April 6, 2022

Re: Concerns Regarding the Revised Article 45 of e-ID Draft Legislative Proposal

Dear distinguished Members of the European Parliament and Representatives of the Council of the European Union,

Thank you for the opportunity to comment on the EU draft proposal to amend the 2014 Electronic Identification, Authentication and Trust Services (eIDAS) Regulation. We offer these comments in our individual and personal capacities. We embrace the goal of the proposed framework to increase interoperability within the EU and to make it easier to maintain safe and secure digital identities. However, we would like to point to a specific provision within the draft proposal that, if adopted as is, would undermine web security.

Under the revised Article 45, browsers will be forced to accept, without reservation, a system of Qualified Web Authentication Certificates (QWACs) from Certificate Authorities (CAs) or Trust Service Providers (TSPs). Unfortunately, this technical requirement is problematic as security teams' must respond at the speed of evolving cybersecurity threats and incidents, and not be stifled by a legislative provision that would hamper such a timely response.

This legislation will have a global impact, even if unintended. Moreover, if other jurisdictions adopt similar but conflicting dictates, we don't see how browser providers and others using Transport Layer Security (TLS)[1] will be able to conform. CA certificates can refer to any identifier, not only domain names. TLS can be used for other than domain name authentication. While well-intended, this legislation does not take into account the scope of use of these techniques and the consequent scope of effect the legislation will have on the operational Internet.

In their present form, QWACs — like Extended Validation (EV) certificates on which they are based — hinder the rapid secure deployment of websites, while providing no benefit to user security.[2] Advocates like the Electronic Frontier Foundation, EFF, have said that requiring QWACs is problematic because, simply put, they have been "debunked as an effective way to

[1] Transport Layer Security is one of the Internet's ways of using cryptography to preserve confidentiality while information is in transit on the Internet.

[2] ETSI, Electronic Signatures and Infrastructures (ESI), Certificate Profile for Web Site Certificates. November 2021, https://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.02.01_60/en_31941204v010201p.pdf.

convey security to users."[3] For example, currently, if a user wants to visit Europa.eu, a web browser must reliably ensure that the user is communicating with the domain 'Europa.eu', and not an attacker on the network impersonating the European Commission's domain.[4]

Every new CA/TSP trusted by a browser increases risk to that browsers' users, as the trusted CA/TSP can issue certificates that are capable of impersonating or intercepting traffic for any website on the Internet. Faulty CAs/TSPs can lead to privacy harms, greater risk of identity and user credential theft, financial crimes, and an overall loss of trust in online services.

This is why today, every CA/TSP is subjected to a rigorous vendor security analysis by browser and operating systems providers to ensure that the high security expectations of their users are met. They are assisted in this assessment by independent third-party audit services, such as developed by WebTrust or ETSI ESI, who provide baseline assurance on which browser and operating system providers build.[5] Article 45 in its current form would undermine this rigorous process already in use by browsers. The Internet Society, ISOC, notes that "Mandating browsers to include CAs authorized by national governments into their root stores, without guaranteeing security parity with current best practices, poses a significant risk to the global Internet."[6]

Many of the current challenges for QWACs have to do with current technical specifications.[7] We believe that there's an opportunity to address the challenges with QWACs, by continuing to work to improve the technical specifications to address these concerns. However, this will require time and innovations in security, ensuring QWACs achieve the desired technological benefits the EU Digital Identity Framework intends. For this reason we believe that Article 45 should be amended to *enable* this future work, rather than to prematurely *mandate* technically flawed mechanisms.

We believe we are working with you towards a common objective, which is to make individuals safer on the Internet — but the conflation of the use of TLS with the validation of a domain

[3] EFF, What the Duck? Why an EU Proposal to Require "QWACs" Will Hurt Internet Security, February 2022, https://www.eff.org/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security, and Global website security ecosystem at risk from EU Digital Identity framework's new website authentication provisions, March 2022, https://www.eff.org/files/2022/03/02/eidas_cybersecurity_community_open_letter_1_1.pdf.

[4] Mozilla, EU Digital Identity framework (eIDAS), November 2021, https://blog.mozilla.org/netpolicy/files/2021/11/eIDAS-Position-paper-Mozilla-.pdf.

[5] For more information visit https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services , and https://www.etsi.org/about.

[6] ISOC, Internet Impact Brief: Mandated Browser Root Certificates in the European Union's eIDAS Regulation on the Internet, November 2021, https://www.internetsociety.org/resources/doc/2021/internet-impact-brief-mandated-browser-root-certificates-in-the-eu-eidas-regulation/.

[7] CDT, An Overzealous Proposal for EU's Digital Identity Would Undermine, Not Fix, Online Trust, March 2022, https://cdt.org/insights/an-overzealous-proposal-for-eus-digital-identity-would-undermine-not-fix-online-trust/.

name must be disambiguated because, as drafted within Article 45, this legislation can mislead users as to the identity of the sites they visit. How can we take advantage of our respective experiences in this space, to achieve an effective result which doesn't inadvertently mislead users?

We look forward to speaking with you more about these issues, and others critical to the future of the Internet!

Sincerely,

Vint Cerf, Internet Pioneer and Former Chairman of ICANN
Andrew Sullivan, President and CEO of the Internet Society
Paul Mockapetris, Inventor of the Internet Domain Name System
Russ Housley, former Chairman of the Internet Engineering Task Force
Steve Crocker, Internet Pioneer and Former Chairman of ICANN
Susan Landau, The Fletcher School and School of Engineering, Tufts University
Mirja Kuehlewind, Chairman of the Internet Architecture Board
Wes Hardaker, Member of the Internet Architecture Board
David Schinazi, Member of the Internet Architecture Board
Mallory Knodel, Member of the Internet Architecture Board
Steve Bellovin, Former Member of the Internet Architecture Board
Jiankang Yao, Member of the Internet Architecture Board