Future of GÉANT Trusted Certificate Service

Overview

Extensive consultation in 2019 resulted in (current service) NRENs unanimously asking GÉANT to reprocure the TCS service with broadly the same parameters as had been offered for the preceding 5 years. This was a challenging service model given the volatility of the CA market (see below).

The services identified by the community as required included:

- SSL certificates – for authenticating servers and establishing secure sessions with end clients.
- Grid certificates – for authenticating Grid hosts and services (IGTF compliant) for both SSL and client use cases.
- Client certificates – for identifying individual users and securing email communications.
- Code signing certificates – for authenticating software distributed over the internet.
- Document signing certificates – for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice. Preferably eIDAS compliant.

GÉANT was able to procure a service that met most of the requirements via Sectigo, although some compromises were needed and two phases of procurement to negotiate on requirements that could not be met.

Recently, the certificate profile types have been changed to meet the requirements of the new S/MIME Baseline Requirements from the CA/B Forum. This has allowed us to more clearly define use cases for client certificates beyond email signing. All current certificate profiles are described at: https://wiki.geant.org/display/TCSNT/TCS+Certificate+Types.

Current Service Provision

TCS is currently provided to 35 GÉANT Member / Associate Member NRENs and 2 non-members (OMREN and the American University Beirut). The full membership can be found at: https://wiki.geant.org/display/TCSNT/TCS+Participants+Sectigo. The only members not currently contracting for TCS are Switzerland, Turkey,Bulgaria, Latvia, Azerbijan, Armenia, Iceland, Georgia and Montenegro.

TCS is supported by one member of staff at GÉANT with less than 0.2 FTE allocated, but consistently requires more effort and support. Billing for TCS is supported separately from the membership fee by the GÉANT finance and procurement teams. TCS is a single contract service with GÉANT as the main contract holder - it is not a framework agreement where NREN's contract directly with the provider.

Pricing for TCS is managed by bands. NRENs from countries with a larger GNI pay more in increments than those from smaller countries to broadly reflect the expected service demand.

Identified Issues

Numerous issues exist in the current market for certificates, as described in the sections below.

Reliability of large Certificate Authorities

There have been numerous issues with both DigiCert and Sectigo over fundamental service delivery functions (incorrectly formed certificates, data breaches etc). These patterns have been noticed anecdotally in some other well known CAs such as Quo Vadis.

Service Provision from Smaller Certificate Authorities

In the procurement phase, smaller CAs like https://www.harica.gr/ were not able to meet the volume requirements for SSL certificates within the GÉANT Community. This is where some of the benefits of the "bulk purchase" approach for NRENs that has resulted in a very agreeable price has also had negative implications in terms of service choice.

Contraction and Volatility of CA Market

The number of commercial Certificate Authorities in operation has shrunk significantly in recent years with multiple take-overs of some of the major players. There is also significant volatility within the market and tension between the Browsers and CAs. These issues have been identified and raised at an EC level by GÉANT.

The position of the major browsers will inevitably lead to more changes in certificate validity periods in a short timeframe, with a likely maximum validity period of 90 days being expected in the next two years or less. This would place a significantly higher focus on automation processes for organisations to be effective in their certificate management.

Significant changes are constantly being introduced by the CA/B Forum. In the last two years this has caused changes to the longevity of certificates, changes to validation process for organisations and domains, changes to requirements for code signing certificates and changes to requirements for all S/MIME certificates. This has created a continuous loop of "fire-fighting" changes rather than service stability.

Barriers Created by Legislation

The EC is making several attempts to control and change the way that internet governance and trust management works, mostly through changes in legislation. The eIDAS regulation, and specifically proposed Article 45, introduces a parallel security structure to the existing CA/B Forum in the form of government legislation. The proposed legislation is seen as problematic in many ways but specifically presents these challenges:

- It attempts to reintroduce the equivalence of an approach akin to EV certificates via QWACS despite the fact that this type of signalling has been proven to be ineffective and misleading.
- It introduces a potential backdoor for government surveillance.
- It requires explicit trust in mandated trust providers without appropriate checks and supervision of those suppliers.
- The attempt is extra-territoral, enforcing EC legislation globally.

The CA/B Forum is currently not operating effectively as a representative body for the organisations effected by changes to the certificate space, but equally the attempt to resolve this through EC legislation is unlikely to yield effective results.

Scope of the Trusted Certificate Service

TCS has been a success story, and has also been in place within the community for a number of years. This has led to scaling issues which bring both benefits and drawbacks. We ask for a significant number of different certificate types and use cases to be supported, and we procure this for a large number of organisations. The procurement process seeks the best possible price for NRENs and TCS customers have enjoyed incredible value for money for certificates over recent years (as low as 5 euros per certificate) despite slight increases in service cost. This price tag has become expected over the years of service provision without much consideration of the comparable cost for the community at normal market rates.

A more balanced review of cost versus service requirements may be required as we consider future service provision.

Disruption of Let's Encrypt / ACME-first Approaches

The introduction of Let's Encrypt brought significant disruption to the CA market and challenged a lot of thinking regarding approaches to certificate management. In a very short period of time, the significance of EV and to a lesser extent OV certificates declined dramatically.

There is a question mark over why TCS does not move to recommending the use of Let's Encrypt or other ACME-first approaches for SSL certificates as a standard and focus on more specialist requirements with TCS. This is a model that could be explored, but there are a number of open issues:

- Let's Encrypt requires the use of ACME. There is a significant skills gap within the Higher Education and Research sector that prevents the large-scale roll out of ACME based services at this point in time.
- There are legitimate concerns over walking into a monopoly situation with Let's Encrypt as the only way to issue certificates. There are no guarantees or checks that this service will continue to be freely available or won't introduce more rate limiting to the service.
- Whilst there is very little interest in EV certificates in the community at this point in time, the benefits of OV are still considered relevant by many organisations. Let's Encrypt only offers DV certificates and believes that shorter certificate validity periods are a better safeguard than organisational validation.

Other ACME-first approaches to consider include ZeroSSL, Buypass, SSL.com and Google Trust Services.

New Requirements

Over the current service period for TCS, we have also seen significant interest in eIDAS certificates and interest in services that can better manage document signing approaches for confused individuals. GÉANT is looking at both of these issues through the EDSSI project and related developments, such as extending edusign.

The CA/B Forum has introduced significant new barriers for various certificate types including new standards for code signing certificates, S/MIME certificates and validity periods for SSL certificates. More disruption is expected in the next 18 months.

The need to move to ACME is inescapable with the inevitability of 90-day certs on the horizon. Significant work is needed to move our community to a point where automation is well understood and standard practice.

Possible Future Approach

Changes are needed within TCS and these changes need to be managed over a phased period of time. There is no expectation of immediate change but we would recommend that work begins as soon as possible to start preparing the community for a future with a different service model. Potential steps could include:

	Requirement	Status	Timescale
1	Strong push for ACME adoption in the community.	Initial steps have been made here with a community infoshare but more work would be need to see large scale adoption	Short-term
2	Complete a more formal risk analysis of using Let's Encrypt / ACME-first for SSL certificates	Not yet started	Short-term
3	Explore brokerage options to support automation of certificates for organisations that do not have the skill set to manage ACME / certbot	Can we provide more services to support the automation process?	Short-term
4	Look at disaggregating provision of certificates across different suppliers	A framework agreement approach with different routes for different certificate types may give a stronger service portfolio to NRENs but would be more complex to offer significant support centrally The concept of running our own CA should not be completely ruled out, although the requirements	Medium-term

		and liability questions are significant	
5	Explore enhancements to service provision around document signing approaches	Services such as edusign are currently already in pilot phase	Medium-term
6	Explore Cloud consequences and new service requirements from alternative certificate approaches	Look at new service approaches such as AWS and Azure Key Vault	Medium-term
7	Continue to raise issues / lobby to find a stronger voice for the R&E community in certificate governance approaches	Work has begun but is currently being pushed with greater urgency through the EC	Long-term

GÉANT will be undertaking a consultation period to look at these proposals, discuss them with the community and make recommendations as to the next steps for certificate management within the research and education community.

References

- https://connect.geant.org/2021/04/14/internet-certificate-regulation-in-europe-geant-position-statement
- https://connect.geant.org/2020/07/15/the-tough-world-of-internet-certificates
- https://connect.geant.org/2021/09/09/validation-changes-coming-for-tcs
- https://connect.geant.org/2023/08/31/tcs-service-changes-to-support-s-mime-baseline-requirements
- https://connect.geant.org/wp-content/uploads/2023/10/GEANT_CONNECT_44_How-do-GEANT-and-the-NRENs-support-Open-Science.pdf - Article on Value of Trust
- https://www.eff.org/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security
- https://last-chance-for-eidas.org/