

Google returns to anti-competitive behavior by limiting all certificates to 90 days only

Will this kill identity certificates and make eIDAS obsolete?

Google recently announced that it may unilaterally force QTSPs to limit 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**.

Google's action would conflict with ETSI specifications for QWACs, which permit QTSPs to issue 398-day certificates.¹

There is no demonstrated security need² for such a change, and this new demand by Google may force many websites to move to automated, non-identity (DV) certificates, rendering QWACs and eIDAS objectives obsolete.

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.

The European Commission, EU Parliament and Member States should act now and **tell Google to take no further action on its 90-day proposal**.

Google's announced conduct is **anti-competitive** and will - as set out below – drive QWACs out of the ecosystem and **undermine eIDAS**.

The European Signature Dialog (ESD)³, representing the leading Trust Service Providers, warns European institutions of the dangers from allowing US big-tech companies to set the rules that control the EU's digital sovereignty.

Here are the unfortunate results likely to occur from Google's actions:

Many high-profile websites reject automation because of security concerns.

In fact, most websites may find it necessary to move to *automated* certificate replacement systems to keep up with a new 90-day replacement demand, which **many high-profile websites don't want**.

Automation has its own security problems, including exposing CA/QTSP credentials on "edge" servers that are directly connected to the open internet, where hackers are constantly on the attack. These credentials can be used by hackers to issue new certificates in the name of the organization without using any multi-factor authentication to confirm the authorized usage.

90-day certificates will likely increase websites workload and expenses four-fold.

As a practical matter, the Google mandate will **increase the workload and expense** to European websites **four-fold**, as Content Delivery Networks (CDN), Cloud Service Providers (CSP) and 'as a service' providers, including Google Cloud, do not allow the use of a specific CA for automatic certificate management and only allow uploading custom certificates such as OV/EV/QWAC through manual processes. Websites will have to replace all certificates four times a year instead of the current one time a year.

Because eIDAS Article 24 requires that the entity behind the website shall be validated 'when issuing a qualified certificate', this means that **identity validation of the website owner** will also have to be done **for QWACs four times a year**.

1. The European Telecommunications Standards Institute (ETSI) is a recognized European Standardization Organization. Many ETSI standards are used worldwide.

2. Google made its announcement on its website – but provided no studies or analysis. Instead, Google just states its own conclusions and preferences. <https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/>

3. <https://www.european-signature-dialog.eu/>

Forced automation from 90-day certificates is not a secure solution for many websites.

The next reason why certificate replacement via automation (which Google's 90-day certificate mandate will likely require) is not supported by everyone in the ecosystem is complex.

A common form of automation uses the ACME protocol⁴ which often relies on a method that requires an "API credential" to connect to a website's DNS provider (DNS is the "switchboard" for the internet, translating website domain names to their servers' IP addresses). These credentials are often unlimited in scope and allow anyone who obtains a copy to manage all DNS records in the account. This could allow changes to all servers for *example.com* and might also provide the hacker access to other domains in the account such as *example.eu* or *otherdomain.nl*.

When DNS credentials are compromised, a hacker can send internet traffic to other servers or perform a "man-in-the-middle" attack (intercept, read and modify traffic such as from or to a website) on anything related to the domain names in the account. Basically, the attacker can control every website or server controlled under the account (e.g., VPN, e-mail, voice).

This automation method is **widely used today** because it's the only method that allows a website to obtain a "wildcard certificate" (*.example.com, which covers many subdomains). Placing an "API credential" on the webserver that connects directly with the internet is like storing the username and password of your DNS provider in the location most vulnerable to hackers. The abuse of DNS credentials is a widely known problem - for example, twitter.com had this issue a few years ago.⁵

Forced automation from 90-day certificates is not a secure solution for many websites. Websites should be allowed to make their *own* decision on automated 90-day certificates versus manual 398-day certificates, and Google should not make this decision for everyone by fiat.

Google's "2-certificate" proposal does not authenticate the entity behind the website as required by eIDAS.

In defense of its 90-day certificate mandate and the **problems it will create for QWACs** (driving them out of the ecosystem), Google says it has a solution – it is proposing that QWACs should be split in two and no longer be used to authenticate traffic from and to a website.

Only domain validated (DV) certificates would be used for that, and QWACS would become a non-authenticated file that only lists an entity which had control over the domain name at some point in time but might not be in control of the current website.

Google's "2-certificate" proposal **does not therefore meet the requirements of eIDAS Article 45** that a QWAC must "authenticate a website" and link the website "to the natural or legal person to whom the certificate is issued".

4. See RFC 8555 <https://www.rfc-editor.org/rfc/rfc8555>

5. <https://www.computerworld.com/article/2522268/twitter-s-own-account-caused-blackout--says-dns-provider.html>

90-day certificates are not a solution to future vulnerabilities in the ecosystem.

Contrary to Google's assertions, the transition to 90-day certificates does not help the ecosystem move quickly to new algorithms when old algorithms are no longer safe because the proposed ACME automation does not consider the client capabilities.

Clients may not support the new configuration or algorithm, which means that switching to a new configuration or algorithm without first knowing if the platform supports it can bring down the server or its relying infrastructure.

For this reason, requiring 90-day certificates is **not a solution to future vulnerabilities in the ecosystem** – it will generally require other updates that need to be performed or authorized first by the server administrator.

Google is both a regulator of QTSPs and a fierce competitor through its own web server certificate issuance – a clear conflict of interest.

Google has imposed its will on QTSPs before, forcing shorter and shorter certificate periods which favor Google's own 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**).

Each forced reduction in permitted TLS certificate validity period pushes more and more market share to Google's **own** products and services.

We note that Google does not even use 90-day certificates for its own cloud services – it uses shorter domain validated certificates than that. We suspect that Google's 90-day certificate mandate is just the first step toward requiring very short-term certificates (e.g., 2 days, which must be replaced every 1 day) in order to avoid the expense of the current best practice that browsers should always check if a certificate has been revoked before trusting it.

If Google succeeds in limiting certificates by fiat to 90 days at this time, it could then act by fiat in the future to limit certificates to 30 days, then 7 days, then 2 days. Such a momentous change to the ecosystem should **not happen on the basis of the preferences of a single US big-tech company** (whose browser currently has a 60% market share in Europe).⁶

6. <https://gs.statcounter.com/browser-market-share/all/europe>

Shorter and shorter certificate periods favor Google's own web hosting business over its competitors.

Google is a major financial contributor to the world's largest Certificate Authority Let's Encrypt⁷, and has served on its advisory boards. Let's Encrypt issues only automated 90-day DV certificates, and according to Netcraft data has a **59%** world market share of TLS certificates (Google also issues only 90-day or shorter certificates, and its own world market share of TLS certificates as a competitor to QTSPs is **8%**).

So, Google's mandate is essentially forcing all competing Certificate Authorities and QTSPs in the world to adopt the Google and Let's Encrypt business model of 90-day DV certificates and full automation.

But Let's Encrypt has experienced major security problems in the past, including when it mis-issued over 3 million certificates, but refused to revoke 1.3 million of them because it couldn't communicate with its own customers (and so decided not to revoke 1.3 million bad certificates because too many websites would have been taken down). **This is not a security model or a practice that the EU wants to copy.**

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.

The German antitrust agency studied this very issue and released a report in January 2022 that concluded Google would likely commit an **antitrust violation under both EU and German competition law** *if it forces further reduction in certificate **validity period** from 398 days to shorter periods* and such a change "affect[s] the purchase of certificates with a higher level of authentication [such as QWACs]."⁸

Conclusion:

US big-tech companies should **not be allowed** to set the rules that control the EU's digital sovereignty.

Instead, the European Commission, EU Parliament and Member States **should tell Google to take no further action on its 90-day proposal.**

In case you wish more information please write or call us:

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

7. <https://letsencrypt.org/sponsors/>

8. See report German Antitrust Authority (Bundeskartellamt) pages 3, 7-8: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2022/B7-250-19.pdf?__blob=publicationFile&v=4
www.european-signature-dialog.eu