IGTF Fabric Updates

status of our authorities and trust fabric news

May 2025

David Groep
davidg@nikhef.nl

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

the work has received co-funding from the European Union

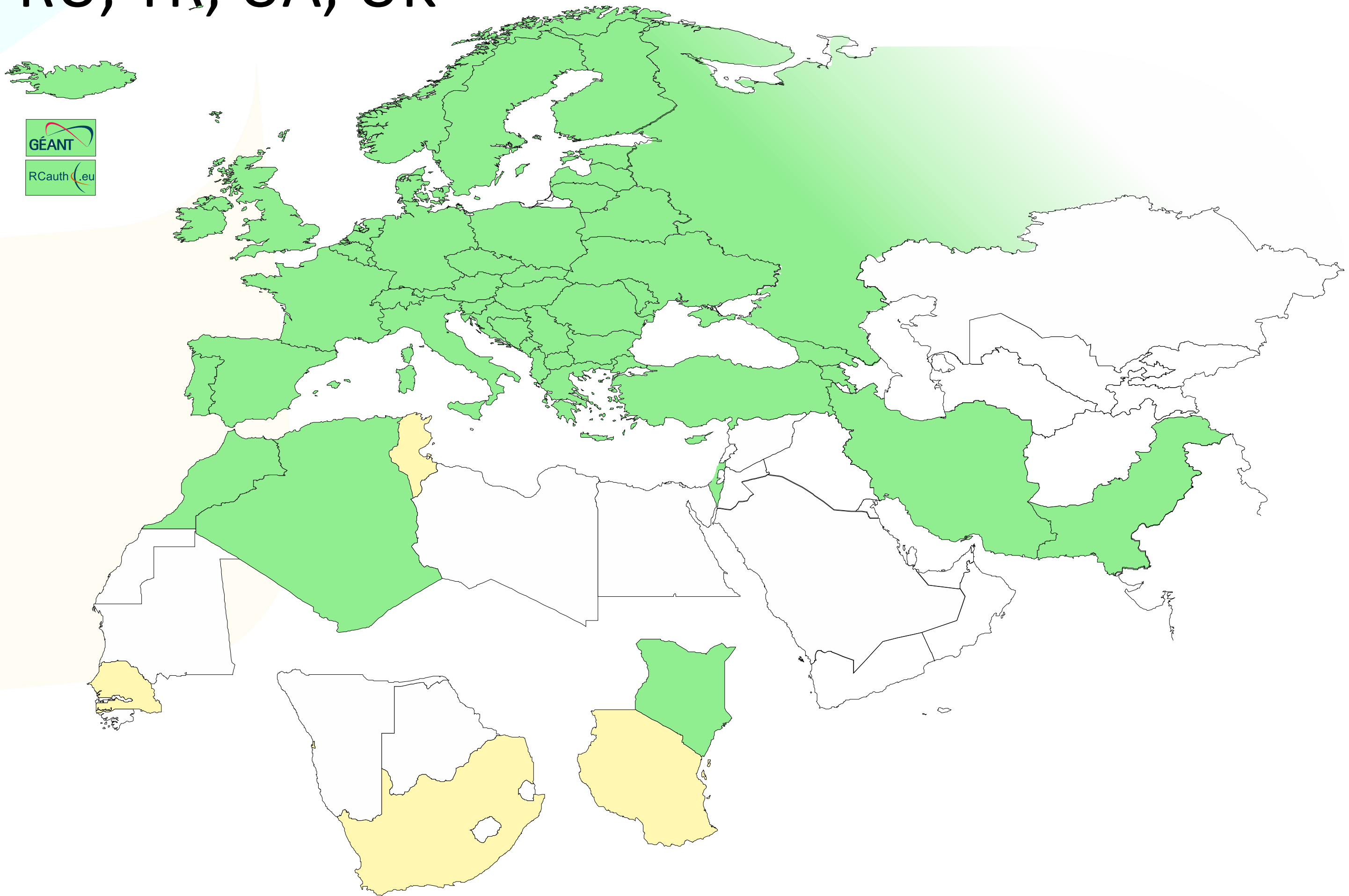
co-supported by Nikhef and the Dutch National e-Infrastructure coordinated by SURF

Meanwhile in Europe …

- EUGridPMA and IGTF distribution matters
  - constituency and developments
- Package signing and SHA confusion
- 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), 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*
  - Discontinued recently: -FR
  - CERN joined TCS also via Renater (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 …

Updates in 1.135

```
Changes from 1.134 to 1.135
---------------------------
(05 May 2025)

NOTE: the _default_ package signing key has changed to the 4th generation
      for increased security and compatibility. The new key is a 2048 bit
      RSA with fingerprint 565F4528EAD3F53727B5A2E9B055005676341F1A.
      The GPG public key file can be retrieved from
        https://dl.igtf.net/distribution/current/GPG-KEY-EUGridPMA-RPM-4
      and imported on rpm-based distributions with 'rpmkeys --import <file>'
      or on Debian (apt) based systems set in Signed-By in sources.list or
      added as a file in /etc/apt/trusted.gpg.d/
```

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
```

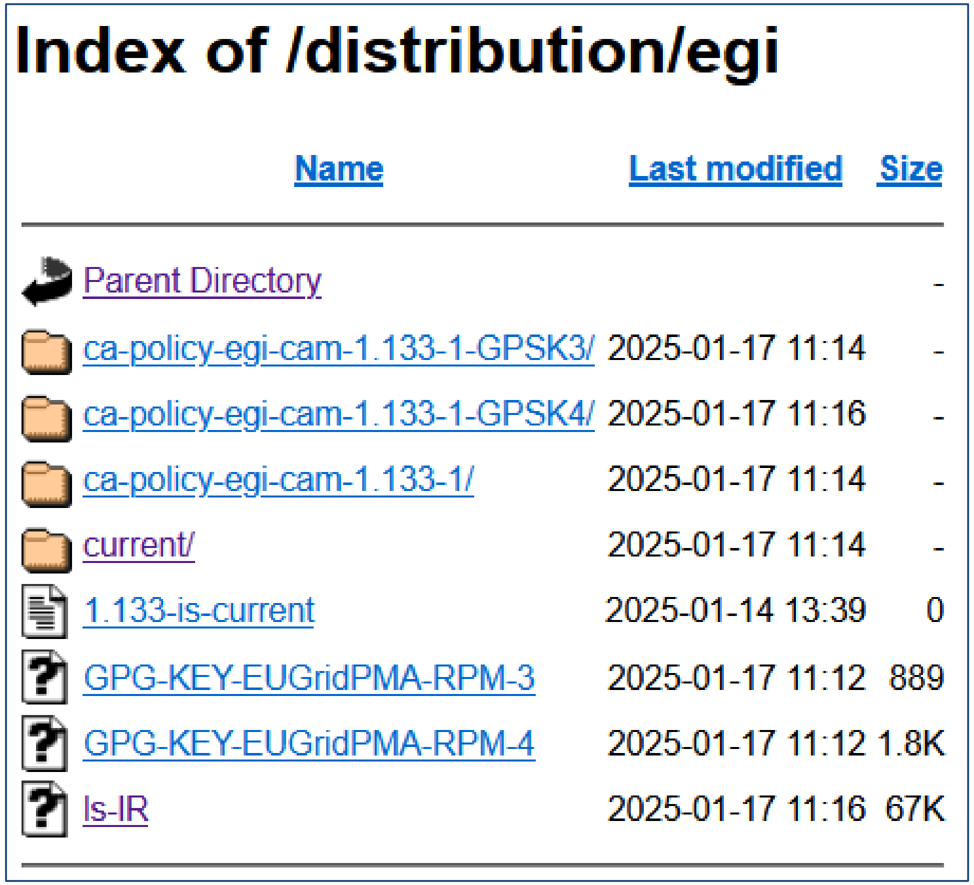
In Fedora Core 38+ (and thus later in its derivatives, and maybe soon in Debian), RSA 1024 package signing no longer supported by default

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

Distribution key update

In 1.135 we move the *default* 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**

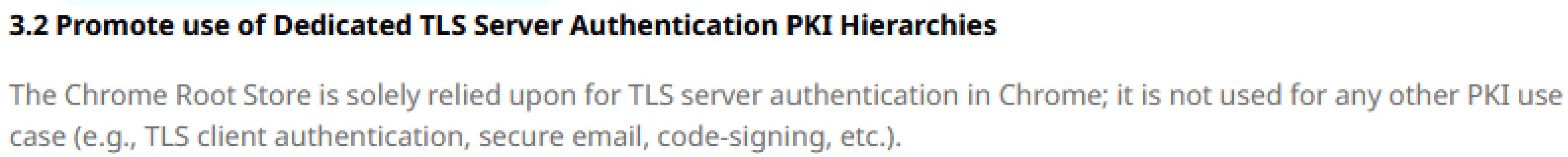


Index of /distribution/egi

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 things to keep in mind, beyond CABF …

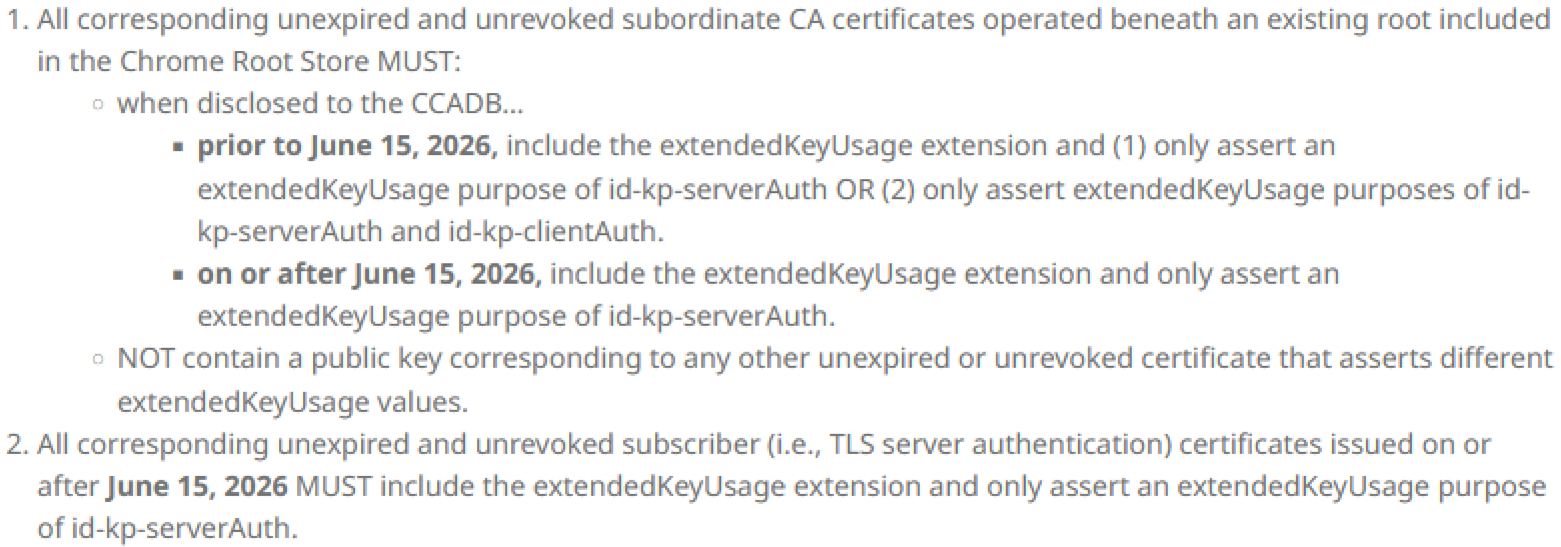
- The pubic end to abusing server certs for client auth? Yeah!
  - https://googlechrome.github.io/chromerootprogram/ section 3.2



3.2 Promote use of Dedicated TLS Server Authentication PKI Hierarchies

The Chrome Root Store is solely relied upon for TLS server authentication in Chrome; it is not used for any other PKI use case (e.g., TLS client authentication, secure email, code-signing, etc.).

  - and it is to be strictly true from early 2027 onwards:



1. All corresponding unexpired and unrevoked subordinate CA certificates operated beneath an existing root included in the Chrome Root Store MUST:
   - when disclosed to the CCADB…
     - **prior to June 15, 2026,** include the extendedKeyUsage extension and (1) only assert an extendedKeyUsage purpose of id-kp-serverAuth OR (2) only assert extendedKeyUsage purposes of id-kp-serverAuth and id-kp-clientAuth.
     - **on or after June 15, 2026,** include the extendedKeyUsage extension and only assert an extendedKeyUsage purpose of id-kp-serverAuth.
   - NOT contain a public key corresponding to any other unexpired or unrevoked certificate that asserts different extendedKeyUsage values.
2. All corresponding unexpired and unrevoked subscriber (i.e., TLS server authentication) certificates issued on or after **June 15, 2026** MUST include the extendedKeyUsage extension and only assert an extendedKeyUsage purpose of id-kp-serverAuth.

will this solve part of LE issue? almost seems triggered by the DCVOTA profile ☺

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

Reissuance of legacy 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

Nikhef

Maastricht University

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