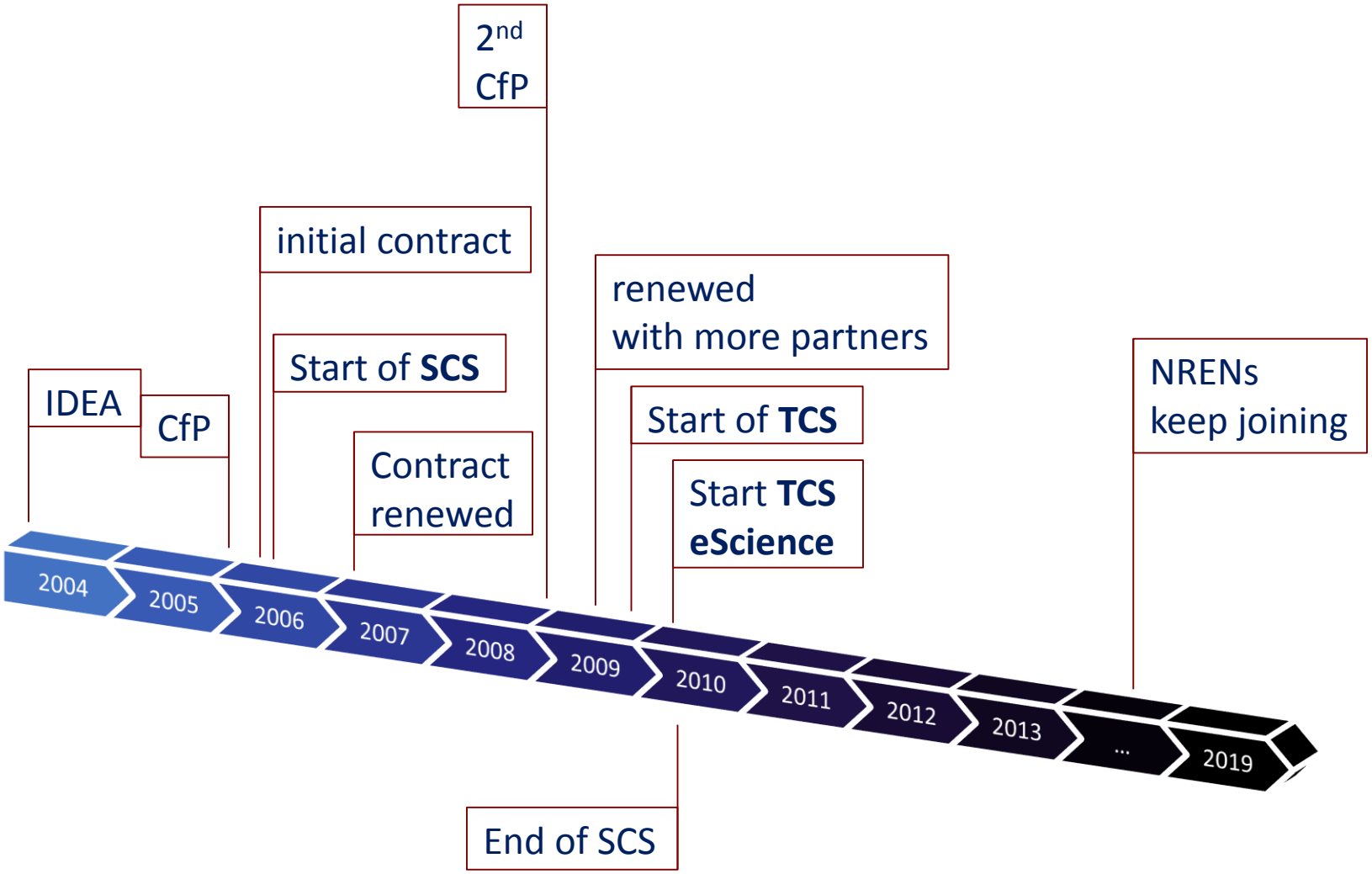
TCSG4 – requirements for Research and e-Infrastructures

David Groep
TCS PMA and Nikhef

EUGridPMA45
January 2019

A long (but rather successful) road



R/E Infrastructure certificates today

- Actually the ‘eScience’ certificates are generally useful for *client authentication purposes*
- Also services act as clients (e.g. for accounting)

- Product types
  - End-user personal certificates (S/MIME and auth variants)
  - Robots (personal, or team ‘email’)
  - Server (OV verified with specific namespace)

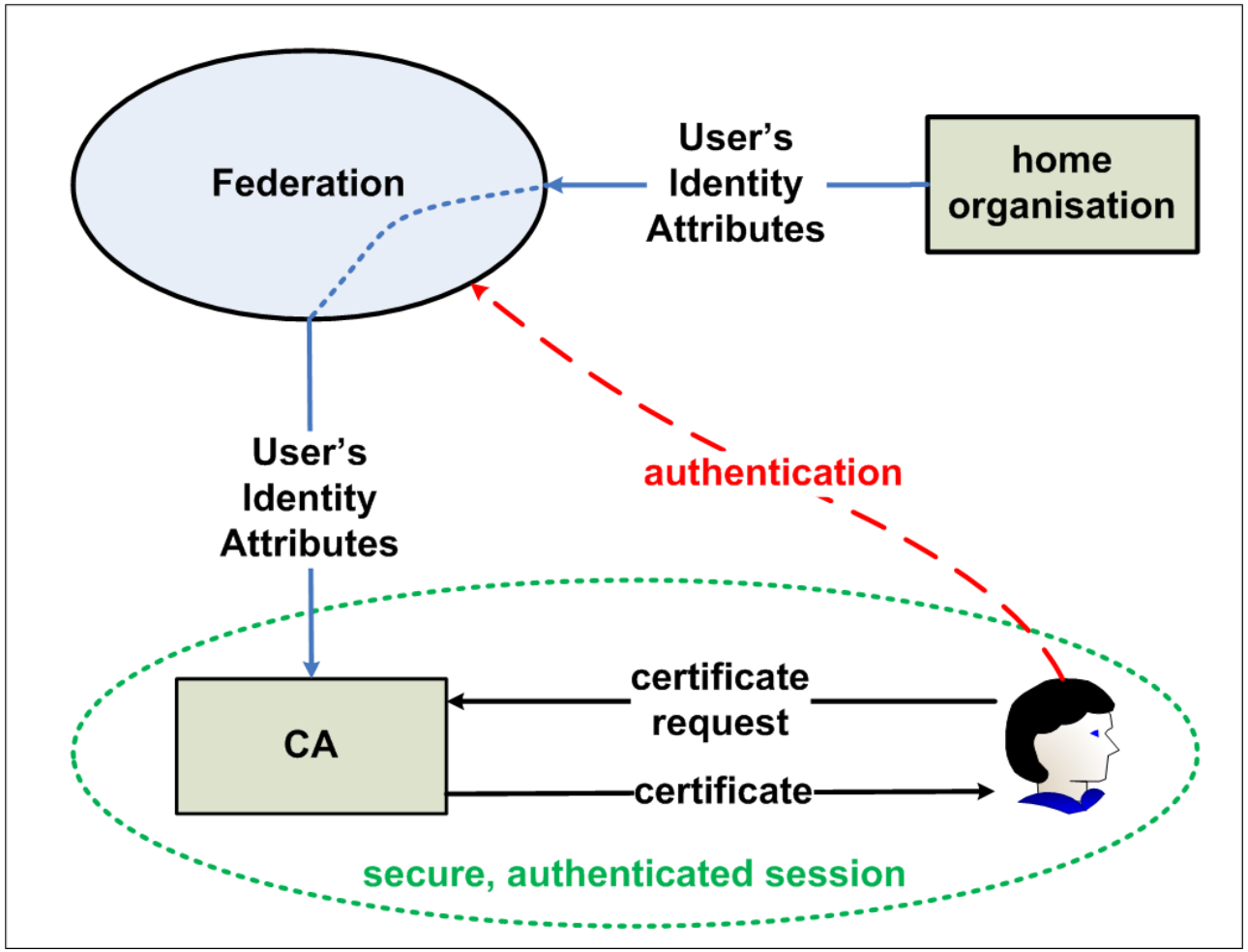
The TCS structure

- GEANT is the ‘owner’ of the certificate services, which is procures on behalf of the participating NRENs (GEANT members)
- It sources the issuing service from a commercial CA service provider and sets the requirements
  - Via the tender/RfP requirements
  - Via updates to the CP/CPS
- NRENs then act as the user-facing end of the service
  - They can (or could) define some of the processes
  - All have to agree to the same CP/CPS and contract(s)
  - Leveraged federated ID from eduGAIN as much as possible for users
  - The TCS PMA controlling the CP/CPS is comprised of experts from across the community

Interesting elements

- By its intention, the TCS CAs should
  - Be *publicly trusted* in all major (mobile) systems
  - Use mechanisms that scale to the European R&E community
  - Don't burden the subscribers (institutions) too much – in particular for auditing
  - Preserve under GEANT's control key elements that ensure continuity (no vendor lock-in) – for eScience, this means e.g. subject namespace
- but of course not everything is under our control
  - Changes to baseline requirements affect us
  - Way the CA interprets those changes affects us even more *organization naming for instance, or ASCII-fication*
  - Server certs are more tightly controlled than personal

TCS eScience and research requirements



Graphic courtesy Jan Meijer, Uninett, 2009(!)

TCS Gen 4

Landscape is changing again

- dynamic ‘DevOps’ provisioning of micro-services and popularity of ACME
- browser reaction to certificate types (and to faults)
- more cross-over between eScience and other authN use cases (credentials and signing by teams and mailing lists)
- ‘weird’ use cases
  (>150 SAN dNSNames in one cert, proxies, &c)
- low-power, mobile, and IoT like use cases
- eIDAS and the ‘electronic campus’
- Google doing its own thing entirely ☹

What key requirements should there be on TCSG4?

What to definitely keep?

- distinguished namespace for OV eInfra certificates (specific profile)
- eduGAIN fedID integration
- single installable trust chain for all platforms
- plenty SAN dNSNames

What to definitely add and request?

- (continued) use of ECC up to an ECC root
- handling (at least) OV with ACME-like protocol – can we push providers to push this one (server API keys, or server oAuth?)
- ***more?***

Thank you

and keep the output of this discussion a bit confidential

davidg@nikhef.nl

GÉANT

Networks · Services · People

www.geant.org