
Verandering zonder Compromissen
PAC als Fundament van Betrouwbaarheid
8 april 2026
cigre
Nederland

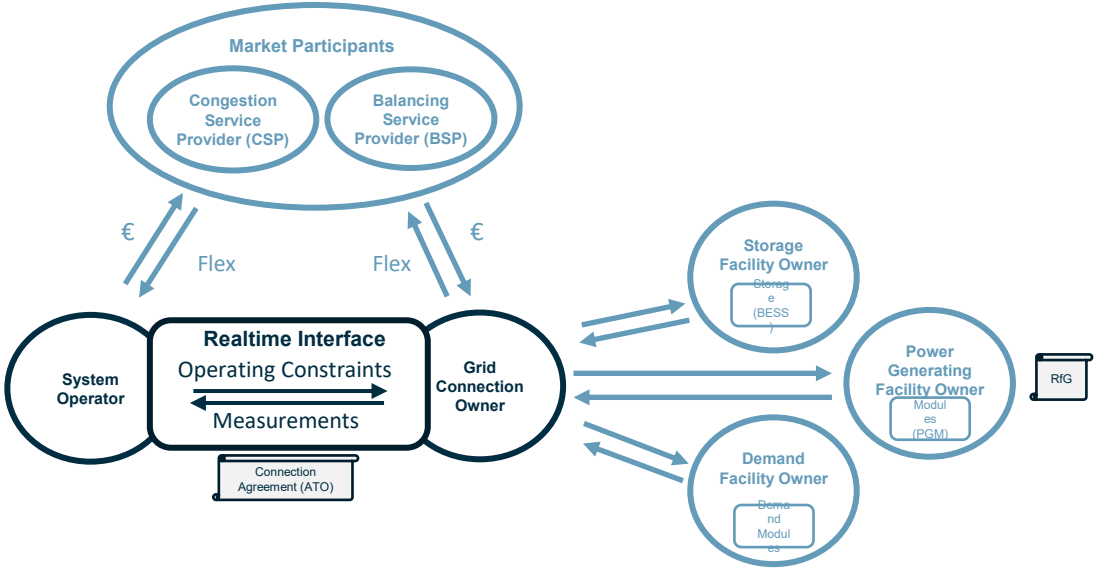
Security by design: De Realtime Interface als voorbeeld

Maarten Hoeve, DNV

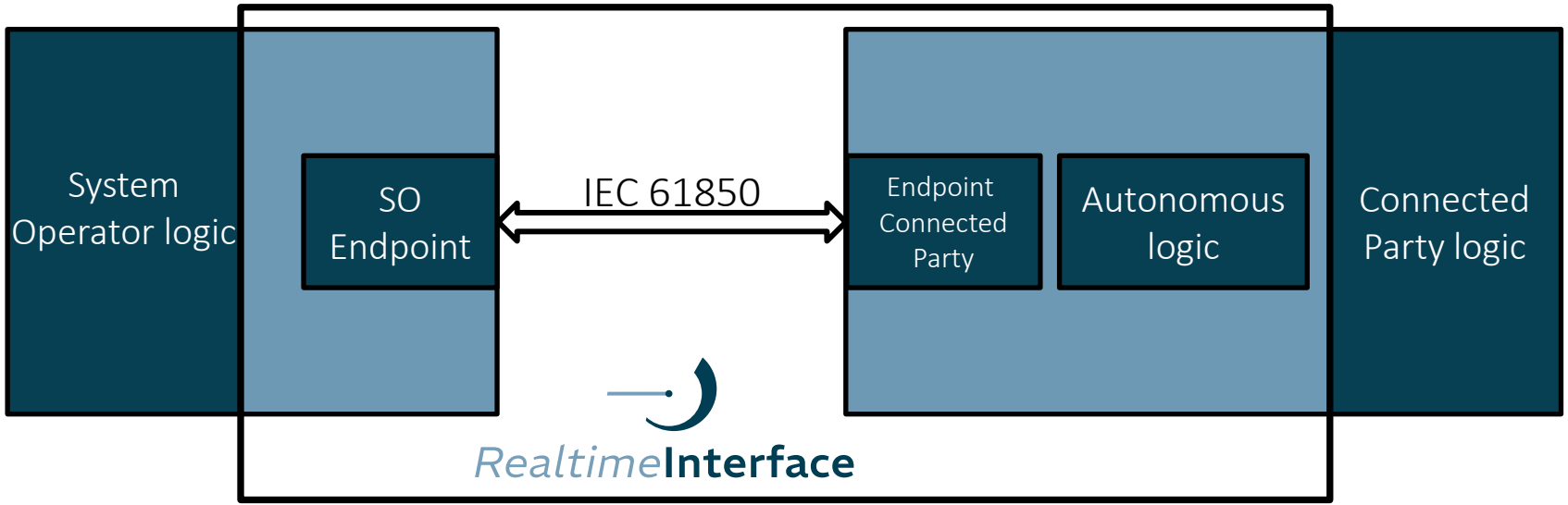
René Troost, Stedin

cigre Nederland

Introductie: De Realtime Interface

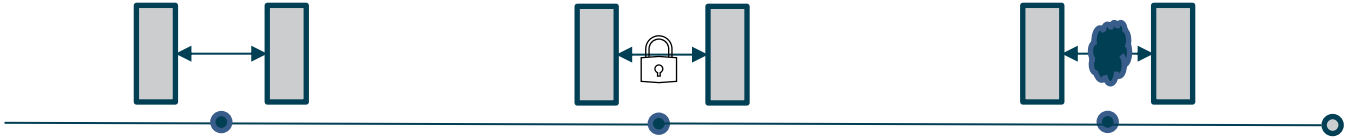


Introductie: De Realtime Interface



Introductie: De Realtime Interface

Realtime Interface: de versies



NBNL RTI v1.0

Doel
Zo snel als mogelijk een oplossing realiseren waarmee het huidige elektriciteit op een veilige manier beter benut kan worden

Kenmerken
Fysieke lokale verbinding tussen end-points netbeheerder en klant

Real-time sturing

Verwachtte aantallen:
≤ 600

Start uitrol:
2024

NBNL RTI v1.1

Doel
Introductie van extra laag veiligheid op RTI v1.0 middels TLS op de dataverbinding.

Kenmerken
Fysieke lokale verbinding tussen end-points netbeheerder en klant

Real-time sturing

Verwachtte aantallen:
≈ 2500

Indicatie start uitrol:
2026

NBNL RTI v2.0

Doel
Toekomstvaste, laagdrempellige en schaalbare oplossing neerzetten

Kenmerken
Internet-gebaseerde verbinding tussen endpoints netbeheerder en klant

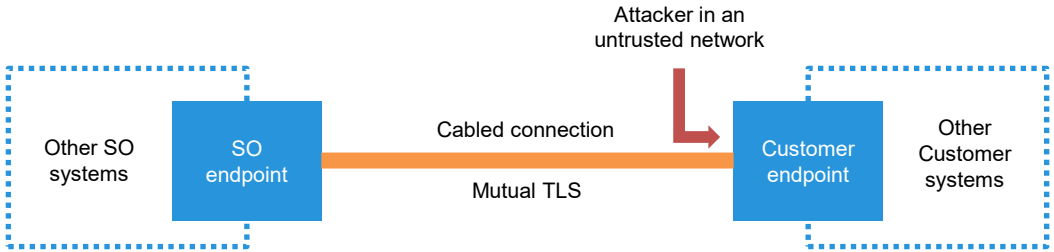
Real-time sturing

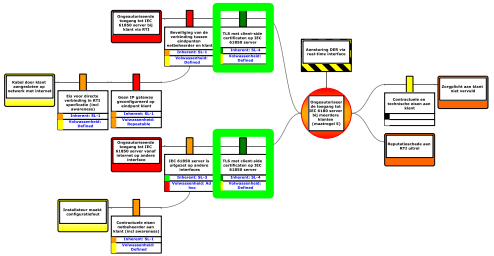
Verwachtte aantallen:
≈ 10000

Indicatie start uitrol:
≥ 2028

Waarom doorontwikkeling versie 1.1?

- Uitbreiding risico analyse: nieuw aanvalspad naar de klant (installatie)
- Kan leiden tot scenario dat klant fake stuursignaal ontvangt
- Klein aantal RTI's: risico verwaarloosbaar. Groter aantal: risico aanzienlijk.
- Risico mitigeren: verschillende opties → TLS





Aanpak doorontwikkeling

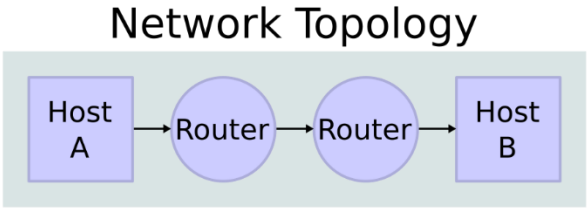
- Toepassing TLS vraag om architectuur- en implementatiekeuzes
- Nieuwe technologie binnen ons domein
- Groot verschil in implementatie volwassenheid
- Verschil van inzicht security experts
- Keuze gemaakt: Proof-of-Concept als basis voor ontwerp

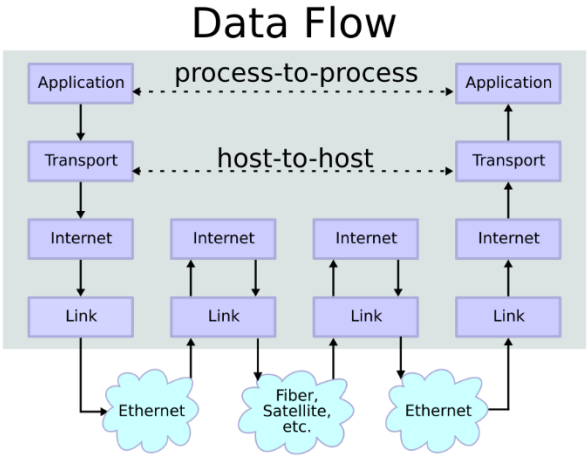
Proof-of-Concept TLS implementatie

- Q3/Q4 2024 uitgevoerd
- Drie implementatievarianten beproefd
- Alle varianten mitigeren het risico
- Groot verschil in volwassenheid en toekomstbestendigheid

Wat is TLS?

- Transport layer security: beveiligde versie van TCP
- MMS in IEC 61850 kan zonder aanpassingen over TLS worden verstuurd en heeft dan sterke beveiliging
- Protocol gebruikt voor web (HTTPS), dus breed ondersteund
- Implementatie kan met open-source bibliotheken

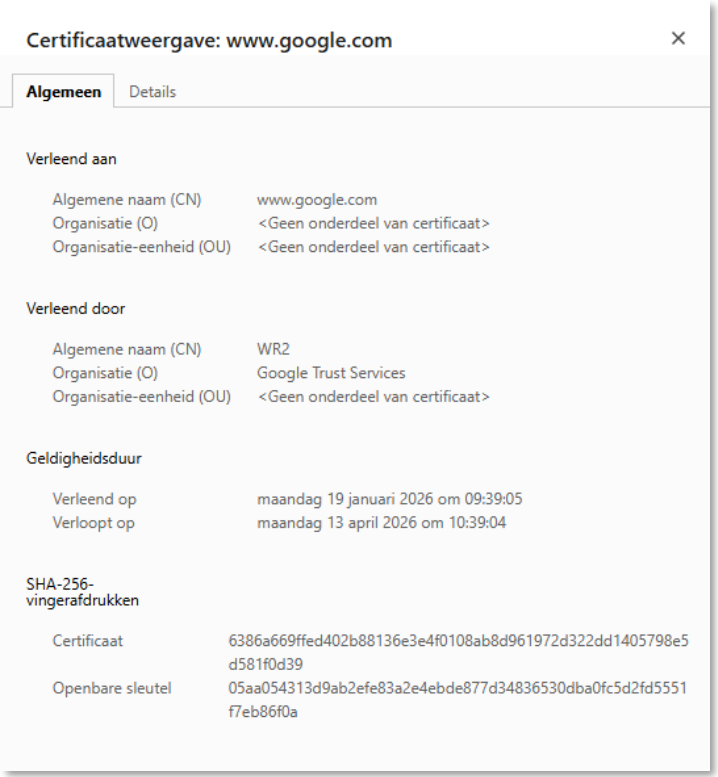




Certificaten en authenticatie in TLS

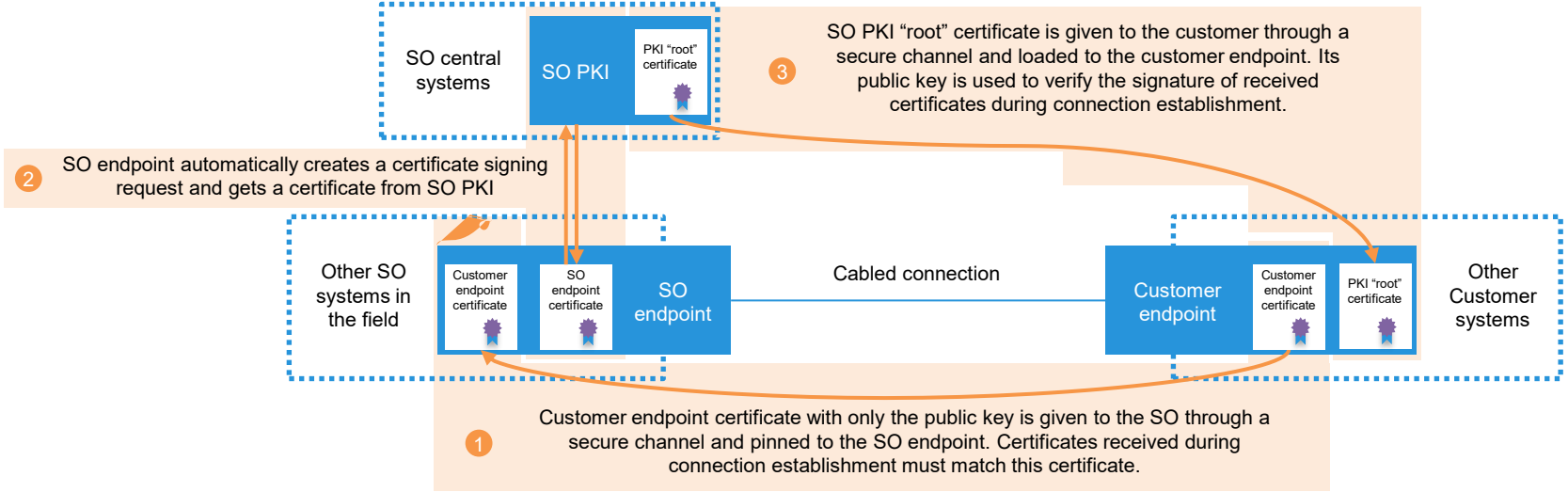
- TLS gebruikt certificaten om identiteit van een eindpunt te controleren (“authenticatie”)
- Certificaat gebruikt publieke sleutel en private sleutels
- Oplossing risico vereist tweezijdige authenticatie: SO endpoint en Customer endpoint hebben beide certificaat nodig

- How koppelen we de certificaten aan de eindpunten?



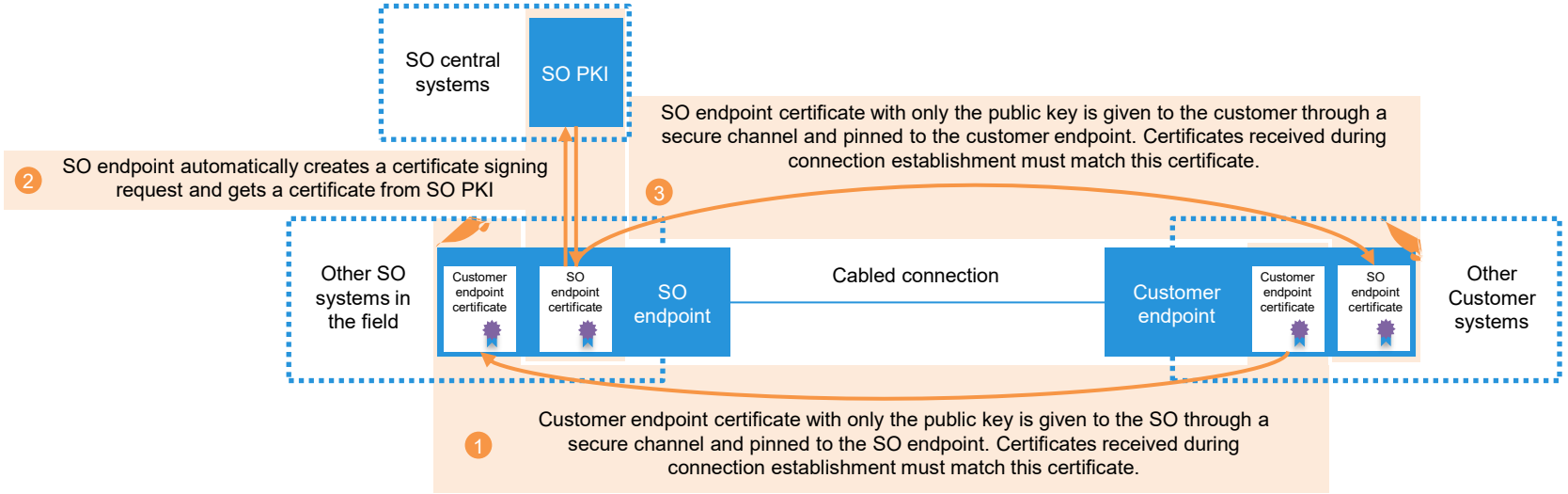
Variant 1

Customer certificates are pinned in the SO endpoint 1
SO endpoint certificates are issued by SO PKI 2
The certification chain of the SO endpoint certificate is checked by the customer endpoint 3



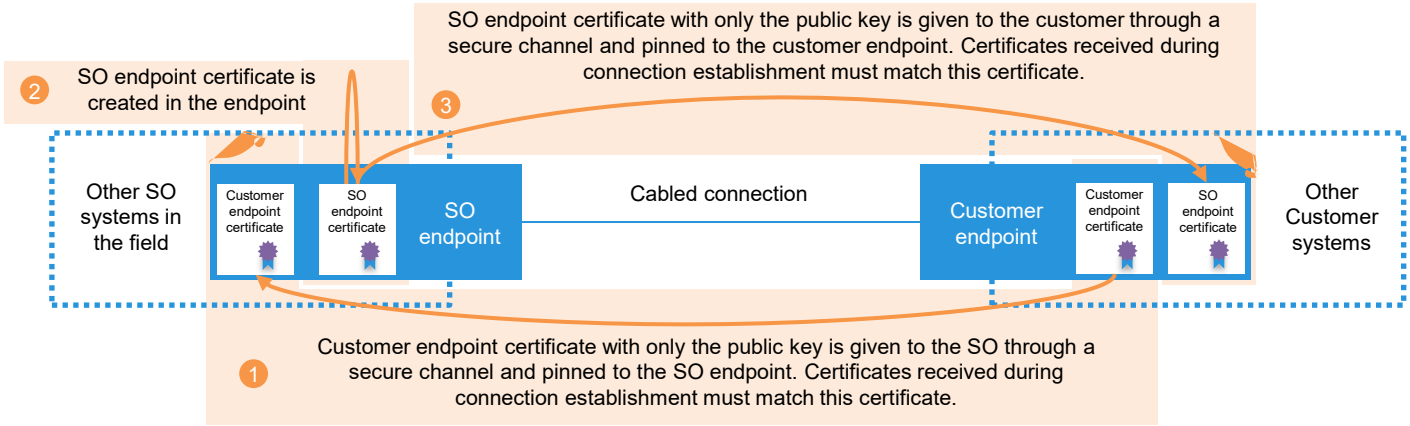
Variant 2

Customer certificates are pinned in the SO endpoint 1
SO endpoint certificates are issued by SO PKI 2
SO endpoint certificates are pinned in the customer endpoint 3



Variant 3

Customer certificates are pinned in the SO endpoint 1
SO endpoint certificates are self-signed 2
SO endpoint certificates are pinned in the customer endpoint 3



Keuze variant

- Op basis van de PoC is variant 1 geselecteerd:
  - Wordt goed ondersteund door leveranciers van de eindpunten
  - Meest geschikt voor het automatiseren van de processen
  - Maakt het mogelijk om de SO endpoint certificaten te updaten
- Netbeheerders richten nu processen in om certificaten te beheren
  - Veilig kanaal om public key van Customer endpoint te delen

BEDANKT VOOR JULLIE AANDACHT

cigre Nederland