Trusted Certificate Service

Separating SMIME and Authentication trust

David Groep

TCS Policy Management Authority

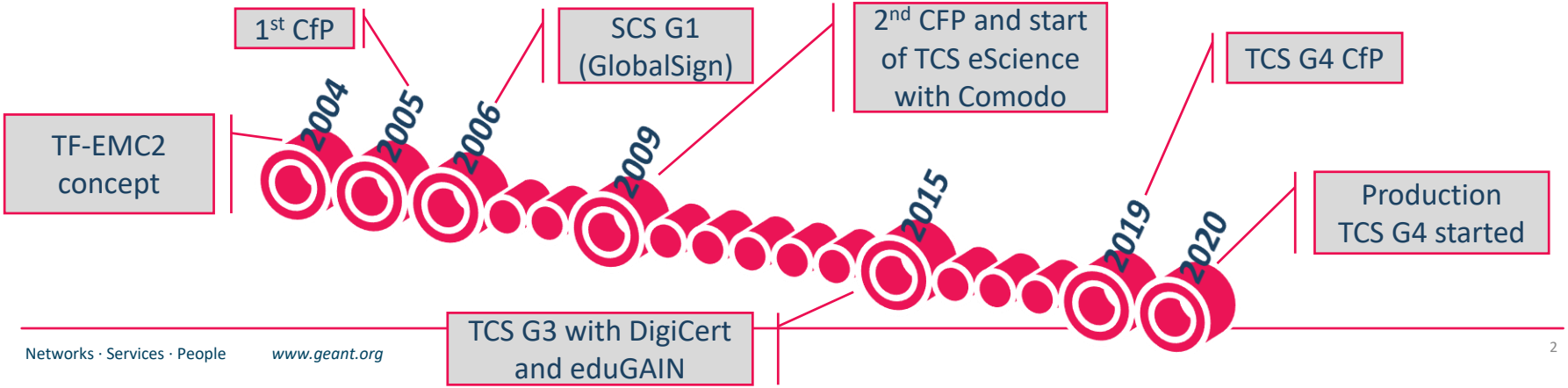
Nikhef PDP and Maastricht University

EUGridPMA58, Amsterdam

22 May 2023

Almost 20 years of TCS service!

- based on a concept by Jan Meijer back in 2004
- driven primarily by the NREN constituency, but with the eScience use cases very much in mind
- NREN (GEANT constituency) requirements on public trust, today esp. EV, but also eIDAS
- in a way that scales to 45 countries and ~100k active certificates today, increasing steadily
- and also ~10000 organisations, most of which cannot deal with certificates … or with much change
- now in its 4th iteration: GlobalSign, Comodo, DigiCert, … and with Sectigo again



TCS constituency

- service is ultimately driven by the GEANT members: 45 national R&E network organisations
- wide range of inputs: some countries adore Qualified Certificated and eIDAS, others don't care
- some countries really need a native-language interface (like .fr, .es, …),
  while others don't care (.nl, .se)
- stakeholders regard EV as mandatory, and many stakeholders pushed for ultimate stability – since the subscribers have actually no knowledge of PKI, nor of validation, and certainly not about chaining
- eScience use cases are important for many, although not the *only* driving factor in the game

TCS is a GEANT service – with the TCS PMA defining the profiles and policy

- TCS PMA drawn from the wider GEANT community (NRENs as well as individual orgs)

- Current PMA members … some of whom you will have seen
  - Kurt Bauer (ACONET, AT)
  - Kent Engström (SUNET, SE)
  - David Groep (Nikhef, NL)
  - Nicole Harris (GEANT)
  - Barbara Monticini (GARR),
  - Jürgen Brauckman (DFN),
  - Tim de Boer (SURF).

The basic structure remains the same … again!

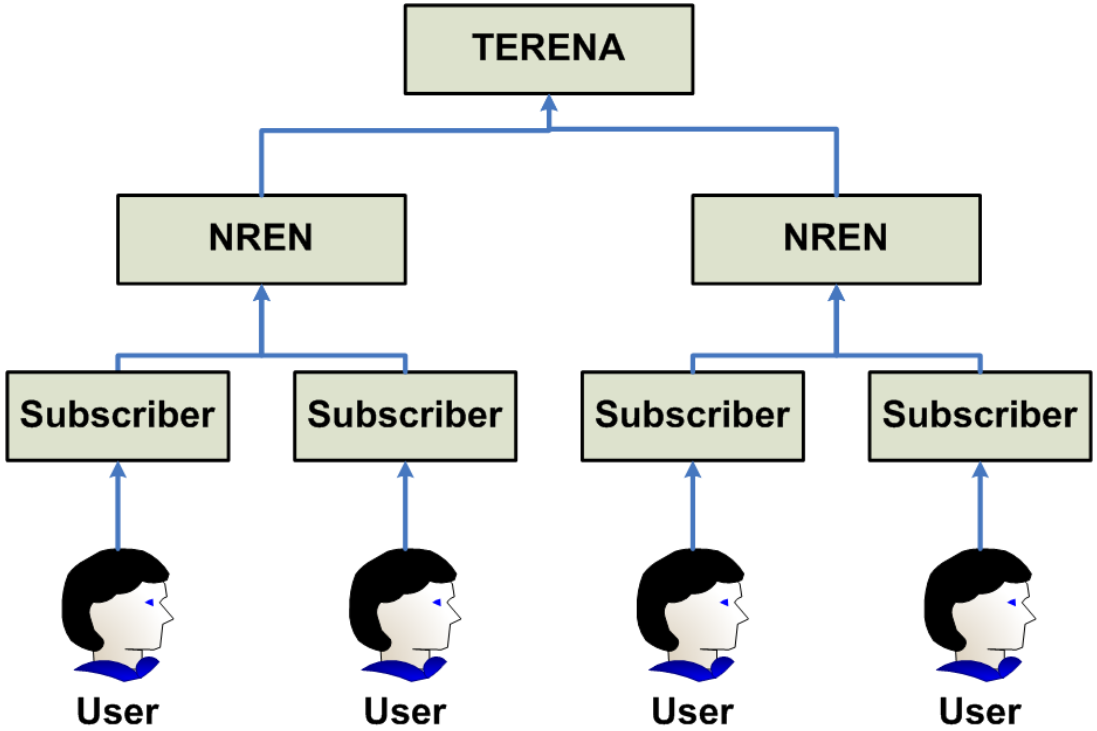
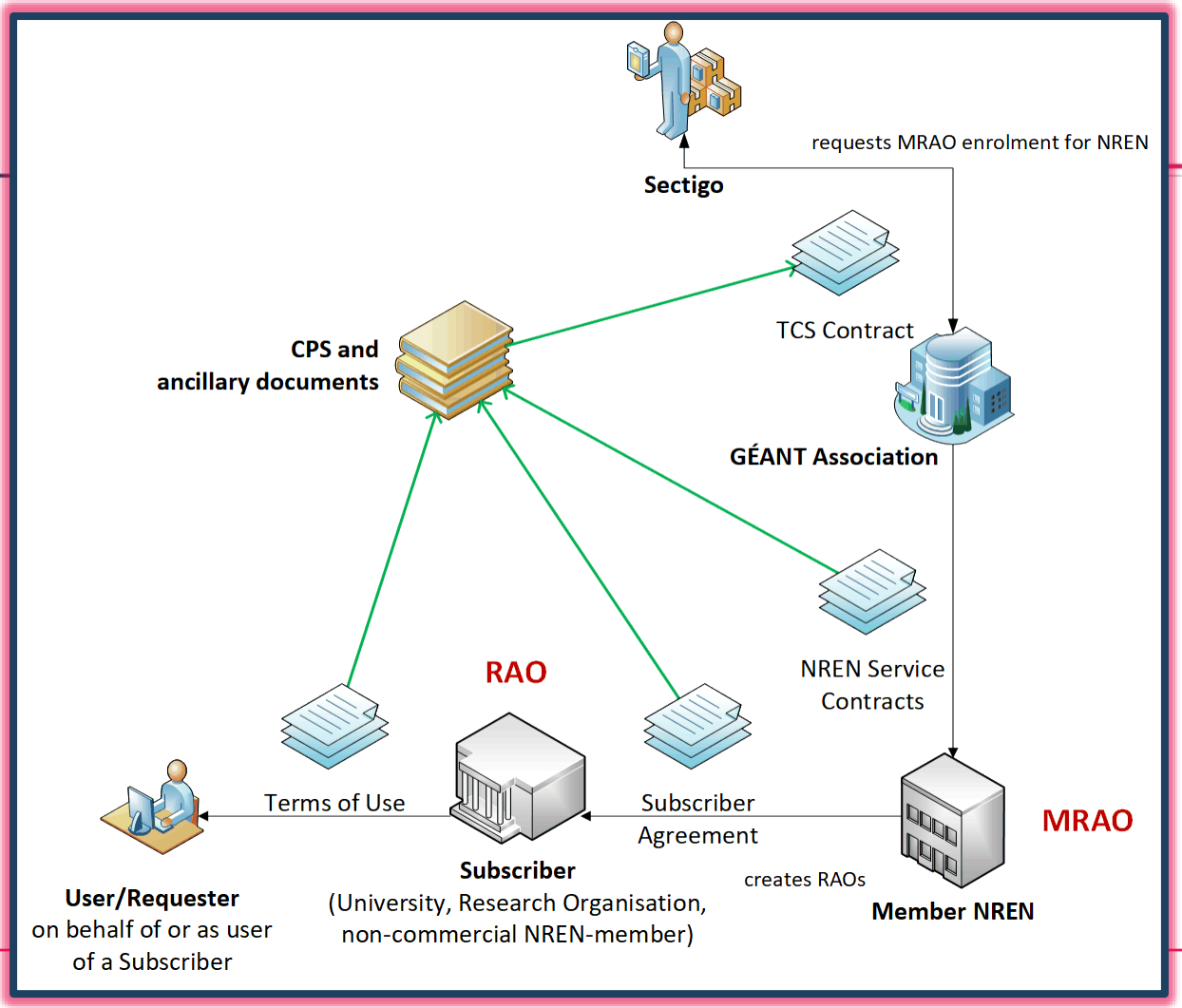


image source: Jan Meijer, 2008

TCS G4


requests MRAO enrolment for NREN
Sectigo
TCS Contract
CPS and
ancillary documents
GÉANT Association
NREN Service
Contracts
RAO
Terms of Use
Subscriber
Agreement
MRAO
creates RAOs
Member NREN
Subscriber
(University, Research Organisation,
non-commercial NREN-member)
User/Requester
on behalf of or as user
of a Subscriber

Assurance levels

Joint Public & IGTF trust: certs all meet CABF OV requirements, exceeding 'IGTF Classic' a bit

- OV validation requires DCV, which is stronger than the RA checks minimally required
- the IGTF+public trust combination is getting more important for S3/cloud like deployments

User and personal robot certs

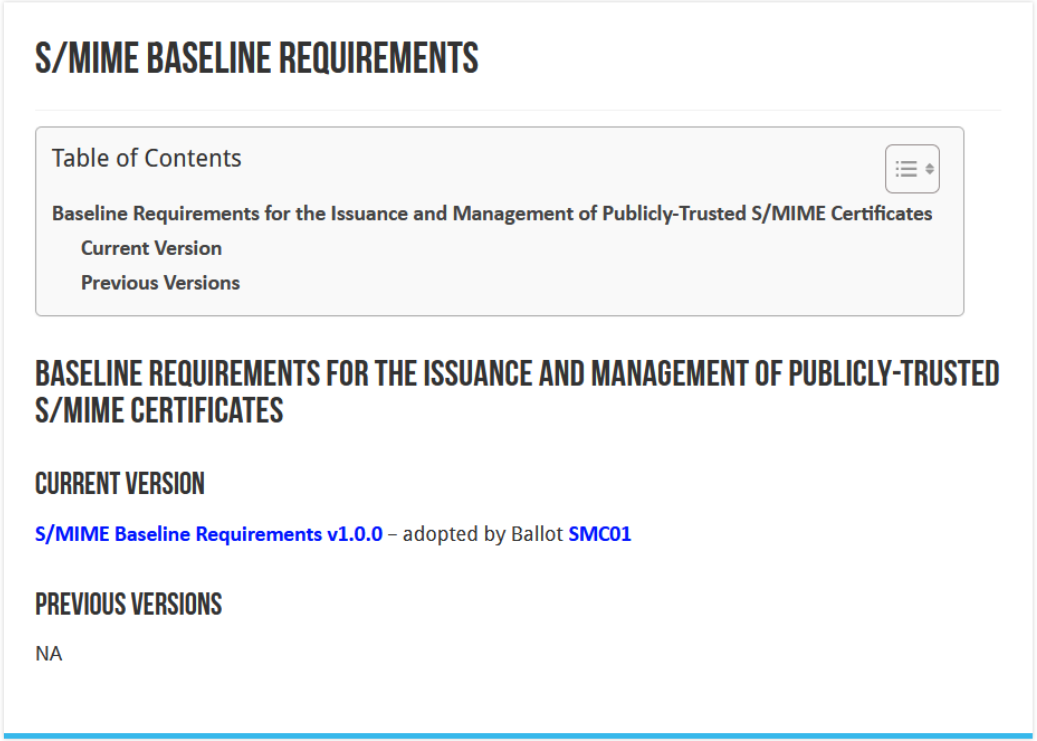
- SAML process, and the eligibility checking by the subscribers (organisations), remains the same *urn:mace:terena.org:tcs:personal-user* in attribute *eduPersonEntitlement*
- real name of the person – by the subscriber agreement and CP/CPS this goes beyond R&S assurance
- manual side-process may remain just like today, based on data entry by the 'RAO/DRAO' in SCM as per https://wiki.geant.org/display/TCSNT/Documentation 'non-SAML issuance model process'
- the CP/CPS requirements though the Subscriber Agreement meet IGTF BIRCH

Audited already for CABF/WebTrust compliance (SSL certs) and similarly for the 'S/MIME' use cases

Certificate profiles today

OV TLS Server (MD)	BR OV validated multi-domain with mixed SANs
EV TLS Server (MD)	BR EV validated multi-domain with mixed SANs
Personal webClientAuth and S/MIME	End-user personal certificate recognised by the major MUAs suitable for identifying the users real name
Personal webClientAuth IGTF and S/MIME	End-user personal certificate adhering to IGTF profile (using IA5String representation of the name with unique prefix /DC=org/DC=terena/DC=tcs/...), suitable both for authentication, and also including validated name and email address
Personal Robot webClientAuth IGTF and S/MIME	End-user personal software agent certificate adhering to IGTF profile (like above) and Robot Profile, suitable both for authentication, and also including validated name and email address
Robot Email webClientAuth IGTF and S/MIME	E-mail validated software agent certificate adhering to IGTF profile (like above) and Robot Profile, suitable both for authentication, and also including validated email address
IGTF OV TLS Server (MD)	BR OV validated multi-domain with mixed SANs including unique prefix "/DC=org/DC=terena/DC=tcs/..."
Document Signing	Adobe AATL compliant signing certificate
Code Signing	Conventional code signing certificate recognised by Oracle, MSFT, &c
EV Code Signing	BR EV Code Signing certificate recognised by MSFT &c

CA/BF now started considering S/MIME trust as well!



S/MIME BASELINE REQUIREMENTS

Table of Contents

BASELINE REQUIREMENTS FOR THE ISSUANCE AND MANAGEMENT OF PUBLICLY-TRUSTED S/MIME CERTIFICATES

CURRENT VERSION

S/MIME Baseline Requirements v1.0.0 – adopted by Ballot **SMC01**

PREVIOUS VERSIONS

NA

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
```

Public Trust S/MIME (personal) is getting regulated

- It was basically a ‘free-for-all’, as long as the email address worked
- most ‘useful use’ for the general public signing was in bespoke certificates types (Adobe) or in Qualified Certificates (EC regulated)
- until now, the IGTF personal requirements were much stricter than ‘public’ email signing, in that we did insist on a reasonable name and a ‘sponsor’ (organization) that was validated

shortest summary: IGTF (BIRCH) assurance level remains >= SMIME BR

https://cabforum.org/wp-content/uploads/CA-Browser-Forum-SMIMEBR-1.0.0.pdf

CABF SMIME BR: different ‘profiles’ and validations

- **Strict**
  - 825-days (2yr), limited RDN attributes allowed
  - intended only for S/MIME
- **Multi-purpose**
  - 825 days (2yr), slightly more eKUs allowed
  - crossover use cases between document signing and secure erossover use cases between document signing and secure emailmail
- **Legacy**
  - 1185 days (3yr)
  - transitional profile (likely to be phased out

- **mailbox-validated**
  - just the rfc822name (only!)
- **organization-validated**
  - includes only Organizational (Legal Entity) attributes in the Subject
- **sponsor-validated**
  - Combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attribute
- **individual-validated**
  - Includes only Individual (Natural Person) attributes in the Subject

Sponsor validated

Sponsor-validated:

'Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the subject:organizationName is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.'

Certificate Type	Description
Mailbox-validated	Subject is limited to (optional) `subject:emailAddress` and/or `subject:serialNumber` attributes.
Organization-validated	Includes only Organizational (Legal Entity) attributes in the Subject.
Sponsor-validated	Combines Individual (Natural Person) attributes in conjunction with an `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA.

Validation requirements

1. If the Certificate Request is for an `Organization-validated` or `Sponsor-validated` profile, the CA SHALL confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1 or Section 3.2.2.3. The CA SHALL confirm that the `subject:organizationName` name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are Affiliated as defined in Section 3.2 or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested email domain falls within the subdomains of ABC Co.'s Registered Domain Name.

commonName

7.1.4.2.2 Subject distinguished name fields

a. **Certificate Field:** `subject:commonName` (OID 2.5.4.3)
Contents: If present, this attribute SHALL contain one of the following values verified in accordance with Section 3.2.

Certificate Type	Contents
`Mailbox-validated`	Mailbox Address
`Organization-validated`	`subject:organizationName` or Mailbox Address
`Sponsor-validated`	Personal Name, `subject:pseudonym`, or Mailbox Address
`Individual-validated`	Personal Name, `subject:pseudonym`, or Mailbox Address

If present, the Personal Name SHALL contain a name of the Subject. The Personal Name SHOULD be presented as `subject:givenName` and/or `subject:surname`. The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but SHALL be a meaningful representation of the Subject's name as verified under Section 3.2.4.

Where does that leave us?

- The ‘Legacy’ profile (still) allowed ‘other’ attributes, so for the moment e.g. DC prefixing would be OK

- **However** the *commonName* is regulated, which
  - impacts uniqueness identifiers (does not allow ePPN in CN as used in TCS)
  - does not allow for ‘`Robot -`’s in the commonName
    these would go to Pseudonym, which is an ill-supported attribute, and anyway inflicts a subjectDN change

- who knows when the legacy profile will be deprecated! Will not be long ☹

However …

… contrary to the host-cert issue, there is

no joint-trust needed for email signing and client authentication!

- separating these chould always have been done:
  using TCS Personal certs for authentication is bad (since they are not unique), and
  using TCS IGTF MICS client certs for S/MIME email is bad (since it's 7-bit ASCII only)
- this just formalizes that move beyond restricting keyUsage & eKU

User awareness

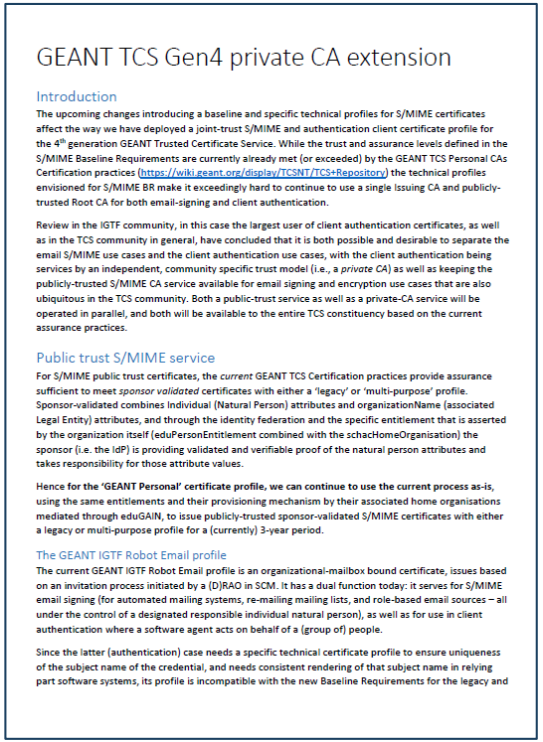
- This is a change in communications and documentation as well, not only a set of technical changes
- In request systems, have to clearly distinguish for users *which product to order*. For example:
  - “Personal” == only for EMAIL and NOT for authentication
  - renaming “IGTF MICS Personal” to “Personal Authentication” and explain
  - renaming “IGTF MICS Robot Personal” to “Personal Automated Authentication”?
  - forking “IGTF Classic Robot Email”
    - Authentication-only (IGTF) profile “Classic Robot Email”
    - Email signing profile “Organisation-validated S/MIME signing” (i.e. team-based or role-based)

The actual proposed changes described

- The “Personal” profile currently used in TCS is UTF-8, and is excellent for email
- Since we want ‘email’ to be served well, this profile may evolve as per the SMIME BR requirements
  not doing so would void the public trust and render these unusable!

- The “IGTF” variants will need to change: new hierarchy, new issuer, same subject DN format, same extensions, ASCII-only, unique naming

See https://www.nikhef.nl/~davidg/tcsg4/TCS-Personal-CPS-2.2/



GEANT TCS Gen4 private CA extension

Introduction

The upcoming changes introducing a baseline and specific technical profiles for S/MIME certificates affect the way we have deployed a joint-trust S/MIME and authentication client certificate profile for the 4th generation GEANT Trusted Certificate Service. While the trust and assurance levels defined in the S/MIME Baseline Requirements are currently already met (or exceeded) by the GEANT TCS Personal CAs Certification practices (https://wiki.geant.org/display/TCSNT/TCS+Repository) the technical profiles envisioned for S/MIME BR make it exceedingly hard to continue to use a single Issuing CA and publicly-trusted Root CA for both email-signing and client authentication.

Review in the IGTF community, in this case the largest user of client authentication certificates, as well as in the TCS community in general, have concluded that it is both possible and desirable to separate the email S/MIME use cases and the client authentication use cases, with the client authentication being services by an independent, community specific trust model (i.e., a *private* CA) as well as keeping the publicly-trusted S/MIME CA service available for email signing and encryption use cases that are also ubiquitous in the TCS community. Both a public-trust service as well as a private-CA service will be operated in parallel, and both will be available to the entire TCS constituency based on the current assurance practices.

Public trust S/MIME service

For S/MIME public trust certificates, the *current* GEANT TCS Certification practices provide assurance sufficient to meet *sponsor validated* certificates with either a ‘legacy’ or ‘multi-purpose’ profile. Sponsor-validated combines Individual (Natural Person) attributes and organizationName (associated Legal Entity) attributes, and through the identity federation and the specific entitlement that is asserted by the organization itself (eduPersonEntitlement combined with the schacHomeOrganisation) the sponsor (i.e. the IdP) is providing validated and verifiable proof of the natural person attributes and takes responsibility for those attribute values.

Hence **for the ‘GEANT Personal’ certificate profile, we can continue to use the current process as-is**, using the same entitlements and their provisioning mechanism by their associated home organisations mediated through eduGAIN, to issue publicly-trusted sponsor-validated S/MIME certificates with either a legacy or multi-purpose profile for a (currently) 3-year period.

The GEANT IGTF Robot Email profile

The current GEANT IGTF Robot Email profile is an organizational-mailbox bound certificate, issues based on an invitation process initiated by a (D)RAO in SCM. It has a dual function today: it serves for S/MIME email signing (for automated mailing systems, re-mailing mailing lists, and role-based email sources – all under the control of a designated responsible individual natural person), as well as for use in client authentication where a software agent acts on behalf of a (group of) people.

Since the latter (authentication) case needs a specific technical certificate profile to ensure uniqueness of the subject name of the credential, and needs consistent rendering of that subject name in relying part software systems, its profile is incompatible with the new Baseline Requirements for the legacy and

Short TCS migration proposal

- Have the S/MIME personal certs move to sponsor-validated (multi-purpose) **BR-compliant certificates** off a public trust CA
- Move the client authentication trust to a **'private CA' (non-public trust anchor),** retaining exactly the same subject DNs, just a different ICA issuerDN
- Add some additional ICAs and non-public Roots to the IGTF distribution – for IGTF RPs the change is minimal and transparent
- Inform relying parties, also outside of the IGTF, that client trust will become a specific decision. This is probably good, also for OpenVPN services, web access (.htpasswd), &c. The IGTF RPs are not impacted, others likely will be.

On robots and email

Current GEANT IGTF Robot Email profile: **organizational-mailbox bound** certificate, issued based on an invitation process initiated by a (D)RAO in SCM

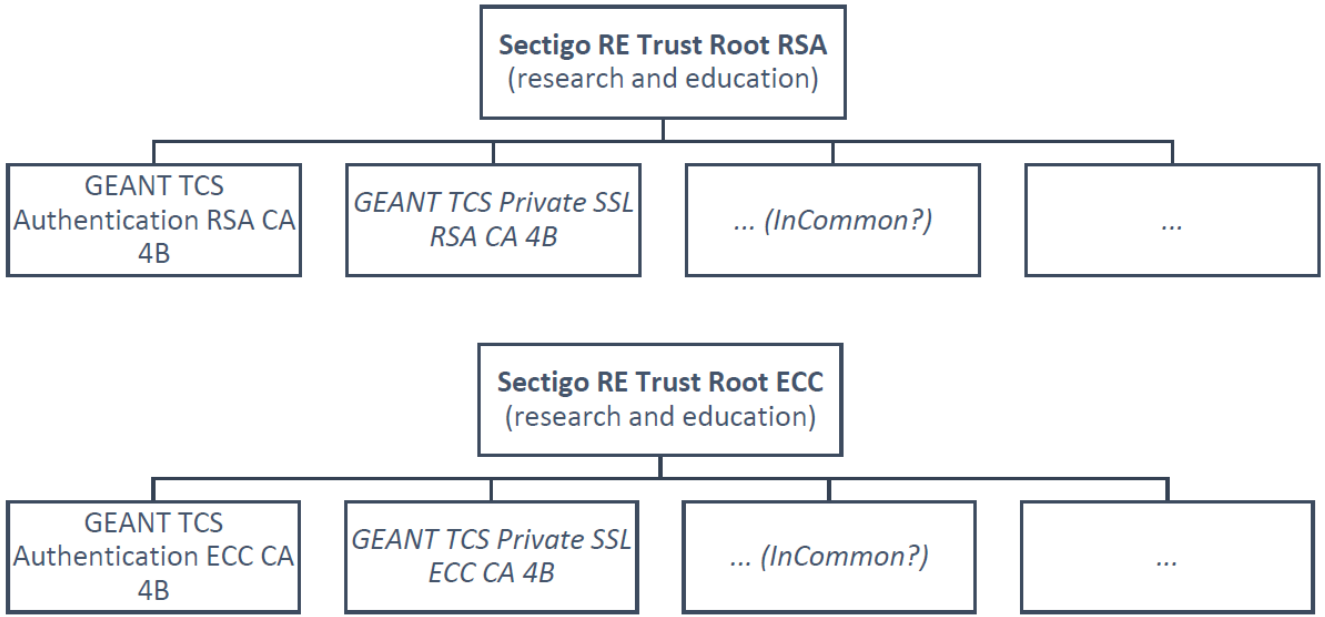
Currently a *dual function*:

- S/MIME email signing
  automated mailing systems, re-mailing mailing lists, and role-based email sources – all under the control of a designated responsible individual natural person,
- client authentication
  where a software agent acts on behalf of a (group of) people

Thus the GEANT IGTF Robot Email must be **split in two new products**:
(1) a publicly-trusted organizational S/MIME certificate and
(2) a client-authentication certificate that can use a private trust model

What we end up with: a new hierarchy

We propose the following **two hierarchies, one for RSA and once for ECC**:



Base technical specifications for the Root

- The Sectigo RE Trust Roots can have any name that is appropriate for a Sectigo-wide private CA root, although a reflection of the constituency name (‘research and education’, or IGTF) is helpful in identifying the root as a community private trust root. The RSA and ECC variants should have similar, but not identical, subject names.
- There should be two Sectigo RE Trust Roots, one using a RSA keys (>=4096 bit, SHA-384 or stronger), and one ECC (P-384 with SHA-384 or stronger)
- The Sectigo RE Trust Roots shall be self-signed
- Shall be valid till at least May 1, 2033 GMT, but MAY be valid until Jan 18 23:59:59 2038 GMT
- It shall be able to issue CRLs for the (subordinate CA) certificates it issues, and the CRL shall have a validity period of at most 400 days (nextUpdate set to no more than 400 days after issuance, and no shorter than 7 days after issuance).
- It shall have OCSP support, and use a globally distributed (reasonably low latency) CDN for responding to OCSP queries

Two GEANT TCS Authentication RSA/ECC CA 4B subordinate CAs

- Two GEANT TCS Authentication CAs, one using an RSA keypair (>=4096 bits, using SHA-384 or stronger) and subordinate to the RSA root, and one with an ECC key (P-384 with SHA-384 or stronger) and subordinate to the ECC root defined above.
- Shall be signed by the corresponding Sectigo RE Trust Root (RSA or ECC)
- Shall be valid until at least May 1, 2033 GMT, MAY be valid until Jan 18, 2038 GMT
- Subject name (in RFC2253 format) shall be
  for RSA: CN=GEANT TCS Authentication RSA CA 4B,O=GEANT Vereniging,C=NL
  for ECC: CN=GEANT TCS Authentication ECC CA 4B,O=GEANT Vereniging,C=NL

All things ASCII …

- The subject distinguished name for end-entity certificates shall be *exactly the same* as the one generated today based on the *ascii-fied* organsiation name (secondary validation) and ascii-fied state or locality name.
- It shall be possible to specify printable 7-bit stings for the Organization field of the subject name during organization enrolment. This name must be validated according to usual standards (CABF OV BR), taking into account that organization names have a printable 7-bit representation that is in line with acceptable national practice and aligned with CABF OV BR guidance.
- In case of inconsistencies, the MRAO responsible for the subscriber organization will indicate the acceptable 7-bit printable representation of organization name.

Our request: approve the new hierarchy and CPS v2.2

- We have circulated the new CP/CPS two weeks ago to the dg-eur-ca list
- We want Sectigo to implement the new CAs before the end of June
- Distribution by early July to the IGTF RPs
- Field-testing in July and August
- Be in time for the subset of non-SMIME-BR-compliant client certificates …

Thank you

davidg@nikhef.nl

GÉANT

Networks · Services · People

www.geant.org