Position paper

Independence of Trust Services Providers from Browser and Operating Systems

Context

SSL/TLS certificates[1] for web servers and clients around the world constitute the basis for encrypted communication via Internet. In addition, the certificates can structure connections in a trustworthy way if they identify the legitimate operator of a website and indicate the trust status.

With the CA/Browser Forum, a platform has been created for exchange between users of certificates (e.g. browsers such as Google, Microsoft, Apple and Mozilla or manufacturers such as CISCO) and trust service providers (TSPs)[2] which seeks to enable coordination of common technical and organisational principles for defined types of certificate (e.g. TLS certificates for trustworthy communication with web servers). This occurs in particular so that TSPs undertake to comply with these principles and rules (including baseline requirements, EV guidelines). For TSPs, the Forum has the advantage that they can agree coordinated principles with certificate users as a group via this platform and do not need to negotiate individually with each one.

Difficulties arise where the de facto requirements of browser manufacturers go beyond the scope of the CA/B Forum (in particular root store policies).

As a result, browsers can exempt themselves from the commonly coordinated principles and impose further individual hurdles on TSPs. Given that the market share of the leading browsers exceeds 95%, TSPs and their trust status – and hence the core of their business model – they are dependent on acceptance by browsers. Accordingly, it has not so far been established that security audits on the basis of ETSI[3] standards, used by European TSPs to demonstrate their conformity, have to be recognised by the browsers in every case. Until then, there is a danger that the only audits still possible are WebTrust audits[4] performed by accountants not based in the EU.

[1] SSL – Secure Socket Layer/ TLS – Transport Layer Security: standards to safeguard communication in the Internet.
[2] Alternatively known in German as “Vertrauensdienstleister” or “Zertifikatsherausgeber”, also called certificate authorities (CA) in English.
[3] European Telecommunications Standards Institute.
[4] WebTrust is an audit program for trust service providers developed by Chartered Professional Accountants Canada (CPA Canada).

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

Rebekka Weiß, LL.M.
Head of Trust & Security
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

This means that there is no neutral decision-making body in this conflict situation; it is therefore urgently necessary to strengthen EU and consumer interests and digital sovereignty.

The following topical examples serve to illustrate the situation:

- Removal of the special labelling of websites with a valid EV certificate[5] in some browsers damages consumer confidence. According to a study by RTWH Aachen[6], 99.6% of phishing attacks are carried out via websites which are not covered by EV certificates.

- The interpretation which has been taken as the norm since creation of the CA/B Forum and is accepted worldwide in the field of standardisation ("everything that is not explicitly banned is allowed") has been transformed into the exact converse: "TSPs are banned from everything that is not explicitly allowed in the guidelines underlying the CA/B Forum". This undermines the TSP business model.

- Shortening by browsers of the validity of TLS server certificates from 27 to 13 months. All TSPs which fail to comply with this must fear being excluded from the root store of the browser in question.

- Blocking by browsers of the inclusion of Legal Entity Identifiers (LEI) und logo types (registered trademarks) in EV certificates and PSD2[7] qualified website authentication certificates (QWAC).

- Browser manufacturers do not support the processing and display of eIDAS[8]-compliant qualified website authentication certificates (QWAC).

This shows that fundamental digital security infrastructures are in a situation of strong dependence on browser manufacturers. A European digital policy which secures the digital sovereignty of citizens and businesses in Europe should therefore now focus on these aspects. Otherwise there is a considerable risk that this market will be closed to European providers and thus the creation of a digital single market will be rendered even more difficult.

[5] Extended validation certificate, https://de.wikipedia.org/wiki/Extended-Validation-Zertifikat
[6] https://www.usenix.org/system/files/soups2019-drury.pdf.
[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.
[8] Regulation (EU) no. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC.

The examples set out above highlight the importance of digital sovereignty for citizens, public administrations and businesses in Europe. Situations of dependence should therefore be dismantled and a new consensus reached between all stakeholders in order to ensure cooperative global work in the context of secure Internet infrastructures. At the same time, this would serve the objective pursued by the EU eIDAS regulation of a European digital single market.

Concrete effects

From the perspective of users, recognising dangers in online communication is made markedly more difficult, whereas for non-specialists it has become almost impossible. Optical labels in browsers intended to enable users to evaluate the trustworthiness of websites will be absent in the future (e.g. green address bar, “Gelbes Schloss” (German yellow lock system). It is not possible for the consumer to verify the identity of a communication counterpart. He or she is therefore exposed to strong phishing and other attacks, posing a challenge for consumer protection (the most recent example is fake websites on corona assistance). Use of the particularly trustworthy qualified website authentication certificates (QWAC)[9] defined in the European legislative framework (EU eIDAS regulation) is possible only to a very limited extent due to the absence of support for the EU trusted lists it establishes[10]. This means that certificates can be recognised as such only by experts. Consumers are today unable to recognise who is responsible for encryption of the communication link within the meaning of the European General Data Protection Regulation (GDPR).

Possible solutions

With a view to a harmonised European digital single market and consistent enforcement of the objectives of the GDPR, in particular in the framework of the German EU Council Presidency, we believe that the following objectives are appropriate:

- Exploration of measures to create European independence from the browsers which currently dominate the market.
- Promotion of the compulsory use of QWAC for encrypted, trustworthy and identity-related communication in national and European legislative acts.
- Comprehensive application of the framework conditions for TLS certificates defined in eIDAS: use of EU-wide standards such as ETSI EN 319 411, independent

[9] Regulation (EU) no. 910/2014, article 45.
[10] Regulation (EU) no. 910/2014, article 22.

compliance monitoring and independently regulated penalties through existing competent supervisory authorities.

- For users: reliable visualisation of security status and identity trust level in systems which use certificates (inter alia through use of the EU trust mark for qualified trust services[11]).

- As part of the process of amending the eIDAS regulation in 2020, a strengthening of the high quality level guaranteed by eIDAS trust services should be agreed through a clear delimitation vis-à-vis other services in order to work against a dilution of the trust status due to greatly simplified criteria.

Means to achieve the proposed solutions

Against the background of a reaction to the existing situation and the concomitant dangers, we believe that the following steps are important and should be initiated at European level as they hold great promise for achieving the objectives defined above:

- Strengthening sovereignty through development of an EU browser with its own EU root store (on the basis of open source).

- Obligation to have protected and trustworthy verification of certificates as well as comprehensible and trustworthy visualisation/labelling for the user.

- Obligation for browser root stores to support eIDAS article 22 (EU trusted lists).

- Adequate Supervision of the activities of browsers with market dominance with regard to abuse of market position and undermining the IT security of European consumers (consumer protection) and businesses with particular attention to the location of European TSPs in root stores.

- Transparent design of ETSI standards for trustworthy identity data in TLS certificates, for example EV or QWAC certificates to protect consumers against phishing and other attacks.

- Coordination of a European interest group, e.g. by ENISA, which represents European aspects (inter alia eIDAS, QWAC, EU rules, ETSI, etc.). Bitkom could act as a partner in this regard.

[11] Commission implementing regulation (EU) 2015/806 of 22 May 2015.

Bitkom represents more than 2,700 businesses in the digital economy, including more than 1,900 direct members. Their annual turnover for IT and telecommunications services alone is 190 billion Euro, including exports of 50 billion Euro. Bitkom members employ more than 2 million people in Germany. These members number more than 1,000 small and medium-sized enterprises, over 500 start-ups and virtually all global players. They offer software, IT services, telecommunications or Internet services, manufacture devices and components, are active in the area of digital media or form part of the digital economy in some other way. 80% of the companies have their head office in Germany, while 8% each come from Europe and the USA, and 4% from other regions. Bitkom promotes and drives the digital transformation of the German economy, and champions broad involvement of society in digital developments. The objective is to make Germany one of the world's leading digital business locations.