstützt alle relevanten Schnittstellen auf allen wichtigen Plattformen.

Starke Authentifizierung

Eine Smartcard oder ein Sicherheits-Token ist das ideale Medium, um einen kryptografischen Schlüssel sicher und bequem zu speichern. Im Gegensatz zu einer Schlüsseldatei auf einem PC kann der Benutzer eine Karte oder ein Token stets bei sich tragen und bei Bedarf darauf zugreifen. Nachdem der Schlüssel in den Karten-/Tokenchip importiert oder auf diesem generiert wurde, hat nur der Prozessor des Chips Zugriff auf diesen. Ein Schlüsselexport gehört nicht zum Funktionsumfang. Um die Karte oder das Token zu nutzen, muss der Anwender eine PIN oder einen Fingerabdruck eingeben.

Eine Smartcard oder ein Token mit einem kryptografischen Schlüssel kann zur Authentifizierung verwendet werden. Eine solche Lösung stellt eine wichtige Alternative zu einem Passwort dar. Darüber hinaus eignet sie sich für die Verschlüsselung und das digitale Signieren.

Smartcards und Sicherheits-Token sind in zahlreichen Formfaktoren erhältlich, beispielsweise als Kontaktkarten, RFID-Chips, USB-Token oder als µSD-Karten.

Um ein Sicherheits-Token auf einem PC zu verwenden, ist eine Software (Middleware) erforderlich, die den Chip mit einer Anwendung verbindet. Das Herzstück einer Middleware ist ein Treiber, der der Anwendung eine Krypto-Schnittstelle zur Verfügung stellt und diese auf elementare Befehle für das Sicherheitstoken abbildet.

Krypto-Schnittstellen

Die wichtigste Krypto-Schnittstelle ist PKCS#11. Diese ist herstellerunabhängig und wird unter anderem vom Mozilla Firefox, HCL Notes und dem Adobe Reader genutzt. Auch viele Anbieter von Thin-Client-Betriebssystemen unterstützen PKCS#11.

Microsoft hat für den gleichen Zweck eigene Schnittstellen geschaffen: zunächst die Microsoft Cryptographic API (MS-CAPI), danach deren Nachfolger CNG (Cryptography API Next Generation). CNG sieht vor allem die Nutzung so genannter Smart-Card-Minidriver-Module vor, die eine einfache Ansprache von Smartcards durch herunterladbare Konnektoren ermöglichen.

Für das macOS gibt es mit dem CryptoTokenKit (CTK) Framework inklusive den entsprechenden Treibern (Crypto Token Driver) eine weitere Krypto-Schnittstelle.

Cryptovision SCinterface unterstützt alle diese Schnittstellen: PKCS#11, MS-CAPI und CNG zusammen mit dem Smart Card Minidriver sowie CryptoTokenKit einschließlich des Crypto Token Driver.

Neun Gründe für cryptovision SCinterface



eIDAS-Konformität

Cryptovision SCinterface unterstützt Siegel-Token und Siegelkarten gemäß der europäischen Signaturrechtlinie eIDAS.



PIN-Caching

Dieses Add-on für cryptovision SCinterface ermöglicht flexibel konfigurierbare PIN-Caching-Funktionen. Diese gewährleisten eine hohe Sicherheit und erhöhen gleichzeitig die Benutzerakzeptanz.



Biometrie

Cryptovision SCinterface unterstützt Fingerabdruck-Authentifizierung mit Match-on-Card-Funktion.



Token-Unterstützung

Cryptovision SCinterface unterstützt über 100 Sicherheits-Token und Profile. Dazu gehören das MS VSC GIDS Profil, die aktuellen Versionen von Java Card sowie Karten von Atos, Infineon, NXP, Gemalto, G&D und Austria Card.



Krypto-Schnittstellen

Cryptovision SCinterface bietet für praktisch jede Anwendung auf dem jeweils verwendeten Betriebssystem die passende Krypto-Schnittstelle.



Virtual Smart Card

Cryptovision SCinterface stellt eine eigene Virtual Smart Card zur Verfügung und unterstützt parallel dazu auch die veraltete Microsoft Virtual Smart Card (MSVSC) einschließlich der zugehörigen Prozesse.



Plugins

Cryptovision SCinterface kann mit Plugins erweitert werden. Auf diese Weise kann cryptovision SCinterface beispielsweise über ablaufende digitale Zertifikate informieren und Wurzelzertifikate importieren.



eID-Karten

Cryptovision SCinterface unterstützt das Protokoll Password Authenticated Connection Establishment (PACE) zum Schutz des kontaktlosen Datenaustauschs.



Betriebssysteme

Cryptovision SCinterface läuft auf Windows, Linux und macOS. Dieselben Token können auf diesen Plattformen verwendet werden.

Wer nutzt cryptovision SCinterface?

Cryptovision SCinterface wird unter anderem von folgenden Kunden genutzt:



Das marktführende deutsche Versicherungsunternehmen mit Sitz in München nutzt cryptovision SCinterface, um Multi-Applikations-Smartcards auf verschiedenen Plattformen an die jeweilige Anwendung anzubinden.



Der deutsche Energieversorger, der weltweit aktiv ist, sichert mit cryptovision SCinterface den Zugriff auf zahlreiche Unternehmensdaten ab. Außerdem setzt E.ON das Produkt an zahlreichen Stellen für digitale Signaturen ein.



Das Europäische Patentamt nutzt cryptovision SCinterface für die Absicherung von Online-Patentanmeldungen. Cryptovision SCinterface ersetzte eine bestehende proprietäre Lösung, die zu einem Vendor-Lock geführt hatte.

Standards und technische Spezifikationen

Betriebssysteme

- » Windows 8.1, 10, 11
- » Windows Server 2012 R2, 2016, 2019
- » Linux: RHEL 7, 8; Ubuntu 20 LTS / 22 LTS;
- » SLED/SLES 15
- » macOS: Big Sur (11), Monterey (12), Ventura (13)

Leser

Alle PCSC 2.0-konformen Leser (macOS, Unix/Linux benötigt „pcsclite“), empfohlen:

- » Identiv CLOUD 2700 F (nicht für macOS)
- » Identiv CLOUD 4700 F
- » Cherry SmartTerminal ST-2000 (Class2)
- » REINER SCT cyberJack® RFID standard
- » REINER SCT cyberJack® wave
- » Identiv SCR3500
- » Identiv SCL3711

Formate

- » PKCS#10 für Zertifikatsanträge
- » PKCS#11
- » PKCS#12 für Schlüssel- und Zertifikateimport
- » PKCS#15
- » ISO/IEC 7816
- » Microsoft CryptoAPI, CNG
- » macOS Crypto Token Driver
- » PC/SC

Weitere Informationen: www.cryptovision.com

Soziale Medien



eviden.com