Bundeskartellamt

Case Summary 21 January 2022

Proceedings in Transport Layer Security Certificates against Google terminated

Sector:	Digital economy
File number:	B7-250/19
Date:	17 January 2022

The Bundeskartellamt has decided for discretionary reasons to terminate an administrative proceeding against Alphabet Inc. and the companies affiliated to it under Section 36(2) of the German Competition Act, GWB, regarding the handling of the so-called more trustworthy Transport Layer Security Certificates ("TLS", previously Secure Socket Layer "SSL") of websites by web browsers and informed Google accordingly on 17 January 2022. The proceeding was initiated to examine whether the preconditions for prohibition under Section 19(1) GWB, Article 102 TFEU had been fulfilled regarding reports about the effects on competition of the modified display of information, in particular about more trustworthy TLS certificates in web browsers, the withdrawal of trust in certain certificate providers and certificates and the increasing trend to shorten the recognised validity periods of the certificates. The termination of the Bundeskartellamt's proceedings against Alphabet does not affect the proceedings initiated against Google in May and June 2021 based on the new provisions for digital companies introduced with the 10th amendment to the GWB. Having determined that Google is of paramount significance for competition across markets under Section 19a GWB (see Press Release and Case Summary of 5 January 2022), the Bundeskartelllamt is now taking a closer look at the company's data processing terms and the Google News Showcase service.

TLS certificates have two different functions: They provide an encrypted and secure connection between the certified website and the individual accessing the website. More trustworthy TLS certificates also authenticate companies operating a website. TLS certificates are issued by so-called trust service providers or certificate authorities which are considered trustworthy by the browsers. Whereas so-called Domain Validated ("DV") certificates only confirm the encryption, the more secure Organisation Validated ("OV") or Extended Validation certificates ("EV")/Qualified Website Authentication certificates ("QWACs") also provide varying degrees of further authentication to even better protect the internet presence of website operators, especially against

fraudulent attacks on their customers (phishing or identity fraud). Until autumn 2019 (Chrome version 77) the more trustworthy OV/EV certificates and QWACs were displayed in the address bar of the Chrome browser in such a way as to enable informed users to recognise the website operator and certificate type from the name, the registered address of the website operator and, in some cases, from additional information such as e.g. registration numbers. The use of a more trustworthy certificate was indicated e.g. by highlighting this information in green in the browser's address bar or at least by highlighting the lock icon in green in the address bar. Now only a standardised grey lock icon appears when an OV/EV or DV certificate is used or a warning appears when a website without a certificate is accessed.

The arguments in favour of **terminating** the proceeding were that the overwhelming majority of internet users were unaware of the significance of the certificates, which limited the added value of differentiated display, and other authentication processes had become available in the meantime, even if they were not completely equal alternatives. In particular, the proposed amendment to Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("eIDAS Regulation") of 3 June 2021 (COM (2021) 281 final) stipulated that the certificates had to be recognised by the web browsers and displayed in a user-friendly manner, taking account of the display problem. In light of this the Bundeskartellamt will not pursue the proceeding further and also refrain from applying the new Section 19a(2) GWB.

Alphabet Inc. is a publicly listed holding company based in Mountain View (USA) which was founded in 2015 to restructure the then existing Google Group. Alphabet's subsidiaries are active in various technology sectors and Google offers in particular internet services and software products through them. Since 2008 the group company **Google** LLC has offered its Chrome browser, which is now the most widely used browser worldwide for the presentation of websites, documents or general data in the internet. Google's open source software Chromium, which is similar to the Chrome browser, also forms the basis for other browsers such as Microsoft Edge and Opera.

Firstly, the **relocation of the display** of the identity information provided by more trustworthy certificates from the browser address bar, which attracts the user's attention, to a secondary user interface raised an initial suspicion of a competition law infringement. Google and other browser providers then started to standardise the visual design of the user interface around the address bar irrespective of the level of authentication of the certificates used, i.e. without differentiating between the different TLS certificate types for websites, but merely displaying a grey lock icon if the website had some kind of valid website certificate. Highlighting the lock icon and address bar in green was no longer supported. What is more, desktop browsers no longer displayed the name of the website operator, including the company location, via a country code in front of the Uniform

Resource Locator ("URL") if an EV certificate was used. In this way the more secure certificates (OV/EV/QWACs) were no longer directly visible to users from the address bar; instead the user now had to click once or even several times on the lock icon for the certificate information to be displayed.

Secondly, it was unclear on what criteria Google based its decision to withdraw its trust in a certificate provider. The **withdrawal of trust** resulted in the fact that the certificates of the provider concerned were no longer accepted in Chrome and instead of the website which used a certificate of this provider, a warning appeared.

Thirdly, there were reasons to suspect that the acknowledgement by the browsers, including Chrome, of a shorter certificate **validity period** of initially two years, and since September 2020 of only 398 days or even only a few months at a later date, could be problematic under competition law.

None of the three developments was based on an unconditional agreement or decision in fora such as the Certificate Authority ("CA")/Browser Forum or the Internet Engineering Task Force ("IETF"), in which the certificate and browser providers can express their interests and contribute to developing industrial standards.

The **investigations** in the form of questions to Google, discussions with certificate providers, browser providers, IT specialists and scientists as well as written questionnaires to website operators and certificate providers ultimately confirmed that the three problem areas already mentioned actually existed between certificate and browser providers. However, it was not conclusively clarified whether the practices constituted violations of competition law because the proceeding was terminated for the discretionary reasons already mentioned.

The **markets** potentially affected were at least the browser and certificate markets, whereby the exact product and geographic definition could initially remain open. Google could have been dominant on browser markets within the meaning of Section 18(1) in conjunction with subsections (4), (3a) and (3) GWB.

There were reasons to believe that Google's practice regarding the display of certificates with a higher level of authentication in Chrome resulted in **impediments** of certificate providers pursuant to Section19(1) GWB and Article 102 TFEU with regard to the three problem areas mentioned above.

With the **removal of the certificate information** from the browser's address bar – except for a grey lock icon for any TLS certificates – certificates with a higher level of authentication lost much

of their appeal for website operators, especially because, unlike the widely used DV certificates, they were often not available free of charge. Since then they could only be sold at lower prices because of their low visibility without the differentiated display and there was less demand for them. With its refusal to display the identification features of more trustworthy certificates on its Chrome browser, Google could insofar have impeded the certificate providers in their sales. The lack of display of the relevant information could have increased the website operator's risk of being imitated by phishing websites. It was easy for phishing websites to obtain DV certificates via the usual automated process but significantly more difficult to obtain more trustworthy certificates due to the necessary authentication process. Genuine and fake DV certified websites or websites with superior certificates were no longer visually distinguishable after the change to the display. The protection of the websites against fake sites was therefore more difficult and in the long term this could have reduced the trust of internet users in the website operators. The undifferentiated browser displays could have posed a higher risk for internet users to fall victim to phishing attacks or identity fraud and so fake news.

Since **Google's withdrawal of trust in individual certificate providers** at least two certificate providers have in the past completely exited the TLS certificate market: Symantec, USA, up to that point one of the leading certificate providers (2017/18), and Camerfirma, Spain (2021). Google's withdrawal of trust resulted in the browser displaying a warning when the website was accessed and according to the current stage of the investigations significantly impeded the marketing of the certificates. In the absence of comprehensive general rules and standards for withdrawing trust and in view of its powerful position on the relevant markets, Google could set its own rules or at least strongly influence the rules within the CA/Browser Forum, monitored compliance with these rules and after consulting the certificate providers concerned independently decided whether the remedies offered by the certificate provider concerned were sufficient or whether to withdraw trust in the certificate provider on its Chrome browser. According to the Bundeskartellamt's preliminary assessments a withdrawal of trust more or less meant that the certificate provider could no longer carry out its business activities in the TLS segment in view of the market position of the Chrome browser. The website operators had to conclude new contracts, leaving a narrower choice of certificate providers.

The certificate's **shorter validity period** could lead to additional effort because of the narrower intervals between the verification of the website operators and over time higher costs for the issue of certificates, especially because personnel was necessary for the authentication of the website operator before issuing certificates with a higher level of authentication; since this process could

only be automated to a limited extent, the number of staff involved in this case was not comparable with the number of staff involved in the authentication of operators using DV certificates. As a result the certificate providers could have suffered losses in the form of lower sales due to higher costs incurred by the website operators, which thus increasingly turned towards other lower-priced certificates. The website operators could conceivably also have been burdened with more work due to the increasing necessity to integrate the certificates in their IT infrastructure.

As part of the examination under Section 19(1) GWB, Article 102 TFEU the individual potential impediments to the certificate providers caused by Google would have had to be examined as to their objective justification. In a weighing of interests to be carried out as part of the **justification test** not only the interests of the parties directly involved (Google as the possible addressee of the law and potentially impeded certificate providers) would have had to be taken into consideration. On the contrary, particular account would also have had to be taken of the interests of the website operators and internet users as well as the public interest in the adequate display, availability and validity periods of more trustworthy certificates, if necessary also of a specific provider. A preliminary assessment established the following status of justification at the time the proceeding was terminated:

The **removal of the certificate information** from the browser's address bar might have been justified by the limited **space** in the browser's display area, the availability of the authentication information by **clicking** on the lock icon and Google's objective to aim for "**security as standard**" for Chrome, and only to display a separate warning if a websites is not secure. The certificate system was also regarded to some extent as **prone to error** because the authentication of more trustworthy certificates was not automated but carried out by humans. Finally, the possible **publication of the certificate information** elsewhere outside the browser's address bar could have justified the removal of the certificate information.

Despite the lack of **space,** which is in particular the reason for not displaying the information in the more limited mobile version of the browser, there was previously still space in the desktop application for the name of the certificate and website owner, including a country code. Moreover, the highlighting of the lock icon or the text line in green as an indication of more trustworthy certificates took up no room. This situation did not change fundamentally. Also highlighting certificate information in colour at least did not conflict with trends towards standardising the stationary and mobile versions. Displaying further certificate and authentication information after the user has **clicked** on the lock icon seemed cumbersome. The information was often not processed in a user friendly manner and only few internet users were aware of this possibility to find further information

by clicking on the icon. The website operators on the other hand used certificates with a higher level of authentication to show the internet users that security was important to them and to provide them with reliable proof that they had been evaluated as secure. Relevant legal obligations for the use of certificates with a higher level of authentication such as in the second Payment Services ("PSD2") Directive from autumn 2019 also confirmed the importance of such certificates. However, without the display there was no obvious identification of the certificate used, which according to the Bundeskartellamt's investigations considerably limited the potential added value for users as well as website operators and which also significantly rendered statutory usage obligations ineffective.

Based on Google's corporate policy to strive for "**security as standard**", the user was only to be made aware of an actual security risk by way of a clear warning. The reason for this was that studies had shown that users reacted more to warnings than to positive security information. Even if that were correct, the extent of Google's security measures was based on an internal definition of security. However, other established mechanisms to protect against phishing, such as Google Safe Browsing, did not have a preventive effect but only came into play in reaction to a website which was already identified as a phishing website. As an additional element of security, the more trustworthy certificates could have consequently also contributed to verifying a secure website where websites deceived users about the identity of the website operator by slightly altering URLs. However, not displaying the relevant information restricted the right of informed users to decide at their own responsibility whether to use web services based on their own risk assessment. This was also expressed in the eIDAS Regulation and the recommendations of the Federal Office for Information Security, BSI, and would have had to be taken into account in the weighing of interests.

The non-display of the certificate information in the address bar could not have been justified by the non-automated and therefore **error-prone** authentication process of more trustworthy certificates either because manual checks or interventions were also common in automated authentication systems, especially if this could offer the internet users additional protection against manipulations. The fact that the certificate information could have **been published** elsewhere in the browser also did not exclude a relevant impediment. According to the Bundeskartellamt's investigations, integrating the certificate information in the browser formed the key solution to successfully providing the information to the users while avoiding manipulation. This provided the interface to the users and by visualising the certificate information in an easily comprehensible way fulfilled

the actual purpose of informing them about the security of an accessed website without the possibility of the website operator to manipulate the certificate. This also formed the basis for the certificate holders to market their certificates.

Google's **withdrawal of trust** in individual certificate providers as a second potential impediment could have been justified by its aim to guarantee the **security** of internet users and website operators. An effective certificate system required that the user can trust the certificate and hence indirectly the certificate provider. Google's justified doubts about this due to faulty certificates or associated processes could have constituted reasons for withdrawing trust.

It was unclear whether the practices of the certificate providers concerned were sufficiently significant to pose an actual **security risk**. Both cases already mentioned, Symantec and Camerfirma, gave rise to a discussion about the providers' trustworthiness. As yet there is no internationally recognised neutral entity for assessing trustworthiness to which the certificate providers can also appeal against the browsers' decisions. However, there were the European Trusted Lists provided for in the eIDAS Regulation, in which all certificate providers were listed which, after examination by state supervisory bodies - in Germany the Bundesnetzagentur and the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) – were classified as trustworthy. Hence a system was in place in Europe that could offer a framework for examining the trustworthiness of the providers and therefore for generally ensuring their identity in the internet. However, Google has not yet acknowledged these European lists and when it recently withdrew its trust in Camerfirma, decided against its classification in these lists in spite of the company having provided a remedy concept and without gaining the consent of the CA/Browser Forum, hence deciding definitively and independently against the certificate provider.

As regards the third possible impediment, there were reasons which could have justified the reduction of the **validity periods** in recent years. The implementation of new certificates involved more work both for the certificate providers and the website operators. However, **circumstances could change** during a long period of validity which were decisive for issuing a certificate. Such changes could pertain to the standards applied in the issue of certificates as well as techniques used, and not least also to real-life situations such as the corruption of a certificate. In the case of certificates with short validity periods, all these changes could be taken into account on a regular basis in order to minimise the risk of incorrect certificates, ensure the website's accessibility and hence maintain the whole purpose of the certificates. Overall the **security level** of the certification process was increased, from which the internet users and ultimately also the website operators benefited, as long as the reduction of the validity periods did not generally affect the

purchase of certificates with a higher level of authentication, for which there is however no indication. These aspects were sufficient to put the theory of harm relating to the reduction of the validity periods into perspective.

At the time at which the proceeding was discontinued, it was unclear whether the possible impediments could be justified and would have required further clarification. However, the Bundeskartellamt decided not to continue its investigations but to terminate the proceeding for the reasons briefly illustrated above and for **discretionary reasons**, which are explained in more detail below.

One the one hand, the use of certificates was even stipulated by law in some security relevant areas. On the other hand, the investigations have shown that **consumers were not only unaware** of the fact that they now had to click on the icon to find out whether a more trustworthy certificate is used; they also had no knowledge of the general meaning of the previously used display features in the browser line, which certificate providers considered important and demanded that they be reinstated, and of the lock icon, which is still displayed. The fact that the way in which certificates with a higher level of authentication were displayed in the address bar in the past varied between browser providers and over time also contributed to the users not paying attention to their individual characteristics. Many users were unaware of how they could check the authentication of a website operator. This was confirmed by the lack of protest by the consumers or website operators after the information had been removed from the browser. Some of the website operators questioned even stated that the reduced display had no initial effect on their certificate procurement because their customers had not noticed the change. In addition, even the operators of reputable websites often did not invest in EV certificates. This only limited use of certificates with a higher level of authentication could also have contributed to the fact that generally a very large number of users did not recognise their added value and the website operators no longer purchased them. All in all, it would have been necessary to raise the users' awareness of the respective security indicators. Their awareness of the security indicators had probably not been sufficient to enable users to reach their own informed judgement about the identity of the website operator and for example to decide whether or not their own personal data should be handed over. Furthermore, other **possibilities of authentication** have meanwhile increased in the internet, although they do not offer an identical level of verification, nor the same guarantee of security in respect of the website operator, and may also differ in other respects.[1]

[1] There were, e.g. also differences in the authentication process (authentication of website operator by the user in the case of TLS certificates or vice-versa, such as in the case of Fast Identity Online “FIDO”) or the

A decision by the Bundeskartellamt against Google alone is unlikely to have resulted in achieving the maximum conceivable added value of more trustworthy certificates. The Bundeskaretllamt's investigations have shown that the idea of authenticating websites based on more secure certificates is fully endorsed by some IT security providers. However, a possible obligation for certain website operators to secure their websites with EV certificates or QWACs combined with a user-friendly display of the certificate information by the browsers as well as general rules pertaining to the withdrawal of trust could **only** be achieved **with legal requirements**-e.g. in the course of the revision of the eIDAS Regulation at European level. In light of these developments and not least based on an effort and benefit analysis, the proceeding against Google regarding TLS certificates and TLS providers was terminated.

time at which the authentication was carried out (actively before the use of TLS certificates or reactively in the blacklist approach as in Google Safe Browsing).