

Werkgroep Techniek

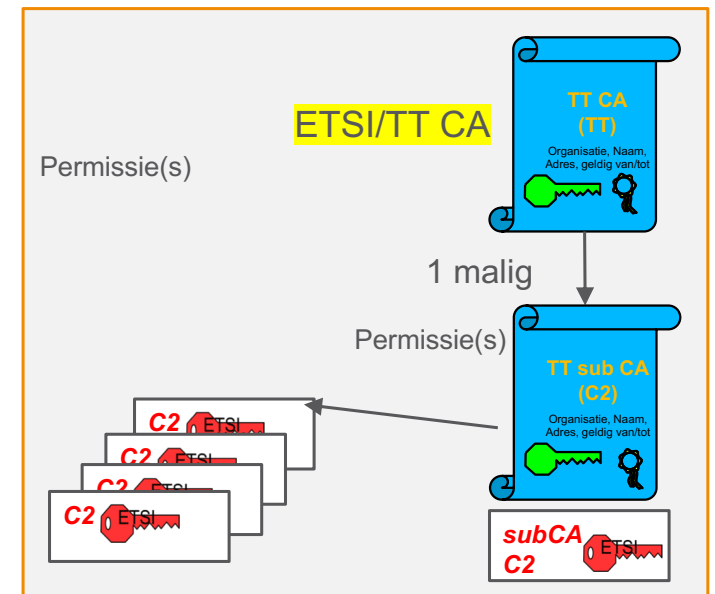
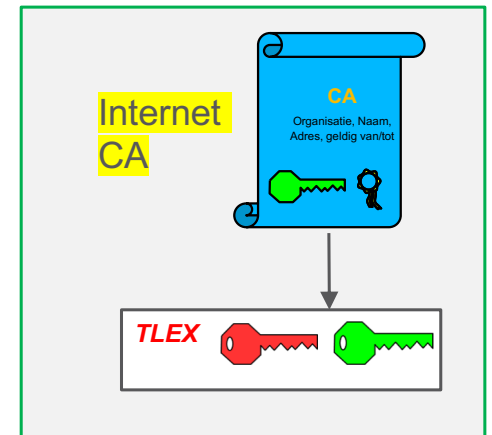
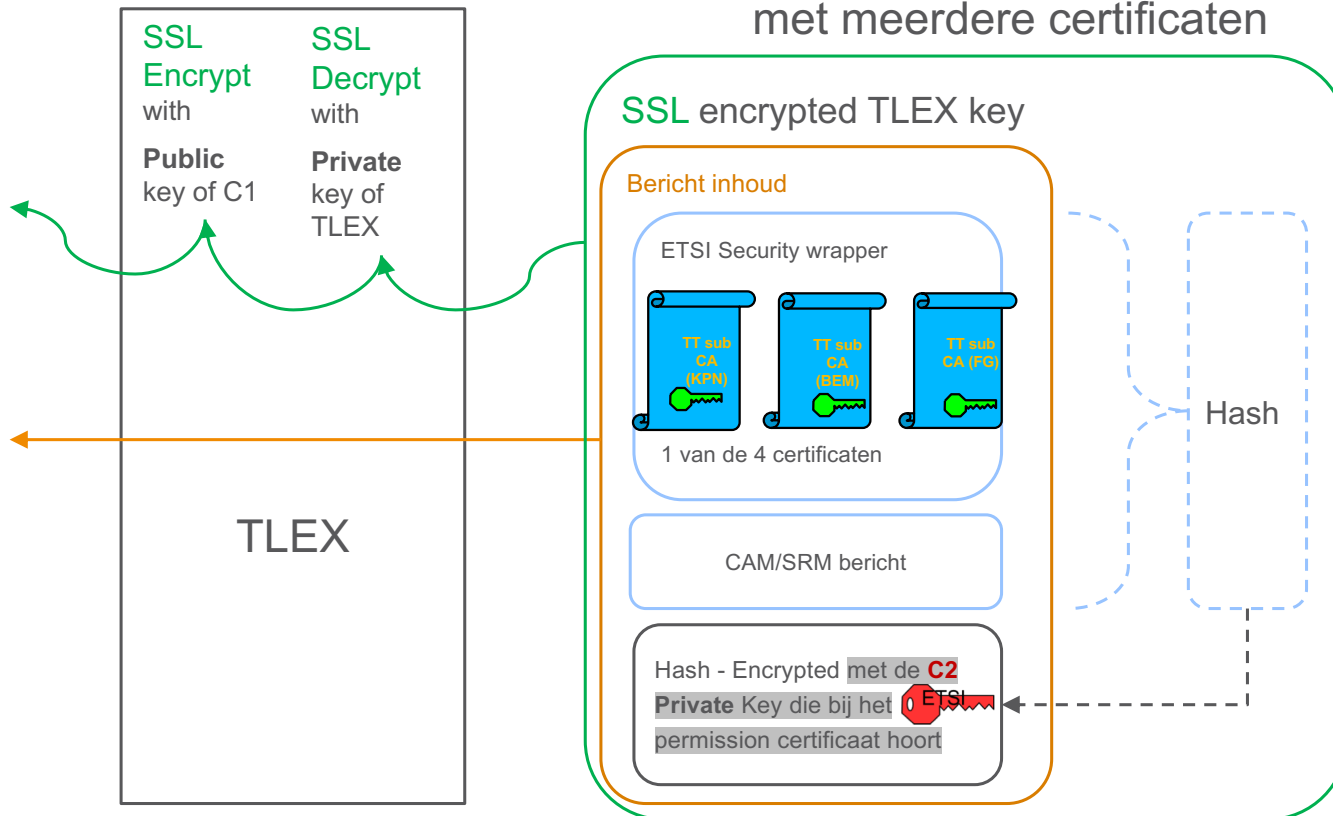
PKI process

Voorstel



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:

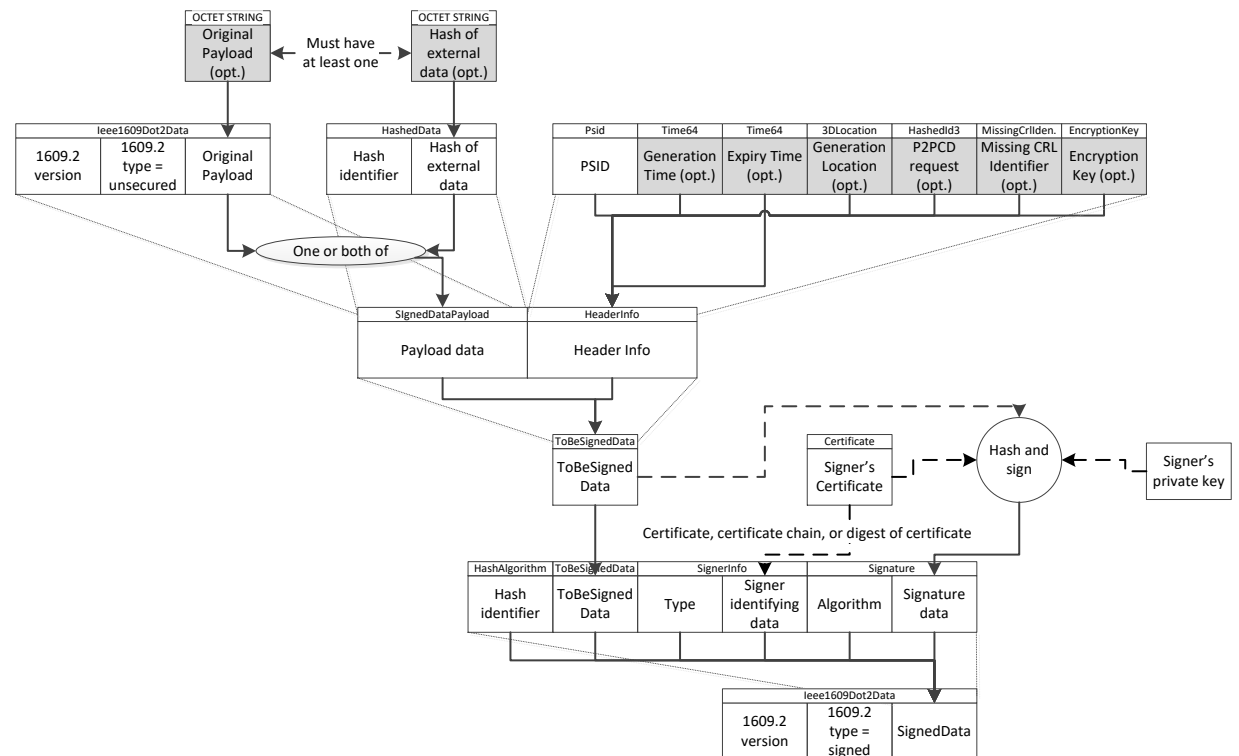
- › Payload
- › Hash of external payload

– 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

Siemens

Be-Mobile

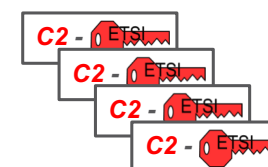
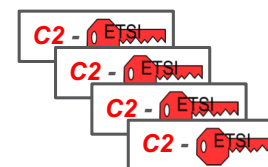
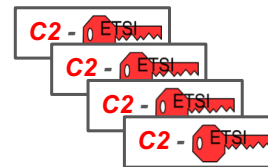
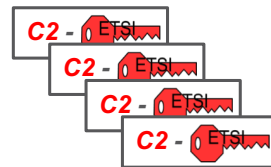
KPN

Fortgång

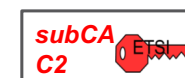
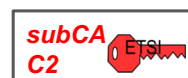
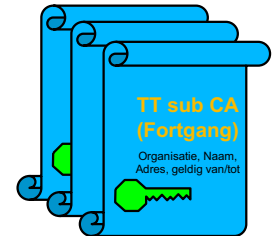
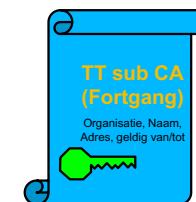
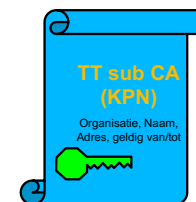
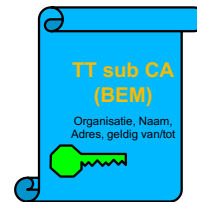
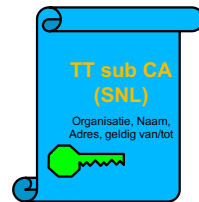
C1 partijen

Permissie

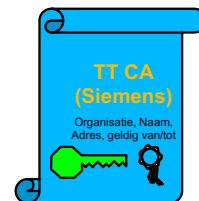
(OV, Logi, NHD, Other)



Sub CA

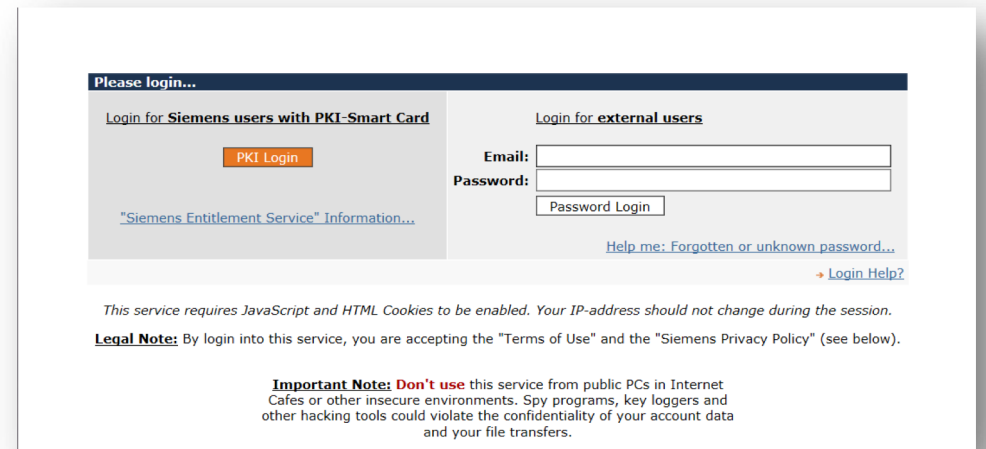


Root



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



The screenshot shows a login interface with a dark blue header containing the text "Please login...". Below the header, there are two main sections. The left section is titled "Login for Siemens users with PKI-Smart Card" and features an orange "PKI Login" button and a blue link for "Siemens Entitlement Service" Information... The right section is titled "Login for external users" and contains input fields for "Email:" and "Password:", a "Password Login" button, and a blue link for "Help me: Forgotten or unknown password...". At the bottom right of the form area is a link for "Login Help?". Below the form, there is a note: "This service requires JavaScript and HTML Cookies to be enabled. Your IP-address should not change during the session." followed by a "Legal Note" stating that logging in implies acceptance of the "Terms of Use" and "Siemens Privacy Policy". At the very bottom, an "Important Note" in red text warns users not to use the service from public PCs in internet cafes or insecure environments due to the risk of confidentiality breaches.



partnership
talking traffic