

Meeting Thursday 1 June 2023, 12:15 pm per videoconference

Google returns to anti-competitive behavior

EU Commission

Liliane KARLINGER, member of cabinet of
Executive Vice-President Margrethe VESTAGER

Werner STENGG, cabinet expert of Executive Vice-
President Margrethe VESTAGER

ESD

Michael BUTZ, chair ESD

Andrea van ARKEL, ESD

Andras BARSÍ, Aruba

Patrick von BRAUNMÜHL, Bundesdruckerei

Paul van BROUWERSHAVEN, Entrust

Agenda

1. Stopping Google's mandate for 90-day certificates
2. eIDAS Art 45.2 – restore Commission/Council language over Parliament language

Google returns to anti-competitive behavior



recently announced that it will unilaterally shorten all TLS server certificates, including Qualified Web Authentication Certificates (QWACs), to a maximum validity period of only 90 days instead of the current validity period of **398 days** (*roughly 1 year*).

Google returns to anti-competitive behavior

- ESD thinks this is a **dangerous precedent**, as it will kill QWACs in its current form.
(Qualified website authentication certificates (QWACS) are there to ensure that users can identify who is behind the website).
- Google's action will **conflict** with ETSI and CA Browser specifications for QWACs, which permit providers (QTSPs) to issue 398-day certificates.
- It will also hinder users from obtaining certificates from their QTSP or CA of choice
- Google did not demonstrate any security need for such change.

Unfortunate results from Google's intended policy

There are no security-needs demonstrated by Google

- ⊗ Intended policy changes favor Google's own Cloud and web hosting business over its competitors.
- ⊗ Google is both a regulator of QTSPs and a fierce competitor through its own web server certificate issuance – a clear conflict of interest.
- ⊗ The German antitrust agency has already raised serious antitrust concerns in 2022 about Google's actions in forcing shorter certificate validity periods on QTSPs and CAs.

Unfortunate results from Google's intended policy

- Many high-profile websites reject automation because of security concerns.
- 90-day certificates will likely increase websites workload/expenses 4 to 6-fold.
- Article 24 eIDAS and browser expectations: identity validation of the website owner will also have to be done 4 to 6 times a year.
- Forced automation from 90-day certificates is *not* a secure solution for many websites.
- 90-day certificates are not a solution to future vulnerabilities in the ecosystem such as the need to change encryption algorithms – those changes require changes in other systems as well and will take much longer than 90 days to implement.
- Shorter and shorter certificate periods favor Google's own certificate authority, Cloud and web hosting business over its competitors.

Google returns to anti-competitive behavior

Also, the **German antitrust agency** studied this very issue and released a report in January 2022 that concluded.....

Google would likely commit a violation under both EU and German competition law *if it forces further reduction in the certificate validity period from 398 days to a shorter period and that reduces the use of certificates with a higher level of authentication, such as QWACs.*

Google returns to anti-competitive behavior

The proceedings dealt in particular with **Google**:

- shortening the **recognised validity periods** of certificates
- **modified display** of information (Art 45 eIDAS)
- **unilateral withdrawal of trust** from a qualified trust service provider (Art 45 eIDAS)

Google returns to anti-competitive behavior

The German antitrust authority however decided to take no action at this time as there is a Commission draft for a v2.0 revision of the eIDAS Regulation that significantly strengthens Article 45.

The German antitrust authority indicated it wishes the legal gap to be remedied by adoption of the proposed Article 45 which will solve the problem at the “European level” and not just in Germany.

Why does Google push ever shorter certificates (1)

- Google profits from automation, as its **business model** for Google Cloud is designed around automation for website certificate renewal and replacement.
- Moving from one year to 90-day certificates will drive websites to automation even faster, and make it easier for Google to service customers from their certificate authority, Cloud and web hosting business.
- This is the same reason why Google doesn't seem to like certificates with a verified identity, as identity verification (not just automated domain validation) is a complex process that involves humans and is therefore hard to automate and costly to perform

Why does Google push ever shorter certificates (2)

- Google is also pushing particularly for ACME automation, the protocol that its own internal CA (Google Trust Services) and Let's Encrypt (of which Google is one of the main financial contributors) both support.
- According to Netcraft those two CAs (Google Trust Services and Let's Encrypt) together have an astonishing 67% market share of all TLS certificates – which is a dangerous market concentration.
- Finally, today most automated ACME clients available to website owners in the market default to Let's Encrypt as the CA where the website's TLS certificate will be obtained, which drives websites to DV certificates from this single CA even if the website would prefer a QWAC or EV certificate – and it's generally too difficult for website owners to figure out how to override that built-in coding preference to Let's Encrypt's DV certificates.

Google returns to anti-competitive behavior

Google overreach is symptomatic

- ⊗ ESD sees here an arbitrary behavior of Google to disregard/bypass legal requirements by way of setting its own technical requirements.
- ⊗ If we put this behavior into the **larger context**, it means that browsers have the power – and are using this power - to NOT ONLY influence European legislation;
- ⊗ but **UNDERMINE** European sovereignty by simply changing their technical standards.
- ⊗ Google and browsers overreach is symptomatic!

Removal of previous website identity UI in 2019, without consensus/reference to any standards organizations/EU

COM Art. 45 ensures European digital sovereignty!

Article 45 eIDAS:

COM proposal: intention to strengthen *qualified certificates for website authentication* (QWACs) by introducing a requirement for web-browsers to:

- ✓ recognize and
- ✓ display QWACs in a user-friendly manner

- With the identity display users and law enforcement can identify website owners.
- Requirement is protecting consumers and fighting cybercrime.
- It also ensures European digital sovereignty as web-browsers can no longer apply their own rules rather than following the eIDAS Regulation.
- Web browsers are always welcome to improve the ecosystem/requirements by participating in standard defining organisations such as ETSI etc.

Browsers steps to disregard/bypass legal requirements

- Browsers have strongly lobbied against Article 45.
- The Commission proposal is supported by the Council.
- **European Parliament's amendment proposal** narrows the definition of QWACs and opens up the possibility for **web-browsers to unilaterally deny the recognition of QWACs by asserting security concerns without any justification** or scrutiny by European authorities.
- This will **leave the interpretation** of eIDAS to Big Tech companies
- It will allow them to continue to refuse trust to QTSPs on the EU Trusted List, just as they have ignored the EU Trusted List in the past but instead applied their own trust rules.

Two necessities to preserve European Digital Sovereignty

The European Commission should act now and tell Google to take no further action on its 90-day proposal.

ESD sees a real danger that seemingly harmless technical adaptations (*such as the 90-day certificates only*) will undermine the European regulatory framework; and with it European sovereignty and the European trust space.

Trilogue should restore Article 45 Commission/Council language

Browsers have indicated they interpret the Parliament language to mean they do not have to accept the EU Trusted List. This leaves them with **exclusive control** over QTSPs and many QWAC issues.

THANK YOU FOR YOUR INTEREST
AND SUPPORT

European Signature Dialog
EU Transparency Register number: 994150833943-81 - Mail to office@european-signature-dialog.eu