EVIDEN

cryptovision SCinterface VSC

Carte à puce virtuelle avec backend flexible

L'utilisation d'une carte à puce physique n'est pas toujours réalisable de manière judicieuse. SCinterface VSC d'Eviden Digital Identity permet d'utiliser un Trusted Platform Module (TPM) comme une carte à puce. L'utilisation sans TPM* ou en mode hybride est également prise en charge. Cette extension du middleware éprouvé de carte à puce cryptovision SCinterface offre plus que le VSC de Microsoft, qui a été retiré, et permet une migration en douceur.

Le TPM comme ancre de sécurité

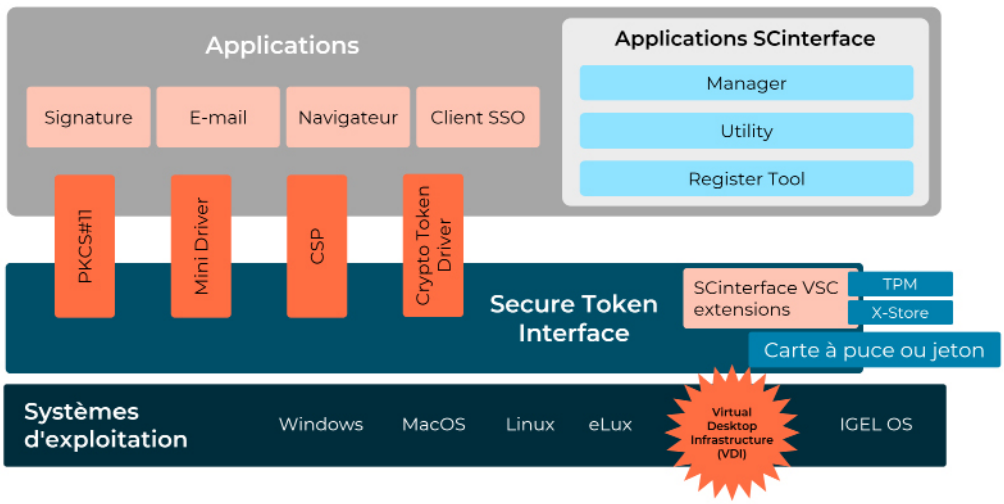
Un Trusted Platform Module (TPM) est une puce de sécurité intégrée de manière fixe dans les PC courants du marché, sur laquelle se trouve entre autres une clé racine fiable. Cette ancre de sécurité matérielle permet de protéger une carte à puce virtuelle contre les manipulations.

La carte à puce virtuelle Microsoft (MS VSC) a longtemps été la principale solution pour émuler une carte à puce à l'aide d'un TPM. Actuellement, Microsoft met l'accent sur les techniques d'authentification sans certificat et a annoncé qu'il ne soutiendrait plus la MS VSC à l'avenir.

Cryptovision SCinterface VSC est une solution VSC innovante qui a été développée comme extension du middleware éprouvé pour cartes à puce cryptovision SCinterface d'Eviden Digital Identity. Elle peut remplacer entièrement la carte à puce virtuelle de Microsoft.

SCinterface VSC offre non seulement toutes les fonctions de la VSC de Microsoft, mais aussi un grand nombre de caractéristiques supplémentaires très performantes, comme par exemple l'injection de clés sécurisées*. Dans la variante de SCinterface VSC basée sur TPM, les opérations avec le matériel de clé privée ont lieu exclusivement sur le TPM.

Il est possible de passer sans problème de la VSC de Microsoft à la nouvelle solution, sans devoir renoncer aux fonctions habituelles. SCinterface VSC est donc le choix idéal pour concevoir des solutions d'authentification à deux facteurs basées sur des certificats qui soient pérennes, sûres et efficaces.



SCinterface VSC permet à une application PC d'utiliser un Trusted Platform Module (TPM) comme une carte à puce.

*** disponible à partir de fin Q3 2024**

EVIDEN

Un backend flexible

Contrairement à MS VSC, SCinterface VSC peut être utilisé en mode hybride avec protection TPM, sur des systèmes Windows sans TPM 2.0* et sur des systèmes basés sur Linux, en plus du mode TPM pur. Cette fonctionnalité, appelée X-Store, élargit considérablement les scénarios d'utilisation possibles.

Le mode hybride permet d'utiliser des clés protégées par TPM qui ne sont pas prises en charge par le TPM existant (par ex. RSA 4K). Dans ce cas, le matériel de la clé est protégé par la clé racine TPM et les crédentiels de l'utilisateur dans le système de fichiers, et n'est déchiffré que brièvement pour l'exécution d'opérations concrètes, rendant ainsi la clé privée utilisable.

Sans TPM, le stockage chiffré et l'utilisation de la clé privée s'effectuent également dans le système de fichiers, les clés privées étant dans ce cas protégées par les codes d'utilisateur (PIN/PUK). En outre, il est possible de lier le matériel de clé à des composants matériels fixes au moyen d'identifiants dédiés afin d'augmenter encore le niveau de sécurité.

Une migration sans heurts

SCinterface VSC étend les fonctionnalités du middleware de cartes à puce éprouvé cryptovision SCinterface.Cryptovision SCinterface supporte une large gamme de cartes et de jetons sur différentes plateformes, en utilisant des interfaces courantes comme PKCS#11, Microsoft CNG et Apple Crypto Token Driver.

Cryptovision SCinterface est utilisé depuis près de deux décennies par de nombreuses entreprises et administrations et est largement répandu, notamment comme middleware pour les cartes d'identité électroniques.

Ce qui distingue particulièrement cryptovision SCinterface, c'est le support supplémentaire de différentes extensions pour la mise en cache sécurisée des PIN, l'utilisation de clés à distance, et une propre carte à puce virtuelle sous la forme de SCinterface VSC. Les clients ont non seulement la possibilité de passer en douceur de la VSC de Microsoft à la VSC de SCinterface, mais ils peuvent aussi passer sans problème de et vers n'importe quelle autre carte ou jeton, ou les utiliser en parallèle. L'expérience utilisateur reste identique, quel que soit le facteur de forme choisi.

Caractéristiques principales

Utilisation comme carte à puce

SCinterface VSC permet d'utiliser le TPM d'un appareil comme une carte à puce. Toutes les fonctions de la carte à puce sont émulées.

Migration facile de Microsoft VSC

SCinterface VSC peut être utilisé parallèlement à Microsoft VSC avec les mêmes fonctionnalités, ce qui permet une migration en douceur.

Clé-formats

SCinterface VSC prend en charge différents formats de clés. En revanche, la VSC de Microsoft nécessite un format conforme à la norme FIPS-186-4, ce qui peut entraîner des incompatibilités, surtout avec les clés anciennes.

Utilisation du X-Store

Grâce au X-Store, qui permet l'utilisation sécurisée de zones de stockage en dehors du TPM, SCinterface VSC prend en charge de nombreuses fonctions que la VSC de Microsoft n'offre pas. Il s'agit notamment du stockage d'un nombre illimité de clés cryptographiques et de l'utilisation de clés RSA 3K et 4K. En outre, les procédures ECC peuvent également être utilisées sur la base de courbes de Brainpool, ce que ne supporte pas la VSC de Microsoft.

Crypto-interfaces

SCinterface VSC utilise le TPM via les interfaces cryptographiques PKCS#11 et Microsoft CNG (y compris Smart Card Minidriver). D'autres plates-formes seront également prises en charge à l'avenir.

ISO/IEC 7816 et PKCS#15

SCinterface VSC prend en charge le système de fichiers des cartes à puce défini dans ISO/IEC 7816 et PKCS#15. Contrairement à la VSC de Microsoft, toutes les fonctions sont disponibles.

Compatible avec autres cartes à puce

Le middleware pour cartes à puce SCinterface prend en charge plus de 100 cartes à puce et jetons. Un fonctionnement parallèle avec la VSC est possible sans problème, ce qui permet une migration facile.

VDI-intégration

SCinterface VSC s'intègre dans une infrastructure de bureau virtuel (VDI).

*** disponible à partir de fin Q3 2024**

EVIDEN

Qui utilise cryptovision SCinterface ?

Cryptovision SCinterface est utilisé entre autres par les clients suivants :

Allianz

La compagnie d'assurance allemande leader sur le marché et basée à Munich utilise cryptovision SCinterface pour connecter des cartes à puce multi-applications sur différentes plates-formes à l'application correspondante.

Fournisseur d'énergie

Un fournisseur d'énergie allemand, qui est actif dans le monde entier, utilise cryptovision SCinterface pour sécuriser l'accès à de nombreuses données d'entreprise. En outre, cette firme utilise le produit à de nombreux endroits pour les signatures numériques.

European Patent Office

L'Office européen des brevets utilise cryptovision SCinterface pour sécuriser les demandes de brevet en ligne. Cryptovision SCinterface a remplacé une solution propriétaire existante qui avait conduit à un verrouillage du vendeur.

Normes et spécifications techniques

Systèmes d'exploitation

» Windows 8.1, 10, 11
» Windows Server 2012 R2, 2016, 2019

Formats

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

TPM

» TPM 2.0

Interfaces cryptographiques

» PKCS#11
» Microsoft CryptoAPI
» Microsoft CNG

Procédés de cryptographie et longueurs de clé

» 2K RSA sur le TPM 2.0
» 3K/4K RSA par X-Store via la crypto-bibliothèque BOTAN
» Elliptic Curve Cryptography (ECC) avec les données du TPM-courbes supportées par le NIST
» Courbes ECC-Brainpool par X-Store via la crypto biblio-thèque BOTAN

En savoir plus sur nous: www.cryptovision.com

Connectez-vous avec nous

eviden.com

20241121