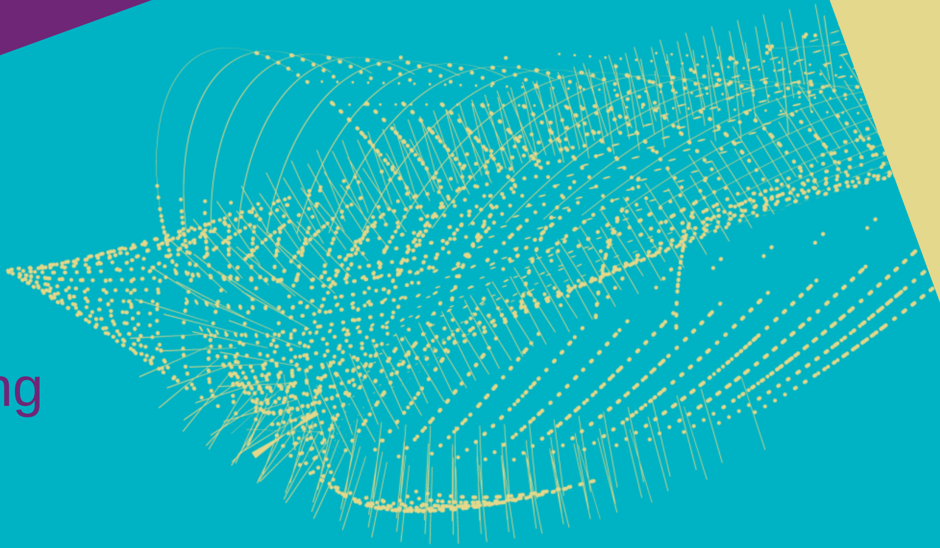


May 2020 EUGridPMA meeting

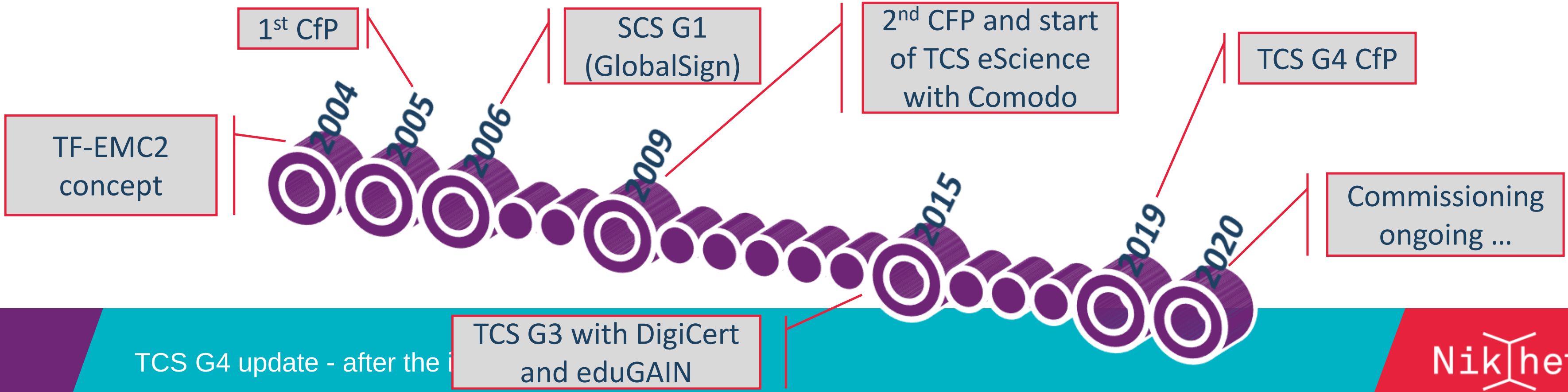
TCS Gen 4

the good, the ^H^H^H, and …

David Groep
Nikhef

15 years of TCS …

- 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 going to its 4th iteration: GlobalSign, Comodo, DigiCert, … and now Sectigo again



TF-EMC2 concept

1st CfP

SCS G1 (GlobalSign)

2nd CFP and start of TCS eScience with Comodo

TCS G3 with DigiCert and eduGAIN

TCS G4 CfP

Commissioning ongoing …

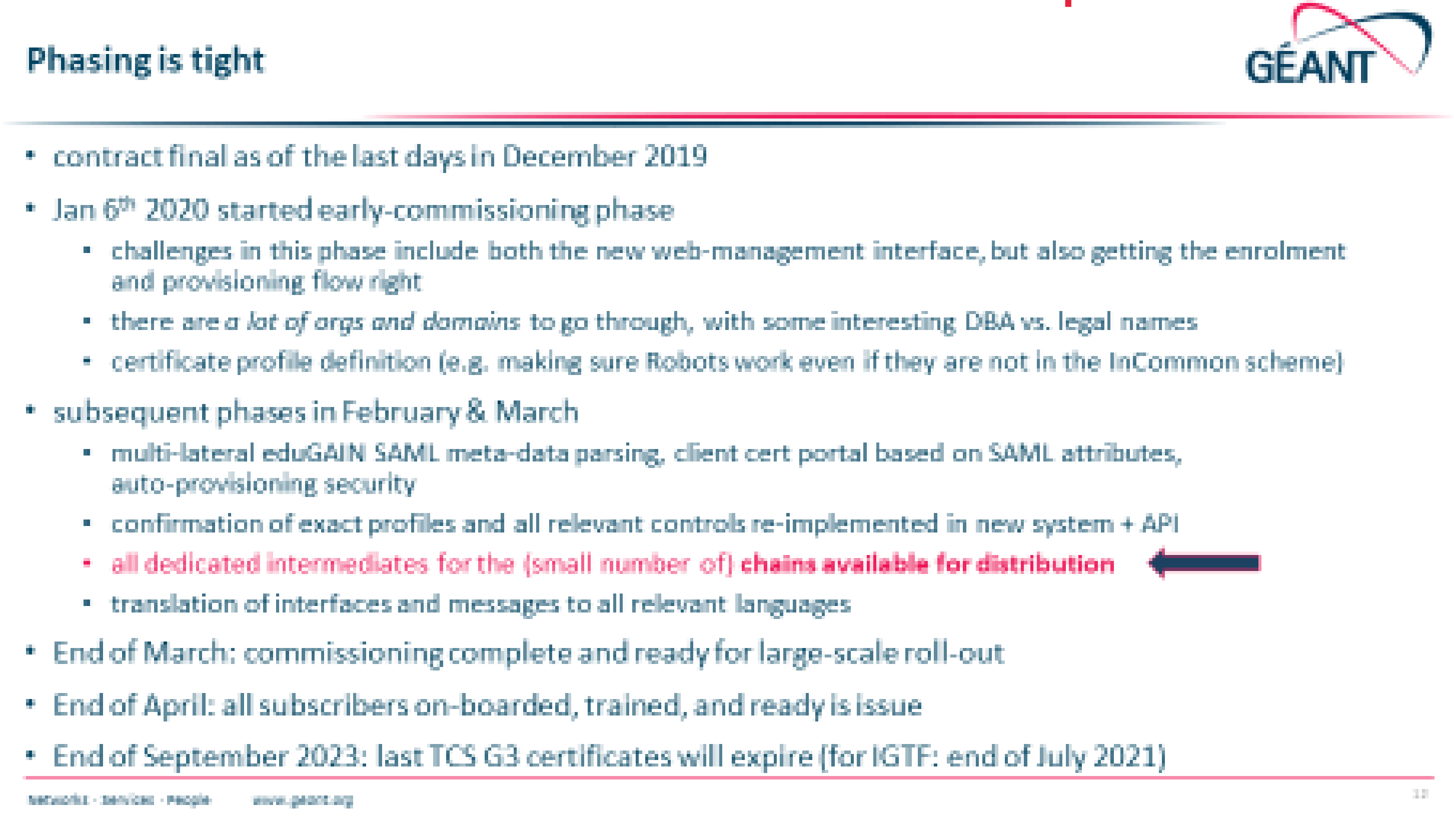
Main IGTF relevant items

- validation for server certs and model for personal/robot **remains the same**
- **adherence to TCS CP/CPS** the same (and augments the provider CP/CPS)
- so now on top of Sectigo's CP/CPS https://sectigo.com/uploads/files/Sectigo-CPS-v5.1.5.pdf

- **it is a new hierarchy** (when installed correctly, ends in self-signed USERTrust CA
- **keeps the current prefix** /DC=org/DC=terena/DC=tcs/…
- **issuer names changed as needed,** and since these show visibly in the UX

- **distributed** the new RSA Root and intermediates in 1.104 release (early April)

Where is the TCSG4 now … ? the plan was:



Phasing is tight

- contract final as of the last days in December 2019
- Jan 6th 2020 started early-commissioning phase
  - challenges in this phase include both the new web-management interface, but also getting the enrolment and provisioning flow right
  - there are *a lot of orgs and domains* to go through, with some interesting DBA vs. legal names
  - certificate profile definition (e.g. making sure Robots work even if they are not in the InCommon scheme)
- subsequent phases in February & March
  - multi-lateral eduGAIN SAML meta-data parsing, client cert portal based on SAML attributes, auto-provisioning security
  - confirmation of exact profiles and all relevant controls re-implemented in new system + API
  - all dedicated intermediates for the (small number of) **chains available for distribution**
  - translation of interfaces and messages to all relevant languages
- End of March: commissioning complete and ready for large-scale roll-out
- End of April: all subscribers on-boarded, trained, and ready is issue
- End of September 2023: last TCS G3 certificates will expire (for IGTF: end of July 2021)

Networks · Services · People www.geant.org

12

< pushed in 1.104

< TCS is ~here now

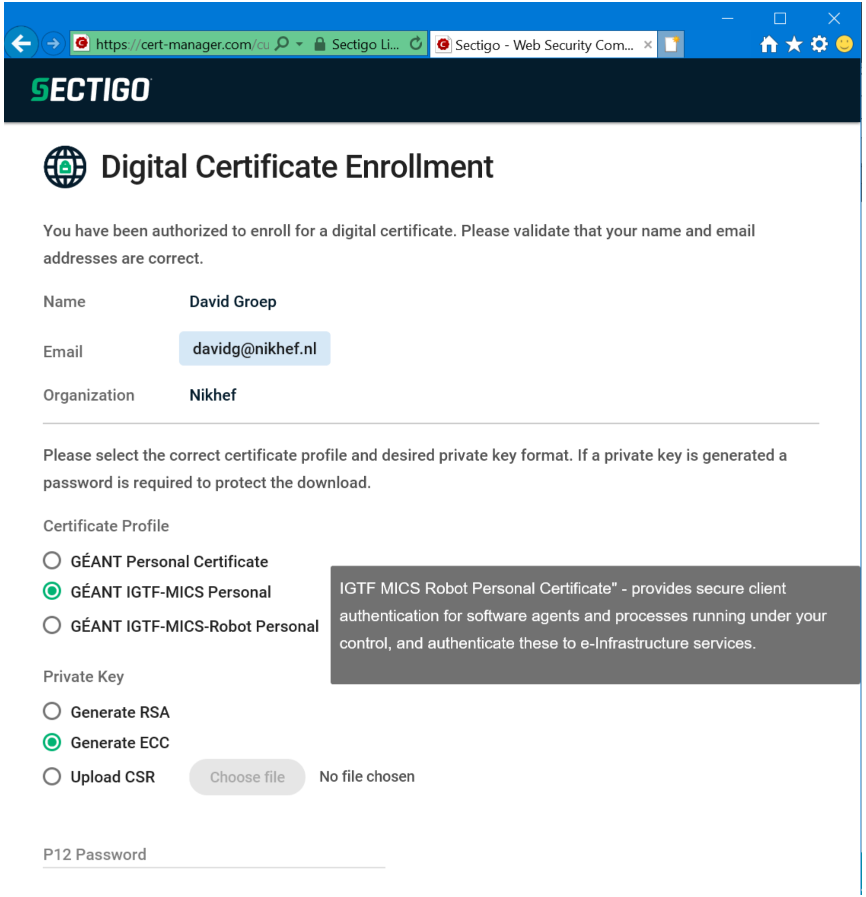
(as seen from an org standpoint at Nikhef)

Current state, end of May 2020

- it is not impossible to get TCS ‘IGTF profile’ compliant end-entity certs ☺
- self-service issuance portal for personal certificates works really great, available in eduGAIN, using the same authorisation model with

  eduPersonEntitlement = urn:mace:terena.org:tcs:personal-user
- can also produce PKCS#12 server-side generated credentials, to address increasing trouble with browsers
- robot email (mailing lists, team robots) work as usual via explicit invite
- non-eduGAIN (explicit invite) personal certs work for the kind of people who otherwise love to write email by typing SMTP commands :)

New ‘SAML portal’



Digital Certificate Enrollment

You have been authorized to enroll for a digital certificate. Please validate that your name and email addresses are correct.

Name	David Groep
Email	davidg@nikhef.nl
Organization	Nikhef

Please select the correct certificate profile and desired private key format. If a private key is generated a password is required to protect the download.

Certificate Profile

○ GÉANT Personal Certificate
● GÉANT IGTF-MICS Personal
○ GÉANT IGTF-MICS-Robot Personal

IGTF MICS Robot Personal Certificate" - provides secure client authentication for software agents and processes running under your control, and authenticate these to e-Infrastructure services.

Private Key

○ Generate RSA
● Generate ECC
○ Upload CSR Choose file No file chosen

P12 Password

Newly developed by Murray @Sectigo

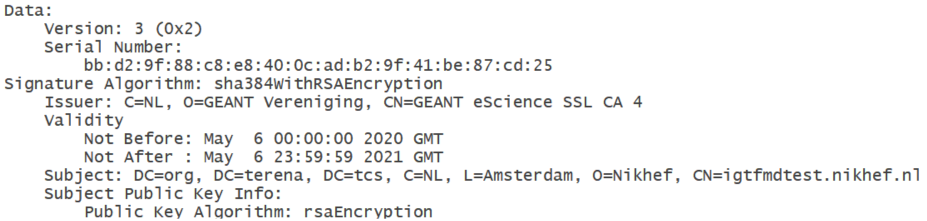
Picks profile and name form directly from product type

includes ePPN as uniqueID
but stores it as the email address! so orgs cannot re-use an ePPN as an email address later …

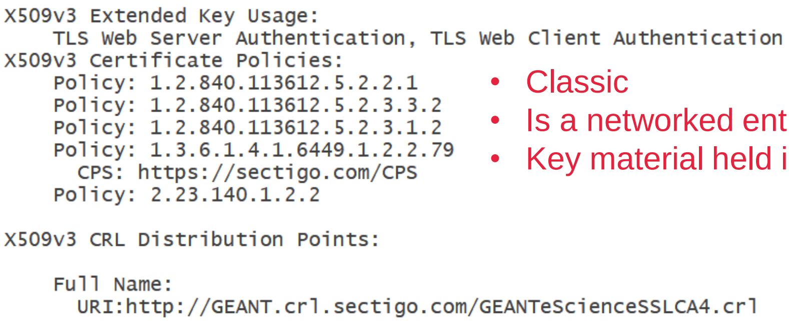
Support .P12 generation and CSR

Policy OIDs – complete and the correct 1SCP suite

Server OV SSL: classic issuance



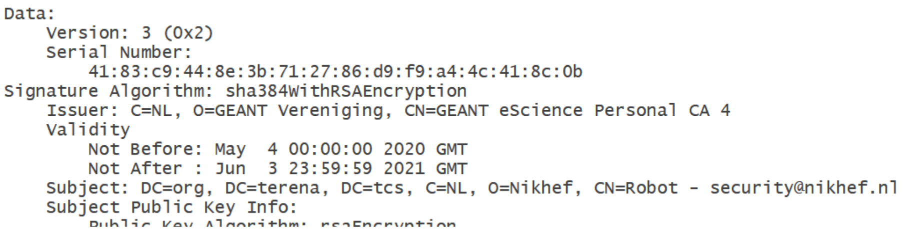
```
Data:
    Version: 3 (0x2)
    Serial Number:
        bb:d2:9f:88:c8:e8:40:0c:ad:b2:9f:41:be:87:cd:25
Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=NL, O=GEANT Vereniging, CN=GEANT eScience SSL CA 4
    Validity
        Not Before: May  6 00:00:00 2020 GMT
        Not After : May  6 23:59:59 2021 GMT
    Subject: DC=org, DC=terena, DC=tcs, C=NL, L=Amsterdam, O=Nikhef, CN=igtfmdtest.nikhef.nl
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
```



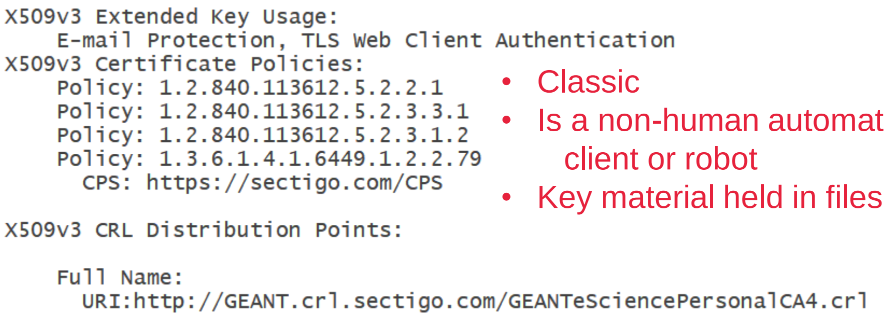
```
X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
    Policy: 1.2.840.113612.5.2.2.1
    Policy: 1.2.840.113612.5.2.3.3.2
    Policy: 1.2.840.113612.5.2.3.1.2
    Policy: 1.3.6.1.4.1.6449.1.2.2.79
      CPS: https://sectigo.com/CPS
    Policy: 2.23.140.1.2.2

X509v3 CRL Distribution Points:

    Full Name:
      URI:http://GEANT.crl.sectigo.com/GEANTeScienceSSLCA4.crl
```

- Classic
- Is a networked entity (host)
- Key material held in files

Robot Email: classic issuance



```
Data:
    Version: 3 (0x2)
    Serial Number:
        41:83:c9:44:8e:3b:71:27:86:d9:f9:a4:4c:41:8c:0b
Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=NL, O=GEANT Vereniging, CN=GEANT eScience Personal CA 4
    Validity
        Not Before: May  4 00:00:00 2020 GMT
        Not After : Jun  3 23:59:59 2021 GMT
    Subject: DC=org, DC=terena, DC=tcs, C=NL, O=Nikhef, CN=Robot - security@nikhef.nl
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
```



```
X509v3 Extended Key Usage:
    E-mail Protection, TLS Web Client Authentication
X509v3 Certificate Policies:
    Policy: 1.2.840.113612.5.2.2.1
    Policy: 1.2.840.113612.5.2.3.3.1
    Policy: 1.2.840.113612.5.2.3.1.2
    Policy: 1.3.6.1.4.1.6449.1.2.2.79
      CPS: https://sectigo.com/CPS

X509v3 CRL Distribution Points:

    Full Name:
      URI:http://GEANT.crl.sectigo.com/GEANTeSciencePersonalCA4.crl
```

- Classic
- Is a non-human automated client or robot
- Key material held in files

A new thing: ECC IGTF certs

- Although ECC certs were available in TCSG3 as well, it was
  ‘a well-hidden option’ and never advertised
  and through the IGTF we never distributed the ECC variants of TCS G3

- New self-service portal for TCS G4 personal – since it generates keypairs on the CA side – now makes ECC certificates very prominent, and
  a first-class citizen of the ecosystem

- TCS G4 ECC intermediates, and the USERTrust ECC CA root, as ‘experimental’ CAs in the IGTF 1.105 release

ECC certs in the main RP contexts

- No idea what will happen to software if they are installed – it … needs testing!
  Proposal: test as far as possible with a few instances and roll in 1.106

- At least *voms-proxy-init* in emi-ui >=3.7 does not explode, which is good™
  (but the same in versions <=3.3 is known to get confused by them)

- Installing as extra trust anchors should be harmless, until a user trigger one

Current state: availability and operation

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

this work is co-funded by and contributing to the Dutch National e-Infrastructure coordinated by SURF