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 multi-purpose profiles. This function needs to be ‘split-off’ from the S/MIME use case described above, for which public trust by email clients is essential, but global name uniqueness and specific structure of the subject name is not.

Thus, **the GEANT IGTF Robot Email needs to be functionally 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 (as described below).

The new IGTF private trust profiles

For client authentication in a global federated ecosystem with a mixed installed software base, the emphasis must be on global uniqueness (key to consistent authentication on the relying-party side) and compatibility with common software solutions (e.g. those based on Apache httpd as well as multiple Java JCEs and BouncyCastle). The consistent representation of subject names in those systems unfortunately needs the subject name to be using the lowest common denominator of the name representation, which is the printable subset of the 7-bit ASCII character set. To ensure global name uniqueness (and thus prevent authentication name collisions) and minimize re-naming confusion in the installed global service ecosystem, it is necessary to ensure the current naming is retained going forward and remains unique through RPDNC-compatible namespacing (GFD.189, GFD.225).

It is not incompatible with the use cases that the **client authentication certificates are issued by a *private CA***. The trust evaluation of these client certificates takes place in relying party (RP) systems that are configured, or can be so configured using currently available software, that additional private trust anchors can be added to the trust stored of RP software and can then be recognized by the services when users authenticate. This is a standard industry design pattern fully supported by software today. One can conceivably state that having a private trust chain for client authentication on the RP (service) side is a conceptual security improvement, since the choice of trust becomes an explicit decision.
In practice, all IGTF relying parties are well accustomed to making such decisions and all major infrastructures have mechanisms in place for managing the configuration of community-specific private CAs for end-user authentication. Where individual relying parties do not (yet) have this in place, configuring explicit trust anchors is a straightforward process (provided the new trust chains are stable over longer periods of time).

The profiles currently used for client authentication and compatible with these requirements are

- GEANT IGTF MICS Personal (via /clientgeant)
- GEANT IGTF MICS Personal Robot (via /clientgeant)
- GEANT IGTF MICS Robot Email (via SCM invites)

Without any changes to the subject name structure and content, the certificates provided via **the first two end-points can be issued from a new private CA hierarchy** (details specified below) once the new private CA hierarchy has been distributed to all relying parties.

The third product, **MICS Robot Email, must be split** in a public S/MIME profile (as discussed previously, possibly with a new name structure) and a **new Robot Email authentication profile** (using the exact same subject name structure as used now).

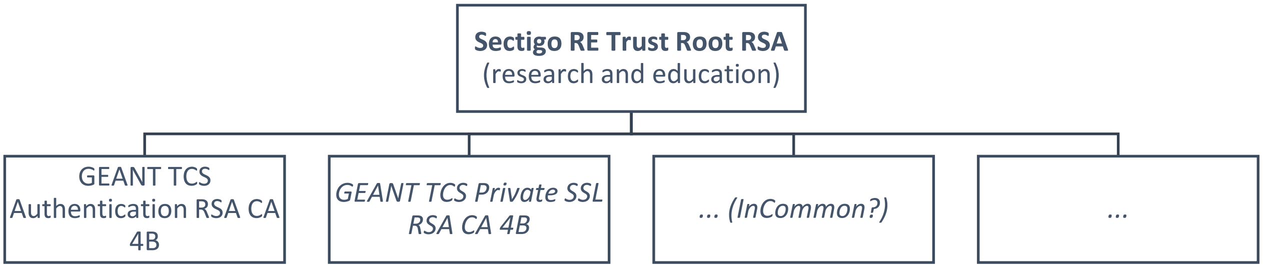
Private CA hierarchy

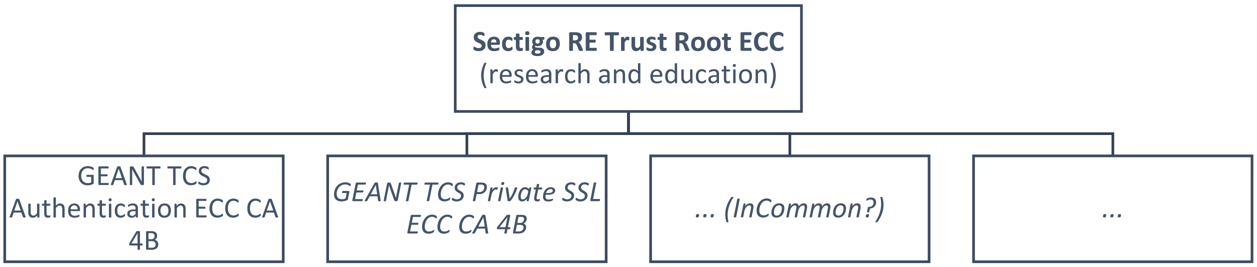
We propose that the new private trust model uses a **root-and-subordinates model**, where the private root may (at the discretion of the provider) be shared by multiple issuing CAs they operate for the IGTF community for different customers (e.g. for both GEANT and InCommon) – but this is not mandatory or a requirement. Having the option for multiple subordinates allows re-use of the same trust anchor for the TCS and IGTF constituency also in case specific server certificate profiles are needed on an ad-hoc bases (e.g. in case transient printablestring mapping issues would otherwise stall any kind of certification issuance in some regions).

> *At this time, we anticipate that the string rendering and validation issues in the OV-validated eScience Server SSL profile for countries where the state or province name includes non-ascii characters will be resolved in a timely fashion. If such cannot be achieved, an interim solution might be needed where – purely as an emergency measure – non-public-trust server based certificates could be issued under the private CA hierarchy, if such would alleviate problems in the validation processing chain for CABF BR OV compliant eScience Server SSL certificates. This would entail adding a second (RSA+ECC) subordinate to the private Root described below, including additional specifics on the asciification of the 'ST' subject RDN attribute, which would be part such a server SSL subject name, but it not a part of the 'GEANT TCS Authentication' certificate subject name used in the profiles described here.*

The Root may have a longer validity period than any of its subordinates, and can therefore also 'outlive' any specific contract between Sectigo and the GEANT TCS (or InCommon) community – the validity period thereof can be controlled either through the issuing subordinates or by certificate service portal accessibility.

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


Sectigo RE Trust Root RSA
(research and education)
GEANT TCS Authentication RSA CA 4B
GEANT TCS Private SSL RSA CA 4B
... (InCommon?)
...


Sectigo RE Trust Root ECC
(research and education)
GEANT TCS Authentication ECC CA 4B
GEANT TCS Private SSL ECC CA 4B
... (InCommon?)
...

With the following **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
- It shall be valid till at least May 1 23:59:59 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

For **both (two) GEANT TCS Authentication RSA/ECC CA 4B issuing subordinate CA**:

- There shall be 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.
- It shall be signed by the corresponding Sectigo RE Trust Root (RSA or ECC)
- It shall be valid until at least May 1 23:59:59 2033 GMT, and MAY be valid until Jan 18 23:59:59 2038 GMT
- Its 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
- It shall have an authorityKeyIdentifier containing a keyID (only)
- It shall have a subjectKeyIdentifier containing a keyID (only)
- It shall have X509v3 Key Usage: critical set to Digital Signature, Certificate Sign, CRL Sign
- It shall have X509v3 Basic Constraints: critical set to CA:TRUE, pathlen:0
- It shall have X509v3 Extended Key Usage set to TLS Web Client Authentication, E-mail Protection
- It may have X509v3 Certificate Policies set to an appropriate value
- It shall have X509v3 CRL Distribution Points set to the CDP for the corresponding Root specified above
- It shall have Authority Information Access set to include a URL for the OCSP reponses
- It shall be able to issue CRLs for the certificates it issues, and the CRL shall have a validity period of at most 7 days (nextUpdate set to no more than 7 days after issuance, and no shorter than 48 hours after issuance).
- It shall have OCSP support, and use a globally distributed (reasonably low latency) CDN for responding to OCSP queries

For the end-entity certificates issued by the GEANT TCS Authentication RSA/ECC CA 4B:

- The subject distinguished name 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
- The subject name shall hence be prefixed (in the ASN.1 DER SEQUENCE) with "DC=org", "DC=terena","DC=tcs", followed by country ISO code and organization name, and then followed by the commonName that must include (like today) the common or displayname of the applicant and the applicant uniqueness-identifier (eduPersonPrincipalName) ("/DC=org/DC=terena/DC=tcs/C=NL/O=Nikhef/CN=David Groep davidg@nikhef.nl")
- Personal and Email Robots will follow the current naming scheme as well
- Validation of organization name shall be done in the same way as for all OV validation public trust (CABF BR OV) validations, including the DCV validation of domain association with the organization (for matching the 'academic code', i.e. the *schacHomeOrganization* attribute)
- It shall be possible to specify printable 7-bit stings for the Organization field of the subject name during organization enrolment, and have this 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.
- The certificate extensions shall be almost the same as today, with the one exception being the policy OIDs for the TCS Personal CA Practice Statement which will be changes to reflect the modification described in this paper:
  Policy: 1.2.840.113612.5.2.2.5
  Policy: 1.2.840.113612.5.2.3.3.3
  Policy: 1.2.840.113612.5.2.3.1.2
  Policy: 1.3.6.1.4.1.25178.2.3.2.2
- Validity period shall be 395 days (as today)
- The issuing CA shall provide an OCSP responder for end-entity certificate status and a CRL (as per above)
- It shall be possible for RAOs and MRAOSs to revoke end-entity certificates issued by the private issuing CAs.

Subject distinguished names and 7-bit (ascii) representations

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.

Deployment timeline considerations

For the new private trust root and issuing subordinates to be useful, these have to be distributed to the relying party community ad service operators should have sufficient time to configure their systems to use the new private trust roots for authentication validation. Before broad community deployment, these may also need to be tested in a controlled environment. Therefore, we propose that there is a **period of at least two (2) months** between the new private trust anchors having been validated, and their use in the SCM and '/clientgeant' issuing services.

For validation purposes, it should be possible to have end-entity client certiicates issues using the new trust chain prior to announcing the service to the whole TCS constituency. During this period either a (dedicated) '/clientgeant' end point or a specific SCM invite process may be used, as long a **consistent profile** is used to issue these new certificates (i.e. the profile must not be different between SCM and '/clientgeant').

UX changes

In all request systems, but especially in the '/clientgeant' portant, clearly distinguish which product provides which capabilities, in a way that is clear for end-users using the portal. The /cientgeant portal will thus offer:

- The 'new style' publicly-trusted S/MIME sponsor-validated certificates
  "GEANT Email signing and encryption certificate"
  "This certificate is for signing email messages and receiving encrypted email messages sent to you. It cannot be used for signing documents, and should not be used to authenticate to systems. You should install these certificates in your email client and/or operating system, but should not use these from your web browser."
- The private-trust authentication personal certificate
  "Personal Authentication certificate"
  "Certificate to prove your identity to web services and infrastructures where you need to authenticate to gain access, or where you authenticate to prove membership of a community."
- The private-trust authentication robot certificate
  "Personal Automated Authentication"
  "Certificate you use to have software agents authenticate and act on your behalf in an automated way. These cannot be used to sign email messages (please use an organizational [or mailbox-validated] S/MIME certificate for email signing"

For the new (split) Robot certificate, the split purpose must be clarified. This one currently only be requested through SCM by *RAOs, so the UX experience is slightly less (but not unimportant). The two Robot Email profiles should be clearly distinguished in SCM.