3 March 2022

Global website security ecosystem at risk from EU Digital Identity framework's new website authentication provisions

Dear Honourable Member of the European Parliament,
Dear Member of TELE Working Party,

We the undersigned are cybersecurity researchers, advocates, and practitioners. We write to you, in our individual capacities, to raise grave concerns regarding certain provisions of the legislative proposal for a European Digital Identity framework (the 'eIDAS revision'), and their impact on security on the web.

While we understand that the intent of these provisions is to improve authentication on the web, they would in practice have the opposite effect of dramatically weakening web security. At a time when two-thirds of Europeans are concerned about being a victim of online identity theft and over one-third believe they are not able to sufficiently protect themselves against cybercrime, weakening the website security ecosystem is an untenable risk.[1] We therefore urge you to amend the revised Article 45.2 to **ensure that browsers can continue to undertake crucial security work** to protect individuals from cybercrime on the web.

Website authentication - a cornerstone of security online

Website authentication is a cornerstone of security online, driving e-commerce and enabling billions of secure interactions in the EU and around the world. Authentication ensures that data and information is sent to the correct recipients, and not to cybercriminals who impersonate domain names. In real terms, this mechanism protects individuals from identity theft, financial crime, malware, and surveillance. It is a crucial building block of digital society, and the basis for e-commerce and e-government. In practical terms, this authentication function is provided by **website certificates**, which attest to the identity of the website.

Website certificates are issued by **certificate authorities**. If a certificate authority issues certificates to entities to whom it should not – whether as a result of poor security and operational standards, or malign intent – the consequences for web users can be catastrophic. For that reason, certificate authorities must be rigorously vetted before their certificates are trusted. This vetting is performed by web browser makers on behalf of their users, with each browser

[1]European Commission (2020) 'Europeans' attitudes towards cyber security (cybercrime)' In: Eurobarometer 499. Available at: https://europa.eu/eurobarometer/surveys/detail/2249

setting policies that certificate authorities must meet to be included in their 'root program' and thus trusted by that browser.

The Digital Identity framework's approach

The Digital Identity framework includes provisions that are intended to increase the take-up of **Qualified Website Authentication Certificates** (QWACs), a specific EU form of website certificate that was created in the 2014 eIDAS regulation but which – owing to flaws with its technical implementation model – has not gained popularity in the web ecosystem. The Digital Identity framework mandates browsers accept QWACs issued by Trust Service Providers, **regardless of the security characteristics of the certificates or the policies that govern their issuance.**[2] This legislative approach introduces significant weaknesses into the global multi-stakeholder ecosystem for securing web browsing, and will significantly increase the cybersecurity risks for users of the web.

Security Implications

Most immediately, these provisions will **make it more difficult to protect individuals from cybercriminals.** As noted above, weaknesses in website authentication – whereby bad actors can impersonate legitimate websites or intercept data in transit – are a key vector for identity theft and financial crime. Most web browsers have rigorous security standards around website certificates *precisely because* of the risk to individuals that will arise from vulnerabilities in this ecosystem. By allowing some website certificates to bypass existing security standards, the revised Article 45 increases the risk that insecure or malicious certificates will be issued to cybercriminals and make it impossible for the cybersecurity community to quickly respond when certificates are found to pose a risk to web users**.**

More broadly, the policy approach with the revised Article 45 **signals a dangerous cybersecurity policy trend**. It compels private actors to forgo their duty to those who use their products and services, by assuming that because government-appointed Certificate Authorities are subject to government security standards, they can pose no cybersecurity risk. This approach of requiring private actors to divest themselves of responsibility for their products' security runs counter to established norms in cybersecurity as well as in risk management across domains. In the field of cybersecurity in particular, where threats evolve constantly and real-time operational responses are essential, regulatory frameworks should not have the effect of *preventing* vendors from taking security measures in the interest of their users.

---

[2] European Commission (2021), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, paragraph 38 (revising article 45 of EU 910/2014). Available at:
https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

Conclusion and recommendations

While we understand that the intent of these revisions is to improve authentication on the web, they would, in practice, have the opposite effect. By creating a means to bypass existing security vetting practices in browsers, the proposed regulation would expose users to increased risk of attack from cybercriminals.

We therefore urge you to amend the revised Article 45.2 to **ensure that browsers can continue to undertake their crucial security work** to protect individuals from cybercrime on the web.

Sincerely,

(affiliation for identification purposes only)

David Awad, Faculty Instructional Associate of Computer Science, Georgia Tech

Andrew Ayer, SSLMate

Gilles Barthe, Max Planck Institute for Security and Privacy, Germany

Daniel J. Bernstein, Research Professor, University of Illinois at Chicago, USA; Ruhr University Bochum, Germany; Academia Sinica, Taiwan

Karthikeyan Bhargavan, Researcher, Inria Paris

Dan Boneh, Professor of Computer Science, Stanford University

Jon Callas, Director of Tech Projects, Electronic Frontier Foundation

Stephen Checkoway, Assistant Professor of Computer Science, Oberlin College

Cas Cremers, Professor of Computer Science, CISPA Helmholtz Center for Information Security

Claudia Diaz, KU Leuven

Zakir Durumeric, Assistant Professor of Computer Science, Stanford University

Roya Ensafi, Assistant Professor of Computer Science and Engineering, University of Michigan

Ian Goldberg, Professor of Computer Science, University of Waterloo, Canada

Seda Gürses, Associate Professor, Faculty of Technology, Policy and Management, TU Delft

Joseph Lorenzo Hall, PhD, Internet Society

J. Alex Halderman, Professor of Computer Science and Engineering and Director of the Center for Information Security and Society, University of Michigan

Alexis Hancock, Director of Engineering, Certbot, Electronic Frontier Foundation

Dr.-Ing. Mario Heiderich, Cure53

Scott Helme, BSc (Hons), Report URI, Security Headers

Tibor Jager, Professor of Computer Science, University of Wuppertal, Germany

Martin Johns, Professor of Computer Science, TU Braunschweig

Mallory Knodel, Center for Democracy & Technology

Tanja Lange, Professor Cryptology, Eindhoven University of Technology, Netherlands and visiting professor AcademiaSinica, Taiwan

Thyla van der Merwe, ETH Zurich

Alec Muffett, Security Researcher

Dr Lukasz Olejnik, independent researcher

Kenneth Paterson, Professor of Computer Science, ETH Zurich

Mark D. Ryan, Professor of Computer Science, University of Birmingham, UK

Peter Schwabe, Tenured Faculty at MPI-SP & Professor at Radboud University

Wendy Seltzer, World Wide Web Consortium

Hovav Shacham, Professor of Computer Science, The University of Texas at Austin

Adam Shostack, Author, Threat Modeling Designing for Security. USA

Nigel Smart, Professor, KU Leuven, Belgium

Eugene H. Spafford, Professor of Computer Science, Purdue University

Carmela Troncoso, EPFL, Switzerland

Michael Veale, Associate Professor of Digital Rights and Regulation, University College London, UK

Kenneth White, Open Crypto Audit Project

Daniel Zappala, Professor of Computer Science, Brigham Young University