TeleTrusT-EBCA "PKI-Workshop" 2022

Berlin, 29.09.2022

Virtual Smart Cards and PKI, a step beyond of today's traditional form factors in the Enterprise

Mauricio Alejandro Fernandez Fernandez, Siemens

Siemens Public Infrastructure in a nutshell

More than 20 years Siemens PKI one of the largest private PKIs worldwide.

~350.000 users
~750.000 user certificates
~12.000 server certificates
~ 7 mill. cert. since 1998

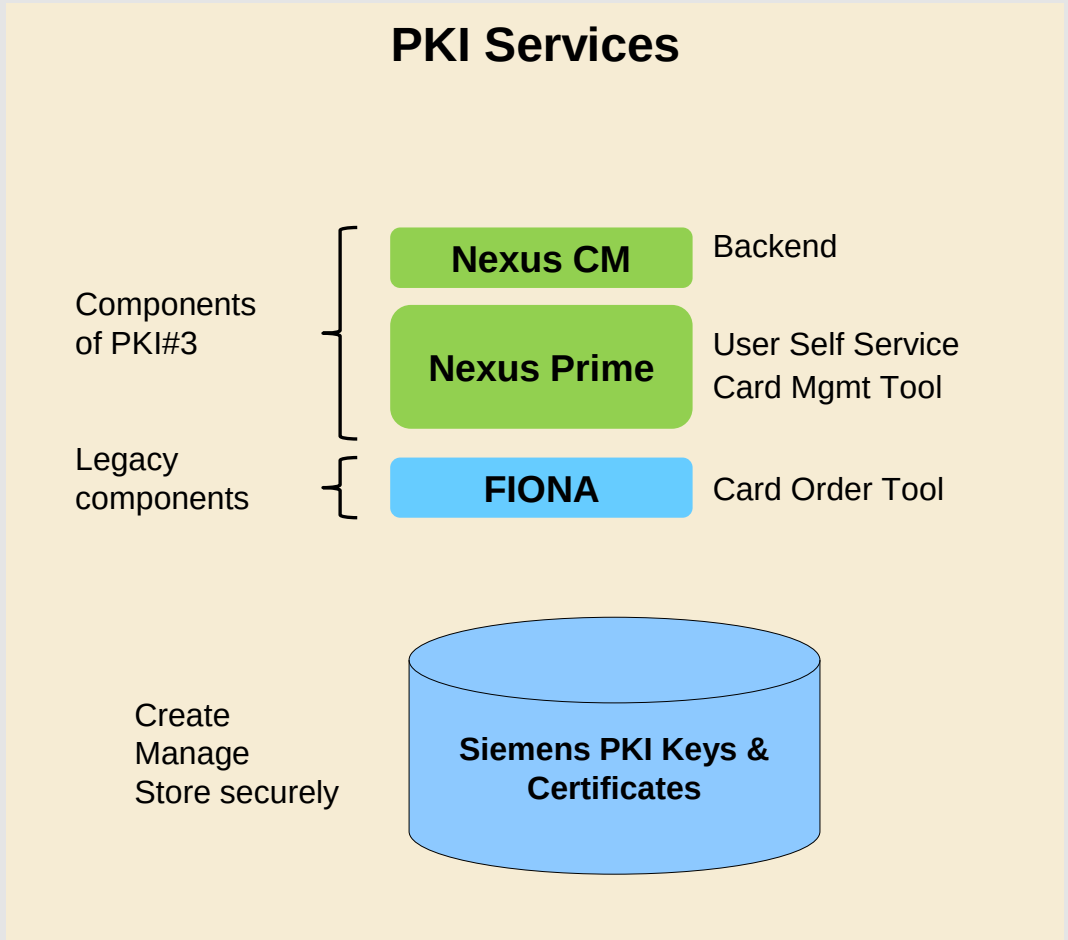
Important Cornerstone for Cyber Security

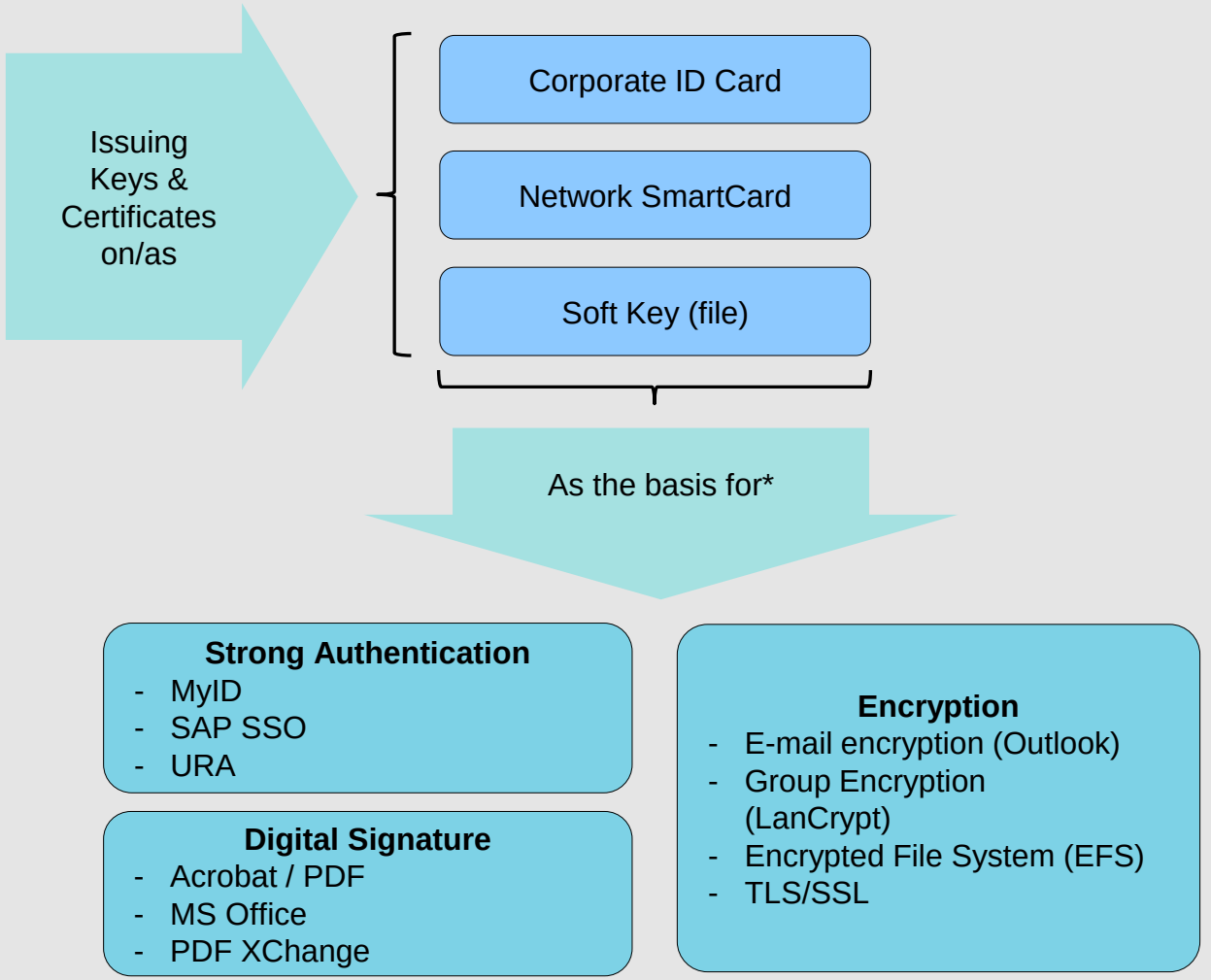
Strong Authentication
- MyID / MS MFA
- SAP SSO
- URA
- Server Certificates

Encryption
- E-mail encryption (Outlook)
- Group Encryption (CLC)
- Encrypted File System (EFS)
- Server Certificates

Digital Signature
- Acrobat / PDF
- MS Office
- PDF Xchange

Siemens Corporate PKI - High level overview





Siemens Tokens and Certificates types

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

Current Token types

•Corporate ID card/codesigning card – Atos CardOS V4.2, 5.3 and 5.3 DI
•Network Smart Card – Gemalto IDConfirm1000

Current certificate types

•Authentication – keygen on card
•Encryption – keygen centrally / history recovered to token according to token capacity
•Soft Authentication – keygen centrally
•Codesigning – keygen on card
•Codesigning – keygen centrally (only for internal trust)

Background information

Organizational	Geographical	Delivery Value Center
▪ All the organization BU's	▪ Global	▪ Core Services

- In Siemens there are multiple Authentication factors for ACP Level 1,2 and 3. Some of them are based on X509 certificates. The VPKI project focuses solely on X509 based credentials and keys.
- X509 certificates and the corresponding keys can be stored in containers secured with a crypto chip or in software based containers.

- For the ACP level classification of x509 certificates two factors are relevant
  i. **Key creation**
  ii. **Key protection**

Level 2
Key creation in the CA & recoverable
Key protection according to AAL 2 based on NIST publication

Level 3
Key creation on the token and not exportable
Key protection according to AAL 3 based on NIST publication

Simenens VPKI 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

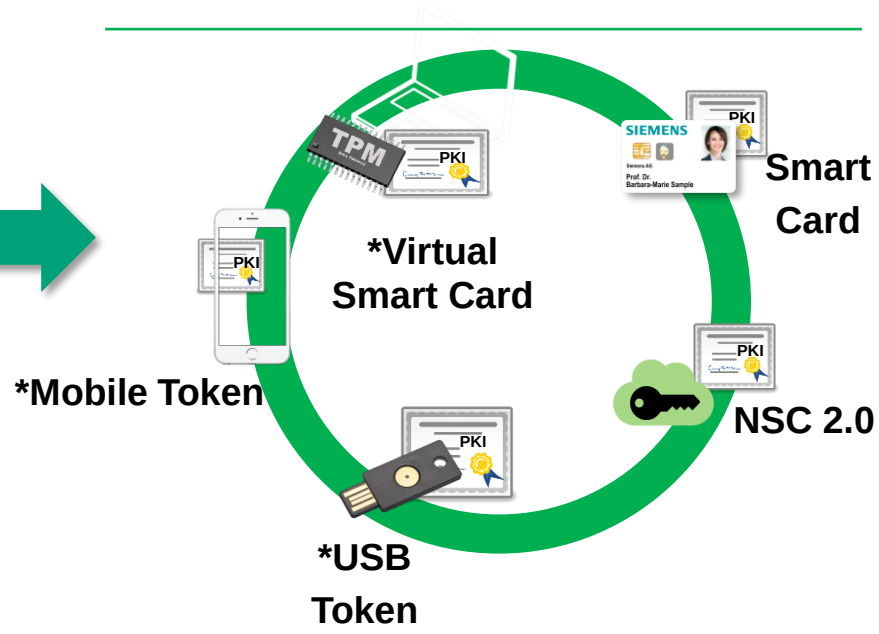
Out of Scope (RFID based usage)

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 new set of tokens to be introduced *(new)

FROM

TO



•Siemens uses smartcard based and HSM based crypto chips to securely create and store the keys on smartcards (corporate id card) or in the trustcenter (network smartcard). These tokens comply to AAL 3 and ACP 3.

•Siemens uses software based containers (pfx/p12) for storing certificates and keys. In case these containers hold authentication certificates this ensures AAL 2 ACP Level 2.

Basic requirements for all token types

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**
- **Comply with NIST**
- **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 (clarify if Nexus CM does support this)**
- **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)**

Usb Token

- **Limit to Siemens certified tokens**
- **NFC support**
- **USB-A and C**
- **Global availability of devices**
- ***Optional* – Fido2 support**
- ***Optional* – Possibility for "corporate design"**

Success Criteria

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

State of the Art technology

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