# Positionspapier

## Unabhängigkeit der Vertrauensdienste von Browser- und Betriebssystemherstellern

### Kontext

**SSL/TLS-Zertifikate[1] für Webserver und Clients bilden weltweit die Basis für eine verschlüsselte Kommunikation via Internet. Die Zertifikate können die Verbindung zusätzlich vertrauenswürdig gestalten, wenn sie den rechtmäßigen Betreiber einer Webseite identifizieren und den Vertrauensstatus anzeigen.**

Mit dem CA/Browser-Forum ist eine Plattform für den Austausch zwischen Zertifikatsanwendern (z.B. Browsern wie Google, Microsoft, Apple und Mozilla oder Hersteller wie CISCO) und Trustservice Provider (TSP)[2] (z.B. T-Systems, D-TRUST, HARICA, Entrust) geschaffen worden, die eine Abstimmung der gemeinsamen technischen und organisatorischen Grundsätze für definierte Zertifikatstypen (wie z.B. TLS-Zertifikate zur vertrauenswürdigen Kommunikation mit Webservern) ermöglichen soll. Dieses geschieht insbesondere, damit sich die TSP verpflichten, diese Grundsätze und Regeln (u.a. Baseline Requirements, EV[3]-Guidelines) einzuhalten. Für die TSP hat das Forum den Vorteil, dass sie über diese Plattform die abgestimmten Grundsätze mit den Zertifikatsanwendern als Gruppe vereinbaren und nicht individuell mit jedem einzeln verhandeln müssen.

Schwierigkeiten ergeben sich jedoch dort, wo durch faktische Vorgaben der Browserhersteller über die Vorgaben des CA/B-Forums hinausgehen (insb. Root Store Policies).

Dadurch können sich Browser den gemeinsam abgestimmten Vorgaben entziehen und legen den TSPs weitere individuelle Hürden auf. Aufgrund des Marktanteils der führenden Browser von über 95 Prozent sind die TSP und ihr Vertrauensstatus und damit der Kern ihres Geschäftsmodells von der Akzeptanz der Browser abhängig. Daher gibt es bisher keine Festlegung dazu, dass die Sicherheitsaudits auf Basis der ETSI[4]-Normen, genutzt von den europäischen TSP zum Nachweis ihrer Konformität, in jedem Fall von den Browsern anerkannt werden müssen. Solange dies nicht gegeben ist, besteht die

[1] SSL – Secure Socket Layer/ TLS – Transport Layer Security: Standards zur Absicherung von Kommunikation im Internet.
[2] Im Deutschen auch: Vertrauensdienstleister oder Zertifikatsherausgeber, im Englischen auch: Certificate Authorities (CA).
[3] EV= Extended-Validation-Zertifikat, https://de.wikipedia.org/wiki/Extended-Validation-Zertifikat.
[4] European Telecommunications Standards Institute.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

**Rebekka Weiß, LL.M.**
**Leiterin Vertrauen & Sicherheit**
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Gefahr, dass nur noch WebTrust-Audits[5] von nicht EU-basierten lizenzierten Wirtschaftsprüfern durchgeführt werden dürfen.

Es existiert somit bisher in dieser Gemengelage keine neutrale Entscheidungsinstanz; EU- und Verbraucherinteressen und digitale Souveränität sollten daher dringend gestärkt werden.

Zur Veranschaulichung der Situation sollen folgende aktuelle Beispiele dienen:

- Die Entfernung der besonderen Kennzeichnung von Webseiten mit gültigem EV-Zertifikat[6] in einigen Browsern schadet dem Verbrauchervertrauen. Laut einer Studie der RTWH Aachen[7] werden 99,6 Prozent der Phishing-Angriffe über Webseiten durchgeführt, die nicht mit EV-Zertifikaten gesichert sind.

- Die seit Gründung des CA/B-Forums übliche und in der Standardisierung weltweit gängige Interpretation („Was in den Richtlinien nicht explizit verboten ist, ist erlaubt.“) wird faktisch in eine international unübliche Ausprägung („Was nicht explizit durch die zugrunde liegenden Richtlinien des CA/B Forum erlaubt ist, ist dem TSP verboten.“) geändert. Dies unterminiert das Geschäftsmodel der TSP.

- Browserseitige Verkürzung der Laufzeit von TLS-Serverzertifikaten von 27 auf 13 Monate. Alle TSP, die dieser Vorgabe nicht folgen, müssen den Ausschluss aus dem Root Store des jeweiligen Browsers fürchten.

- Browserseitige Blockierung der Einführung von Legal Entity Identifiers (LEI) und Logotypes (registered trademarks) bei EV-Zertifikaten und PSD2[8] Qualifizierten Website-Authentifizierungszertifikaten (QWAC) .

- Die Browserhersteller unterstützen die Verarbeitung und Anzeige der eIDAS[9]-konformen Qualifizierten Website-Authentifizierungszertifikate (QWAC) nicht.

Aus diesen Punkten lässt sich ableiten, dass eine starke Abhängigkeit der grundlegenden digitalen Sicherheitsinfrastrukturen von den Browserherstellern besteht. Eine europäische

[5] WebTrust ist ein Prüfprogramm für Trustservice Provider der Chartered Professional Accountants Canada (CPA Canada) – kanadische Wirtschaftsprüfer.
[6] Extended-Validation-Zertifikat, https://de.wikipedia.org/wiki/Extended-Validation-Zertifikat
[7] https://www.usenix.org/system/files/soups2019-drury.pdf.
[8] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt.
[9] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Digitalpolitik, welche die digitale Souveränität der Bürger und der Wirtschaft in Europa sicherstellt, sollte diese Aspekte daher nun in den Blick nehmen. Es besteht andernfalls ein erhebliches Risiko, dass dieser Markt den europäischen Anbietern entzogen und dadurch die Schaffung eines digitalen Binnenmarktes weiter erschwert wird.

Die Bedeutung digitaler Souveränität der Bürger, der öffentlichen Verwaltung und der Wirtschaft in Europa wird anhand der vorgenannten Beispiele sehr plastisch. Abhängigkeiten sollten daher abgebaut und neuer Konsens zwischen allen Beteiligten hergestellt werden, um kooperatives, globales Arbeiten im Kontext sicherer Internetinfrastrukturen sicherzustellen. Dies würde gleichzeitig das durch die EU-Verordnung eIDAS angestrebte Ziel eines digitalen europäischen Binnenmarktes stärken.

**Konkrete Auswirkungen**

Aus Anwenderperspektive wird das Erkennen von Gefahren in der Onlinekommunikation deutlich erschwert, für Laien wird es nahezu unmöglich gemacht. Optische Kennzeichen in Browsern, anhand derer sich die Vertrauenswürdigkeit von Webseiten bewerten ließe, fehlen zukünftig (z. B. die grüne Adressleiste, das gelbes Schloss). Für den Verbraucher ist es nicht möglich, die Identität der Kommunikationsgegenstelle zu verifizieren. Er ist dadurch starken Angriffen, etwa durch Phishing, ausgesetzt, was eine Herausforderung für den Verbraucherschutz darstellt (jüngstes Beispiel sind gefälschte Webseiten zur Corona-Hilfe). Eine Nutzung der im europäischen Rechtsrahmen (EU-Verordnung eIDAS) definierten besonders vertrauenswürdigen Qualifizierten Website-Authentifizierungszertifikate (QWAC)[10] ist, aufgrund des Fehlens der Unterstützung der dort etablierten EU-Trusted List[11], nur sehr eingeschränkt möglich. Daher sind Zertifikate als solche ausschließlich für Experten erkennbar. Verbraucher können heute nicht erkennen, wer für die Verschlüsselung der Kommunikationsverbindung im Sinne der europäischen Datenschutzgrundverordnung (GDPR) verantwortlich ist.

**Lösungsmöglichkeiten**

Im Sinne eines einheitlichen digitalen europäischen Binnenmarktes und einer konsequenten Durchsetzung der Ziele der europäischen Datenschutzgrundverordnung, insbesondere im Rahmen der deutschen EU-Ratspräsidentschaft, halten wir die folgenden Ziele für angemessen:

- Prüfung von Maßnahmen zur Schaffung einer europäischen Unabhängigkeit von den aktuell marktbeherrschenden Browsern.

[10] Verordnung (EU) Nr. 910/2014, Artikel 45.
[11] Verordnung (EU) Nr. 910/2014, Artikel 22.

- Förderung der verpflichtenden Nutzung von QWAC für die verschlüsselte, vertrauenswürdige und identitätsbezogene Kommunikation in nationalen und europäischen Rechtsakten.

- Umfassende Anwendung der durch die eIDAS definierten Rahmenbedingungen für TLS-Zertifikate: Nutzung EU-weiter Standards wie ETSI EN 319 411, eigenständige Überprüfung der Einhaltung und eigenständig regulierte Sanktionierung durch die bereits zuständigen Aufsichtsbehörden.

- Aus Anwenderperspektive: Verlässliche Visualisierung des Sicherheitsstatus und des Vertrauensniveaus der Identität in zertifikatsanwendenden Systemen (u. a. durch Verwendung des „EU trust mark for qualified trust services[12]“).

- Im Zuge der Novellierung der eIDAS-Verordnung im Jahr 2020 soll eine Stärkung des durch eIDAS-Vertrauensdienste garantierten hohen Qualitätsniveaus durch klare Abgrenzung gegenüber anderen Diensten vereinbart werden, um einer Verwässerung des Vertrauensstatus durch stark vereinfachte Kriterien entgegenzuwirken.

[12] Durchführungsverordnung (EU) 2015/806 der Kommission vom 22. Mai 2015.

**Mittel zur Erreichung der vorgeschlagenen Lösungen**

Vor dem Hintergrund einer Reaktion auf die bestehende Situation und der sich daraus ergebenden Gefahren, halten wir die folgenden Lösungsvarianten, die auf europäischer Ebene angestoßen werden sollten, für vielversprechend, um die hier definierten Ziele zu erreichen:

- Schaffung eines kräftigen Hebels durch die Entwicklung eines EU-Browsers mit eigenem EU Root Store (auf Basis von Open Source).
- Verpflichtung zur geschützten und vertrauenswürdigen Prüfung der Zertifikate sowie zur verständlichen und vertrauenswürdigen Visualisierung/Kennzeichnung für den Anwender.
- Verpflichtende Unterstützung der eIDAS Artikel 22 (EU Trusted List) durch die Browser Root Stores.
- Verschärfte Überwachung der Aktivitäten der marktbeherrschenden Browser im Hinblick auf Missbrauch der Marktposition und Unterwanderung der IT-Sicherheit der europäischen Konsumenten (Verbraucherschutz!) und Industrien mit besonderem Augenmerk auf den Verbleib von europäischen TSP in den Root Stores.
- Transparente Gestaltung von ETSI-Standards für vertrauenswürdige Identitätsdaten in TLS-Zertifikaten, wie z.B. EV- oder QWAC-Zertifikaten, zum Schutz der Konsumenten z.B. vor Phishing-Angriffen.
- Koordinierung einer europäischen Interessensgemeinschaft z.B. durch die ENISA, die europäische Aspekte (u.a. eIDAS, QWAC, EU-Regularien, ETSI, ...) vertritt. Bitkom bietet sich hier gerne als Partner an.

Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.