EVIDEN

cryptovision SCinterface VSC

Virtuelle Smartcard mit flexiblem Backend

Nicht immer ist der Einsatz einer physikalischen Smartcard sinnvoll umsetzbar. SCinterface VSC von Eviden Digital Identity ermöglicht es, ein Trusted Platform Module (TPM) wie eine Smartcard zu nutzen. Die Verwendung ohne TPM* oder in einem hybriden Modus wird gleichermaßen unterstützt. Diese Erweiterung der bewährten Smartcard-Middleware cryptovision SCinterface bietet mehr als die abgekündigte Microsoft VSC und erlaubt eine reibungslose Migration.

Das TPM als Sicherheitsanker

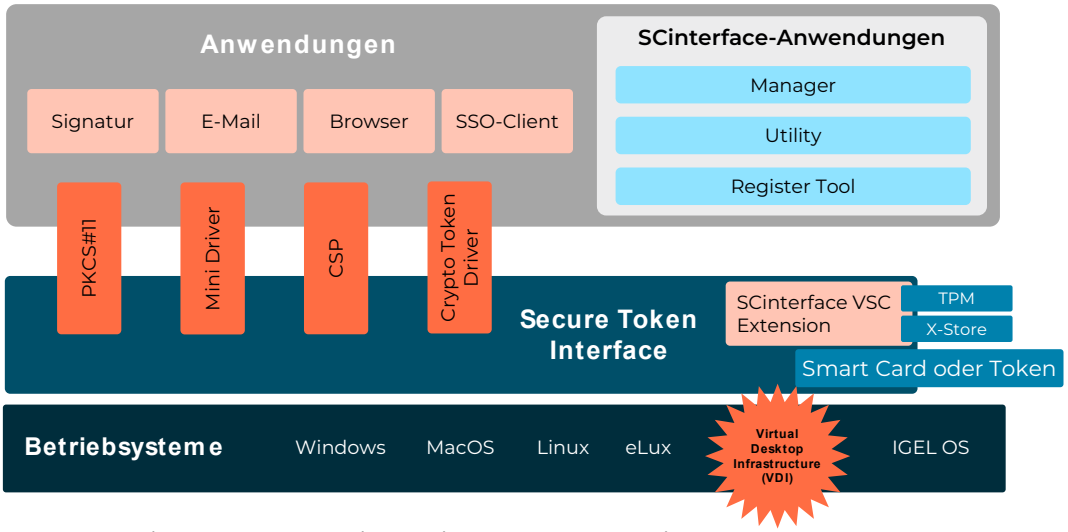
Ein Trusted Platform Module (TPM) ist ein in marktüblichen PCs fest integrierter Sicherheitschip, auf welchem sich unter anderem ein vertrauenswürdiger Wurzelschlüssel befindet. Mit diesem Hardware-Sicherheitsanker kann eine Virtuelle Smartcard vor Manipulation geschützt werden.

Die Microsoft Virtual Smart Card (MS VSC) war lange Zeit die führende Lösung zur Emulation einer Smartcard mithilfe eines TPM. Gegenwärtig legt Microsoft den Fokus auf zertifikatslose Authentifizierungstechniken und hat angekündigt, die MS VSC zukünftig nicht mehr zu unterstützen.

Cryptovision SCinterface VSC ist eine innovative VSC-Lösung, die als Erweiterung der bewährten Smartcard-Middleware cryptovision SCinterface von Eviden Digital Identity entwickelt wurde. Sie kann die Microsoft Virtual Smart Card vollwertig ersetzen.

SCinterface VSC bietet nicht nur sämtliche Funktionen der Microsoft VSC, sondern auch eine Vielzahl zusätzlicher leistungsstarker Features, wie zum Beispiel Secure Key Injection*. Bei der TPM-basierten Variante der SCinterface VSC finden Operationen mit privatem Schlüsselmaterial ausschließlich auf dem TPM statt.

Eine reibungslose Umstellung von der Microsoft VSC auf die neue Lösung ist problemlos möglich, ohne auf gewohnte Funktionen verzichten zu müssen. SCinterface VSC ist damit die ideale Wahl, um zertifikatsbasierte Zwei-Faktor-Authentifizierungslösungen zukunftsfähig, sicher und effizient zu gestalten.



SCinterface VSC ermöglicht es einer PC-Anwendung, ein Trusted Platform Module (TPM) wie eine Smartcard zu nutzen.

*** verfügbar ab Ende Q3 2024**

EVIDEN

Flexibles Backend

Anders als die MS VSC, kann SCinterface VSC neben dem reinen TPM-Modus sowohl in einem hybriden Modus mit TPM-Schutz, als auch auf Windows-Systemen ohne TPM 2.0* und auf Linux-basierten Systemen eingesetzt werden. Diese so genannte X-Store Funktionalität erweitert die möglichen Verwendungsszenarien ungemein.

Der hybride Modus ermöglicht die TPM-geschützte Verwendung von Schlüsselmaterial, welches durch das vorhandene TPM nativ nicht unterstützt wird (z.B. RSA 4K). Hierbei wird das Schlüsselmaterial durch den TPM-Wurzelschlüssel und die Nutzer-Credentials geschützt im Dateisystem abgelegt, und nur für die Durchführung von konkreten Operationen kurzzeitig entschlüsselt und der private Schlüssel somit verwendbar gemacht.

Ohne TPM erfolgt die verschlüsselte Ablage und die Verwendung von privatem Schlüsselmaterial ebenfalls im Dateisystem, wobei private Schlüssel in diesem Fall durch die Nutzer-Credetials (PIN/PUK) gesichert sind. Zusätzlich ist eine Bindung des Schlüsselmaterials an fest verbaute Hardwarekomponenten mittels dedizierter IDs möglich, um das Sicherheitsniveau weiter zu erhöhen.

Reibungslose Migration

SCinterface VSC erweitert den Funktionsumfang der bewährten Smartcard-Middleware cryptovision SCinterface.Cryptovision SCinterface unterstützt eine breite Palette von Karten und Token auf verschiedenen Plattformen, wobei es gängige Schnittstellen wie PKCS#11, Microsoft CNG und Apple Crypto Token Driver nutzt.

Cryptovision SCinterface wird seit fast zwei Jahrzehnten von zahlreichen Unternehmen und Behörden genutzt und ist weit verbreitet, insbesondere als Middleware für elektronische Ausweise.

Was cryptovision SCinterface besonders auszeichnet, ist die zusätzliche Unterstützung verschiedener Extensions für sicheres PIN-Caching, die Nutzung von Remote-Schlüsseln, und einer eigenen virtuellen Smartcard in Form von SCinterface VSC. Kunden haben nicht nur die Möglichkeit, reibungslos von der Microsoft VSC auf die SCinterface VSC umzusteigen, sondern sie können auch problemlos von und zu jeder anderen Karte oder Token wechseln oder diese parallel verwenden. Die Nutzererfahrung bleibt ungeachtet des gewählten Formfaktors identisch.

Key Features

TPM-Nutzung als Smartcard

SCinterface VSC ermöglicht, das TPM eines Geräts wie eine Smartcard zu nutzen. Hierbei werden alle Smartcard-Funktionen emuliert.

Einfache Migration von Microsoft VSC

SCinterface VSC kann mit gleicher Funktionalität parallel zur Microsoft VSC betrieben werden, was eine reibungslose Migration ermöglicht.

Schlüssel-formate

SCinterface VSC unterstützt unterschiedliche Schlüssel-formate. Die Microsoft VSC benötigt dagegen ein FIPS-186-4-konformes Format, was vor allem bei älteren Schlüsseln zu Inkompatibilitäten führen kann.

Zusatzfunktionen durch X-Store

Durch den X-Store, der die sichere Nutzung von Speicherbereichen außerhalb des TPM ermöglicht, unterstützt SCinterface VSC zahlreiche Funktionen, die die Microsoft VSC nicht bietet. Dazu gehört die Speicherung beliebig vieler Krypto-Schlüssel sowie die Nutzung von 3K- und 4K-RSA-Schlüsseln. Darüber hinaus können ECC-Verfahren auch auf Basis von Brainpool-Kurven eingesetzt werden, die die Microsoft VSC nicht unterstützt.

Krypto-Schnittstellen

SCinterface VSC nutzt das TPM über die Krypto-Schnittstellen PKCS#11 und Microsoft CNG (inklusive Smart Card Minidriver). Zukünftig werden auch andere Plattformen unterstützt.

ISO/IEC 7816 und PKCS#15

SCinterface VSC unterstützt das in ISO/IEC 7816 und PKCS#15 festgelegte Smart-card-Dateisystem. Anders als bei der Microsoft VSC sind alle Funktionen verfügbar.

Kompatibel mit anderen Smartcards

Die Smartcard-Middleware SCinterface unterstützt über 100 Smartcards und Token. Ein Parallelbetrieb mit der VSC ist problemlos möglich, was eine einfache Migration ermöglicht.

VDI-Integration

SCinterface VSC lässt sich in eine Virtual Desktop Infrastructure (VDI) integrieren.

*** verfügbar ab Ende Q3 2024**

EVIDEN

Wer nutzt cryptovision SCinterface?

Cryptovision SCinterface wird unter anderem von folgenden Kunden genutzt:

Allianz

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

Energieversorger

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

European Patent Office

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

Formate

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

TPM

» TPM 2.0

Krypto-Schnittstellen

» PKCS#11
» Microsoft CryptoAPI
» Microsoft CNG

Krypto-Verfahren und Schlüssellängen

» 2K RSA auf dem TPM 2.0
» 3K/4K RSA per X-Store über die Krypto-Bibliothek BOTAN
» Elliptic Curve Cryptography (ECC) mit den vom TPM unterstützten NIST-Kurven
» ECC-Brainpool-Kurven per X-Store über die Krypto-Bibliothek BOTAN

Weitere Informationen: www.cryptovision.com

Soziale Medien

eviden.com

 20241121