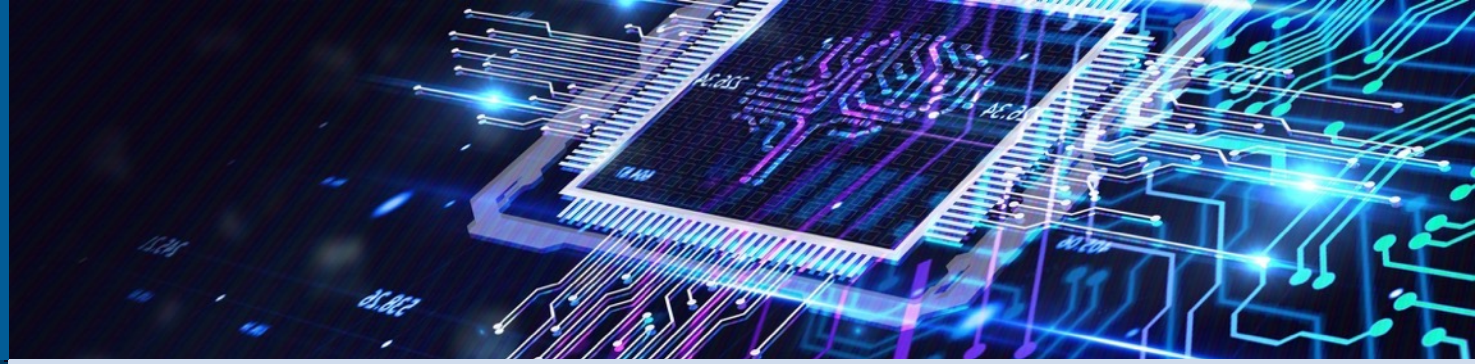
CSC

ICT Solutions for Brilliant Minds



GÉANT TCS certificate service - risks and challenges

SIG-MSP 13.03.2024

Harri.Kuusisto@csc.fi

FUNET

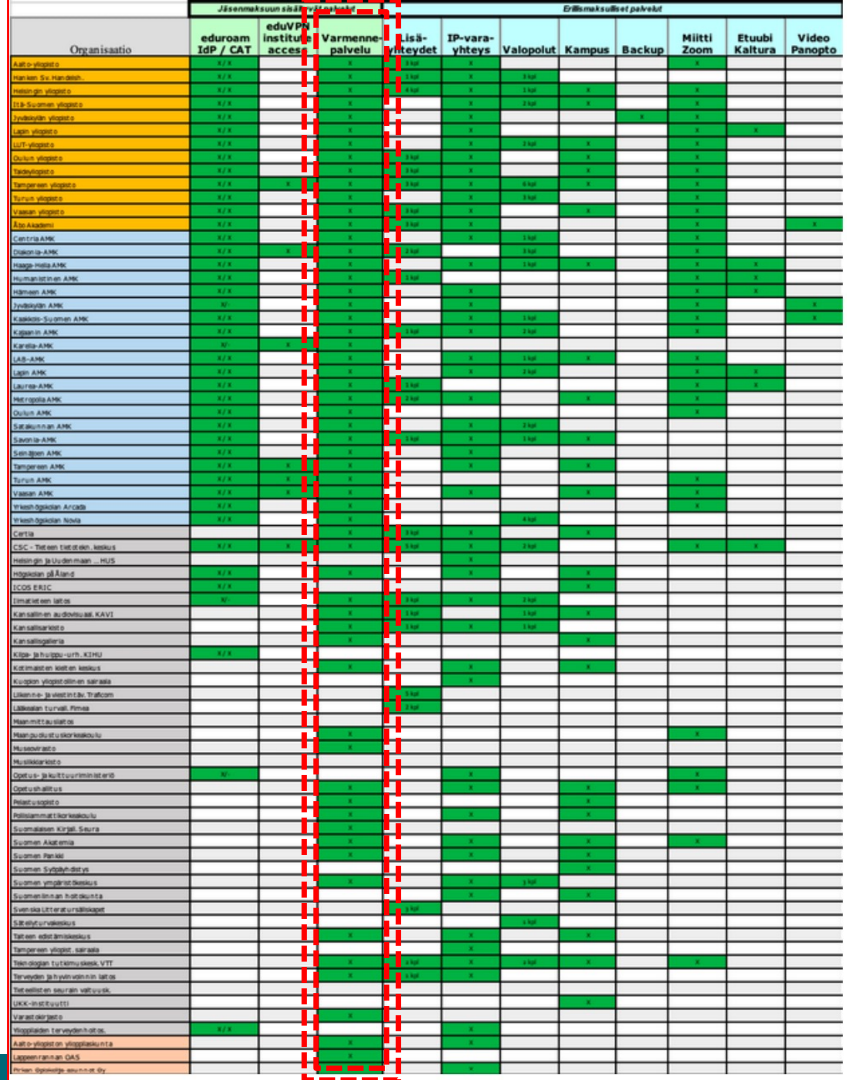
GÉANT TCS – a brief history

Brokering cheap certificate service with foreign CA, with helpdesk working in time zone 12 hours different from yours, with no SLA's, can be ~~sometimes~~ pain in the… head.

- **Local teleoperator years until 2010:** Slow and manual service
- **TCS: Comodo years until 2015**: Days or sometimes weeks of delays in delivering certificates, call-backs etc…
- **TCS: Digicert years until 2020**: Mostly OK, but some slowness in domain and organisation validations
- **TCS: Sectigo years ongoing:**
  - Past: Major issues with lots of fast and unexpected certificates revocations (new rules from CA/Browser Forum)
  - https://connect.geant.org/2020/07/15/the-tough-world-of-internet-certificates
  - Current: Major issues with several weeks of delays in organisation validations all over the European NRENs

Example: Funet Certificate Service

- Usage of the certificate service is high
- Importance of the certificate service is high
- Current price of the certificate service is very low
  - In our case, no separate billing, service fee is included in Funet membership fee
  - 8000 certificates per year => 2-3 eur/certificate
  - Commercial solutions can be 200-300 eur/certificate



Major problem at the moment: Organisation validation process by Sectigo is not working

- Real life example:
  - 11.12.2023 organisation validations for 26/72 Funet-organisations pending
    - No reaction from Sectigo received. CSC raised manually helpdesk-tickets to Sectigo.
  - 16.12.2023 still pending 10/72 organisation validations
    - CSC eskalated problem to "premium support" and GÉANT
  - 1.1.2024 still pending 5/72 organisation validations
  - 18.1.2024 all the Funet organisation validations done. Case closed for a while, but just for a while…

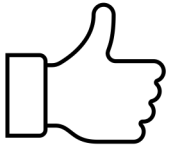
Light reverse engineering the problem

- Sectigo organisation validation team (= first line support)
  - …works in different countries with different time zones (anti-European time zones)
  - …mainly uses same copy-pastes (“Our validation team has received your ticket… case number…)
- The real process behind the organisation validation seems to be a black box, usually black hole, with no interaction if validation fails and status stays as ”pending”.
- Dozens of manual ”Hello Sectigo, organisation validation of nnnnn is still pending, please validate as soon as possible!” needed. Not sure if these messages help or not.

Other challenges (upcoming) in the whole CA world

- (still a rumor?): Server certificate lifetimes are limited to 90 days (currently still one year) as soon as before end of year 2024.
  - In practise this means, that in the near future certificate renewals MUST be done automatically using ACME (or similar) tools.
  - Challenge #1: Need to inform customer organisations how to start using ACME
  - Challenge #2: Server Certificates are also used in places where ACME can not be supported

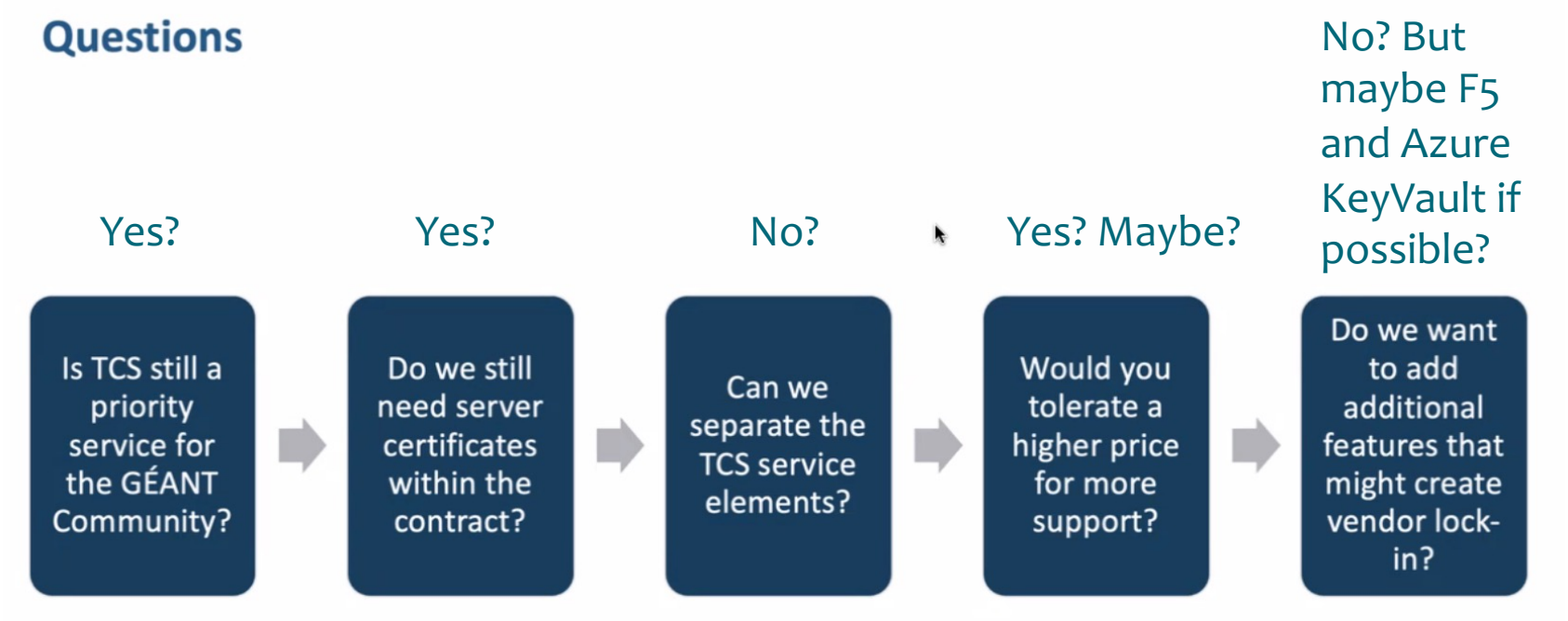
GÉANT actively plan the future



- Following on from the briefing paper we shared last year (https://wiki.geant.org/download/attachments/133771845/Future%20of%20GE%CC%81ANT%20Trusted%20Certificate%20Service.pdf) we would now like to invite you to join us at one of three consultation meetings on the Trusted Certificate Service and what future changes we need to make to the service to support our needs. We invite all TCS service owners and those within the NREN space with an interest in technical deployment, but specifically would like input from senior managers as to the strategy and direction they would like to take for future service delivery. You can sign up for the sessions below - each will be a repeat of the same material to give you options, you only need to attend one:

- 21st February 2024: https://events.geant.org/event/1606/
  28th February 2024: https://events.geant.org/event/1607/
  27th March 2024: https://events.geant.org/event/1608/

Q&"A" from one of these consultation meetings



Some “NREN thoughts” about the possible future plans…

- **Future of the certificate service as NREN service?**
  - Other and better (and more expensive?) options to provide certificate service are also considered.
    - For Funet, maybe Finnish, Nordic or at least European CA would work better?
    - https://letsencrypt.org/ “Let's Encrypt is a free, automated, and open certificate authority brought to you by the non-profit Internet Security Research Group (ISRG)”

- **Q**: Is it going to be possible for GÉANT re-tendering yet another CA for providing better, probably more expensive and (most important) working certificate service for European NRENs ?
  - **A**: ?