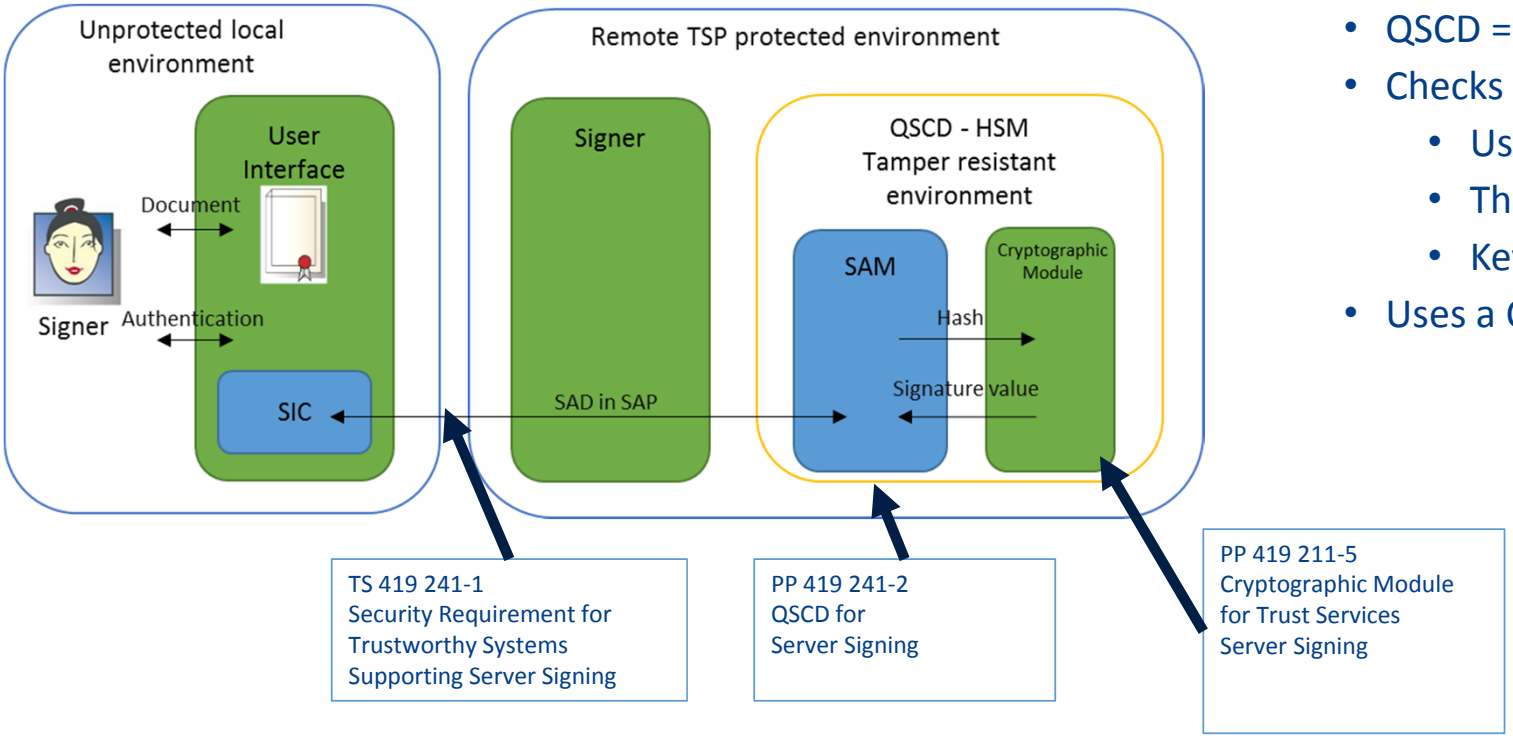
CRYPTOMATHIC

419 241-2

Jan Ulrik Kjærsgaard
Senior Cryptography Manager
Editor CEN EN 419 241-2

2016 – Copyrights reserved

419 241-2



- QSCD = HSM + SAM
- Checks the SAD:
  - User is authenticated
  - The hash
  - Key identifier
- Uses a CM for signature operation

CRYPTOMATHIC

Protection Profile

- Dependent on:
  - CM 419 211-5
  - SSA, SIC 419 241-1
- Like CM, EAL 4+

CRYPTOMATHIC

Flexible

- Supports
  - One-time and long term keys
  - Signature keys can generated by either Signer or Privileged Users
  - DTBS/R can be supplied by either Signer or Privileged Users
- Signature operation through SAP (SIC -> SAM)
- Authentication
  - Direct by SAM
  - Indirect by authentication server or IdP
- Host:
  - Local application in 419 211-5
  - Or similar proctection
- External storage of data

CRYPTOMATHIC

Important assets

- Privileged Users
- Signer, signature key identifiers, authentication data
- Signature Activation Data cryptographically binds:
  - User Authentication
  - Set of DTBS/R – may be an identifier
  - Signature key identifier - implicit