IGTF
Interoperable Global Trust Federation
AP | EU | TAG

eugridpma

EUGridPMA Status Updates

status of our authorities and trust fabric news

March 2026

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+ …

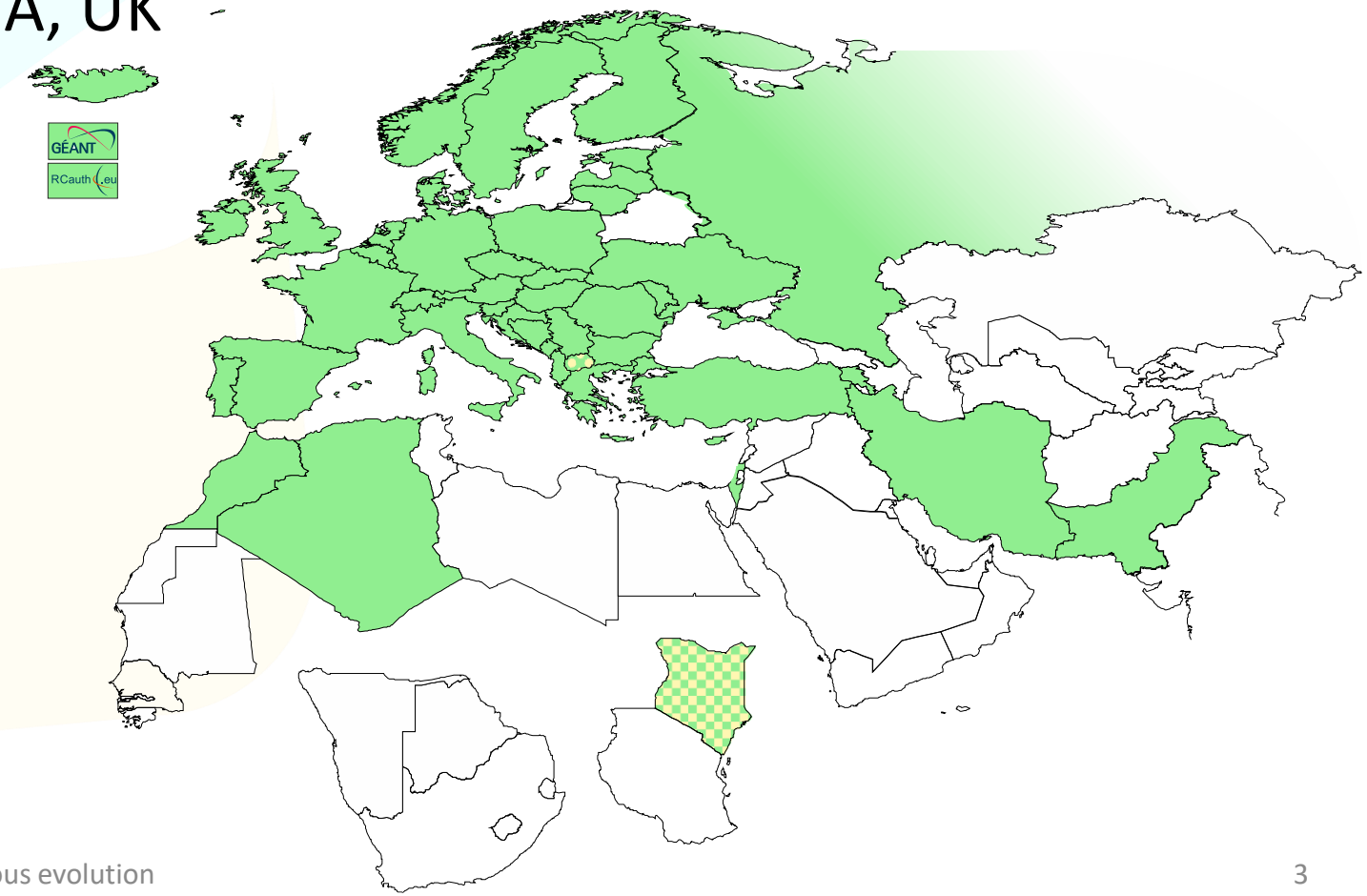
- EUGridPMA and IGTF distribution matters
  - constituency and developments
  - Inclusion of DCVOTA in 1.139 (released yesterday)
- Lifetime of server certificates for non-WebPKI certs
- Client eKU in server certs – deadline deferred
- SHA-1 migration
- IPv6 support
- Many discussion points (knowledge base, token trust …)

https://eugridpma.org/minutes/66

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

- TCS 2027+ procurement about to start



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
  - With reduced number of issuers this effort tends to get less attention
  - real-time interaction between authority and reviewers helps, but …

- .ch is now served by eMudhra – also the backend to .cl and fall-back .ae (retail)

Updates in 1.139

```
Changes from 1.138 to 1.139
---------------------------
(16 March 2026)

* Update ArmeSFo CA re-issued based on SHA-2 family digest (AM)
* The IGTF DCVOTA assurance profile has been added. For details, please refer
  to https://www.igtf.net/ap/dcvota/
```

Other open questions:

- can we start deprecating SSLeay/OpenSSL 0.9.x old-style (MD5 of the BER encoding) hashes at some point?
- retirement of the PGP Gen-3 package signing key?

Other CABF things to keep in mind

- Validity period of public server certs down to 200 days

- But expect shorter validity periods in the future (90, 45, …)
  - 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.endpoint.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.

The policy override (legacy; sha1) has gone away in EL10

This is currently causing operational issues with major RPs, and the result may be that all SHA-1 roots are (implicitly) disabled relatively soon:

- Not an ‘active’ measure,
  but the OS settings will not be changes to accommodate SHA-1 CA roots

Reissuance of roots – state and progress

ASGCCA-2007

DZeScience
~~DigiCertGridRootCA-Root~~
KEK
~~MARGI~~

SRCE (planned soon)
TRGrid

CESNET-CA-Root
~~DigiCertAssuredIDRootCA-Root~~
IHEP-2013

RomanianGRID
SiGNET-CA (planned)
seegrid-ca-2013

Fixed by 'now': ArmeSFo, RDIG, GridCanada,UKeScienceRoot-2007
Removed: DigiCertGridCA-*, DFN-GridGermany, CNIC, BYGCA , LIPCA, MARGI (suspended)
Pending withdrawal: DigiCert*

IPv6, anyone?

Use case is LHCOPN
(i.e. might be less relevant for CAs that do not need to support LHCOPN)

- There is a fall-back location that works, and RPs can enable it with a two-line configuration can be set at the default for CLRs in, e.g., `/etc/fetch-crl.d/ipmirror`

  `postpend_url=http://dl.igtf.net/certificates/@ANCHOR@.r0`
- Recommended solution is for sites to have a **local web cache proxy** which then should support ipv6 and will hide any v4-only CRLs effectively without any per-system config.
- Request to CAs is to consider support IPv6 on their native CDP
  - Adding IPv6 support via CDNs (e.g. CloudFlare) works, but will compromise digital sovereignty.
  - Do NOT disable IPv4, since the majority outside of LHCOPN relies on it everywhere ☺

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