Werkgroep Techniek

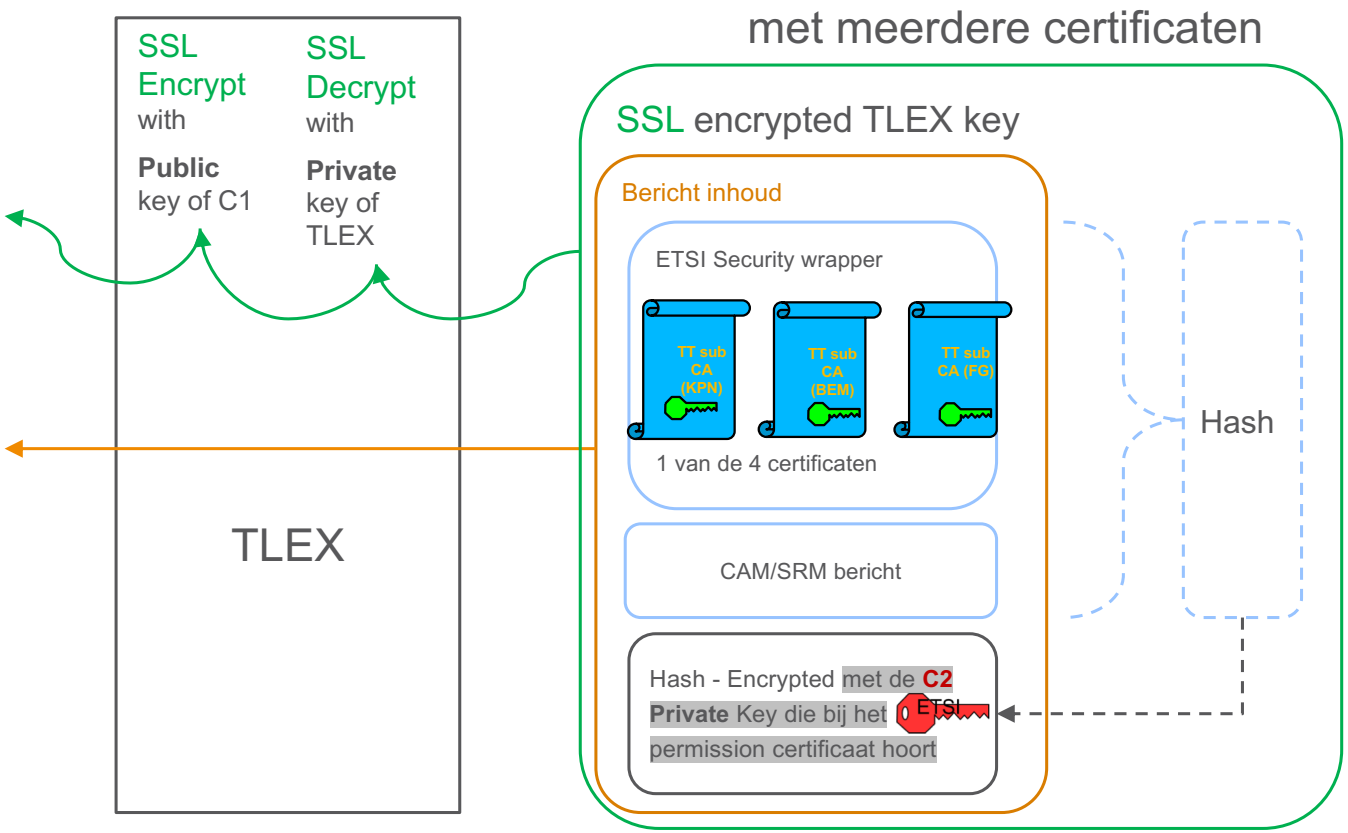
PKI process

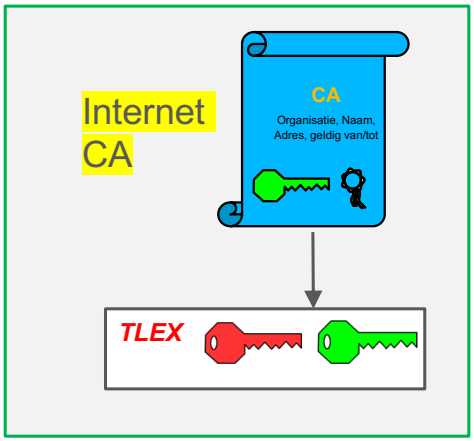
Voorstel

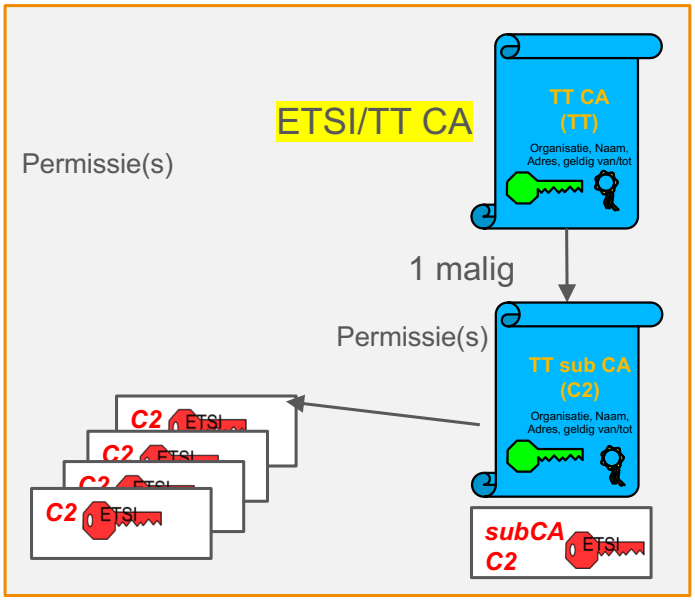
partnership
talking traffic

Naar C1 op basis van ETSI CAM/SRM - interface C

Voorbeeld waarbij C2 ondertekent met meerdere certificaten

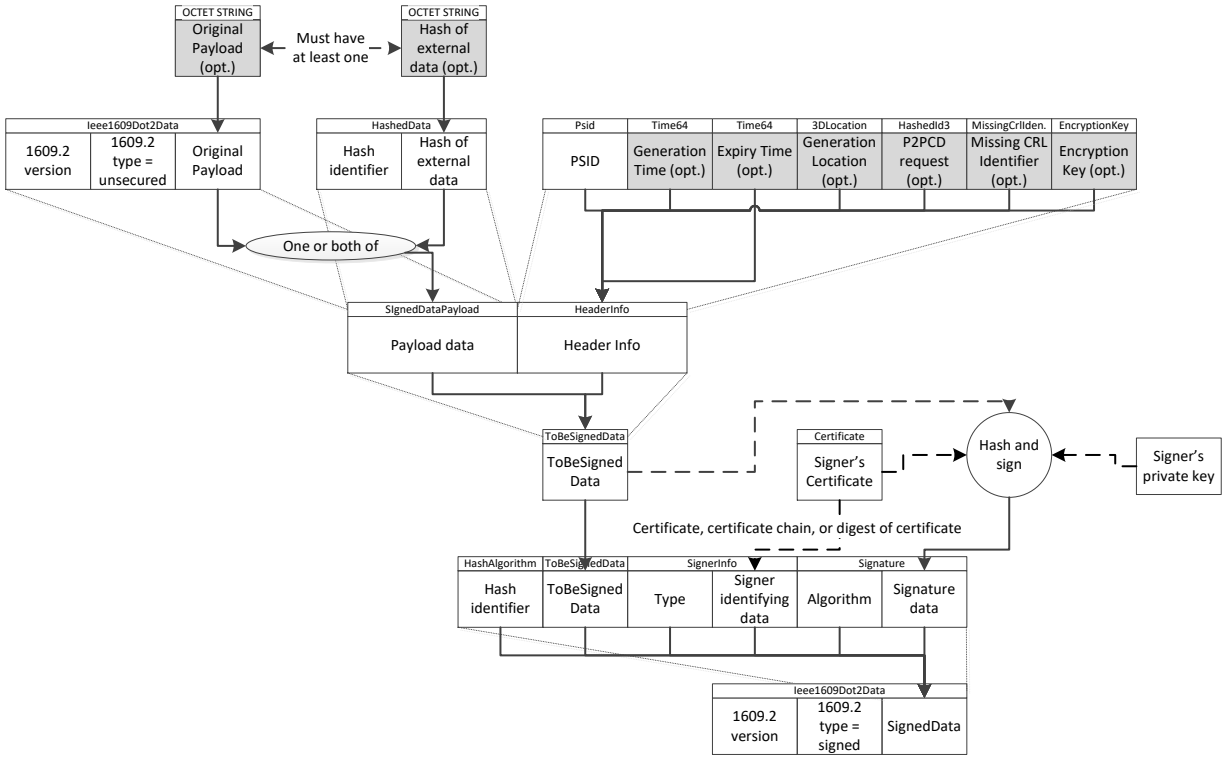




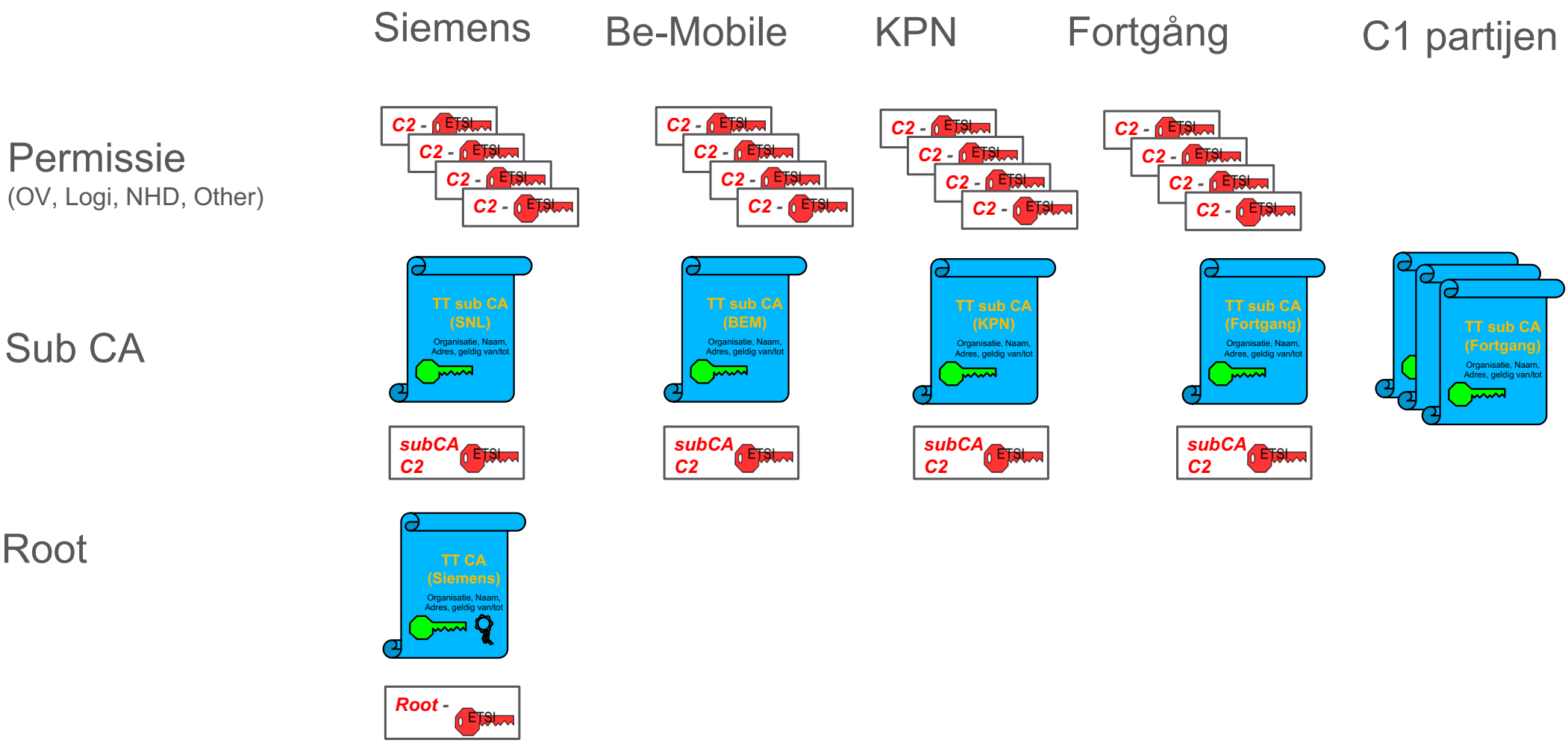


Constructing an IEEE 1609.2 signed PDU

- Signed PDU contains
  - At least one of:
    - Payload
    - Hash of external payload
  - Provider Service ID to indicate permissions
  - Optional additional header fields – generation time, expiry time, generation location, security management fields
  - Reference to signing certificate (certificate itself or hash of certificate)
  - Signature

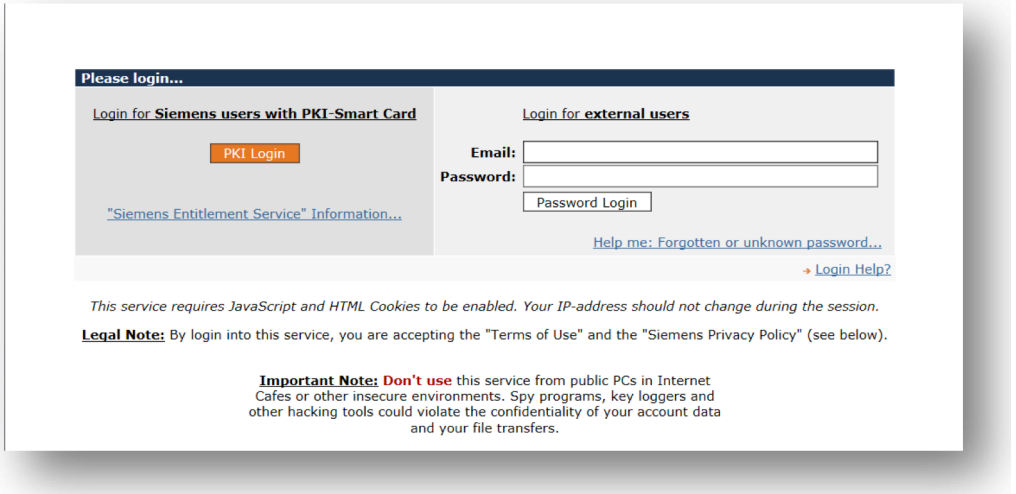


Te overhandigen



Distributie

- C2 en C1 partijen wijzen een Security Officer aan
- Security Officer krijgt via Secufex de betreffende keys
- Siemens bewaart keys in digitale kluis
- Security Officer kan altijd de eigen keys opvragen
- Verversing:
  - 4 x per jaar (voorstel)
  - Na toewijsbaar security incident




partnership
talking traffic