FZI-Positionspapier zur Novellierung der eIDAS-Verordnung

Ohne kohärente datenschutzrechtliche Regelungen und eine europaweit kompatible technische Lösung für die European Digital Identity Wallets werden die Sicherheit und Selbstbestimmtheit aller EU-Bürger*innen ab dem Jahr 2026 auf der Strecke bleiben.

FZI-Wissenschaftler*innen des Forschungsbereichs Cybersecurity and Law sehen in der aktuellen Neuregelung der eIDAS-Verordnung neben den Chancen für eine weitgehendere Digitalisierung viele konkrete Risiken, insbesondere durch die Art der eingesetzten Zertifikate (QWAC). Auch seien kohärente datenschutzrechtliche Regelungen in der eIDAS-Verordnung nicht erkennbar, so dass Regierungen über die Verwendung der EUDI-Wallet in verschiedenen Lebensbereichen das Nutzungsverhalten von EU-Bürger*innen ablesen könnte. Lösungsvorschläge hierzu bringt das FZI in den BMI-Konsultationsprozess zur EUDI-Wallet ein.

Am 08. November 2023 haben sich Vertreter*innen des EU-Parlaments, der Europäischen Kommission und des Europäischen Rats auf die Novellierung der eIDAS-Verordnung geeinigt. Die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt soll Behörden, Unternehmen und Bürger*innen ermöglichen, nahtlos elektronisch und sicher miteinander zu interagieren.[1]

Die bisher geltende Regelung stammt noch aus dem Jahr 2014. Deswegen musste sie dringend den aktuellen politischen Herausforderungen und dem technologischen Fortschritt angepasst werden. Kernelement der eIDAS-Verordnung ist die European Digital Identity Wallet (EUDI-Wallet)[2]. In dieser digitalen Brieftasche können digitale Versionen von Dokumenten hinterlegt und dann elektronisch abgerufen werden. Das lässt sich beispielsweise für den Personalausweis, den Führerschein oder die Gesundheitskarte nutzen.

Der gewünschte Nutzen

Mittels dieser Methode können sich Behörden, Unternehmen und Bürger*innen gegenüber anderen ausweisen und notwendige Nachweise unkompliziert elektronisch erbringen. Bis zum Jahr 2026 müssen alle EU-Mitgliedstaaten ihren Bürger*innen die EUDI-Wallet kostenlos zur Verfügung stellen, sodass diese in der Wallet auf ihren mobilen Endgeräten verschiedene Identitätsnachweise speichern können. Personen, welche das Wallet nicht nutzen wollen oder können, darf dadurch kein Nachteil entstehen.

---

[1] https://digital-strategy.ec.europa.eu/de/policies/eidas-regulation
[2] https://ec.europa.eu/commission/presscorner/detail/de/ip_23_5651

Neuregelung beinhaltet Chancen und Risiken

Die nun besprochene Novellierung im Trilog-Verfahren erweitert den Anwendungsbereich der Verordnung auch auf den privaten Sektor. Dies bietet neben Chancen für eine weitgehendere Digitalisierung leider auch viele konkrete Risiken.

Ein entscheidender Kritikpunkt an der Neufassung adressiert eine auch anders gestaltbare technische Regelung, wie sie in der Novelle festgelegt werden soll: die Art der eingesetzten Zertifikate.

Zertifikate dienen im Allgemeinen dazu, die Verbindung zwischen den Websites und den Personen, welche diese besuchen, zu verschlüsseln und abzusichern. Des Weiteren werden durch sie die Betreiber der Websites authentifiziert[3] gegenüber den Besuchenden.

Doch gemäß eIDAS-Novelle sollen zukünftig Qualified Website Authentication Certificates (QWAC)[4] eingesetzt werden. Browser sollen diese QWACs als vertrauenswürdig akzeptieren. Personen, welche die Websites aufrufen, sollen erkennen können, wer hinter einer Website steht. So soll Vertrauen geschaffen werden. Die Zertifikate werden von den jeweiligen EU-Mitgliedstaaten bereitgestellt, kontrolliert und dürfen nur mit Zustimmung der entsprechenden Regierung wieder entfernt werden.

Problem 1: Gefahr der Ausspähung der Bürger*innen

Beim Einsatz von QWACs besteht nach Ansicht vieler Expert*innen und Forschenden für IT-Sicherheit das Risiko, dass staatliche Behörden die von ihnen selbst erstellten Zertifikate nutzen können, um das Verhalten der eigenen Bürger*innen auszuspähen und Informationen über sie zu sammeln[5]. Darum haben sich diese Expert*innen und Forschenden während des Trilogs in einem offenen Brief[6] kritisch zu diesem Aspekt der notwendigen Novelle der eIDAS-Verordnung geäußert.

Problem 2: Gravierender Verstoß gegen die DSGVO

Ein weiterer, in dem offenen Brief diskutierter Punkt betrifft das Verhältnis der eIDAS-Verordnung zu datenschutzrechtlichen Vorgaben. Obwohl in dem Entwurf der eIDAS-Verordnung in Bezug auf die Verarbeitung personenbezogener Daten auf die Datenschutzgrundverordnung verwiesen wird, sind kohärente datenschutzrechtliche Regelungen in der eIDAS-Verordnung nicht erkennbar. Deshalb ist nach aktuellem Stand nicht auszuschließen, dass Regierungen über die Verwendung

---

[3] NZKart 2022, 97 – 100.
[4] https://www.heise.de/news/Elektronische-Identitaet-EU-Gremien-einigen-sich-auf-staatliche-Root-Zertifikate-9358024.html
[5] https://background.tagesspiegel.de/digitalisierung/eidas-das-sind-die-kompromisse
[6] https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr

der EUDI-Wallet in verschiedenen Lebensbereichen das Nutzungsverhalten ablesen könnte, was dem Datenschutzrecht stark zuwiderläuft.

Art. 6a Absatz 7 des Entwurfs der eIDAS-Verordnung sieht zwar vor, dass das Nutzungsverhalten unbeobachtet und die Daten untereinander unverknüpft bleiben sollen. Auf die EUDI-Wallet Zugriffsberechtigte können jedoch von Bürger*innen ein Einverständnis zur Datennutzung einwerben. Da die auf der Wallet hinterlegten Daten nur geringfügig voneinander getrennt sind, könnten anschließend mehrere oder gar aller Daten zusammengeführt und so ein Personenprofil erstellt werden[7].

„Ohne kohärente datenschutzrechtliche Regelungen und eine europaweit kompatible technische Lösung für die EUDI-Wallets werden die Sicherheit und Selbstbestimmtheit aller EU-Bürger*innen ab dem Jahr 2026 auf der Strecke bleiben“, befürchten Aline Vugrincic und Antonio Scaduto, wissenschaftliche Mitarbeitende im FZI-Forschungsbereich Cybersecurity and Law.

Die Lösung

Bislang stehen konkrete Schritte zur Umsetzung eIDAS-Verordnung noch aus. Deswegen gibt es die Möglichkeit für eine sichere technische Regelung und für eine bürgerfreundlichere Umsetzung.

Um allen EU-Bürger*innen bis zum Jahr 2026 eine funktionierende und sichere EUDI-Wallet anbieten zu können, welche wirklich EU-weit genutzt werden kann, muss eine Lösung jeweils auf Basis der gleichen technischen Architektur entwickelt werden. Für die entsprechenden Details und konkreten Anforderungen ist eine technische Arbeitsgruppe im Einsatz[8].

Nach Ansicht von FZI-Wissenschaftler*innen des Forschungsbereichs Cybersecurity and Law muss im Bereich der technischen Umsetzung neben der Benutzungsfreundlichkeit vor allem die Sicherheit, die Transparenz und die Selbstbestimmtheit im Vordergrund stehen. Dafür sollte Bürger*innen, die die EUDI-Wallet nutzen wollen, klar die Chancen und Risiken der EUDI-Wallet kommuniziert werden. Dann können sich diese der Folgen einer erteilten Zustimmung bewusst sein und informiert entscheiden.

Über das FZI Forschungszentrum Informatik

Das FZI Forschungszentrum Informatik erforscht sichere digitale Identitäten sowie die dazu notwendigen rechtliche Rahmenbedingungen, unter anderem in den Projekten SDIKA (https://www.sdika.de, BMWK-Programm Schaufenster sichere digitale Identitäten) und SDI4Ecom (https://www.sdi4ecom.de, Innovationsförderung der Invest BW). Das FZI beteiligt sich zudem am BMI-Konsultationsprozess zur EUDI-Wallet.

---

[7] https://netzpolitik.org/2023/eidas-reform-digitale-brieftasche-mit-ausspaehgarantie/#netzpolitik-pw
[8] https://background.tagesspiegel.de/digitalisierung/eidas-2-0-staerkt-europas-digitale-zukunft

Das FZI Forschungszentrum Informatik mit Hauptsitz in Karlsruhe und Außenstelle in Berlin ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Es bringt die neuesten wissenschaftlichen Erkenntnisse der Informationstechnologie in Unternehmen und öffentliche Einrichtungen und qualifiziert für eine akademische und wirtschaftliche Karriere oder den Sprung in die Selbstständigkeit. Betreut von Professoren verschiedener Hochschulen entwickeln die Forschungsgruppen am FZI interdisziplinär für ihre Auftraggeber Konzepte, Software-, Hardware- und Systemlösungen und setzen die gefundenen Lösungen prototypisch um. Mit dem FZI House of Living Labs steht eine einzigartige Forschungsumgebung für die Anwendungsforschung bereit. Das FZI ist Innovationspartner des Karlsruher Instituts für Technologie (KIT) und strategischer Partner der Gesellschaft für Informatik (GI).

Weitere Informationen

Jérôme Nguyen, Communications
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
Telefon: +49 721 9654-924
E-Mail: presse@fzi.de
Internet: www.fzi.de