Bundeskartellamt

Fallbericht 21. Januar 2022

Verfahren gegen Google im Bereich der Transport Layer Security-Zertifikate eingestellt

Branche:	Digitalwirtschaft
Aktenzeichen:	B7-250/19
Datum:	17.01.2022

Das Bundeskartellamt hat ein kartellrechtliches Verwaltungsverfahren gegen Alphabet Inc. einschließlich der mit ihr gemäß § 36 Abs. 2 GWB verbundenen Unternehmen zur Prüfung der Untersagungsvoraussetzungen gemäß § 19 Abs. 1 GWB, Art. 102 AEUV hinsichtlich der Behandlung sogenannter höherwertiger Transport Layer Security-Zertifikate („TLS“, früher Secure Socket Layer „SSL“) durch Webbrowser aus Ermessensgründen eingestellt und Google am 17.01.2022 entsprechend informiert. Dabei ging es um die Prüfung von Hinweisen hinsichtlich der wettbewerblichen Auswirkungen der geänderten Darstellung der Informationen insbesondere über höherwertige TLS-Zertifikate in Webbrowsern, des Vertrauensentzugs gegenüber bestimmten Zertifikatsanbietern und Zertifikaten sowie der zunehmend verkürzten anerkannten Geltungsdauern der Zertifikate. Unberührt von dieser Verfahrenseinstellung bleiben die im Mai und Juni 2021 eingeleiteten Verfahren gegen Google nach den mit der 10. GWB-Novelle neu eingeführten Vorschriften für Digitalkonzerne. Nach Feststellung der überragenden marktübergreifenden Bedeutung Googles für den Wettbewerb im Sinne des § 19a Abs. 1 GWB (vgl. Pressemitteilung und Fallbericht vom 5. Januar 2022) befasst sich das Bundeskartellamt derzeit mit den Datenverarbeitungskonditionen Googles und dem Nachrichtenangebot des Google News Showcase.

TLS-Zertifikate haben zwei verschiedene Funktionen: Sie bieten eine verschlüsselte und sichere Verbindung zwischen der zertifizierten Internetseite und dem Einzelnen, der auf die Webseite zugreift. Höherwertige TLS-Zertifikate authentifizieren zudem Unternehmen, die eine Internetseite betreiben. Die TLS-Zertifikate werden von sog. Vertrauensdiensteanbietern oder Zertifizierungsstellen erstellt, die von den Browsern als vertrauenswürdig eingestuft wurden. Während sog. Domain Validated („DV“)-Zertifikate nur die Verschlüsselung bestätigen, haben die höherwertigen Organisation Validated („OV“) oder Extended Validation-Zertifikate („EV“)/Qualified

Webseite Authentification Certificates („QWACs“) zusätzlich in unterschiedlichem Maße die Authentifizierungsfunktion zur weitergehenden Absicherung des Internetauftritts vor allem gegen betrügerische Angriffe auf die Kunden der Webseitenbetreiber (Phishing oder Identitätsbetrug). Bis zum Herbst 2019 (Chrome Version 77) wurden die höherwertigen OV-/EV-Zertifikate und QWACs in der Adresszeile des Browsers Chrome kenntlich gemacht, so dass der informierte Nutzer den Webseitenbetreiber und den Zertifikatstyp dort über den Namen, den Sitz und teilweise noch zusätzliche Informationen wie z.B. Registrierungsnummern erkennen konnte. Die Hervorhebung eines höherwertigen Zertifikats erfolgte z.B. über die Nennung dieser Informationen in der Adresszeile des Browsers in grüner Farbe oder zumindest über eine Grünfärbung des Schlosssymbols in der Adresszeile. Inzwischen wird jedoch nur noch, sowohl für höherwertige als auch für DV-Zertifikate, einheitlich ein graues Schloss oder eine Warnmeldung bei Aufruf einer Webseite ohne Zertifikat angezeigt.

Für die **Einstellung** des Verfahrens sprachen neben der Unkenntnis des weit überwiegenden Teils der Internetnutzer über die Bedeutung der Zertifikate, wodurch der Mehrwert einer differenzierten Darstellung eingeschränkt wurde, auch inzwischen vorhandene andere Authentifizierungsverfahren, wenn es sich dabei auch nicht um vollständig gleichwertige Alternativen handelte. Insbesondere aber legte der Änderungsvorschlag der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt („eIDAS-VO“) vom 3. Juni 2021 (COM (2021) 281 final) fest, dass die Zertifikate durch die Webbrowser anerkannt und in einer nutzerfreundlichen Art und Weise angezeigt werden mussten, womit dem Darstellungsproblem Rechnung getragen wurde. Angesichts dessen verfolgt das Bundeskartellamt sein Verfahren auch nicht auf Basis des neuen § 19a Abs. 2 GWB weiter.

Die Alphabet Inc. ist eine im Jahr 2015 zur Umstrukturierung des bis dahin bestehenden Google-Konzerns errichtete, börsennotierte Holdinggesellschaft mit Sitz in Mountain View (USA), deren Tochtergesellschaften in verschiedenen Technologie-Bereichen tätig sind und über die Google insbesondere Internetdienste und Softwareprodukte anbietet. Das Konzernunternehmen **Google** LLC bietet seit 2008 im Softwarebereich den inzwischen weltweit am stärksten verbreiteten Browser Chrome zur Darstellung von Webseiten, Dokumenten oder allgemein Daten im Internet an. Die dem Browser Chrome ähnliche Open Source Software Chromium von Google bildet zudem die Basis für andere Browser wie Microsoft Edge und Opera.

Ein kartellrechtlicher Anfangsverdacht bestand erstens im Hinblick auf die **Verlagerung der Anzeige** der Identitätsinformationen höherwertiger Zertifikate aus der die Aufmerksamkeit des Nutzers auf sich ziehenden Adresszeile des Browsers in eine sekundäre Benutzeroberfläche. Google

und andere Browseranbieter gingen dazu über, die Benutzeroberfläche im Bereich der Adresszeile unabhängig vom Authentifizierungsumfang der hinterlegten Zertifikate visuell zu vereinheitlichen, also nicht mehr zwischen unterschiedlichen TLS-Zertifikatstypen für Webseiten zu differenzieren, sondern lediglich ein graues Schlosssymbol anzuzeigen, sofern die Webseite über irgendein gültiges Zertifikat verfügte. Eine grüne Hervorhebung des Schlosssymbols sowie der Adresszeile wurde nicht mehr unterstützt. Die Desktop-Versionen der Browser zeigten zudem den Namen des Webseitenbetreibers, einschließlich des Unternehmenssitzes via Ländercode, vor dem Uniform Ressource Locator („URL“) bei Vorliegen eines EV-Zertifikats nicht mehr an. Dadurch waren die höherwertigen Zertifikate (OV/EV/QWACs) für die Nutzer nicht mehr direkt über die Adresszeile erkennbar, sondern nur noch über einen Klick auf das Schlosssymbol, der – teilweise sogar erst über weitere Klicks – zur Anzeige der Zertifikatsinformationen führte.

Zweitens war unklar, welche Kriterien Google der Entscheidung zugrunde legte, einem Zertifikatsanbieter das Vertrauen zu entziehen. Folge des **Vertrauensentzuges** war, dass die Zertifikate des betroffenen Anbieters in Chrome nicht mehr akzeptiert wurden und statt der Webseite, die ein Zertifikat dieses Anbieters nutzte, ein Warnhinweis erschien.

Drittens bestand der Verdacht, die Anerkennung einer nur noch verkürzten **Geltungsdauer** der Zertifikate von zunächst zwei Jahren und seit September 2020 nur noch 398 Tagen, eventuell später sogar nur noch von einigen Monaten, seitens der Browser einschließlich Chrome könnte wettbewerbsrechtlich problematisch sein.

Keine der drei Entwicklungen war auf eine bedingungslose Einigung oder Entscheidung in Foren wie dem Certificate Authority („CA“)/Browser-Forum oder der Internet Engineering Task Force („IETF“) gestützt, in denen die Zertifikats- und Browseranbieter ihre Interessen zum Ausdruck bringen und an der Entwicklung von Industriestandards mitwirken können.

Die **Ermittlungen** in Form von Fragen an Google, Gesprächen mit Zertifikatsanbietern, Browseranbietern, IT-Spezialisten und Wissenschaftlern sowie schriftlichen Befragungen von Webseitenbetreibern und Zertifikatsanbietern ergaben, dass die angeführten drei Problemfelder zwischen Zertifikats- und Browseranbietern als solche tatsächlich bestanden. Ob die Verhaltensweisen Verstöße gegen Kartellrecht darstellten, wurde jedoch nicht abschließend geklärt, da das Verfahren aus den genannten Ermessensgründen eingestellt wurde.

Als betroffene **Märkte** kamen zumindest Browser- und Zertifikatsmärkte in Betracht, wobei deren genaue sachliche wie geographische Abgrenzung zunächst offenbleiben konnte. Google hätte auf Browsermärkten marktbeherrschend im Sinne des § 18 Abs. 1 i.V.m. Abs. 4, 3a und 3 GWB sein können.

Es stand im Raum, dass der Umgang Googles mit höherwertigen Zertifikaten in Chrome hinsichtlich der o.g. drei Problempunkte **Behinderungen** der Zertifikatsanbieter gemäß § 19 Abs. 1 GWB und Art. 102 AEUV zur Folge hatte.

Durch die **Streichung der Zertifikatsinformationen** aus der Adresszeile des Browsers – bis auf ein graues Schloss für jegliche TLS-Zertifikate – verloren höherwertige Zertifikate für Webseitenbetreiber an Attraktivität, zumal sie nicht, wie die weit verbreiteten DV-Zertifikate, häufig kostenlos verfügbar waren. Sie konnten seither angesichts der ohne Anzeige geringen Außenwirkung nur noch zu geringeren Preisen vertrieben werden und wurden weniger nachgefragt. Insofern könnte Google über den Browser Chrome mit der Weigerung, die Merkmale höherwertiger Zertifikate anzuzeigen, die Zertifikatsanbieter in ihrem Absatz behindert haben. Für die Webseitenbetreiber könnte durch die fehlende Anzeige die Gefahr gestiegen sein, von Phishing-Webseiten imitiert zu werden. Denn für Phishing-Seiten war es einfach, über den üblicherweise automatisierten Prozess DV-Zertifikate zu erhalten, aber wegen des dafür erforderlichen Authentifizierungsverfahrens deutlich schwieriger, höherwertige Zertifikate zu bekommen. Echte und gefälschte nur DV-zertifizierte Webseiten ließen sich nach der Änderung der Anzeige optisch kaum voneinander oder gegenüber Seiten mit höherwertigen Zertifikaten unterscheiden. Die Absicherung der Webseiten vor Fälschungen war damit schwieriger, wodurch langfristig das Vertrauen der Internetnutzer gegenüber den Webseitenbetreibern hätte sinken können. Für die Internetnutzer hätte wegen der undifferenzierten Browseranzeigen womöglich eine höhere Gefahr bestanden, Phishing-Attacken oder Identitätsbetrügen und damit Fake News zum Opfer zu fallen.

Nach dem **Vertrauensentzug Googles gegenüber einzelnen Zertifikatsanbietern** kam es in der Vergangenheit mindestens zweimal, bei Symantec, USA, einem bis dahin führenden Zertifikatsanbieter 2017/18, und bei Camerfirma, Spanien, 2021, zum kompletten Rückzug des betroffenen Anbieters aus dem TLS-Zertifikatsmarkt. Der jeweilige Vertrauensentzug führte zu einer Warnanzeige des Browsers bei Aufrufen der Webseite und beeinträchtigte dadurch nach derzeitigem Ermittlungsstand die Vermarktung der Zertifikate erheblich. Mangels umfassender allgemeingültiger Regelungen und Standards für den Vertrauensentzug und angesichts der starken Stellung Googles auf den relevanten Märkten konnte Google eigene Regeln setzen oder im Rahmen des CA/Browser-Forums zumindest maßgeblich beeinflussen, kontrollierte deren Einhaltung und entschied nach Anhörung eigenständig, ob Abhilfemaßnahmen des betroffenen Zertifikatsanbieters hinreichend waren oder ein Vertrauensentzug durch Chrome erfolgte. Ein solcher schloss angesichts der Marktposition des Chrome-Browsers nach vorläufigen Einschätzungen

der Beschlussabteilung eine wirtschaftliche Tätigkeit des Zertifikatsanbieters im TLS-Bereich danach quasi aus. Die Webseitenbetreiber mussten neue Verträge schließen, wobei eine geringere Auswahl an Zertifikatsanbietern verblieb.

Die **Verkürzung der Geltungsdauer der Zertifikate** konnte wegen der engeren Taktung der Prüfungen zu zusätzlichem Aufwand und über die Zeit damit höheren Kosten für die Zertifikatserstellung führen, insbesondere da für die Authentifizierung des Webseitenbetreibers bei höherwertigen Zertifikaten ein personeller Aufwand notwendig war, der sich im Gegensatz zu dem Prüfaufwand bei den DV-Zertifikaten nur begrenzt automatisieren ließ. In der Folge hätten die Zertifikatsanbieter möglicherweise einen Schaden in Form eines geringeren Absatzes aufgrund höherer Kosten der Webseitenbetreiber und damit der Tendenz zu anderen günstigeren Zertifikaten erlitten. Für die Webseitenbetreiber wäre zudem ein höherer Aufwand durch die häufiger erforderliche Einbindung der Zertifikate in ihre IT-Infrastruktur denkbar gewesen.

Im Rahmen einer Prüfung nach § 19 Abs. 1 GWB, Art. 102 AEUV wären die einzelnen möglichen Behinderungen der Zertifikatsanbieter durch Google im Hinblick auf ihre sachliche Rechtfertigung zu prüfen gewesen. Bei einer im Rahmen der **Rechtfertigungsprüfung** vorzunehmenden Interessenabwägung hätten nicht nur die Interessen der unmittelbar Beteiligten berücksichtigt werden müssen (Google als möglicher Normadressat und potentiell behinderte Zertifikatsanbieter). Vielmehr wären insbesondere auch die Interessen der Webseitenbetreiber und Internetnutzer sowie das öffentliche Interesse an der angemessenen Darstellung, Verfügbarkeit sowie Geltungsdauer höherwertiger Zertifikate, ggf. auch eines bestimmten Anbieters, zu berücksichtigen gewesen. Im Rahmen einer vorläufigen Würdigung stellte sich die Rechtfertigungslage bei Einstellung des Verfahrens folgendermaßen dar:

Die **Streichung der Zertifikatsinformationen** aus der Adresszeile des Browsers hätte durch den begrenzten **Platz** im Anzeigenbereich des Browsers, die nach einem **Klick** auf das Schlosssymbol noch auffindbaren Authentifizierungsinformationen sowie das Ziel Googles, für Chrome „**Sicherheit als Standard**“ anzustreben und nur auf unsichere Webseiten gesondert hinzuweisen, gerechtfertigt gewesen sein können. Das Zertifikatssystem wurde teilweise zudem als **fehleranfällig** angesehen, da die Authentifizierung bei höherwertigen Zertifikaten nicht automatisiert, sondern durch Menschen durchgeführt wurde. Zuletzt hätten anderweitig mögliche **Bekanntmachungen der Zertifikatsinhalte** außerhalb der Adresszeile der Browser die Streichung der Informationen rechtfertigen können.

Trotz des knappen **Platzes,** insbesondere dem Grund der Nichtanzeige in der begrenzteren mobilen Version des Browsers, war früher im Desktopbereich noch Raum für den Namen des Zertifikats- und Webseiteninhabers einschließlich eines Länderkürzels. Zudem nahm die Grünfärbung des Schlosses oder der Schriftzeile als Hinweis auf höherwertige Zertifikate keinen Platz in Anspruch. Diese Situation änderte sich nicht grundsätzlich. Auch Vereinheitlichungstendenzen der stationären und mobilen Versionen sprachen zumindest nicht gegen farbig gekennzeichnete Zertifikatshinweise. Der Weg, über **Klicks** auf das Schlosssymbol weitergehende Zertifikats- und Authentifizierungsinformationen zu finden, erschien umständlich. Die Informationen waren oftmals nicht benutzerfreundlich aufbereitet und die Kenntnis der Internetnutzer hinsichtlich dieser Klick-Möglichkeit war gering. Die Webseitenbetreiber wiederum verwendeten höherwertige Zertifikate, um den Internetnutzern zu demonstrieren, dass Sicherheit für sie wichtig war, und ihnen belastbare Hinweise für ihre Sicherheitsbewertung an die Hand zu geben. Auch entsprechende gesetzliche Pflichten zur Verwendung höherwertiger Zertifikate, wie in der zweiten Zahlungsdiensterichtlinie („PSD2“)-Regulierung ab Herbst 2019, bestätigten die Bedeutung entsprechender Zertifikate. Ohne die Anzeige fehlte jedoch die offensichtliche Kenntlichmachung des Zertifikats, was den möglichen Mehrwert für Nutzer wie Webseitenbetreiber nach Ermittlungen des Bundeskartellamts deutlich einschränkte und auch diesbezügliche gesetzliche Nutzungspflichten weitgehend ins Leere laufen ließ.

Die Firmenpolitik Googles, „**Sicherheit als Standard**“ anzustreben, sollte die Aufmerksamkeit des Nutzers durch konkrete Warnungen nur in Anspruch nehmen, wenn tatsächlich ein Sicherheitsrisiko bestand. Denn Studien deuteten darauf hin, dass Nutzer eher auf Warnungen als auf positive Sicherheitshinweise reagierten. Auch wenn das zuträfe, basierte der Umfang sicherheitstechnischer Maßnahmen Googles auf einer firmenspezifischen Definition der Sicherheit. Andere etablierte Mechanismen zum Schutz gegen Phishing, wie Google Safe Browsing, wirkten jedoch nicht präventiv, sondern nur reaktiv bei einer schon bekannten Phishing-Webseite. Die höherwertigen Zertifikate hätten folglich zur Authentifizierung als zusätzliches Sicherheitselement beitragen können, wenn Webseiten über leicht abgewandelte URLs die Nutzer hinsichtlich der Identität des Webseitenbetreibers täuschten. Deren fehlende Anzeige beeinträchtigte aber das Recht des informierten Nutzers, selbstverantwortlich über die Nutzung von Webdiensten auf Basis einer eigenen Risikobewertung entscheiden zu können, was auch in der eIDAS-VO und den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik („BSI“) zum Ausdruck kam und bei der Interessensabwägung zu berücksichtigen gewesen wäre.

Auch die nicht automatisierte und damit **fehleranfällige** Authentifizierung bei den höherwertigen Zertifikaten hätte die mangelnde Anzeige der Zertifikatsmerkmale in der Adresszeile insofern

nicht rechtfertigen können, als manuelle Überprüfungen bzw. Eingriffe auch in automatisierten Systemen üblich waren, insbesondere wenn sie dem Internetnutzer zusätzlichen Schutz vor Manipulationen bieten konnten. Eine relevante Behinderung schied auch nicht deshalb aus, weil die Zertifikate anderweitig hätten **bekannt gemacht** werden können. Die Berücksichtigung im Browser bildete nach den Ermittlungen der Beschlussabteilung den zentralen Anwendungsbereich für eine nicht manipulierbare und erfolgreiche Adressierung der Nutzer. Sie stellte die Schnittstelle zu jenen dar und erfüllte über eine verständliche Visualisierung ihren eigentlichen Zweck der Information über die Sicherheit einer aufgerufenen Webseite unabhängig von Manipulationsmöglichkeiten des Webseitenbetreibers. Somit bildete sie auch die Basis der Vermarktungsmöglichkeit seitens der Zertifikatsinhaber.

Der **Vertrauensentzug** Googles gegenüber einzelnen Zertifikatsanbietern als zweite mögliche Behinderung hätte durch die Gewährleistung der **Sicherheit** der Internetnutzer sowie der Webseitenbetreiber zu rechtfertigen sein können. Ein funktionierendes Zertifikatssystem setzte voraus, dass der Nutzer dem Zertifikat und damit indirekt dem Zertifikatsanbieter vertrauen kann. Berechtigte Zweifel Googles daran aufgrund fehlerhafter Zertifikate oder diesbezüglicher Prozesse hätten Gründe für einen Vertrauensentzug darstellen können.

Offen war, inwieweit die Verhaltensweisen der betroffenen Zertifikatsanbieter so bedeutend waren, dass sie tatsächlich ein **Sicherheitsrisiko** darstellten. In beiden erwähnten Fällen, Symantec und Camerfirma, gab es Anlass für eine Diskussion über die Vertrauenswürdigkeit der Anbieter. Eine weltweit anerkannte neutrale Instanz für solche Beurteilungen, bei der die Zertifikatsanbieter auch Berufung hinsichtlich der Browserentscheidungen einlegen können, existiert bisher zwar nicht. Allerdings gab es die in der eIDAS-Verordnung vorgeschriebenen European Trusted Lists, in der alle Zertifikatsanbieter aufgeführt waren, die nach einer Prüfung durch staatliche Stellen – in Deutschland die Bundesnetzagentur und das BSI – als vertrauenswürdig eingestuft wurden. In Europa wurde damit ein System betrieben, das einen Rahmen für die Prüfung der Vertrauenswürdigkeit der Anbieter und damit insgesamt für die Identitätssicherstellung im Internet bieten konnte. Google erkannte diese europäischen Listen aber bisher nicht an und entschied zuletzt bei dem Vertrauensentzug gegenüber Camerfirma entgegen der Einstufung im Rahmen dieser Listen trotz eines Abhilfekonzepts und ohne Abstimmung im CA/Browser-Forum endgültig und eigenständig gegen den Zertifikatsanbieter.

Hinsichtlich der dritten möglichen Behinderung gab es Gründe, die die in den letzten Jahren vorgenommenen Verkürzungen der **Geltungsdauern** hätten rechtfertigen können. Zwar war die Implementierung neuer Zertifikate mit einem Mehraufwand sowohl der Zertifikatsanbieter als auch

der Webseitenbetreiber verbunden. Während einer langen Geltungsdauer konnten sich jedoch die **Umstände ändern**, die für die Ausstellung eines Zertifikats maßgeblich waren. Dies konnte sowohl die Standards betreffen, nach denen Zertifikate ausgestellt wurden, als auch die Techniken, die in diesem Zusammenhang verwendet wurden, nicht zuletzt aber auch die Änderung von Lebenssachverhalten wie die Korrumpierung eines Zertifikats. Alle diese Änderungen konnten bei kurzen Geltungsdauern regelmäßig berücksichtigt werden, um so die Risiken inkorrekter Zertifikate zu minimieren, die Erreichbarkeit der Webseite sicherzustellen und somit den Sinn und Zweck der Zertifikate aufrecht zu erhalten. Insgesamt wurde das **Sicherheitslevel** der Zertifizierung erhöht, wovon die Internetnutzer und damit letztlich auch die Webseitenbetreiber profitierten, soweit die Verkürzung nicht den Kauf höherwertiger Zertifikate generell einschränkte, wofür aber keine Anhaltspunkte bestanden. Vor diesem Hintergrund wurde die Schadenstheorie hinsichtlich der Verkürzung der Geltungsdauer relativiert.

Die Rechtfertigung der möglicherweise vorliegenden Behinderungen war bei Einstellung des Verfahrens offen und hätte weiterer Aufklärung bedurft. Das Bundeskartellamt entschied jedoch, die Ermittlungen nicht fortzuführen, sondern das Verfahren aus den oben kurz aufgezählten und im Folgenden weiter ausgeführten **Ermessensgründen** einzustellen.

Die Zertifikatsnutzung war zwar in einigen sicherheitsrelevanten Bereichen sogar gesetzlich vorgeschrieben. Die Ermittlungen haben aber ergeben, dass die **Unkenntnis der Verbraucher** im Hinblick auf Zertifikate sich nicht nur auf die aktuelle Notwendigkeit weiterer Klicks zur Feststellung eines vorliegenden höherwertigen Zertifikats bezog, sondern schon allgemein auf die Bedeutung der früheren, von den Zertifikatsanbietern als wichtig erachteten und wieder geforderten Anzeigenmerkmale in der Browserzeile sowie das verbliebene Anzeigenmerkmal des Schlosses. Dass die Darstellungsweisen höherwertiger Zertifikate in der Adresszeile in der Vergangenheit zwischen Browseranbietern und im Zeitverlauf variierten, trug ebenfalls zu der Nichtbeachtung der speziellen Merkmale bei. Sehr vielen Nutzern fehlte das Bewusstsein, wie sie die Authentifizierung eines Webseitenbetreibers überprüfen konnten. Dafür sprach auch der ausgebliebene Protest der Verbraucher oder der Webseitenbetreiber nach Abschaffung der Anzeige. So gaben einige befragte Webseitenbetreiber sogar an, dass die veränderte Darstellung zunächst keine Auswirkungen auf ihren Bezug von Zertifikaten gehabt habe, da die Veränderung kundenseitig nicht bemerkt worden sei. Dazu kam, dass selbst die Betreiber reputabler Webseiten oft nicht in EV-Zertifikate investierten. Auch diese nur begrenzte Nutzung höherwertiger Zertifikate konnte dazu beigetragen haben, dass insgesamt sehr viele Nutzer ihren Mehrwert nicht erkannten und die Webseitenbetreiber sie nicht mehr kauften. Insgesamt wäre eine stärkere Sensibilisierung der Internetnutzer für entsprechende Sicherheitsindikatoren notwendig gewesen. Sie war bisher aber

wohl nicht ausreichend, um ihnen – dem Leitbild des informierten Nutzers entsprechend – zu ermöglichen, sich ein Urteil über die Identität der Webseitenbetreiber zu bilden und beispielsweise zu entscheiden, ob eigene personenbezogene Daten herausgegeben werden sollten oder nicht. Zudem gab es inzwischen zunehmend **andere Möglichkeiten zur Authentifizierung** im Internet, wenn auch nicht mit identischem Prüfungsumfang, keiner gleichen Sicherheitsgarantie hinsichtlich des Webseitenbetreibers und mit anderen Abweichungen.[1]

Eine Entscheidung des Bundeskartellamts allein gegen Google hätte absehbar nicht zu einer Ausschöpfung des denkbaren Mehrwerts höherwertiger Zertifikate geführt. Die Ermittlungen der Beschlussabteilung haben ergeben, dass die Idee der Authentifizierung über höherwertige Zertifikate in IT-Sicherheitskreisen teilweise durchaus befürwortet wird. Eine mögliche Verpflichtung bestimmter Webseitenbetreiber zur Absicherung durch EV-Zertifikate oder QWACs kombiniert mit einer nutzerfreundlich ausgestalteten Anzeige darauf hindeutender Merkmale durch die Browser sowie allgemeingültige Regelungen des Vertrauensentzugs könnten aber umfassend **nur durch gesetzliche Vorgaben** - z.B. im Rahmen der Überarbeitung der eIDAS-VO auf europäischer Ebene - erreicht werden. Vor dem Hintergrund dieser Entwicklungen und nicht zuletzt wegen des Verhältnisses des Aufwandes zum möglichen Ertrag wurde das Verfahren gegen Google hinsichtlich der TLS-Zertifikate und -Anbieter eingestellt.

[1] So unterschied sich beispielsweise zusätzlich die Authentifizierungsrichtung (Authentifizierung des Webseitenbetreibers durch den Nutzer bei TLS-Zertifikaten oder umgekehrt, wie bei der Fast Identity Online „FIDO“) oder der Erkenntniszeitpunkt der Authentifizierung (aktiv vor Nutzung bei den TLS-Zertifikaten oder reaktiv bei Blacklist-Ansätze wie Google Safe Browsing).