Interoperable Global Trust Federation

AP | EU | TAG

IGTF Fabric Updates

status of our authorities and trust fabric news

February 2025

David Groep
davidg@nikhef.nl

Nikhef

Maastricht University

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

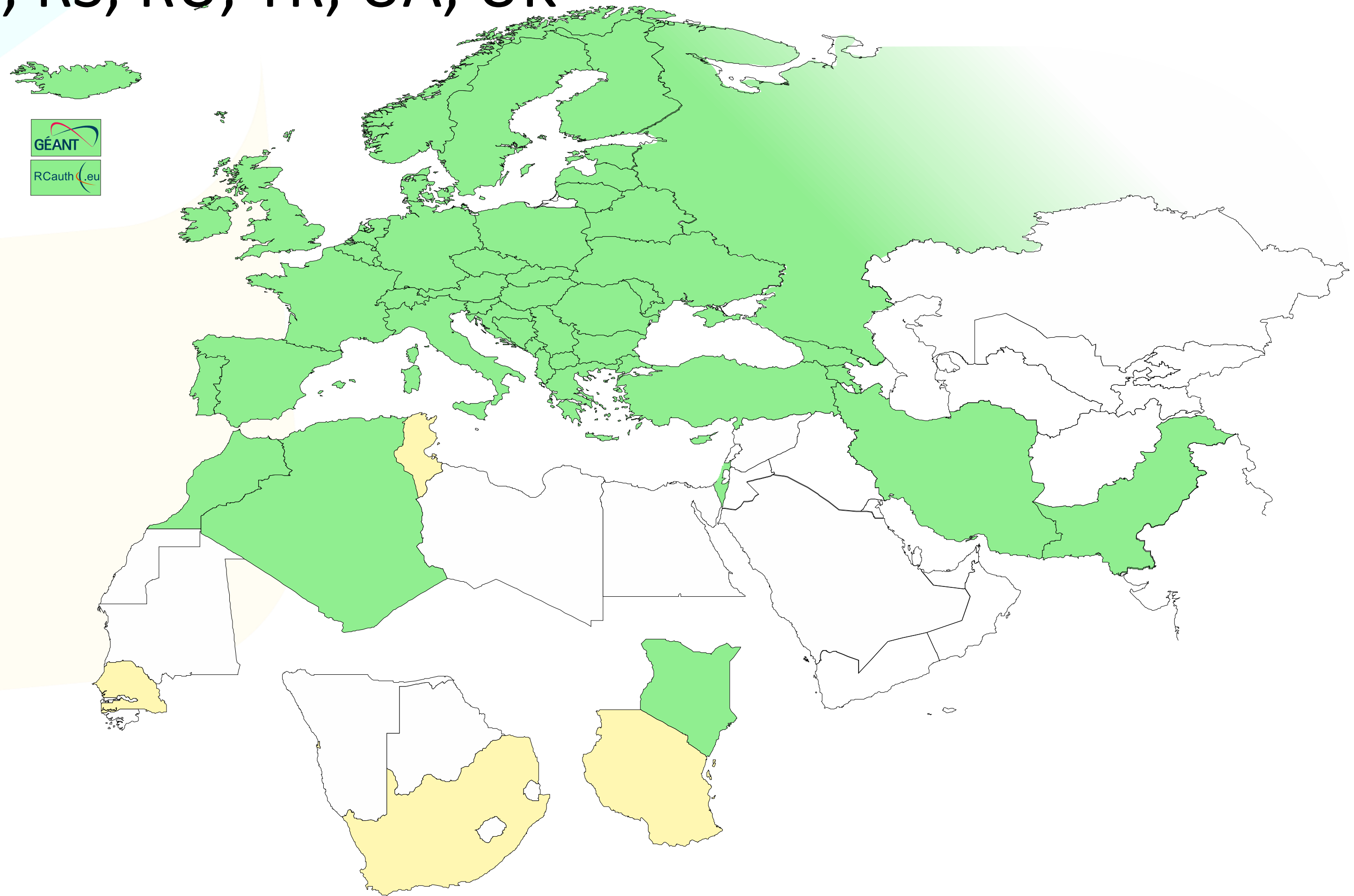
Meanwhile in the EUGridPMA+ …

- EUGridPMA and IGTF distribution matters
  - constituency and developments

- Root migration update for EL9+ (or: why people bother the fetch-crl devs)

EMEA area membership evolution

- Europe$^+$: GEANT TCS, and CZ, DE, DK(+FI+IS+NO+SE), FR, GR, HR, NL, PL, RO, SI, SK; AM, MD, ME, MK, RS, 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
  - 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

```
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)
```

holding off for ‘a few more days’ to get GEANT TCS Private (AuthN) Root and ICA in

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
```

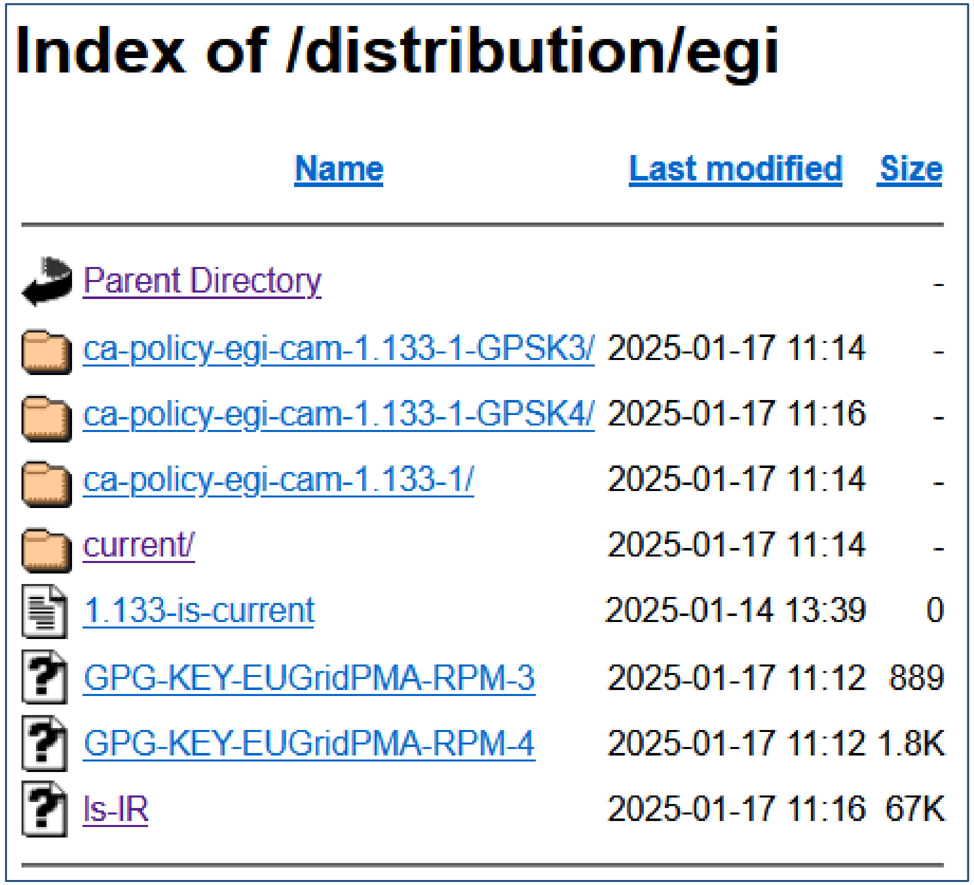
In Fedora Core 38+ (and thus later in its derivatives, and maybe soon in Debian), RSA 1024 package signing no longer supported by default

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

Distribution key update

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

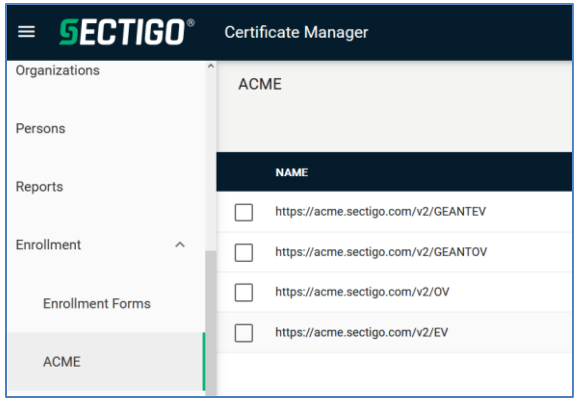
- RSA-2048
- called GPG-KEY-EUGridPMA-RPM-4
- distributed with 1.122+ releases
- Retrieve new public key file from https://dl.igtf.net/distribution/GPG-KEY-EUGridPMA-RPM-4
- or from the public key servers: rsa/2048 dated 2023-07-29T12:06:23Z
- fingerprint: 565f 4528 ead3 f537 27b5 a2e9 b055 0056 **7634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



Index of /distribution/egi

Name	Last modified	Size
Parent Directory		-
ca-policy-egi-cam-1.133-1-GPSK3/	2025-01-17 11:14	-
ca-policy-egi-cam-1.133-1-GPSK4/	2025-01-17 11:16	-
ca-policy-egi-cam-1.133-1/	2025-01-17 11:14	-
current/	2025-01-17 11:14	-
1.133-is-current	2025-01-14 13:39	0
GPG-KEY-EUGridPMA-RPM-3	2025-01-17 11:12	889
GPG-KEY-EUGridPMA-RPM-4	2025-01-17 11:12	1.8K
ls-lR	2025-01-17 11:16	67K

Other CABF things to keep in mind



ACME

NAME
□ https://acme.sectigo.com/v2/GEANTEV
□ https://acme.sectigo.com/v2/GEANTOV
□ https://acme.sectigo.com/v2/OV
□ https://acme.sectigo.com/v2/EV

- 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:

Questions?

BUILDING OUR GLOBAL TRUST FABRIC

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

Nikhef
Maastricht University