IGTF
Interoperable Global Trust Federation
AP | EU | TAG

eugridpma

EUGridPMA Status Updates

status of our authorities and trust fabric news

March 2025

David Groep
davidg@nikhef.nl

Nikhef
Maastricht University

eugridpma

part of the work programme of GEANT 5-1 EnCo, and AARC TREE

the work has received co-funding from the European Union

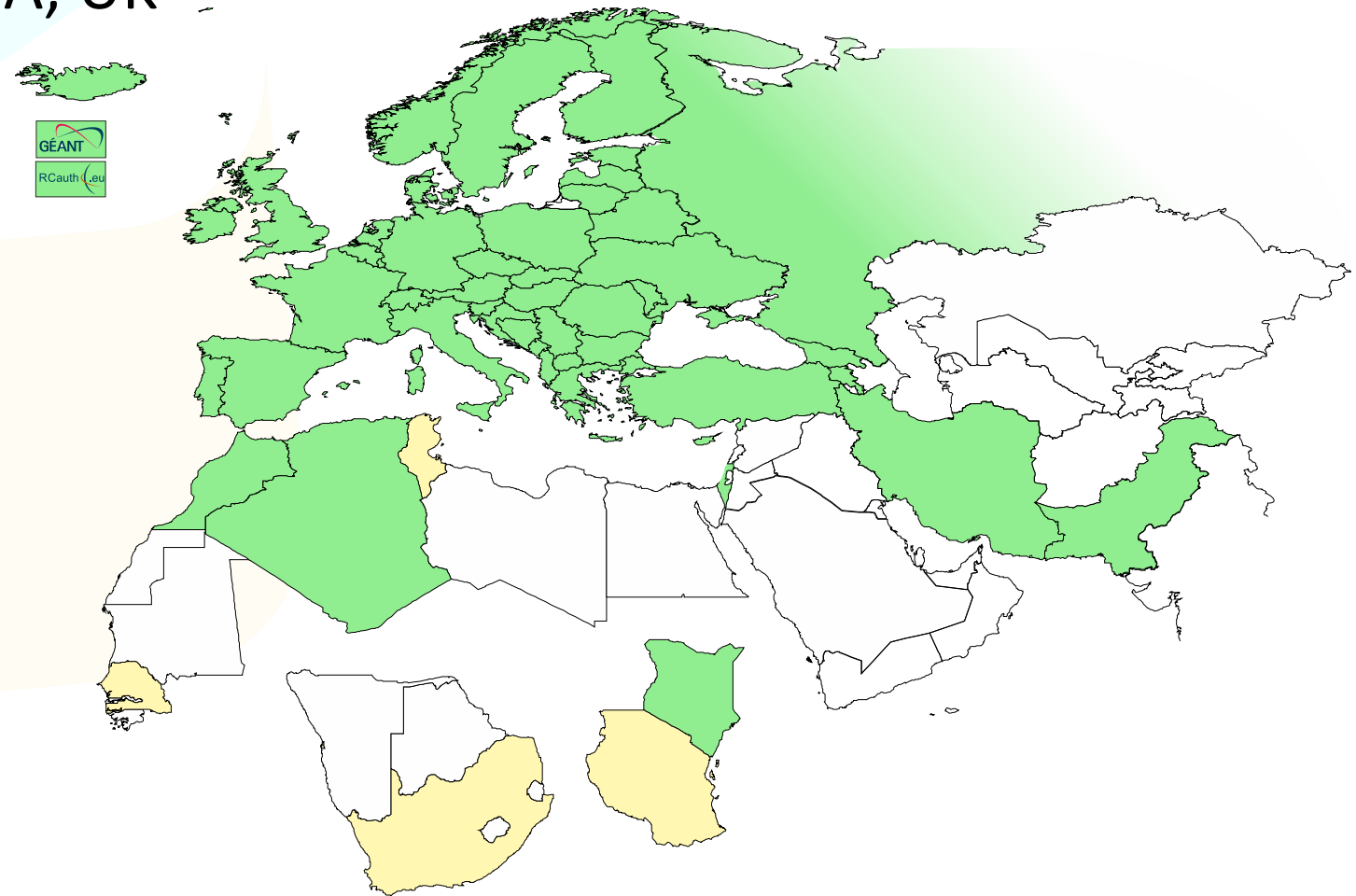
co-supported by Nikhef and the Dutch National e-Infrastructure coordinated by SURF

Meanwhile in the EUGridPMA+ …

- EUGridPMA and IGTF distribution matters
  - constituency and developments
- Root migration update for EL9+ (or: why people bother the fetch-crl devs)
- TCS Gen5 update

EMEA area membership evolution

- Europe[+]: GEANT TCS, and CZ, DK(+FI+IS+NO+SE), HR, NL, PL, RO, SI, SK, AM, MD, ME, ~~MK~~, RU, TR, UA, UK
- Middle East: IR, PK
- Africa: DZ, ~~KE~~, MA
- CERN, RCauth.eu



Membership and other changes

- Identity providers: both reduction and growth
  - migration to GEANT TCS continues
    https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo
  - CERN joined TCS via Renater (FR)
  - Discontinued: -GE, -BY, -PT, -AE, -FR
  - Suspended: -KE, -MK
- Self-audit review
  - Cosmin Nistor tracks the status on the PMA Wiki
  - real-time interaction between authority and reviewers helps, but …
- .ch is now served by eMudhra

Updates in 1.133 and 1.134

```
Changes from 1.132 to 1.133
---------------------------
(XX February 2025)

* Updated re-issued GridCanada root with extended validity period (CA)
* Added GEANT TCS Generation 5 TLS ICAs and corresponding HARICA roots (EU)
* updated SHA-256 root CA for RDIG mitigating EL9/FedoraCore deprication
* MARGI put on hold due to domainname resolution issues (MK)
```

```
Changes from 1.133 to 1.134
---------------------------
(5 March 2025)

* New ANSPGrid CA 2 roll-over for root-issuer key pair (BR)
* Withdrawn discontinued AC-GRID-FR series authorities (FR)
```

Distribution signing key update

```
error: Verifying a signature using certificate
 D12E922822BE64D50146188BC32D99C83CDBBC71
 (EUGridPMA Distribution Signing Key 3 <info@eugridpma.org>):
 Key C32D99C83CDBBC71 invalid: not signing capable
```

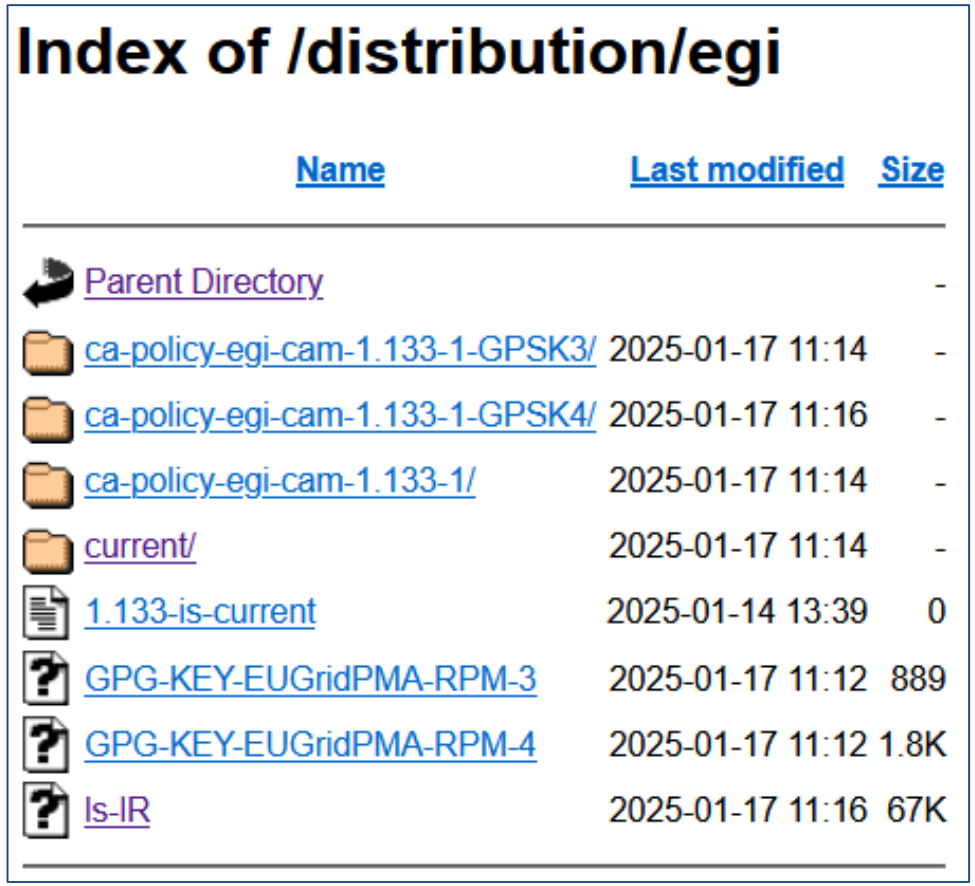
In Fedora Core 38+ (and thus later in its derivatives, and maybe soon in Debian), RSA 1024 package signing no longer supported by default

(work-around with bespoke crypto-policies possible, not recommended)

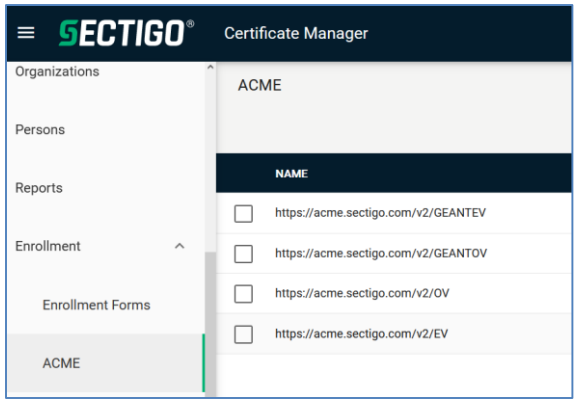
Distribution key update

In future releases we move to a **new GPG package key**

- RSA-2048
- called GPG-KEY-EUGridPMA-RPM-4
- distributed with 1.122+ releases
- Retrieve new public key file from https://dl.igtf.net/distribution/GPG-KEY-EUGridPMA-RPM-4
- or from the public key servers: rsa/2048 dated 2023-07-29T12:06:23Z
- fingerprint: 565f 4528 ead3 f537 27b5 a2e9 b055 0056 **7634 1f1a**



Other CABF things to keep in mind



- Server SSL BR has already been updated
  - the provision for using DC prefixing has been retained
- But expect shorter validity periods in the future
  - start preparing for 90-day max in your service deployment automation systems
  - increased use of automation (ACME OV using client ID+secret)

```
[root@hekel ~]# certbot certonly \
  --standalone --non-interactive --agree-tos --email davidg@nikhef.nl \
  --server https://acme.sectigo.com/v2/GEANTOV \
  --eab-kid DUniqueID_forthisclient --eab-hmac-key mv_v3ryl0n9s3cr3tK3y \
  --domain hekel.nikhef.nl --cert-name OVGEANTcert
```

THE CHALLENGE OF SELF-SIGNED ROOTS

AND FF & REDHAT' S IDEA OF WHAT SELF-SIGNED MEANS …

Rocky9+, AlmaLinux9+, RHEL9+ and

With RHEL9 also deprecating SHA-1, but *at the same time*
still having self-signed SHA-1 based root certs in the ca-certificates package, depends on a RedHat/OSSL proprietary set of ‘bonus bits’ appended to the end of the ASN.1 certificate blob.

For the others, there is – for now – a policy override:

```
update-crypto-policies --set DEFAULT:SHA1
update-crypto-policies --set LEGACY
```

even if that is a rather course-grained and blunt tool

Mitigations: SHA migration

Still,

- if you still have a SHA-1 root
- and you are able to re-issue with the same key (and new serial)
- and your EECs *do not* have dirname+serial in their AKI

your CAs should probably re-issuing its root because that is just easier.

But:

- for large ones, esp. e.g. the DigiCert Assured ID Root (2006), that will be hard
- migrating to another (SHA-2 rooted) signing hierarchy will take at least 395 days ... and a lot of engineering on the RP and CA side

Root cause is with RH not understanding what a self-signed trust anchor is, but that will not help us in the short term.

Reissuance of roots – state and progress

ASGCCA-2007

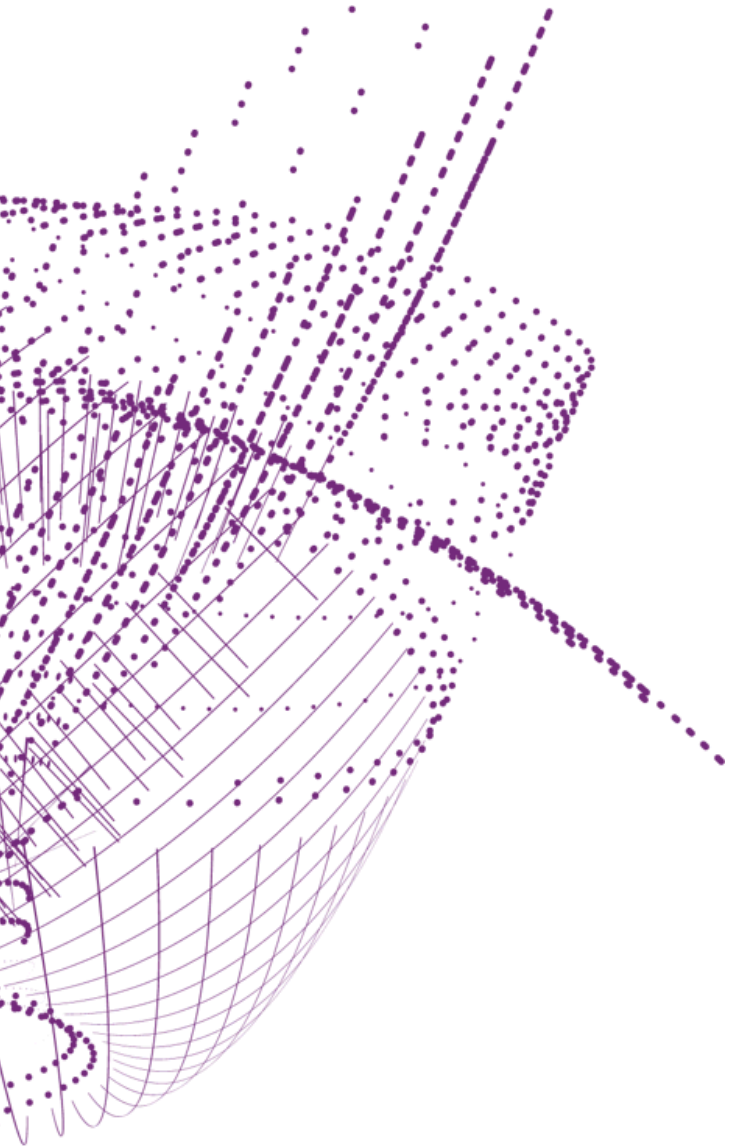
DZeScience
DigiCertGridRootCA-Root
KEK
~~MARGI~~

SRCE
TRGrid

ArmeSFo
CESNET-CA-Root
DigiCertAssuredIDRootCA-Root
IHEP-2013

RomanianGRID
SiGNET-CA
seegrid-ca-2013

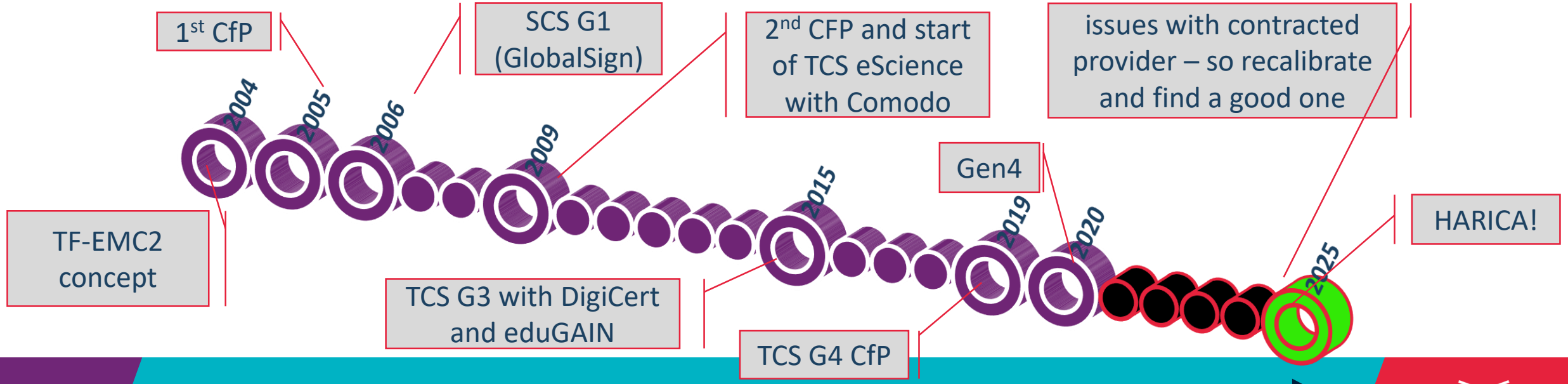
Fixed by ‘now’: RDIG, GridCanada, CILogon basic/silver/OpenID, UKeScienceRoot-2007
Removed: DigiCertGridCA-*, DFN-GridGermany, CNIC, BYGCA , LIPCA, MARGI (suspended)
Pending withdrawal:



TCS Gen 5

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

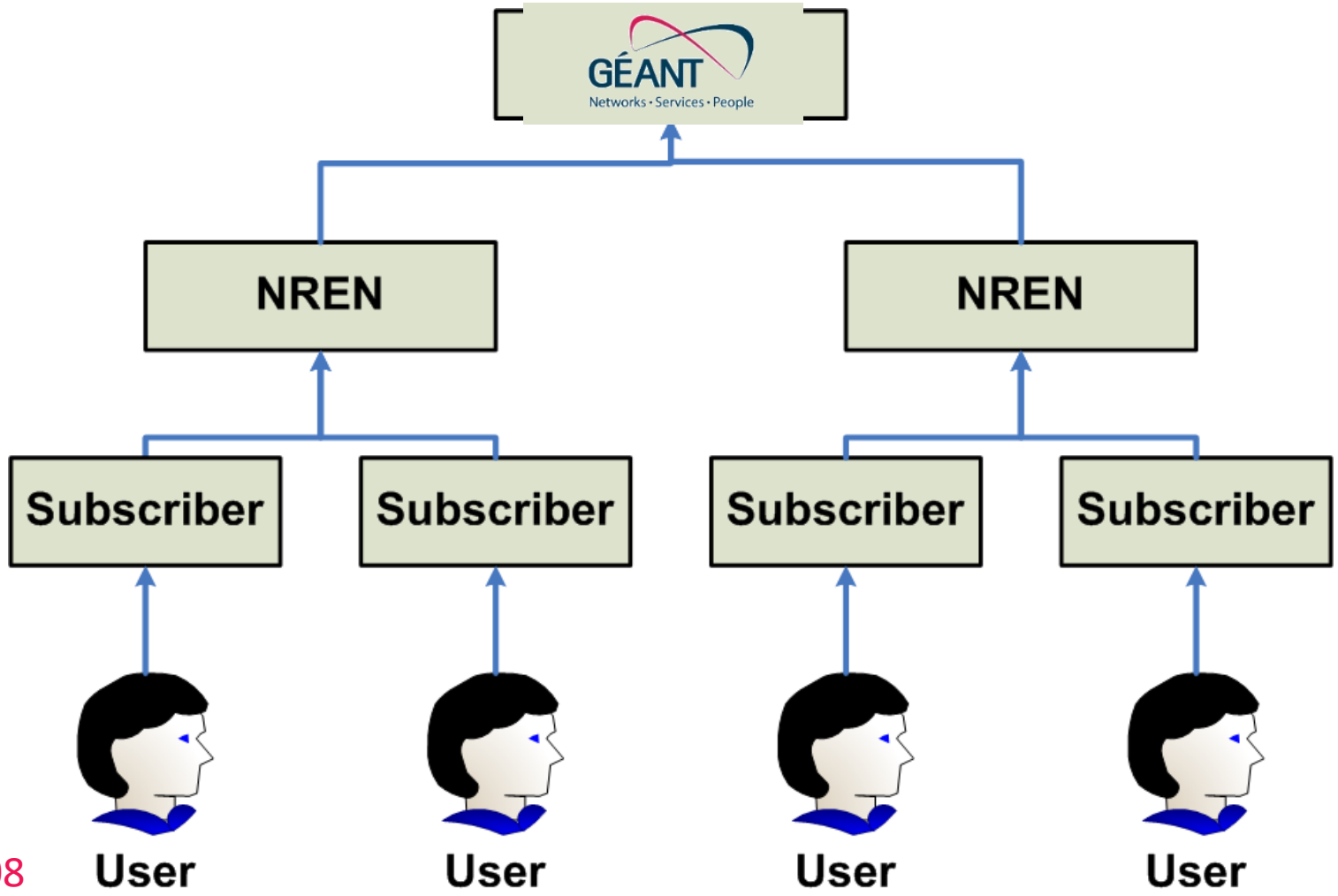
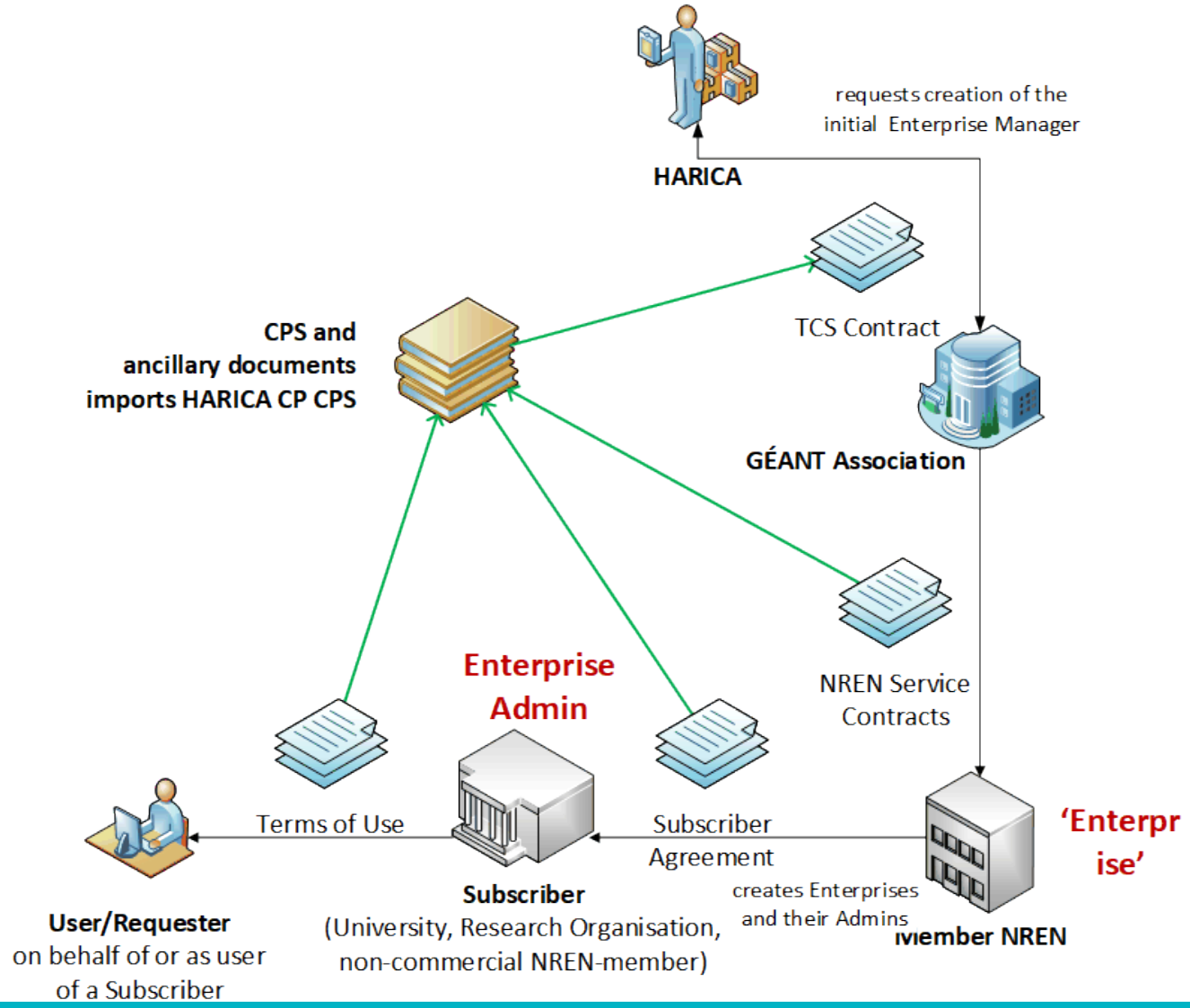


image source: Jan Meijer, 2008
Updates for TERENA – GEANT change in 2017

TCS G5 controls structure follows same model



Main IGTF relevant items

Europe joined TCS Gen 3 and Gen 4 on a large scale,
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)** from Gen 4 TCS remains the same
  augmenting the publicly trusted accredited provider CP/CPS for joint trust

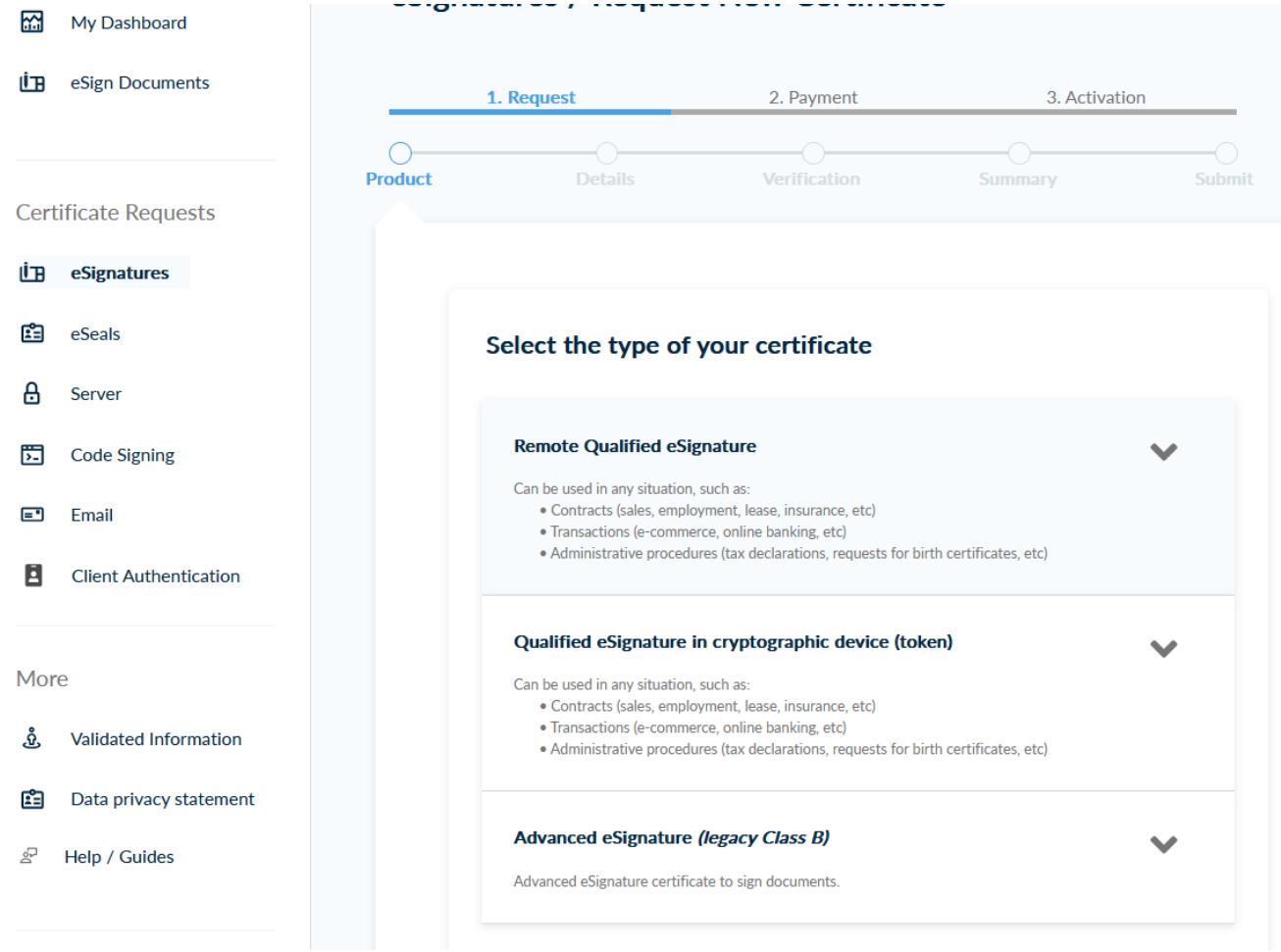
- so now on top of HARICA's CP and CPS ✓HARICA

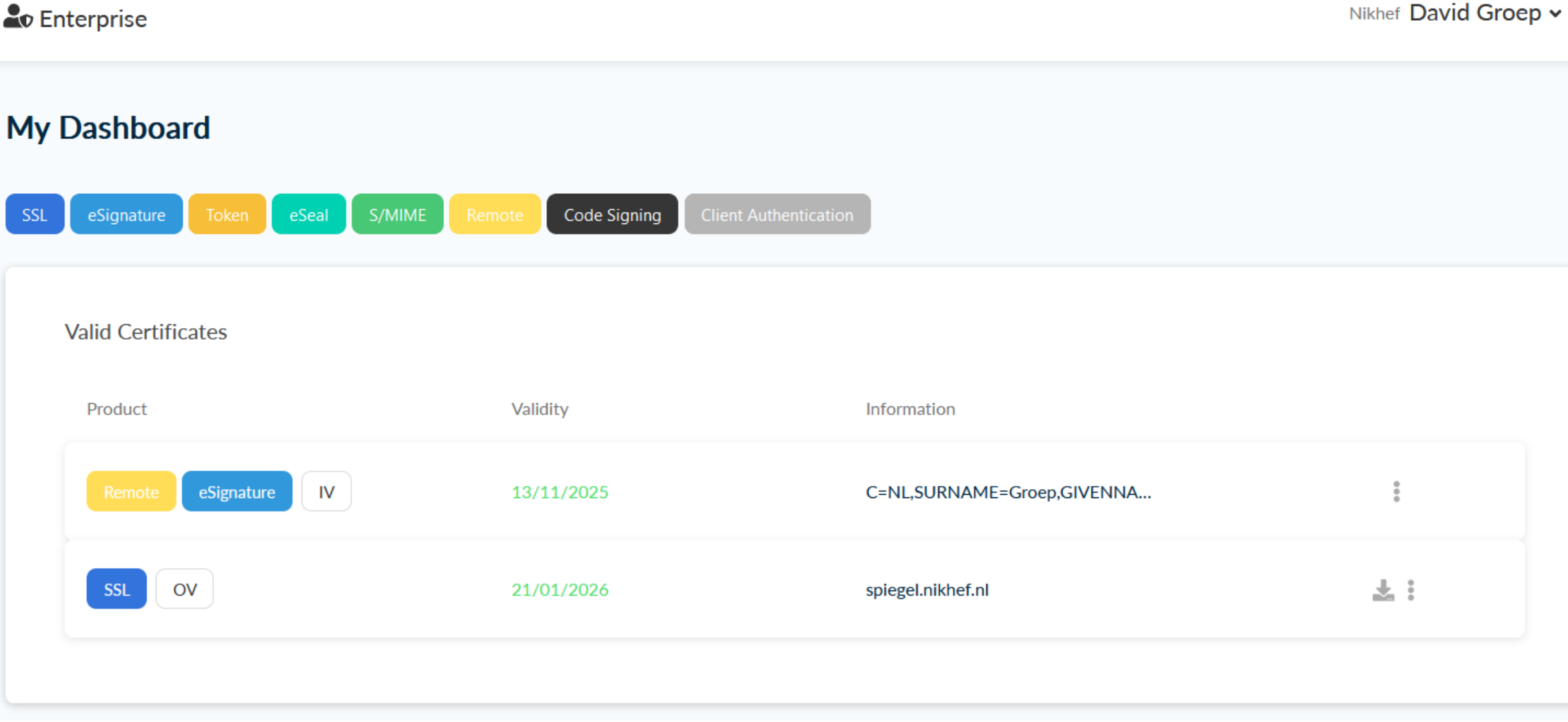
HARICA: "Hellenic Academic & Research Institutions Certification Authority"

- 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

IGTF specific updates

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

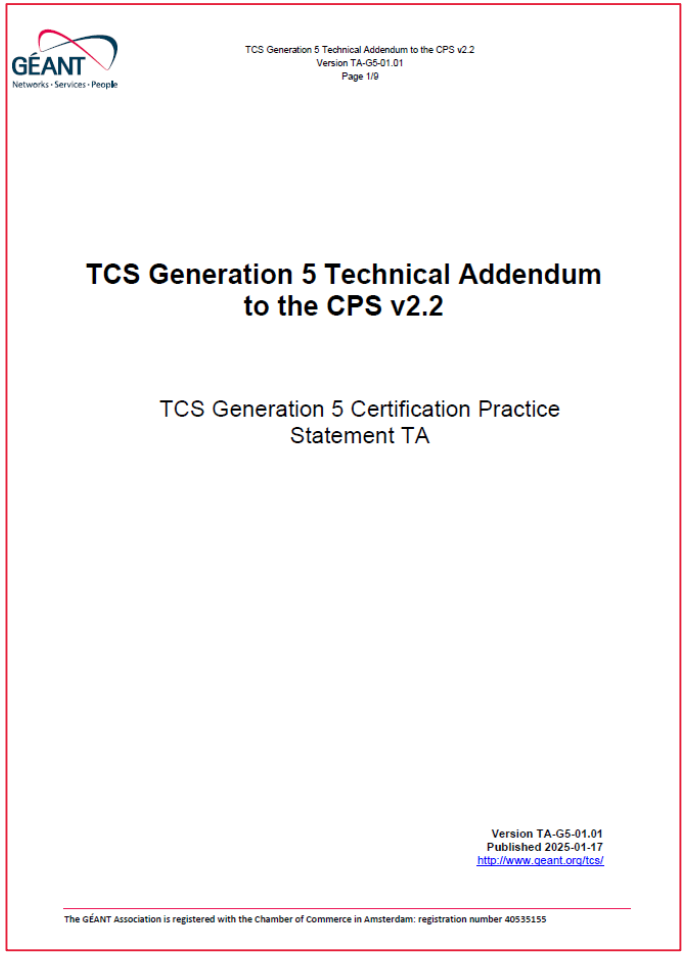
- **distributed** the new RSA Root and intermediates in 1.133 release (February ‘25)
- **continues both RSA and ECC**

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.

TCS Gen5 OV joint-trust certificates work

```
$ x509i tcs-ligbox.nikhef.nl/cert-ligbox.nikhef.nl.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            73:65:f1:60:95:cb:a5:a7:3d:d4:de:e2:e1:d5:37:35
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GR, O = Hellenic Academic and Research Institutions CA, CN = GEANT TLS RSA 1
        Validity
            Not Before: Mar 17 01:16:28 2025 GMT
            Not After : Mar 17 01:16:28 2026 GMT
        Subject: DC = org, DC = terena, DC = tcs, C = NL, L = Amsterdam, O = Nikhef, CN = ligbox.nikhef.nl
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b5:32:91:bb:9e:43:f3:d9:c4:e5:b3:5a:a3:93:
```

but the ASCIIfication is still work in progress – for countries with more than 7 bits …

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

- Done: 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)
- client SAML authentication issuance (ePEntitlement based)
- S/MIME self-issuance

And, paraphrasing Wittgenstein, …

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

(the rest of this page intentionally left blank)

Questions?

BUILDING OUR GLOBAL TRUST FABRIC

Nikhef

Maastricht University

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