eIDAS regulation 2.0: the trilogue outcome is still unacceptable

23 November 2023

At the beginning of November 2023, more than 500 scientists and numerous NGOs signed an open letter (https://eidas-open-letter.org) expressing serious concerns about the upcoming eiDAS 2.0 regulation (Regulation on electronic identification and trust services for electronic transactions in the internal market). The focal point of the letter was that the regulation opens the door to mass surveillance of citizens by Member States – while the European Court of Justice has repeatedly pointed out that mass surveillance would violate the fundamental right to privacy.

As a consequence of the public debate following our letter, the regulation was revised. On 8 November, the European Commission announced the completion of the negotiations. The agreed draft (https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf) was released by the ITRE committee on 16 November, twelve days before the vote in the ITRE committee of the EU parliament on 28 November.

We have carefully studied the outcome of the trilogue, and we are pleased to see that the text has been moving in the right direction. Unfortunately – despite the claims by the European Commission (https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_2664) – we do not believe that our concerns with respect to mass surveillance have been addressed in a satisfactory way.

We will try to clarify why without repeating the detailed arguments from the open letter.

The revised draft of the regulation intends to provide additional safeguards against mass surveillance by adding a clause stating that its goal is "*not to affect the freedom of web-browser providers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate*." Unfortunately, this protection is only included in Recital 32 rather than in Art. 45. Legal experts have pointed out that text in a recital has very limited legal value while the inclusion of this text in Art. 45 would have been a strong guarantee for the protection of the right to privacy.

A second clarification was added to Recital 32 stating that *"web-browsers should not deny the authenticity of qualified certificates for website authentication* ***for the sole purpose*** *of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued and confirming the identity of that person*." This has been interpreted by some as implying that Qualified Web Authentication Certificates (QWACs) would not be used to protect the encryption between the browser and web server. In the TLS protocol, website authentication is intricately linked to the protection of the connection with encryption and this is also the interpretation in the current standards for QWACs. It would be possible to develop a new standard that separates the linkage from the domain name to the legal identity provided by a QWACs certificate from the TLS certificate that links a domain name to a public key. This

would require a strong mandate to create such a standard. Similar to the previous statement, the legal value seems to be limited in any case.

Finally, the mobile wallet part of the regulation mentions in multiple places the need for the European Digital Identity Wallet to protect privacy, including data minimization, and prevention of profiling. However, our concerns remain that the draft regulation still enables large-scale tracking of citizens based on government-issued identifiers. Our concern that unobservability (towards the Wallet provider) and unlinkability are not sufficiently assured has not been addressed: this means the technical implementation will decide on core privacy safeguards and that relying parties will choose the Member State with the weakest protection. The current reference architecture does not use the state-of-the-art technologies such as anonymous credentials that have been developed more than 20 years ago. It is clear that, once mobile wallets are rolled out on a large scale, it will become exceedingly difficult to make further changes.

In view of the above, we strongly urge the European Parliament to condition the adoption of the outcome of the trilogue agreement on the prior publication by the European Commision and the Council of a clear and unambiguous mandate for the European Standardization bodies to draft standards that i) ensure that there will be no interference with how connections with web servers are authenticated, or the technology used to encrypt web traffic and instead only apply to displayed identity information and ii) guarantee strong unobservability and unlinkability for mobile identity wallet users. The European Parliament should also use its powers and dedicate resources to closely monitor the implementation of the regulation.

If those additional guarantees are not offered, we cannot recommend that the Members of the European Parliament accept the current draft. We acknowledge that it contains several positive elements, such as discrimination protection, use-case regulation and a right to pseudonymity, which are missing in most national digital identity frameworks. But we also believe that it does not adequately respect the right to privacy of citizens and secure online communications and it substantially increases the risk of harm.

Sincerely,

Dr. Ali Abbasi, CISPA Helmholtz Center for Information Security, Germany

Dr. Aysajan Abidin, KU Leuven, Belgium

Prof. Elena Andreeva, TU Wien, Austria

Dr. Daniele Antonioli EURECOM, France

Prof. Giovanni Apruzzese, University of Liechtenstein, Liechtenstein

Prof. Diego F. Aranha, Aarhus University, Denmark

Prof. Manuel Barbosa, University of Porto, Portugal

Prof. Diogo Barradas, University of Waterloo, Canada

Prof. Olivier Blazy, École Polytechnique, France

Dr. Ian Brown Visiting Professor, Fundação Getulio Vargas, Brazil
Prof. Christopher Brzuska, Aalto University, Finland
Dr. Anne Canteaut, Inria, France
Prof. Srdjan Capkun, ETHZ, Switzerland
Sofía Celi, Brave, Portugal
Prof. Nicolas Christin, Carnegie Mellon University, United States of America
Dr. Véronique Cortier, CNRS, France
Prof. Cas Cremers, CISPA Helmholtz Center for Information Security, Germany
Prof. Claudia Diaz, KU Leuven, Belgium
Prof. Enrique Soriano-Salvador, Universidad Rey Juan Carlos, Spain
Prof. Jordi Domingo, UPC Barcelona, Spain
Prof. Orr Dunkelman, co-director Center for Cyber, Law and Policy, University of Haifa, Israel
Dr. Stephen Farrell, Trinity College Dublin, Ireland
Prof. Aurélien Francillon, EURECOM, France
Prof. Gilbert Fridgen, University of Luxembourg
Prof. Kevin Gallagher, NOVA School of Science and Technology, Portugal
Prof. Kristian Gjøsteen, NTNU, Norway
Dr. Maximilian Golla, CISPA Helmholtz Center for Information Security, Germany
Dr. Seda F. Gurses, TU Delft, The Netherlands
Prof. Daniel Gruss, TU Graz, Austria
Prof. Hamed Haddadi , Imperial College London
Prof. Kimmo Halunen, University of Oulu, Finland
Prof. Tibor Jager, University of Wuppertal, Germany
Dr. Philipp Jovanovic, University College London, UK
Prof. Stefan Katzenbeisser, University of Passau, Germany
Prof. Miroslaw Kutylowski, NASK-National Research Institute, Warsaw, Poland
Prof. Susan Landau, Tufts University, USA
Prof. Tanja Lange, TU Eindhoven, The Netherlands
Prof. Anja Lehmann, Hasso-Plattner-Institute, University of Potsdam, Germany
Prof. Douglas Leith, Trinity College Dublin, Ireland
Dr. Gaëtan Leurent, Inria, France
Dr. Wouter Lueks, CISPA Helmholtz Center for Information Security, Germany
Prof. Matteo Maffei, TU Wien, Austria
Prof. David Malone, Maynooth University, Ireland
Prof. Vashek Matyas, Masaryk University, Czech Republic

Prof. Jan Tobias Muehlberg, ULB, Belgium

Prof. Steven J. Murdoch, University College London, UK

Prof. Claudio Orlandi, Aarhus University, Denmark

Prof. Panos Papadimitratos, KTH Royal Institute of Technology, Stockholm, Sweden

Dr. Giancarlo Pellegrino, CISPA Helmholtz Center for Information Security, Germany

Prof. Olivier Pereira, UCLouvain, Belgium

Prof. Günter Pernul, University of Regensburg, Germany

Prof. Thomas Peters, UCLouvain, Belgium

Prof. Bart Preneel, KU Leuven, Belgium

Dr. Tobias Pulls, Karlstad University, Sweden

Prof. Jean-Jacques Quisquater, UC Louvain, Belgium

Prof. Dr. Kai Rannenberg, Goethe University Frankfurt, DE

Prof. Kasper Rasmussen, University of Oxford, UK

Dr. Raphael M. Reischuk, National Test Institute for Cybersecurity and Zühlke Engineering AG, Switzerland

Prof. Moritz Riede, University of Oxford, UK

Prof. Ronald L. Rivest, MIT, United States of America

Prof. Eyal Ronen, Tel Aviv University, Israel

Prof. Peter Y A Ryan, University of Luxembourg, Luxembourg

Prof. Nuno Santos, INESC-ID / Instituto Superior Técnico, University of Lisbon, Portugal

Dr. Kris Shrishak, Senior Fellow at the Irish Council for Civil Liberties, Ireland

Prof. Thomas Schneider, TU Darmstadt, Germany

Prof. Peter Schwabe, MPI-SP Germany & Radboud University, The Netherlands

Dr. Johannes Sedlmeir, University of Luxembourg

Prof. Nigel Smart, KU Leuven, Belgium

Dr. David M. Sommer, Zühlke Engineering AG, Switzerland

Prof. François-Xavier Standaert, UC Louvain, Belgium

Dr.-Ing. Ben Stock, CISPA Helmholtz Center for Information Security, Germany

Prof. Juan Tapiador, Universidad Carlos III de Madrid, Spain

Prof Cihangir Tezcan, MIddle East Technical University, Turkey

Dr. Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security, Germany

Prof. Carmela Troncoso, EPFL, Switzerland

Prof. Narseo Vallina-Rodriguez, IMDEA Networks, Spain

Prof. Ingrid Verbauwhede, KU Leuven, Belgium

Prof. Ivan Visconti, University of Salerno, Italy