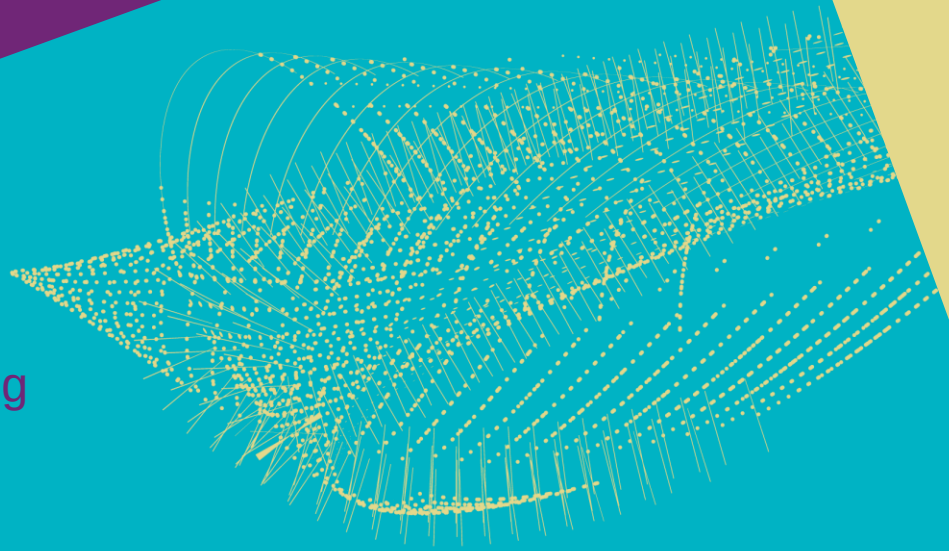
Nikhef

Maastricht University

GÉANT
Networks • Services • People



January 2025 EUGridPMA meeting

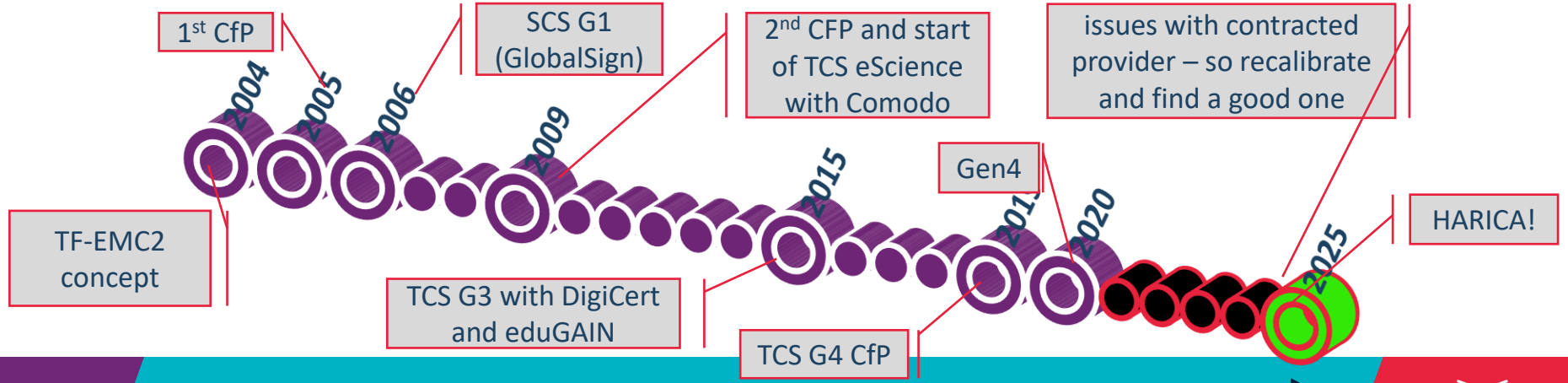
GEANT TCS Gen 5

doing ++n while reflecting on n-1

David Groep
Nikhef

by now 20 years of TCS …

- based on a concept by Jan Meijer back in 2004
- driven primarily by the NREN constituency, but with the e-Infra use cases very much in mind
- NREN (GEANT constituency) requirements on public and (IGTF) authentication trust
- in a way that scales to 45 countries and >500k active certificates today, increasing steadily
- and also >10000 organisations, at varying states of automation maturity
- now in its 5th iteration: GlobalSign, Comodo, DigiCert, S***tigo, and now HARICA!



TCS: a stable constant factor

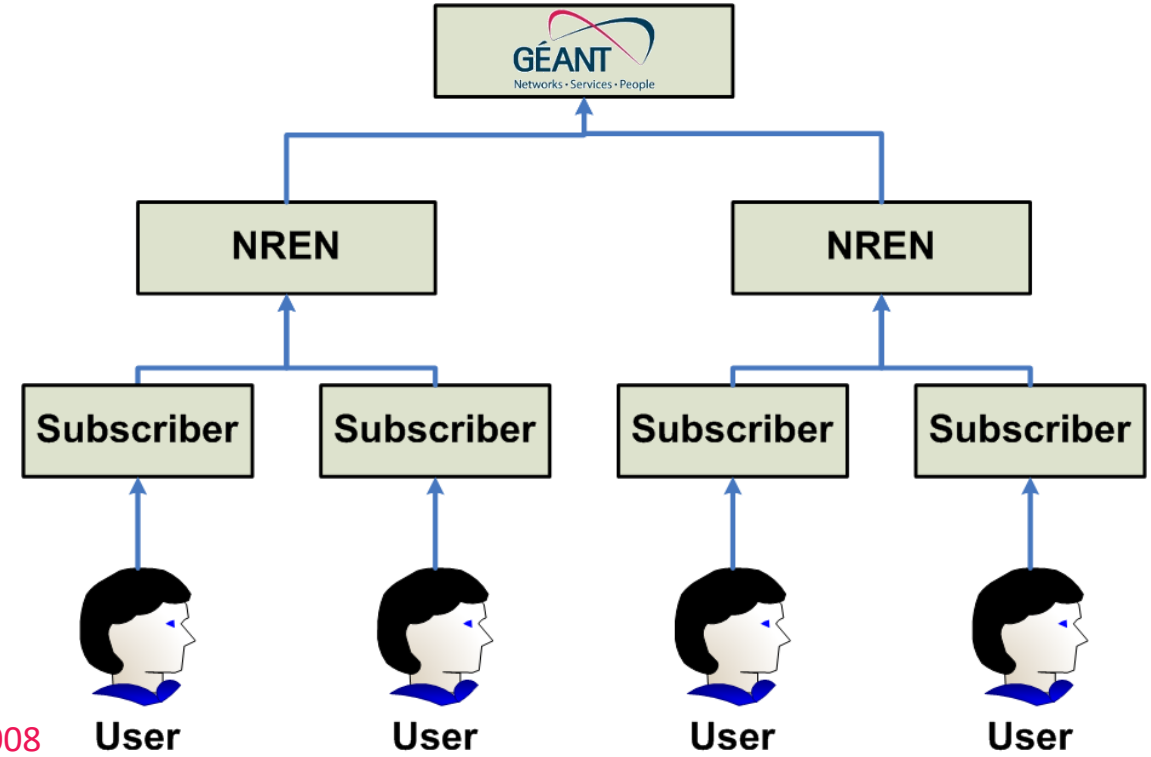
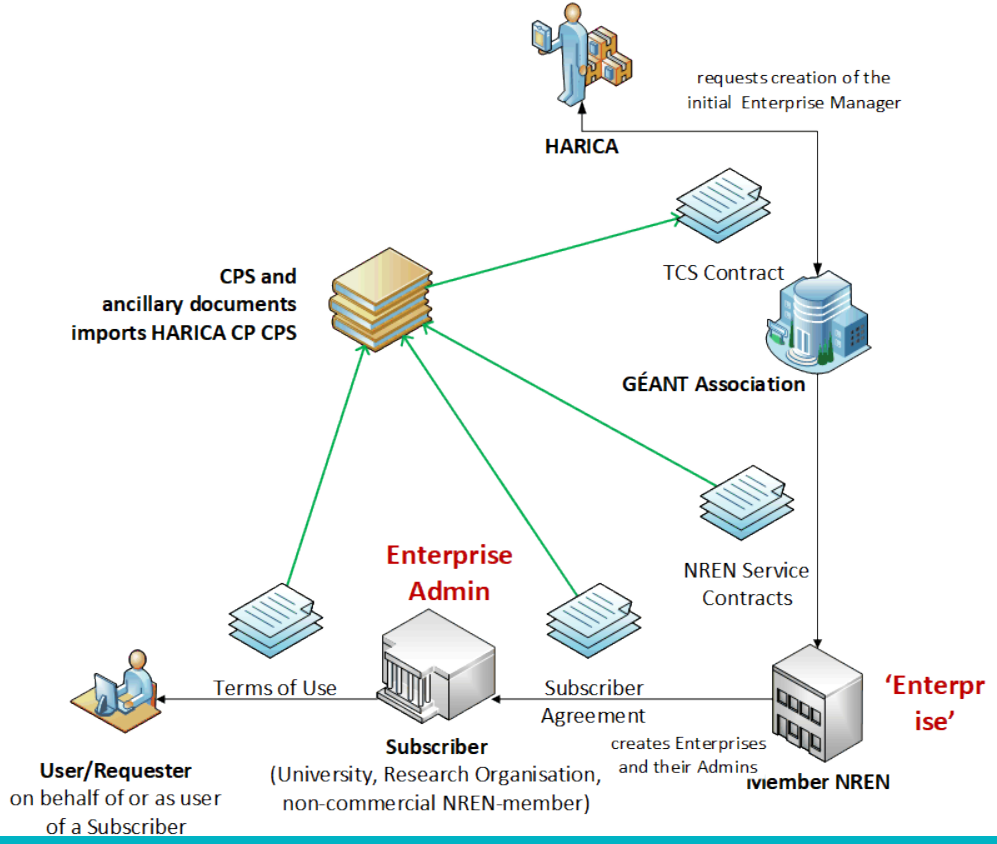


image source: Jan Meijer, 2008
Updates for TERENA – GEANT change in 2017

TCS G5 controls structure follows same model



Main IGTF relevant items

You all loved TCS Gen 4, so we keep it as similar as possible

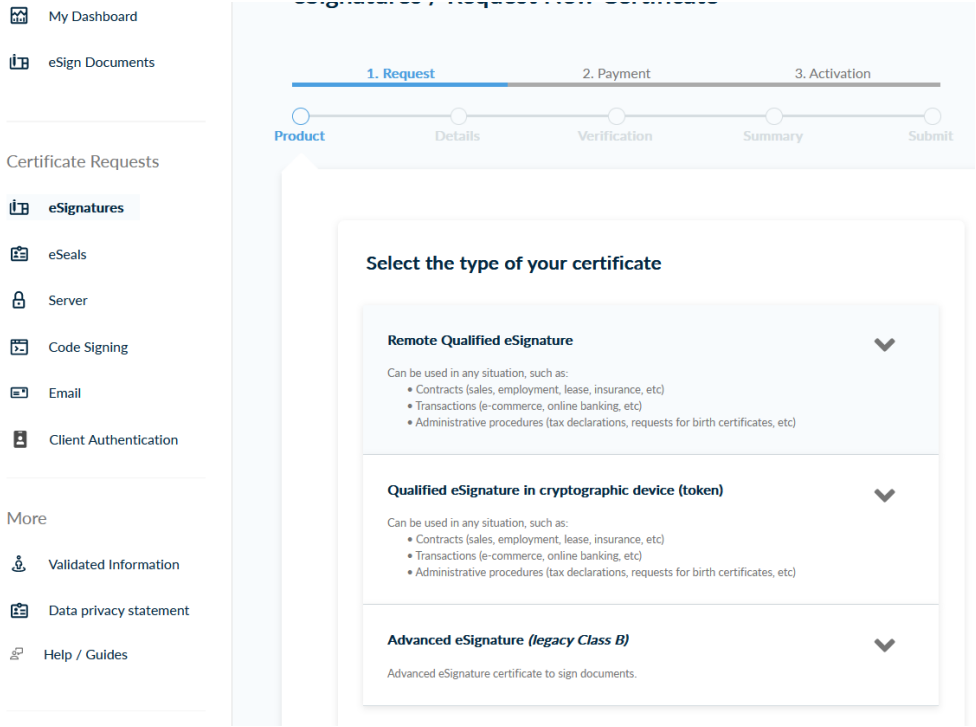
- validation for server certs (CABF OV)
  and model for personal/robot **remains the same**
- **adherence to TCS CP/CPS (v2.2)** the same
  augmenting the publicly trusted accredited provider CP/CPS for joint trust
- so now on top of HARICA's CP and CPS

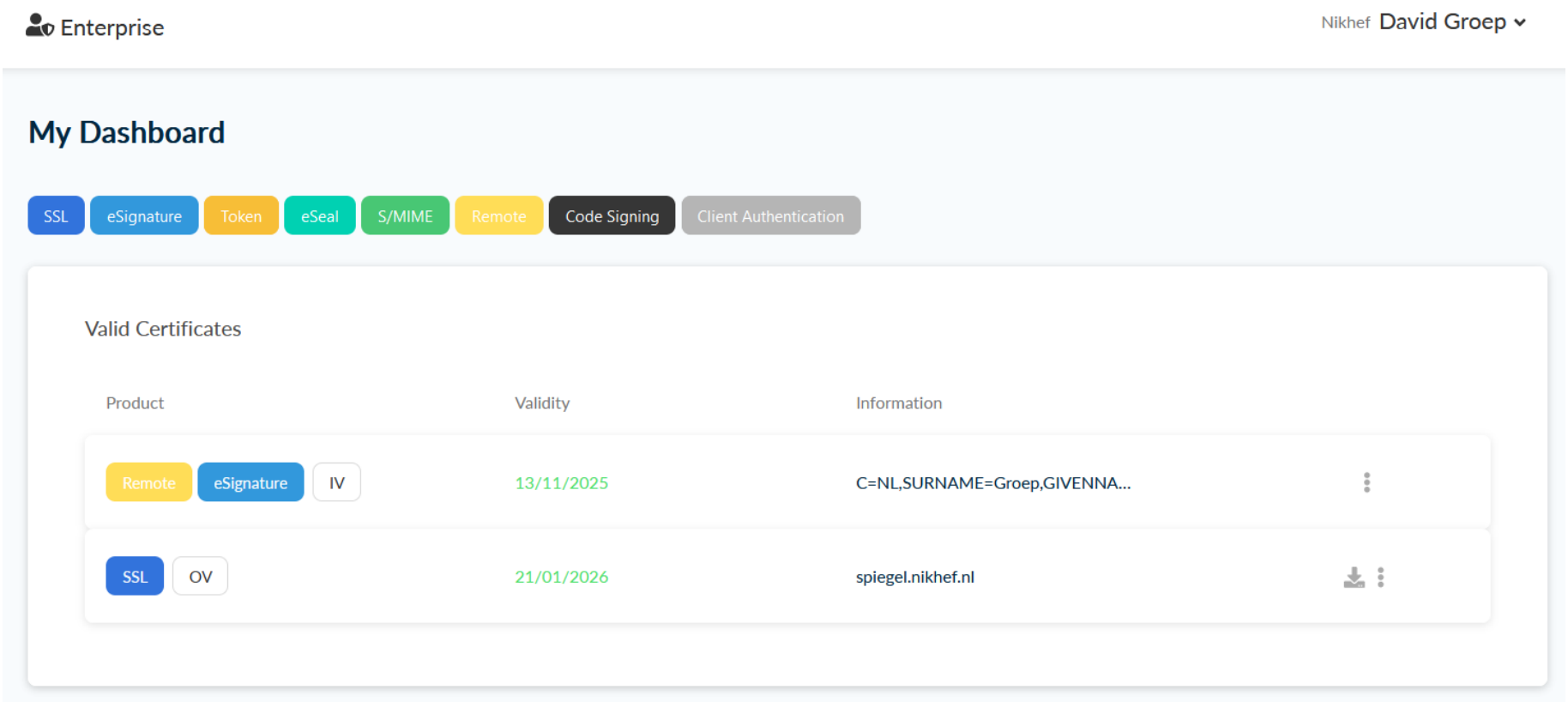
HARICA: "Hellenic Academic & Research Institutions Certification Authority"

- GREEK UNIVERSITIES NETWORK (GUnet)
- University of Athens – Network Operation Center

See https://www.harica.gr/

Some background on TCS G5 backed by HARICA




Enterprise
Nikhef David Groep
My Dashboard
SSL
eSignature
Token
eSeal
S/MIME
Remote
Code Signing
Client Authentication
Valid Certificates
Product
Validity
Information
Remote
eSignature
IV
13/11/2025
C=NL,SURNAME=Groep,GIVENNA...
SSL
OV
21/01/2026
spiegel.nikhef.nl

Main IGTF relevant items

Updates in the (compact) Technical Addendum

- **it is a new hierarchy** (when installed correctly, ends in self-signed HARICA 2015)
- **keeps the current prefix** /DC=org/DC=terena/DC=tcs/…
- **issuer names changed as needed,** and since these show visibly in the UX
- **joint OV browser trust** (and mail agent trust for personal certs) retained

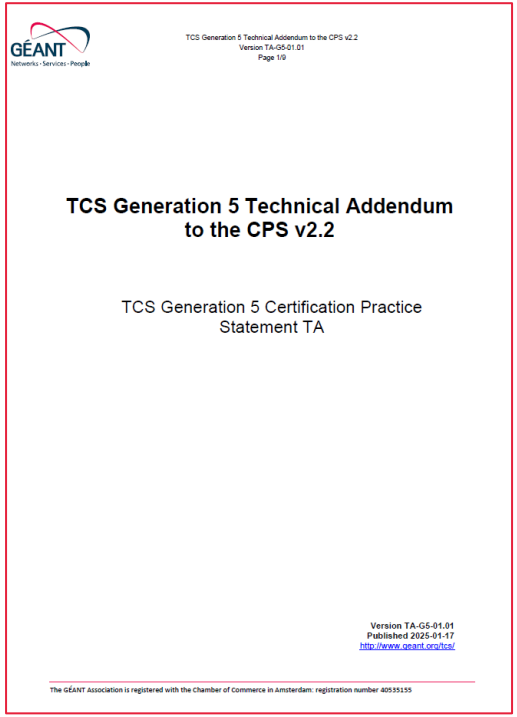
- **distributed** the new RSA Root and intermediates in 1.133 release (February ‘25)
- **continues both RSA and ECC**

and besides regular TCS and joint-trust products, there are nice new things: eIDAS remote vetting for qualified signatures, remote e-signature, European Trust List, …

TCS G5 Technical Addendum

RFC 3647 – but only those section with stipulations are in:

- 1.3.1 Certification Authorities
- 2.1 Repositories
- 3.1.1 Types of Names (to highlight it remain the same)
- 3.1.5 Uniqueness of Names
  allow for new SAML subject-id
- 7.1 Certificate profile
  new root “CN=HARICA TLS RSA Root CA 2021”
- 7.1.4 Name forms
  “The structure of subject distinguished names of TCS Authentication End Entity Certificates remains unchanged by this TA”


TCS Generation 5 Technical Addendum to the CPS v2.2
Version TA-G5-01.01
Page 1/9

TCS Generation 5 Technical Addendum to the CPS v2.2

TCS Generation 5 Certification Practice Statement TA

Version TA-G5-01.01
Published 2025-01-17
http://www.geant.org/tcs/

The GÉANT Association is registered with the Chamber of Commerce in Amsterdam: registration number 40535155

TLS joint-trust effects in ‘participants’ section 1.3.1

Server Certificate services

For the *Server Certificate* services, both OV web-public trusted and joint OV and IGTF Classic (OV) certificates are issues by the “HARICA OV TLS RSA” (2021) and “HARICA OV TLS ECC” (2021), and GEANT TCS specific “GEANT TLS RSA 1” and “GEANT TLS ECC 1” issuing CAs:

- https://repo.harica.gr/certs/HARICA-OV-TLS-Sub-R1.der
- https://repo.harica.gr/certs/HARICA-OV-TLS-Sub-E1.der
- https://repo.harica.gr/certs/HARICA-GEANT-TLS-R1.der
- https://repo.harica.gr/certs/HARICA-GEANT-TLS-E1.der

the difference between the OV and IGTF Classic (OV) certificates is solely in the profile of the end-entity certificates, where IGTF Classic (OV) profiles are prefixed with the domainComponent sequence assigned by GEANT to the TCS (“dc=org”, “dc=terena”, “dc=tcs”, in encoding-order in the subject distinguished name).

The root of trust for all Server certificates are the “HARICA TLS RSA Root CA 2021” and the “HARICA TLS ECC Root CA 2021”:

- https://repo.harica.gr/certs/HARICA-TLS-Root-2021-RSA.der
- https://repo.harica.gr/certs/HARICA-TLS-Root-2021-ECC.der

For transitional compatibility purposes, cross-signed certificates exist to the 2015 trust roots. All certificates are available from the HARICA Repository mentioned in section 2.1.

Personal S/MIME and authentication

Personal Certificate service

For the *Personal (also known as email or S/MIME) Certificate* service, certificates are issued by the "GEANT S/MIME RSA 1" and "GEANT S/MIME ECC 1":

- https://repo.harica.gr/certs/HARICA-GEANT-SMIME-R1.der
- https://repo.harica.gr/certs/HARICA-GEANT-SMIME-E1.der

The root of trust for Personal certificates is the "HARICA Client RSA/ECC Root CA 2021"

- https://repo.harica.gr/certs/HARICA-Client-Root-2021-RSA.der
- https://repo.harica.gr/certs/HARICA-Client-Root-2021-ECC.der

Authentication Certificate services

The *Personal Authentication, Personal Automated Authentication, and Organisation Authentication (Robot Email) Certificate* services, are issued by the "GEANT Authentication RSA 1" and "GEANT Authentication ECC 1". These are provided in a subsequent version of this Addendum.

The root of trust for Authentication certificates is a private (enterprise specific) trust root for the GEANT TCS Research and Education community. These are provided in a subsequent version of this Addendum.

Other Certificate Services

Other certificate services, including Organisation validated S/MIME, OV and EV Code Signing, Qualified Certificates, and any IV certificates are not covered by this technical addendum.

Current state, January 2025

if you're connected to eduGAIN, TCS 'IGTF profile' end-entity certs just work

- native integration to eduGAIN via Seamless Access
- using the same authorisation model
  eduPersonEntitlement = urn:mace:terena.org:tcs:personal-user
- credentials are either CSR upload,
  or browser generated

On the to-do list

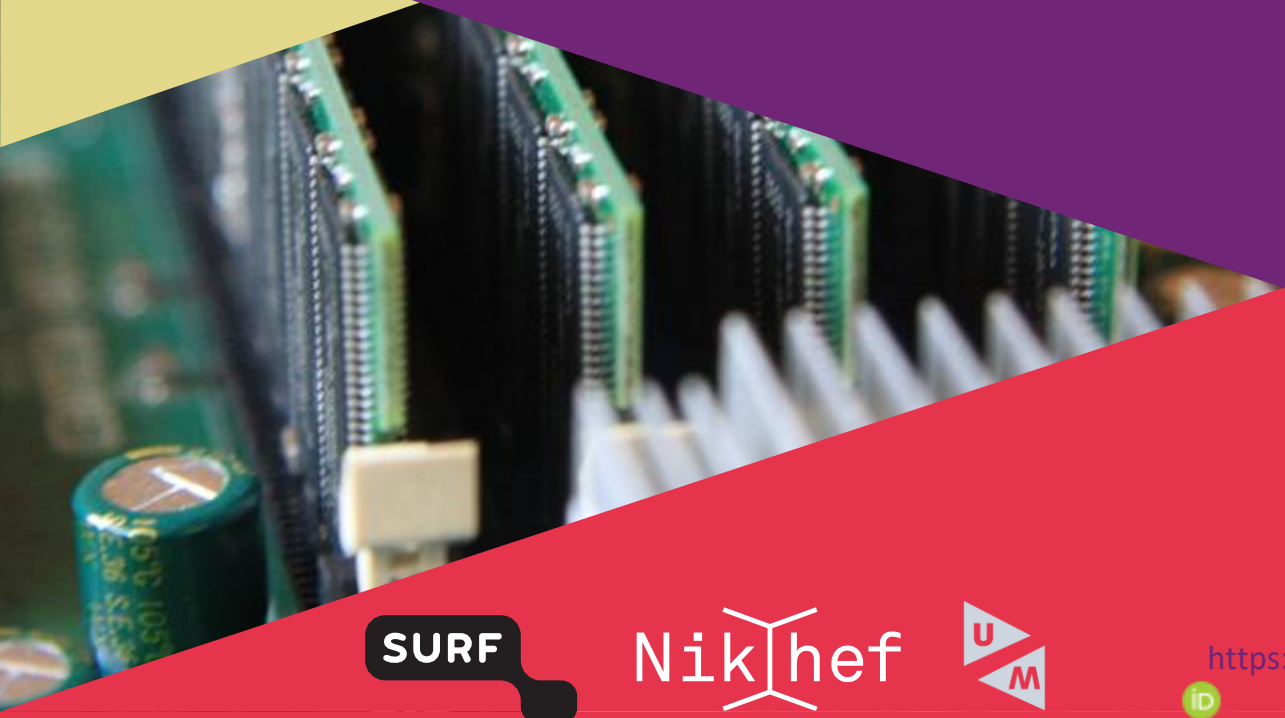
We got the trust roots and the TLS certificates,
we have mailbox-validated S/MIME, but ongoing items include

- client SAML authentication issuance (ePEntitlement based)
- mechanism to actually *select* the IGTF OV joint-trust profile
  subscriber access to joint-trust profiles in ~March,
  just OV (and DV) for now
- ability to request Client Robot Email (org-role client authentication)
- S/MIME self-issuance

And, paraphrasing Wittgenstein, …

‚Wovon man nicht schreiben kann, darüber muss man sprechen‘

(the rest of this page intentionally left blank)



David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

this work co-funded by and contributing to the Dutch National e-Infrastructure coordinated by SURF