The text beginning on the next page is an open letter on the position of scientists and NGOs on the EU's proposed digital identity reform.

As of the 26th November 2023, the letter has been signed by 551 scientists and researchers from 42 countries, as well as numerous NGOs.

For press inquiries please contact:

Scientists

Juan Tapiador - jestevez@inf.uc3m.es (Spain)
Steven J. Murdoch - s.murdoch@ucl.ac.uk (UK)
Jaap-Henk Hoepman - jhh@cs.ru.nl (The Netherlands)
Anja Lehmann - anja.lehmann@hpi.de (Germany)
Peter Schwabe - peter@cryptojedi.org (Germany)
Cas Cremers - cremers@cispa.de (Germany)
René Mayrhofer - rm@ins.jku.at (Austria)
Manuel Barbosa - mbb@fc.up.pt (Portugal)
Raphael M. Reischuk - raphael.reischuk@zuehlke.com (Switzerland)
Gaëtan Leurent - gaetan.leurent@inria.fr (France)
Olivier Blazy - olivier.blazy@polytechnique.edu (France)
Stephen Farrell - stephen.farrell@cs.tcd.ie (Ireland)
TJ McIntyre - tjmcintyre@ucd.ie (Ireland)
Ivan Visconti - visconti@unisa.it (Italy)
Bart Preneel - bart.preneel@esat.kuleuven.be (Belgium)
Vashek Matyas - matyas@fi.muni.cz (Czech Republic)
Diego Aranha - dfaranha@cs.au.dk (Denmark)

Civil Society - NGOs

Thomas Lohninger - press@epicenter.works (Europe)
Alexis Hancock - alexis@eff.org (Worldwide)

For information on signing the letter, please see the end of this document.

Joint statement of scientists and NGOs on the EU's proposed eIDAS reform

2nd November 2023

Dear Members of the European Parliament,
Dear Member States of the Council of the European Union,

We the undersigned are cybersecurity experts, researchers, and civil society organisations from across the globe.

We have read the near-final text of the eIDAS digital identity reform which has been agreed on a technical level in the trilogue between representatives from the European Parliament, Council and Commission. We appreciate your efforts to improve the digital security of European citizens; it is of utmost importance that the digital interactions of citizens with government institutions and industry can be secure while protecting citizens' privacy. Indeed, having common technical standards and enabling secure cross-border electronic identity solutions is a solid step in this direction. However, we are extremely concerned that, as proposed in its current form, this legislation will not result in adequate technological safeguards for citizens and businesses, as intended. In fact, it will very likely result in less security for all.

Last year, many of us wrote to you to highlight some of the dangers in the European Commission's proposed eIDAS regulation. After reading the near-final text, we are deeply concerned by the proposed text for Article 45. The current proposal radically expands the ability of governments to surveil both their own citizens and residents across the EU by providing them with the technical means to intercept encrypted web traffic, as well as undermining the existing oversight mechanisms relied on by European citizens. Concretely, the regulation enables each EU member state (and recognised third party countries) to designate cryptographic keys for which trust is mandatory; this trust can only be withdrawn with the government's permission *(Article 45a(4))*. This means any EU member state or third party country, acting alone, is capable of intercepting the web traffic of any EU citizen and there is no effective recourse. We ask that you urgently reconsider this text and make clear that Article 45 will not interfere with trust decisions around the cryptographic keys and certificates used to secure web traffic.

Article 45 also bans security checks on EU web certificates unless expressly permitted by regulation when establishing encrypted web traffic connections *(Article 45(2a))*. Instead of specifying a set of minimum security measures which must be enforced as a baseline, it effectively specifies an upper bound on the security measures which cannot be improved upon without the permission of ETSI. This runs counter to well established global norms where new cybersecurity technologies are developed and deployed in response to fast moving developments in technology. This effectively limits the security measures that can be taken to protect the European web. We ask that you reverse this clause, not limiting but encouraging the development of new security measures in response to fast-evolving threats.

The current text also mentions in multiple places the need for the European Digital Identity Wallet to protect privacy, including data minimization, and prevention of profiling. Yet, the legislation still allows relying parties like governments and service providers to unnecessarily link together and gain full knowledge about the uses of credentials in the new European Digital Identity System. Given the broad intended uses of this system, which span all areas of life from health, finance, commerce, online activity up to public transport, we believe that failing to require both unlinkability and unobservability will severely compromise the privacy of EU citizens. Article 6a(7)(a) should be aligned with the negotiation mandate from the European Parliament lead Industry Committee and thereby prevent technologically that such information can be obtained by governments and other parties without the explicit consent of users. Article 6a(7a)(b) should "mandate" instead of "enable" that interactions cannot be linked by relying parties or other actors, where identification of the user is not mandatory. Lastly, forum-shopping from 'Big Tech' and other bad actors can only be prevented by a harmonised implementation of the Regulation that allows national eIDAS agencies to be overruled should they fail to act.

Finally, we would like to highlight our frustration that decisions crucial for the security and privacy of citizens, businesses, and governments, are being taken behind closed doors in trilogue negotiations without public consultation of experts about the potential consequences of the proposed regulations. We urge the European Parliament, Commission, and Council to reconsider their legislative processes and commit to greater transparency so that experts and the public can effectively contribute to the development of new regulations.[1]

In summary, we strongly warn against the currently proposed trilogue agreement, as it fails to properly respect the right to privacy of citizens and secure online communications; without establishing proper safeguards as outlined above, it instead substantially increases the potential for harm.

[1] T-540/15 - De Capitani v Parliament

1. Undermining website authentication undermines communications security

The current text of Article 45 mandates that browsers must accept any root certificates provided by any Member State (and any third party country approved by the EU) and will have severe consequences for the privacy of European citizens, the security of European commerce, and the Internet as a whole.

Root certificates, controlled by so-called certificate authorities, provide the authentication mechanisms for websites by assuring the user that the cryptographic keys used to authenticate the website content belong to that website. The owner of a root certificate can intercept users' web traffic by replacing the website's cryptographic keys with substitutes he controls. Such a substitution can occur e*ven if the website has chosen to use a different certificate authority with a different root certificate.* **Any root certificate trusted by the browser can be used to compromise any website**. There are multiple documented cases of abuse, because the security of some certificate authorities has been compromised. To avoid this, there exists legislation that regulates certificate authorities, complemented by public processes and continuous vigilance by the security community to reveal suspicious activities.

The proposed eIDAS revision gives Member States the possibility of inserting root certificates at will, with the aim to improve the digital security of European citizens by giving them new ways to obtain authentic information of who operates a website. In practice, this does exactly the opposite. Consider the situation in which one of the Member States (or any of the third party states recognized now or in the future) were to add a new authority to the EU Trusted List. The certificate would have to be immediately added to all browsers and distributed to all of their users across the EU as a trusted certificate. By using the substitution techniques explained above, the government-controlled authority would then be able to **intercept the web traffic of not only their own citizens, but all EU citizens**, including banking information, legally privileged information, medical records and family photos. This would be true even when visiting non-EU websites, as such an authority could issue certificates for any website that all browsers would have to accept. Additionally, although much of eIDAS2.0 regulation carefully gives citizens the capability to opt out from usage of new services and functionality, this is not the case for Article 45. **Every citizen would have to trust those certificates**, and thus every citizen would see their online safety threatened.

Even if this misbehaviour was discovered, under the current proposal it would not be possible to remove this certificate without the ultimate approval of the country having introduced the certificate authority. Neither eIDAS's article 45 nor any provisions in adjacent EU legislation such as the NIS2 Directive provide any independent checks and balances on these decisions. Further, European citizens do not have an effective way to appeal these decisions. This situation would be unacceptably damaging to online trust and safety in Europe and across the world. We believe this legislative text must be urgently reworked to avoid these serious consequences by clarifying that eIDAS does not impose obligations to trust cryptographic keys used for encrypted web traffic.

The proposed legislation also prevents the introduction of security checks when verifying the certificates used for encrypted web traffic in Art 45, (2a). As written, this language requires that the EU's website certificates not be subjected to any mandatory requirements beyond those specified in ETSI standards. Mandatory requirements on certificates are essential when browsers validate certificates presented for use in encrypted web connections. Preventing these additional security checks has no useful purpose and only hampers the improvement of cybersecurity for European citizens. The detailed rules on certificate validation and display are constantly being adapted based on new research results and consensus in the security community. Existing security mechanisms, well-studied and accepted by the security community at large, such as TLS 1.3 and certificate transparency logs currently enable browsers to quickly adapt to changing threats and improve global web security. It is essential that this regulation establishes a mandatory minimum set of security standards, but does not impose a limited set of requirements which would hamper the adoption of new security technology within the EU.

While Article 45 could be understood as reducing the power of the large companies behind the major web browsers, from a technical perspective, this is not the case. There already exists a large number of certificate authorities capable of issuing certificates trusted in every web browser, many of which are European and also recognised under the EU's existing eIDAS legislation. Websites have a free choice about which certificate authority they use and all of the approved certificate authorities are treated equally in the browser. Should issues arise, the EU is already well-equipped to tackle them through the recently passed Digital Markets Act, which specifically identifies popular browsers and cloud services and bans self-preferencing behaviour by gatekeepers. Article 45 itself does nothing to assist this process or to enable European scrutiny of trust decisions by 'Big Tech', instead it only enables the interception of EU citizens' web traffic by European governments. It further prevents concerned users, who may have serious and substantiated concerns about being subject to state surveillance, from choosing, or even creating, a browser that has stricter security checks.

In summary, this regulation allows misbehaviour by any individual Member State (or approved third party countries) to compromise the safety and security of other Member State's citizens. If it is implemented, it would result in citizens having to, **without a choice**, trust **all** certificate authorities defined by Member States (and recognized third countries) **in addition** to the parties they trust today. This regulation does not eliminate any existing risk. Instead, by undermining the existing secure web authentication processes, introduces new risks with no gain by European citizens, businesses, and institutions. Moreover, if this regulation becomes a reality, it is only to be expected that **other countries will put pressure on browsers to obtain similar privileges** as EU Member States — as some have unsuccessfully attempted in the past — globally endangering web security.

In order to address these concerns and avoid the security issues introduced by the current legislation proposal which could result in incalculable damage, we recommend:

- The text be clarified to ensure that this legislation will not interfere with trust decisions around the cryptographic keys or certificates used to secure web traffic and the consequent impact on privacy and security of European citizens.

- Additional checks independent from those envisioned in the legislation are not only permitted but encouraged to enable browsers to rapidly incorporate advances made by the security community to improve the security of communications.

In particular:

- The re-introduction of text to Article 45 (2) limiting its scope: “Such recognition, support and interoperability means solely that web-browsers shall ensure that the identity data attested in the certificate provided using any of the methods is displayed in a user-friendly manner.”
- The deletion of Article 45 (2a) so that new security checks can be implemented effectively
- In Recital 32: Adding clarification that the obligations of recognition, interoperability and support in Article 45 do not extend to the use of encryption and authentication technologies for securing web traffic.

We also explicitly note that established processes clearly allow new certificate authorities to be added to browser root trust stores; nation states wishing to establish a new CA legitimate and lawful purposes need to go through the same security certification procedures that existing authorities do, without requiring new regulation. Fostering the development of an EU-native browser, or strengthening the supervision of certificate authorities across the EU, would have a much more positive impact on the overall security of European citizens than attempting to change the status quo of web security from within the eIDAS regulation.

2. A complex system only provides the security and privacy guarantees of its weakest component

The European Digital Identity Wallet (EDIW) is designed to identify and authenticate users with a high level of assurance. The Wallet includes identity information from national IDs (age, sex, etc), and can be extended with additional attributes. These attributes could include very sensitive information such as medical certificates, or important information for the future of European citizens such as their professional qualifications. The eIDAS regulation foresees the creation of an ecosystem of public and private entities that will benefit from the Wallet to have access to certified personal information about citizens.

We welcome the provisions crafted in the legislation, which advocate for strong protections to preclude tracking and profiling, that enable the option of revealing attributes in a selective manner or via zero-knowledge attestation, that attribute providers should not learn about with whom users share their attributes, or that mention that the wallet should allow for unlinkability when identification is not needed. These are essential to promote the use of technologies that can provide these properties by design, and we commend the legislators for including them.

Yet, the legislation only enables the existence of privacy-preserving technologies, but does not mandate them (Article 6a(7a)(b)). We are concerned that this legal ambiguity could lead to a

deterioration of privacy-safeguards that ultimately leaves too much room for technical implementation on member state level. Importantly, operators of the EDIW can still obtain knowledge about concrete user behaviour even when the user has not consented to this. With a privacy-respecting architecture such information is not necessary for the provision of the EDIW. With the current legal text the architecture of the whole system risks undermining trust from citizens in the whole system (Article 6a(7)). A fully harmonised European system for the benefit of the private sector also needs a fully harmonised level of safeguards European citizens can rely upon. Moreover, relying parties (service providers with access to the wallet) can also register in any of the Member States, thus the effective regulatory regime that bad actors and 'Big Tech' can exploit is the weakest of all Member States as we have seen with the GDPR and DSA. This is particularly challenging because of the necessity of cross-border interoperability. Hence, we recommend in Article 46e to empower the European Digital Identity Cooperation Group to overrule the decisions of national eIDAS regulators in order to prevent the circumvention of these important protections.

In order to address these concerns and avoid that the eIDAS regulation results in a new privacy problem with no security gain in terms of authentication, we recommend:

- Make unlinkability a mandatory rather than optional requirement by Replacing "enable" with "mandate" in Article 6a(7a)(b).
- Align the technical architecture with the strong protections established in the lead Industry committee of the European Parliament in Article 6a(7).
- Provide a majority in the European Digital Identity Cooperation Group according to Article 46e the power to overrule the decision of national eIDAS regulators in order to ensure a harmonised enforcement of this regulation.

Without these necessary amendments the eIDAS regulation risks becoming a gift to Google and other Big Tech actors. A European solution to the central question of handling sensitive identity information needs to protect citizens against surveillance capitalism through strong technical mechanisms and be resilient against attempts to exploit the regulatory system through jurisdiction-shopping.

Signatures

Organisations

AG Nachhaltige Digitalisierung
Associação de Empresas de Software Open Source Portuguesas (ESOP)
Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
Asociatia pentru Tehnologie si Internet (ApTI)
Center for Democracy and Technology
Chaos Computer Club
Council of European Professional Informatics Societies
D64 - Zentrum für Digitalen Fortschritt e. V.
Defesa dos Direitos Digitais (D3)
deSEC
Digital Courage
Digitale Gesellschaft
Electronic Frontier Finland (Effi)
Electronic Frontier Foundation (EFF)
Emerald Onion
Entropia e.V.
Epicenter.works
European Digital Rights (EDRi)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.
Foundation for Information Policy Research (FIPR)
Gesellschaft für Informatik e.V.
Homo Digitalis
IETF Internet Architecture Board (IAB)
Innovationsverbund Öffentliche Gesundheit e.V.
Internet Governance Project
Internet Architecture Board
Internet Society
Internet Society Catalan Chapter
Internet Society Switzerland Chapter
Internet Society UK Chapter
IT-Pol
LOAD e.V.
La Quadrature du Net
Özgür Yazılım Derneği
Petites Singularités
Privacy & Access Council of Canada
Privacy First
Rhizomatica
SICEH Foundation
SUPERRR Lab

The Digital Freedom and Rights Association
The Document Foundation
The Matrix.org Foundation
The Syncthing Foundation
The Tor Project
Trust in Digital Life

Scientists and Researchers

The letter has been signed by 551 scientists and researchers from 42 countries.

Australia

Dr. Shaanan Cohney	University of Melbourne

Austria

Prof. Elena Andreeva	TU Wien
Dr. Gaëtan Cassiers	Graz University of Technology
Prof. Maria Eichlseder	Graz University of Technology
Dipl.-Ing. Paul Fuxjäger	Research Group Cooperative Systems, University of Vienna
Prof. Daniel Gruss	Graz University of Technology
Prof. Martina Lindorfer	TU Wien
Univ.-Prof. Dr. Matteo Maffei	TU Wien
Univ.-Prof. Dr. René Mayrhofer	Johannes Kepler University Linz
Dr. Peter Meerwald-Stadler	Universität Salzburg
Dr. Martin Riener	TU Wien
Dr. Michael Roland	Johannes Kepler University Linz
Dr. Marco Squarcina	TU Wien
Univ.-Prof. Dr. Edgar Weippl	Universität Wien

Belgium

Dr. Aysajan Abidin	KU Leuven
Prof. Olivier Bonaventure	UCLouvain
Prof. Bart Coppens	Ghent University
Dr. Lesly-Ann Daniel	KU Leuven
Prof. Geert Deconinck	KU Leuven
Prof. Claudia Diaz	KU Leuven
Prof.Dr. Jacques Folon	Ichec Brussels management school
Dr. Benedikt Gierlichs	KU Leuven
Prof. Gregory Lewkowicz	Université libre de Bruxelles
Prof. Jan Tobias Muehlberg	Universite Libre de Bruxelles, Cybersecurity Research Centre
Dr. Svetla Nikova	KU Leuven
Prof. Olivier Pereira	UCLouvain

Prof. Thomas Peters	UCLouvain
Prof. Bart Preneel	KU Leuven
Prof. Frederik Questier	Vrije Universiteit Brussel
Prof. Jean-Jacques Quisquater	UCLouvain
Prof. Florentin Rochet	UNamur
Dr. Enrique Argones Rúa	COSIC - KU Leuven
Prof. Nigel Smart	KU Leuven
Prof. Sophie Stalla-Bourdillon	VUB
Prof. François-Xavier Standaert	Université catholique de Louvain
Prof. Mathy Vanhoef	KU Leuven
Prof. Ingrid Verbauwhede	KU Leuven
Dr. Karin Verelst	Vrije Universiteit Brussel
Dr. Plixavra Vogiatzoglou	KU Leuven Centre for IT & IP Law

Brazil

Prof. Marcos A. Simplicio Jr.	Universidade de São Paulo
Dr. Ian Brown	Visiting Professor, Fundação Getulio Vargas
Prof. Emerson Ribeiro de Mello	Federal Institute of Santa Catarina
Prof. Frederico Schardong	Instituto Federal do Rio Grande do Sul

Bulgaria

Dr. Vesselin Bontchev	Bulgarian Academy of Sciences
Dr. Konstantin Delchev	IMI-BAS

Canada

Prof. Diogo Barradas	University of Waterloo
Prof. Claude Crépeau	McGill University
Prof. Ian Goldberg	University of Waterloo
Mr Mark Lizar	CEO 0PN Transparency Lab
Prof. Simon Oya	The University of British Columbia
Prof. Joel Reardon	University of Calgary
Dr. Stacey Watson	University of Waterloo
Paul Wouters	The Libreswan Project

Chile

Prof. Alejandro Hevia	Universidad de Chile

China

Prof. Dr.-Ing. Dirk Kutscher	The Hong Kong University of Science and Technology (Guangzhou)

Czech Republic

Dr. Václav Bartoš	CESNET
Vlad Iliushin	ELLIO Technology

Jan Jancar	Masaryk University
Prof. Vashek Matyas	Masaryk University
Prof. Petr Svenda	Masaryk University
Dr. Martin Ukrop	Masaryk University

Denmark

Prof. Diego F. Aranha	Aarhus University
Prof. Carsten Baum	Technical University of Denmark
Prof. Ivan Damgård	Aarhus University
Prof. Dr. Florian Echtler	Aalborg University
Peter Kruse	SIE Europe
Prof. Christian Majenz	Technical University of Denmark
Prof. Claudio Orlandi	Aarhus University
Prof. Peter Scholl	Aarhus University
Dr. Shreyas Srinivasa	Aalborg University

Estonia

Dr. Arnis Parsovs	University of Tartu

Finland

Prof. N. Asokan	University of Waterloo and Aalto University
Prof. Christopher Brzuska	Aalto University
Dr. Lars Eggert	NetApp
Dr. Lachlan Gunn	Aalto University
Prof. Kimmo Halunen	University of Oulu
Dr. Marko Helenius	Tampere University
Prof. Antti Honkela	University of Helsinki
Dr. Michael Klooß	Aalto University
Prof. Russell W. F. Lai	Aalto University
Juhani Naskali	University of Turku

France

Dr. Valérie Berthé	CNRS
Dr. Daniele Antonioli	EURECOM
Prof. Simone Aonzo	EURECOM
Florent Autréau	Université Grenoble Alpes
Prof. Jean Claude Bajard	Sorbonne Université
Prof. Davide Balzarotti	EURECOM
Dr. Gustavo Banegas	Independent Researcher
Dr. Sébastien Bardin	Université Paris-Saclay, CEA
Dr. Sonia Belaïd	CryptoExperts
Prof. Thierry Berger	University of Limoges
Mr. Karthikeyan Bhargavan	Cryspen
Dr. Bruno Blanchet	Inria

Prof. Olivier Blazy	Ecole Polytechnique
Dr. Xavier Bonnetain	Inria
Dr. Beyza Bozdemir	
Dr. Isabelle Le Brun	Université grenoble alpes
Dr. Olivier Buffet	INRIA
Prof. Sébastien Canard	Télécom Paris
Dr. Anne Canteaut	Inria
Dr. Thibault Cholez	Université de Lorraine
Dr. Véronique Cortier	CNRS
Dr. Clément Dallard	École Normale Supérieure de Lyon
Dr. Alexandre Debant	Inria
CR. Thomas Debris-Alazard	Inria
Dr. Daniel Demmler	Zama
Dr. Jean-Christophe Deneuville	ENAC, Université de Toulouse
Dr. Patrick Derbez	Université de Rennes
Dr. Julien Deseigne	Emlyon business school
Prof. Matthieu Dien	Université de Caen
Dr. Jannik Dreier	Université de Lorraine
Dr. Cyril Drocourt	Université de Picardie Jules Verne
Dr. Sébastien Duval	Université de Lorraine, Loria, CNRS, Inria
Dr. Christoph Egger	Université Paris Cité, CNRS, IRIF
Dr. Antonio Faonio	EURECOM
Prof. Jessica Feldman	American University of Paris
Prof. Barbara Fila	IRISA, INSA Rennes
Prof. Caroline Fontaine	CNRS
Prof. Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Prof. Joaquin Garcia-Alfaro	Institut Mines-Telecom
Dr. Pierrick Gaudry	CNRS
Dr. Louis Gesbert	Inria
Dr. Lénaïck Gouriou	ENS
Dr. Michaël Hauspie	Université de Lille
Dr. Vincent Hugot	INSA Centre Val de Loire
Dr. Charlie Jacomme	Inria
Dr. Nesrine Kaaniche	Telecom SudParis, Institut Polytechnique de Paris
Prof. Marc-Olivier Killijian	UQAM/CNRS
Dr. Nadim Kobeissi	Symbolic Software
Dr. Adrien Koutsos	Inria Paris
Dr. Steve Kremer	Inria
Prof. Pascal Lafourcade	University Clermont Auvergne (LIMOS)
Dr. Joseph Lallemand	CNRS
Philippe Langlois	P1 Security
Dr. Vincent Laporte	Inria Nancy
Prof. Maryline Laurent	Télécom SudParis

Dr. Vincent Lefèvre	Inria
MCF Joël Legrand	CentraleSupélec
Dr. Gaëtan Leurent	Inria
Dc Claire Levallois-Barth	IMT Atlantique
Prof. Francoise Levy	INRIA
Dr. Benoît Libert	Zama
Prof. Nadia EL MRABET	Mines Saint Etienne
Prof. (Honorary) Traian MUNTEAN	Aix-Marseille Université
Dr. Damien Marion	University of Rennes
Dr. Stephan Merz	Inria Nancy
Dr. Brice Minaud	Inria and ENS-PSL
Brad Moldenhauer	Zscaler
Dr. Camille Monière	Université Bretagne Sud
Dr. María Naya-Plasencia	Inria
Prof. Benjamin Nguyen	INSA Centre Val de Loire
Dr. Phong Nguyen	Inria
Dr. Andrea Oliveri	EURECOM
Dr. Charles Olivier-Anclin	LIMOS
Dr. Cristina Onete	Université de Limoges
Dr. Léo Perrin	Inria
Dr. Maxime Puys	University Clermont Auvergne (LIMOS)
Dr. Tamara Rezk	INRIA
Dr. Matthieu Rivain	CryptoExperts
Dr. Léo Robert	Université de Picardie Jules Verne
Dr. Thomas Roche	NinjaLab
Prof. Christophe Rosenberger	ENSICAEN
Dr. Yann Rotella	Université Paris-Saclay
Dr. Merve Sahin	
Hervé Schauer	HS2
Dr. Jacques André Fines Schlumberger	Université Panthéon Assas Paris 2
Dr. André Schrottenloher	Inria
Dr. Benjamin Smith	Inria and École polytechnique
Dr. Valentin Suder	University of Rouen Normandy
Dr. Emmanuel Thomé	Inria
Dr. Jean-Pierre Tillich	Inria
Dr. Michael Toth	
Prof. Yannick Toussaint	LORIA
Dr. Alexandre Wallet	Inria, Centre de l'Université de Rennes
Prof. Melek Önen	EURECOM

Germany

Dr. Ali Abbasi	CISPA Helmholtz Center for Information Security
Prof. Dr. Florian Adamsky	Hof University od Applied Sciences
Prof. Dr. Dr. h.c. Michael Backes	CISPA Helmholtz Center for Information Security

Prof. Gilles Barthe	Max Planck Institute for Security and Privacy (MPI-SP)
Prof. Dr.-Ing. Robert Baumgartl	Dresden University of Applied Sciences
Dr.-Ing. Olaf Bergmann	Universität Bremen, TZI
Privatdozent Dr. Roland Bless	Karlsruhe Institute of Technology
Prof. Dr. Kevin Borgolte	Ruhr University Bochum
Prof. Dr.-Ing. Carsten Bormann	Universität Bremen, TZI
Dr. Jacqueline Brendel	TU Darmstadt
Dr. Samira Briongos	NEC Laboratories Europe
Prof. Dr. Stefan Brunthaler	uCSRL - FI Code - Universität der Bundeswehr München
Dr.-Ing. Jiska Classen	Hasso Plattner Institute, University of Potsdam
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security
Marco Falke	Open Source Developer
Dr. Niels Fallenbeck	Leibniz Supercomputing Centre
Dr. Aurore Fass	CISPA Helmholtz Center for Information Security
Markus Feilner	Feilner IT (Open Source Consulting and Journalism)
Jens Finkhaeuser	Interpeer gUG
Dr. Oliver Gasser	Max Planck Institute for Informatics
Dr.-Ing. Stefane Gerdes	Universität Bremen, TZI
Dr. Maximilian Golla	CISPA Helmholtz Center for Information Security
Dr. Lorenzo Grassi	Ruhr-University Bochum
Werner Haas	Cyberus Technology GmbH
Prof. Dr. Andreas Heinemann	Hochschule Darmstadt / ATHENE - National Research Center for Applied Cybersecurity
Dr.-Ing. Dominik Helm	Technische Universität Darmstadt
Prof. Dr. Dominik Herrmann	Otto-Friedrich-Universität Bamberg
Prof. Dr. Peter Hertkorn	Hochschule Reutlingen
Prof. Dr. Matthias Hollick	TU Darmstadt
Prof. Thorsten Holz	CISPA Helmholtz Center for Information Security
Prof. Ralph Holz	University of Münster
Dr. Detlef Hühnlein	ecsec GmbH
Prof. Dr. Luigi Lo Iacono	H-BRS University of Applied Sciences
Dr. Fabian Ising	Fraunhofer SIT, FH Münster
Prof. Tibor Jager	University of Wuppertal
Dr. Heiko Jakubzik	Ruprecht-Karls-Universität Heidelberg
Dr. Gregor Joeris	CTO SERgroup
Prof. Dr. Antoine Joux	CISPA Helmholtz Center for Information Security
Christian Kahlo	c-base e.V.
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Franziskus Kiefer	Cryspen
Jörg Knappen	Saarland University
Dr. Konrad Kohbrok	Phoenix R&D
Prof. Dr. Christoph Krauß	Darmstadt University of Applied Sciences

Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Roman Kuznetsov	Systola GmbH
Dr. Robert Künnemann	CISPA Helmholtz Center for Information Security
Prof. Gregor Leander	Ruhr University Bochum
Prof. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Christoph Lenzen	CISPA Helmholtz Center for Information Security
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Prof. Dr. Klaus-Peter Löhr	Freie Universität Berlin
Dr. Philipp Markert	Ruhr University Bochum
Dr. Matthias Minihold	Ruhr University Bochum
Prof. Esfandiar Mohammadi	University of Lübeck
Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Dr.-Ing. Jörg Ott	Technical University of Munich
Dr. Sebastian Pape	Social Engineering Academy
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Prof. Dr. Guenther Pernul	University of Regensburg
Prof. Dr. Joachim Posegga	University of Passau
Dr. Henrich C. Pöhls	University of Passau
Prof. Dr. Kai Rannenberg	Goethe University Frankfurt
Dr. Rainer Rehak	Weizenbaum Institute for the Networked Society
Prof. Dr. Konrad Rieck	Technische Universität Berlin
Prof. Julian Rohrhuber	Robert-Schumann-Hochschule
Prof. Dr. Stefanie Roos	University of Kaiserslautern-Landau
Prof. Dr. Christian Rossow	CISPA Helmholtz Center for Information Security
Dr.-Ing. Tim Ruffing	Blockstream Research
Dr. Christoph Saatjohann	Fraunhofer SIT
Prof. Dr. Florian E. Sachs	University of Cologne
Dr. Martin Schanzenbach	Fraunhofer AISEC
Prof. Dr. Sebastian Schinzel	Münster University of Applied Sciences and Fraunhofer SIT and Athene
Prof. Thomas Schneider	TU Darmstadt
Dr. Jonas Schneider-Bensch	Cryspen
Prof. Dr.-Ing. Thomas Schreck	Munich University of Applied Sciences
Prof. Dominique Schröder	Friedrich-Alexander Universität Erlangen-Nürnberg
Prof. Dr. Peter Schwabe	MPI-SP & Radboud University
Dr. Patrick Schweitzer	FernUniversität Hagen
Prof. Dr. Jörg Schwenk	Ruhr University Bochum
Prof. Dr. Marcus Schöller	Reutlingen University
Dr. Lea Schönherr	CISPA Helmholtz Center for Information Security
PD Dr. Karsten Sohr	Center for Computing Technologies at the University of Bremen
Dr.-Ing. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Dr. Sven Strickroth	LMU Munich
Prof. Dr. Thorsten Strufe	KIT and CeTI TU-Dresden

Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Dr. Oleksandr Tkachenko	DFINITY
Prof. Dr. Peter Trapp	Hochschule München
Dr.-Ing. Amos Treiber	
Dr.-Ing. Tobias Urban	Westphalian University of Applied Sciences & Institute for Internet Security
Dr. Anjo Vahldiek-Oberwagner	Intel Labs
Prof. Jilles Vreeken	CISPA Helmholtz Center for Information Security
Dr.-Ing. Felix Walter	D3TN GmbH
Dr. Christiane Weis	NEC Laboratories Europe (views are my own)
Prof. Dr. Matthias Wählisch	TU Dresden
York Yannikos	Fraunhofer SIT / ATHENE
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Prof. Michael Zohner	Hochschule Fulda

Greece

Prof. Stefanos Gritzalis	University of Piraeus
Prof. Sotiris Ioannidis	Technical University of Crete
Prof. Christos Kalloniatis	University of the Aegean
Prof. Georgios Kambourakis	University of the Aegean
Prof. Spyridon Kokolakis	University of the Aegean
Prof. Costas Lambrinoudakis	University of Piraeus
Prof. Panagiotis Rizomiliotis	Harokopio University of Athens

Hong Kong SAR, China

Dr. Xavier de Carné de Carnavalet	The Hong Kong Polytechnic University

Hungary

Dr. Balazs PEJO	CrySyS Lab

Iceland

Mr. Stefán Jökull Sigurðarson	Have I Been Pwned Contributor, Microsoft MVP
Prof. Thomas Welsh	University of iceland

Ireland

Dr. Stephen Farrell	Trinity College Dublin
Dr. Aikaterini Kanta	University College Dublin
Prof. Douglas Leith	Trinity College Dublin
Prof. David Malone	Maynooth University
Dr. TJ McIntyre	University College Dublin, Sutherland School of Law
Dr. Hazel Murray	Munster Technological University
Dr. Kris Shrishak	Irish Council for Civil Liberties

Israel

Prof. Orr Dunkelman	Computer Science Dept. and the Center for Cyber, Law and Policy at the University of Haifa
Dr. Eyal Ronen	Tel Aviv University
Dr. Mahmood Sharif	Tel Aviv University

Italy

Prof. Alessandro Barenghi	Politecnico di Milano
Dr. Antonia Bezenchek	INFORMAPRO, Rome
Prof. Carlo Blundo	University of Salerno
Dr. Daniele Cono D'Elia	Sapienza University of Rome
Dr. Matteo Dell'Amico	University of Genoa
Dr. Salvatore Manfredi	Fondazione Bruno Kessler
Dr. Emmanuela Orsini	Bocconi University
Prof. Stefano Paraboschi	University of Bergamo
Prof. Silvio Ranise	Università di Trento and Fondazione Bruno Kessler, Trento
Filippo Valsorda	
Prof. Daniele Venturi	Sapienza University of Rome
Prof. Ivan Visconti	University of Salerno
Prof. Stefano Zanero	Politecnico di Milano

Japan

Prof. Masayuki Hatta	Surugadai University
Dr. Octavio Perez Kempner	NTT Social Informatics Laboratories
Prof. Toshimaru Ogura	JCA-NET
Prof. Kazue Sako	Waseda University
Dr. Mehdi Tibouchi	NTT Social Informatics Laboratories

Latvia

Dr. Pēteris Paikens	University of Latvia

Liechtenstein

Prof. Giovanni Apruzzese	University of Liechtenstein

Luxembourg

Dr. Afonso Arriaga	University of Luxembourg
Prof. Gilbert Fridgen	University of Luxembourg
Dr. Dmitry Khovratovich	Ethereum Foundation
Dr. Baptiste Lambin	University of Luxembourg
Dr. Johannes Müller	University of Luxembourg
Dr. Claudia Negri-Ribalta	President of OptIA and researcher at the University of Luxembourg
Dr. Peter Roenne	University of Luxembourg
Prof. Peter Y A Ryan	University of Luxembourg

Dr. Johannes Sedlmeir	Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
Dr. Marjan Škrobot	University of Luxembourg
Mauritius	
Loganaden Velvindron	cyberstorm.mu
New Zealand	
Dr. Vladimir Mencl	Research and Education Advanced Network New Zealand
Norway	
Prof. Anamaria Costache	NTNU
Prof. Kristian Gjøsteen	NTNU
Prof. Nils Gruschka	University of Oslo
Prof. Tjerand Silde	Norwegian University of Science and Technology
Prof. Iain Sutherland	Noroff University College
Prof. Mohsen Toorani	University of South-Eastern Norway
Prof. Dr. Michael Welzl	University of Oslo
Poland	
Prof. Miroslaw Kutylowski	NASK - National Research Institute
Prof. Jan Sładkowski	Institute of Physics, University of Silesia
Portugal	
Prof. Manuel Barbosa	Faculty of Science of the University of Porto
Sofia Celi	Brave
Prof. Alex Davidson	Universidade NOVA de Lisboa
Prof. Kevin Gallagher	NOVA School of Science and Technology
Prof. Nuno Santos	INESC-ID / Instituto Superior Técnico, University of Lisbon
Saudi Arabia	
Prof. Marc Dacier	KAUST
Singapore	
Prof. Thomas Peyrin	Nanyang Technological University
Slovenia	
Prof. Marko Hölbl	University of Maribor, Faculty of Electrical Engineering and Computer Science
Spain	
Dr. Jorge Blasco Alis	Universidad Politécnica de Madrid

Dr. Juan Caballero	IMDEA Software Institute
Dr. Ignacio Cascudo	IMDEA Software Institute
Prof. Jordi Domingo	Universitat Politècnica de Catlaunya (UPC BarcelonaTECH)
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili
Prof. Luis Fernández-Sanz	Universidad de Alcalá
Dr. Dario Fiore	IMDEA Software Institute
Prof. José María de Fuentes	Universidad Carlos III de Madrid
Dr. David Arroyo Guardeño	Spanish National Research Council
Prof. Marco Guarnieri	IMDEA Software Institute
Dr. Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona
Prof. Dr. Oscar Lage	TECNALIA
Prof. Lorena González Manzano	Universidad Carlos III de Madrid
Dr. Pedro Moreno-Sanchez	IMDEA Software Institute
Dr. Gorka Guardiola Múzquiz	Universidad Rey Juan Carlos
Prof. Antonio Nappa	UC3M Madrid
Prof. Jose A. Onieva	University of Malaga
Dr. Sergio Pastrana	University Carlos III de Madrid
Prof. Fernando Pérez-González	University of Vigo
Prof. Ricardo J. Rodríguez	Universidad de Zaragoza
Dr. Carla Ràfols	Universitat Pompeu Fabra
Prof. Enrique Soriano-Salvador	Universidad Rey Juan Carlos
Dr. Guillermo Suarez-Tangil	IMDEA Networks Institute
Prof. Juan Tapiador	Universidad Carlos III de Madrid
Dr. Ida Tucker	Indra
Prof. Narseo Vallina-Rodriguez	IMDEA Networks Institute
Prof. María Isabel González Vasco	Universidad Carlos III de Madrid

Sweden

Dr. Simon Bouget	RISE Research Institutes of Sweden AB
Dr. Michele Cascella	Lund University
Dr. Felix Engelmann	Lund University
Prof. Dr.-Ing. Meiko Jensen	Karlstad University
Dr. Leonardo Martucci	Karlstad University
Dr. Tobias Pulls	Karlstad University

Switzerland

Dr. Imad Aad	EPFL
Prof. David Basin	ETH Zurich
Dr. ir. Bram Bonné	Google
Prof. Dr. Kai Brünnler	Bern University of Applied Sciences
Prof. Christian Cachin	University of Bern
Dr. Jan Camenisch	DFINITY Foundation
Prof. Srdjan Capkun	ETH Zurich

Antonios Chariton	
Dr. Anastasija Collen	University of Geneva
Dr. Aisling Connolly	DFINITY
Dr. Olivier Crochat	EPFL
Dr. Damien Desfontaines	Tumult Labs (views my own)
Prof. Bryan Ford	EPFL
Dr. Tommaso Gagliardoni	Kudelski Security (views are my own)
Dr. Giacomo Giuliari	ETH Zurich
Prof. Dr. Christian Grothoff	Bern University of Applied Sciences
Prof. Andreas Habegger	Bern University of Applied Sciences
Dr. Harry Halpin	Nym Technologies
Prof. Jean-Pierre Hubaux	EPFL
Prof. Lukas Ith	Bern University of Applied Sciences
Prof. Ralf Jung	ETH Zurich
Dr. Nikos Karapanos	Futurae Technologies AG
Prof. Marc Langheinrich	Università della Svizzera italiana (USI)
Prof. Dr. Annett Laube-Rosenpflanzer	Bern University of Applied Science (BFH)
Dr. Markus Legner	Mysten Labs
Prof. Rebekah Overdorf	University of Lausanne
Prof. Kenneth Paterson	ETH Zurich
Prof. Mathias Payer	EPFL
Prof. Dr. Adrian Perrig	ETH Zürich
Prof. Kaveh Razavi	ETH Zurich
Dr. Raphael M. Reischuk	National Test Institute for Cybersecurity; Zühlke Engineering AG
Prof. Dr. Kenneth A. Ritley	Bern University of Applied Sciences
Dr. Lutz Rosenpflanzer	Berne University of Applied Sciences / BFH
Dr. Benjamin Rothenberger	Zühlke
Dr. Alessandro Sorniotti	IBM Research Europe (views are my own)
Dr. Björn Tackmann	DFINITY
Prof. Carmela Troncoso	EPFL
Dr. Piet De Vaere	ETH Zürich
Prof. Isabel Wagner	University of Basel
Dr. Rob van Weelderen	CERN
Dr. Taras Zakharko	University of Zurich

Taiwan

Dr. Matthias Kannwischer	
Dr. Bo-Yin yang	Academia Sinica

The Netherlands

Dr. Gunes Acar	Radboud University
Dr. Luca Allodi	TU Eindhoven
Dr. Greg Alpár	Open University of the Netherlands

Prof. Dr. H. Bos	VUSec / Vrije Universiteit Amsterdam
Dr. Léo Colisson	CWI
Dr. Andrea Continella	University of Twente
Prof. Joan Daemen	Radboud University
Prof. Sandro Etalle	Eindhoven Technical University
Dr. Simona Etinski	Centrum Wiskunde & Informatica
Dr. Seda Gurses	TU Delft
Dr. Florian Hahn	University of Twente
Prof. Dr. Jaap-Henk Hoepman	Radboud University / University of Groningen / Karlstad University
Prof. Andreas Hülsing	Eindhoven University of Technology
Dr. Ralph Koning	University of Amsterdam
Dr. Matthijs Koot	University of Amsterdam
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Drs. Jaap van der Straaten MBA	Chief Executive Officer Civil Registration Centre for Development
Dr. Luca Mariot	University of Twente
Prof. Giovane C. M. Moura	TU Delft
Dr. Kostas Papagiannopoulos	University of Amsterdam
Dr. Simona Samardjiska	Radboud University
Prof. Christian Schaffner	University of Amsterdam
Dr. Savio Sciancalepore	TU Eindhoven
Prof. Georgios Smaragdakis	Delft University of Technology (TU Delft)
Dr. Monika Trimoska	Eindhoven University of Technology
Dr. Jeroen van der Ham-de Vos	University of Twente
Dr. Barbara Vreede	Netherlands eScience Center
Dr. Yury Zhauniarovich	TU Delft

Turkey

Prof. Dr. Atilla Elçi	Hasan Kalyoncu University
Prof. Cihangir Tezcan	Middle East Technical University

United Arab Emirates

Prof. Christina Pöpper	New York University Abu Dhabi

United Kingdom

Prof. Martin Albrecht	King's College London
Prof. Ross Anderson	Universities of Edinburgh and Cambridge
Prof. David Aspinall	University of Edinburgh
Prof. Ioana Boureanu	Surrey Centre for Cyber Security, University of Surrey
Dr. Jaya Klara Brekke	Nym technologies
Prof. Achim Brucker	University of Exeter
Prof. Lorenzo Cavallaro	University College London

Dr. Giovanni Cherubin	Microsoft
Prof. Tom Chothia	University of Birmingham
Dr. Michele Ciampi	The University of Edinburgh
Dr. Richard Clayton	University of Cambridge
Dr. Kovila Coopamootoo	King's College London
Ray Corrigan	The Open University
Dr. Elizabeth Crites	University of Edinburgh
Prof. Jon Crowcroft	University of Cambridge
Prof. Simon Dobson	University of St Andrews
Dr. Benjamin Dowling	The University of Sheffield
Dr. Tariq Elahi	University of Edinburgh
Prof. Hamed Haddadi	Imperial College London
Dr. Neil Hanley	Queen's University Belfast
Mr Scott Helme	Independent Security Researcher
Dr. Michio Honda	School of Informatics, University of Edinburgh
Prof. Alice Hutchings	University of Cambridge
Dr. Rikke Bjerg Jensen	Royal Holloway, University of London
Dr. Philipp Jovanovic	University College London
Dr. Marc Juarez	University of Edinburgh
Prof. Vasilis Katos	BU-CERT, Bournemouth University
Prof. Aggelos Kiayias	University of Edinburgh
Prof. Markulf Kohlweiss	University of Edinburgh
Prof. Douwe Korff	Emeritus professor London Metropolitan University
Prof. Andrew Martin	University of Oxford
Prof. Sarah Meiklejohn	University College London
Prof. Andrew W Moore	University of Cambridge
Alec Muffett	Security Consultant
Prof. Steven J. Murdoch	University College London
Dr. David Nadlinger	University of Oxford
Prof. Bill Buchanan OBE	Edinburgh Napier University
Dr. Oleksii Oleksenko	Azure Research
Dr. Colin Perkins	University of Glasgow
Dr. Fabio Pierazzi	King's College London
Dr. Sasa Radomirovic	University of Surrey
Prof. Kasper Rasmussen	University of Oxford
Prof. Moritz Riede	University of Oxford
Dr. Luc Rocher	University of Oxford
Prof. Steve Schneider	Surrey Centre for Cyber Security, University of Surrey
Dr. Andrei Serjantov	
Dr. Siamak Shahandashti	University of York
Prof. Peter Sommer	Birmingham City University
Dr. Ian Stark	The University of Edinburgh
Dr. Yiannis Tselekounis	Royal Holloway, University of London

Prof. Dr. Luca Viganò	King's College London
Dr. Mikhail Volkhov	The University of Edinburgh
Dr. Christian Weinert	Royal Holloway, University of London
Prof. Alan Woodward	Surrey Centre for Cyber Security, University of Surrey

United States of America

Dr. Clément Aubert	Augusta University
Prof. Lujo Bauer	Carnegie Mellon University
Prof. Joseph Bonneau	New York University
Prof. Mahdi Cheraghchi	University of Michigan
Dr. Omar Haider Chowdhury	Stony Brook University
Prof. Nicolas Christin	Carnegie Mellon University
Prof. Lorrie Cranor	CyLab Security and Privacy Institute, Carnegie Mellon University
Prof. Álvaro Cárdenas	UCSC
Prof. Sanchari Das	University of Denver
Prof. Zakir Durumeric	Stanford University
Arthur Edelstein	PrivacyTests.org
Prof. Michael Franz	University of California, Irvine
Dr. Christina Garman	Purdue University
Dr. Joseph Lorenzo Hall	Internet Society
Prof. Umar Iqbal	Washington University in St. Louis
Prof. Gabriel Kaptchuk	Boston University
Mallory Knodel	Internet Research Steering Group member
Prof. Susan Landau	Tufts University
Dr. Per Larsen	Immunant, Inc.
Prof. Dave Levin	University of Maryland
Prof. Milton L Mueller	Georgia Institute of Technology
Prof. Adwait Nadkarni	William & Mary
Dr. Neha Narula	MIT
Prof. Nick Nikiforakis	Stony Brook University
Prof. Riccardo Paccagnella	Carnegie Mellon University
Christopher Patton	
Prof. Michalis Polychronakis	Stony Brook University
Dr. Niels Provos	
Prof. Amir Rahmati	Stony Brook University
Prof. Aanjhan Ranganathan	Northeastern University
Prof. Ronald L. Rivest	MIT
Prof. Mike Rosulek	Oregon State University
Dr. Sarah Scheffler	Massachusetts Institute of Technology
Dr. Phillipp Schoppmann	Google
Dr. Sergi Delgado Segura	Chaincode Labs
Prof. Hovav Shacham	The University of Texas at Austin

Prof. Micah Sherr	Georgetown University
Dr. David Sidi	The University of Arizona & Yale University
Prof. Michael A. Specter	Georgia Tech
Prof. Deian Stefan	University of California San Diego
Prof. Santiago Torres-Arias	Purdue University
Prof. Blase Ur	University of Chicago
Prof. Matthew Wright	Rochester Institute of Technology
Dr. Pieter Wuille	Chaincode Labs
Prof. Daniel Zappala	Brigham Young University

Signing the letter

If you are a scientist or researcher and want to sign please fill out this form hosted by the Chaos Computer Club of Vienna (PhD or demonstrated research track record required).

If you are a representative of an NGO, you can sign via adding your organisation to this spreadsheet also hosted by the Chaos Computer Club of Vienna.