TeleTrusT-EBCA "PKI-Workshop" 2023

Berlin, 21.09.2023

"Lessons learned - Virtual Smart Cards and PKI"

Mauricio A. Fernandez, Siemens AG

Siemens Virtual Smart Card (VSC) main goal

In Scope (PKI based usage)

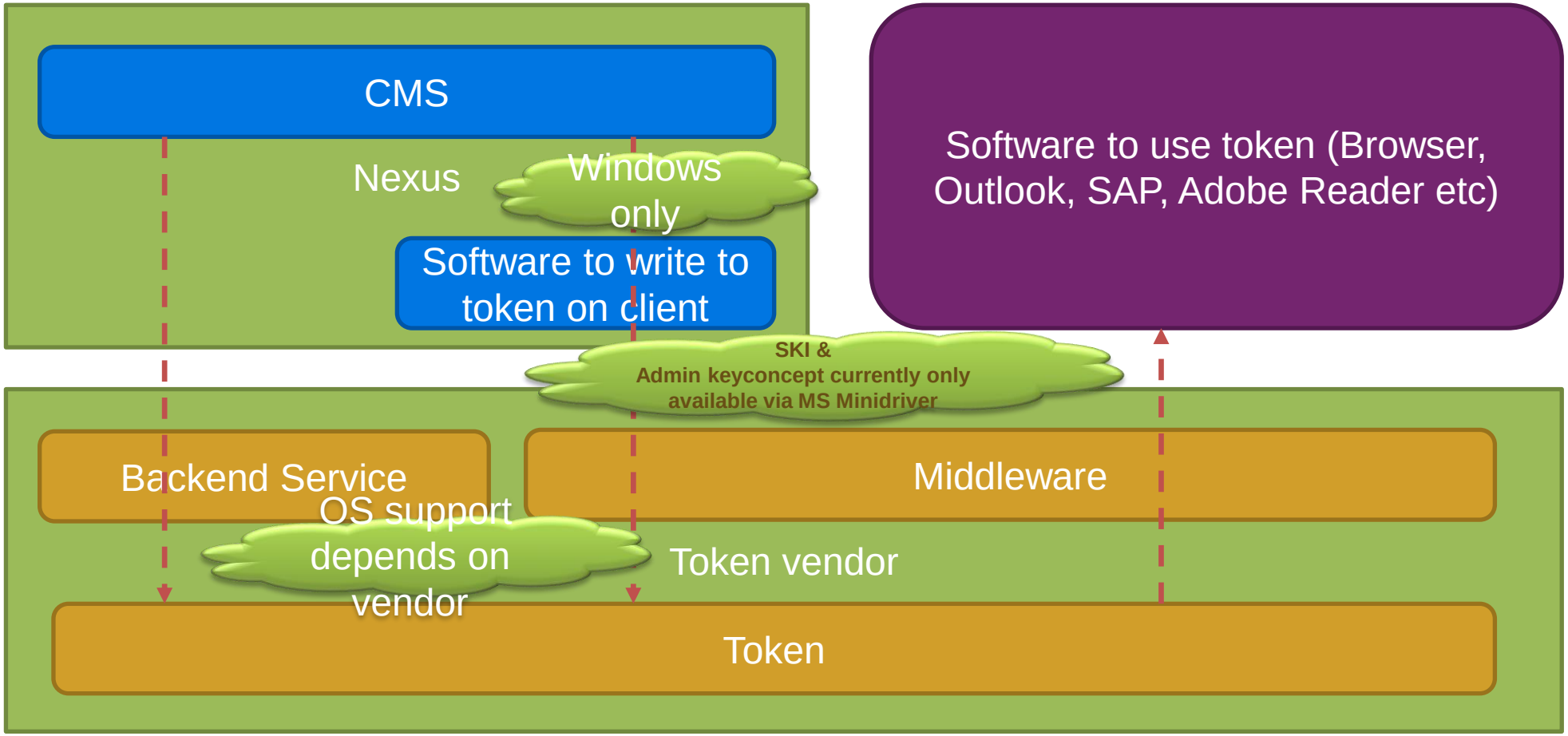
Find and implement alternative solutions to reduce the need to provide PKI certificates (private keys) on Siemens Corporate ID cards to a maximum extend

Out of Scope (RFID based usage)

For building access, time recording and payment, MIFARE Classic is used, which communicates with the corresponding readers via an antenna (RFID) embedded in the plastic body.

Siemens generic archeticture for all token types

Siemens is extending the platform reach beyond Windows, but technology-wise this is still a limitation on most other platforms.



Baseline requirements

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

All Tokens must

- Support Secure key injection
- Support key length up to 4K RSA – currently we use 2K but 3 or 4K envisaged
- Usability is key success factor
- Support high degree of process automation
- For integration into IDM:
  MS minidriver and pkcs#11 interface available
- Ability to integrate into a Token “allow List” e.g. based on firmware version

Virtual Smart Card

- Support Key Attestation
- Provide API for card management (create/modify/delete) and cryptographic functions

Mobile Token

- Main use: Smart Card = store keys and certs on device and connect Smartphone via BT or NFC to client = insert SC into card reader.
- Optional but highly wanted: Use keys and certs on the device itself e.g. for Outlook mobile (S/MIME)

Success criteria for Virtual smart card (VSC)

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Empower employees

- Digital Workplace: Seamless integration and better user experience
- Reduced dependency from IT services to physical Smartcard

Reduced complexity

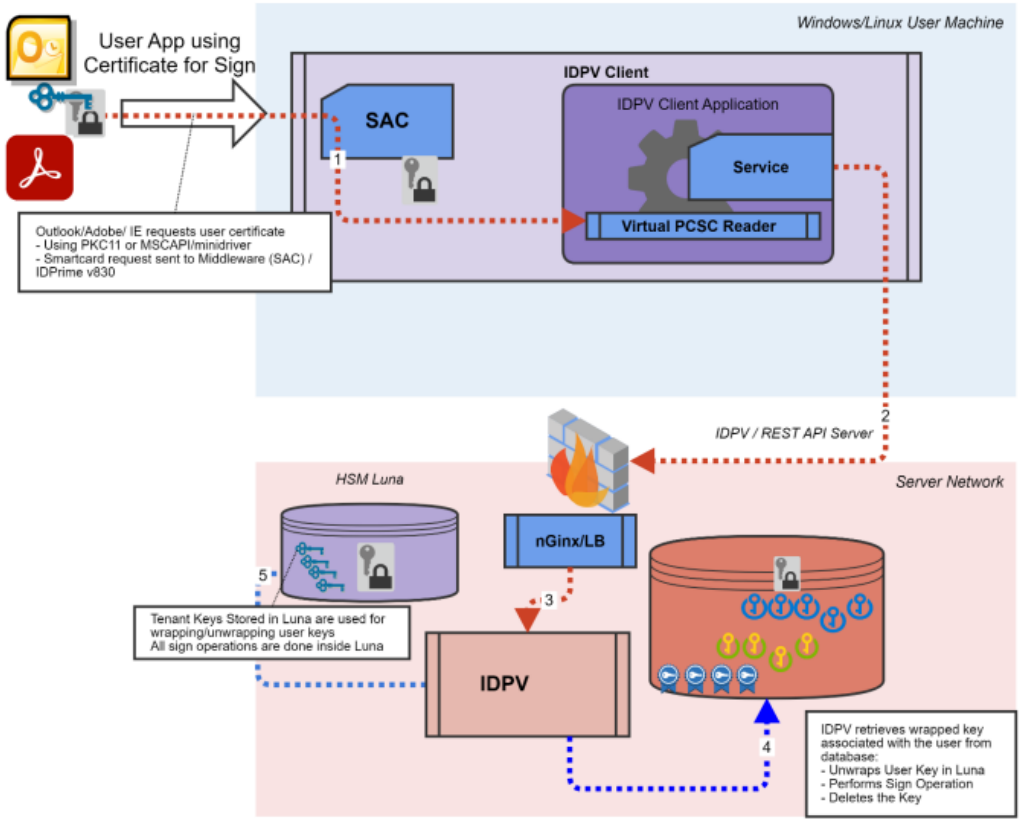
- Software-based usage
- No card reader required
- Easier processes e.g. re-keying and can be triggered centrally.

State of the Art technology

- Higher flexibility
- Easier way to distribute and manage certificates
- Less physical touch points

Lessons Learned

- **Strong 2 Factor Authentication**
  corporate ID card vs virtual smart card – proof of possession (2nd factor)



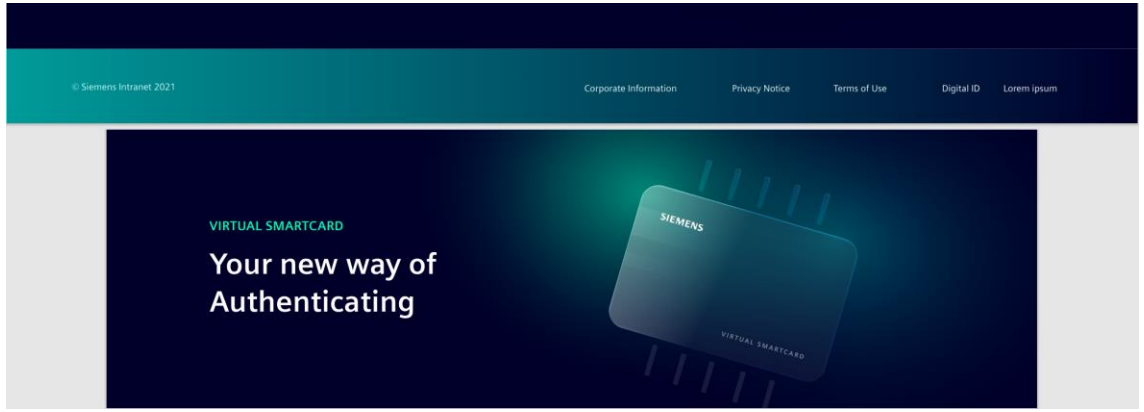
Lessons Learned

- **Strong 2 Factor Authentication**
  corporate ID card vs virtual smart card – proof of possession (2nd factor)

- **The virtual smartcard is stored securely in the Siemens Trust Center and potentially on the TPM chip of a computer** the virtual smartcard is inserted.
- The strong binding to the end user's identity is ensured during the ordering of a token. To order a Virtual token, the user must authenticate with a strong authenticator e.g. (Corporate Smart cards).
- To ensure that only an authorized identity has access to this virtual smartcard the user must authenticate to Siemens IdP and insert the smartcard – [This authentication is considered as proof of possession].
- **As the virtual smartcard is not capable of detecting if the user leaves the computer**, the smartcard should be ejected as soon as the workstation is locked. This would be especially important as the domain login allows username and password to login. If the token is not be ejected, this weakens the proof of possession considerably.

Lessons Learned

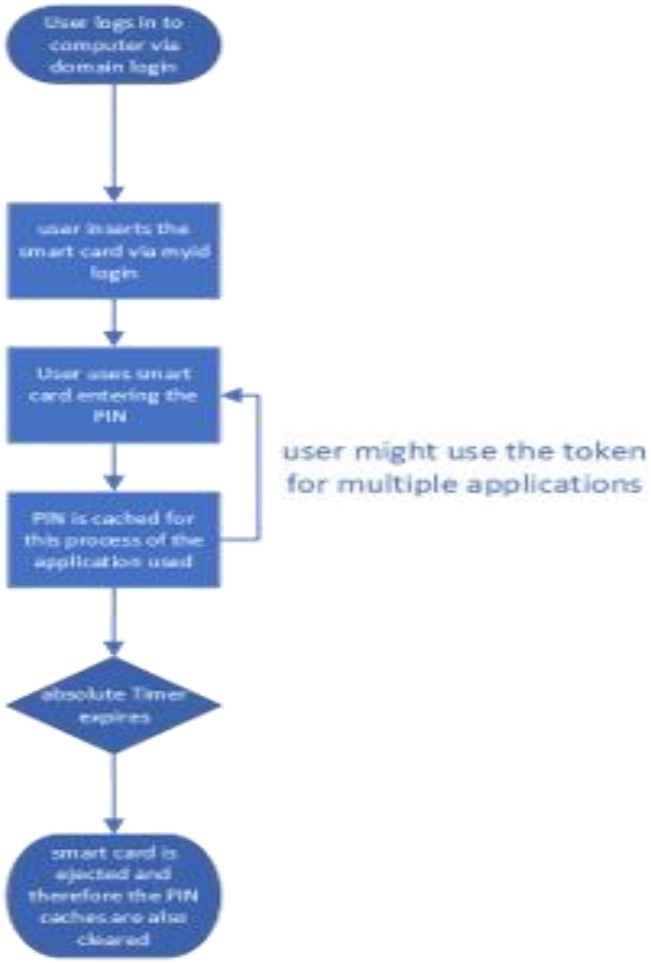
- **Virtual smart card usage - A primer**



- The virtual smartcard can be used in an online and offline mode. The behaviour of the virtual smartcard must be the same regardless of the mode it operates in.

- All the following suggestions are based on the user locking the workstation in case the user leaves the desk which is not only considered a security best practice, it’s not so unusual, and a recurrent behaviour on the field.

Lessons Learned



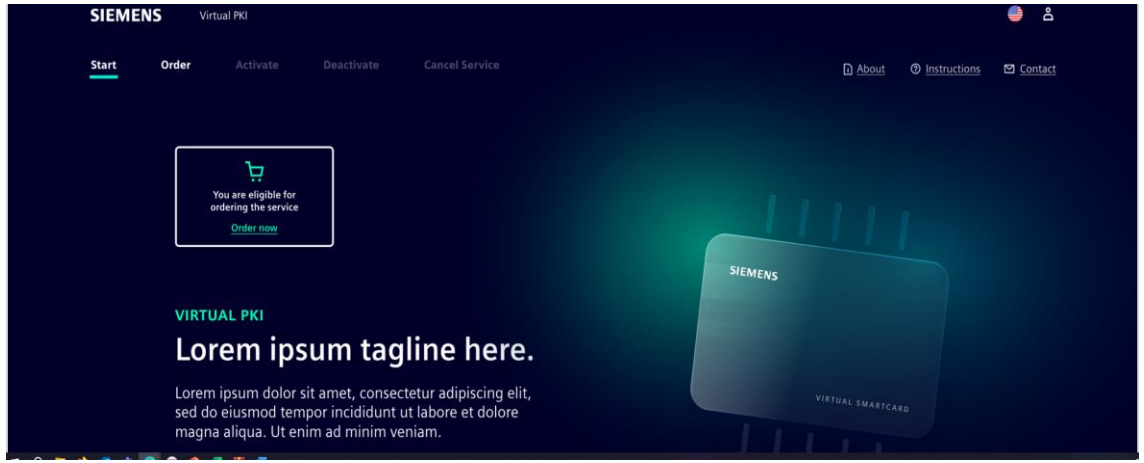
- Virtual smartcard is using the windows standard mechanism to cache PINs.
- The PIN is therefore cached per process as long as that process lives.
- After 8 hours (in on and offline mode) the card is ejected and the user has to login again.
- A sliding timer expiration, to avoid the risk – [Proof of possession is weakened for 8 hours].

- **Suggestion**: To develop a feature for a sliding expiration.
- Set the fixed timer to 10 hours (instead of 8 with the NSC to cover for longer workdays) and set the sliding timer to 2 hours (to cover for lunch breaks).
- Until the sliding timer is available set the fixed timer to 8 hours.

Behaviour in Clarification - we are still working on finding the best time out and re-auth experience.

Lessons Learned

- **Virtual smart card usage – way to “touchless”**



- Migrate to AzureAD (Microsoft Entra) to have SSO with WHFB. This way on windows the user would only need to use WHFB for the domain login and insert the token.

Additional improvement:

- Asked to add an “auto-insertion” of the token during startup of the windows session.

Lessons Learned

- **Infineon TPM rejected certain RSA keys**

Reason for Issue

- Infineon TPM enforce FIPS compliance of RSA keys (FIPS 140-2 and FIPS 186-4)
- IDPV server doesn't enforce FIPS compliance of RSA keys during key generation (FIPS compliance is delegated to the HSM).
- A Non FIPS HSM may choose to generate keys which may or may not be FIPS compliant (RSA keys are generated randomly without any constraints (some of them are FIPS and some are not)
- A FIPS compliant TPM does not allow to import RSA keys that are not FIPS compliant.

Issue Remedy:

- Modify IDPV server to enforce FIPS compliance of generated RSA keys during enrolment.
- Existing users affected by this problem (since they are having non FIPS RSA keys on the HSM) will have to re-enroll once new IDPV server is delivered.

Lessons Learned

- **Key wrapping feature in IDPV for 2K and 4K to mitigate the current certificate FIPS non-compliance of encryption keys**

Issue Remedy:
- A fix/patch was developed to support RSA 3K/4K keys + offline key wrapping and non-FIPS keys in TPM

- **Virtual Card to support RSA 4K key length in Online mode**

Issue Remedy:
- Support RSA 4K keys by upgrading the virtual card applet currently based on IDPrime 830 to IDPrime 930 ongoing

- **Virtual Card to support RSA 4K key length in Offline mode**

Issue Remedy:
- To research the use of 4k key size in offline mode (TPM 2.0 doesn’t support it).

- **Key Attestation**

Issue Remedy:
- To distinguish between imported keys and keys created on the virtual card SecOps can read the HSM key attribute “CKA_LOCAL”. This should already be visible from the Minidriver and is available via REST API

Lessons Learned

- **Linux Offline mode (TPM Chip)**

Issue Remedy:
- Virtual Card will support offline mode (TPM chip)

- **Support of MacOS - Online Mode**

Issue Remedy:
- MacOS support must be on the roadmap and planned

- **Support of MacOS - Offline Mode**

Issue Remedy:
- To use Secure Element or equivalent on Mac and Siemens to evaluate the strengths offered by the solution.

- **Support of offline PIN unblock**

Issue Remedy:
- Offline PIN unblock is a requirement and the options will be investigated. Consistency between local card and the card on server side shall be ensured.

Lessons Learned

- **Support of end-to-end encryption between IDPV backend and TPM**

Issue Remedy:

- Wrapping of virtual card keys is currently done outside of the TPM in memory which is seen as a security issue. Other options to do this within the TPM itself (like TPM Seal).

- **Support automated renewal of tokens**

Issue Remedy:

- The renewal of tokens shall be possible in the background based on the lifecycle of the certificates stored on the token.

- **Support Azure Virtual Desktop environment in online mode**

Issue Remedy:

- Will be tested.

- **Prevent caching on virtualized environment**

Issue Remedy:

- The system will provide a configurable feature to prevent caching on virtualized environments

Questions?