Berlin. 02.09.2021

Stellungnahme

zur Neufassung des regulatorischen Frameworks eIDAS (electronic IDentification, Authentication and trust Services)

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de

Ansprechpartner für Rückfragen:

Dr. André Kudra
TeleTrusT-Vorstand
Leiter der TeleTrusT-AG "Blockchain" & TeleTrusT-AK "Secure Platform"
a.kudra@esatus.com

TeleTrusT kommentiert eIDAS 2.0

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) begrüßt den Vorschlag der Europäischen Kommission, auf Basis einer novellierten Fassung des regulatorischen Frameworks eIDAS (electronic IDentification, Authentication and trust Services) - hier subsumiert unter *eIDAS 2.0* - vertrauenswürdige und sichere Digitale Identitäten für alle Europäer zu etablieren. TeleTrusT-Mitglieder aus der Arbeitsgruppe "Blockchain" und dem Arbeitskreis "Forum elektronische Vertrauensdienste" haben die am 03.06.2021 publizierten Entwürfe einer detaillierten Analyse unterzogen und die entstandenen Ergebnisse und Forderungen zusammengefasst.

Self-Sovereign Identity (SSI) wird berücksichtigt und ermöglicht - ein Vertrauensmodell für SSI wird geschaffen

Eine "digitale Identität" ist ein Hilfsmittel für den Menschen, mit einem Computersystem zu interagieren. Für den Computer müssen Menschen, besonders in der vernetzten Welt, erreichbar und wiedererkennbar sein. Die eIDAS schafft dafür die notwendigen gesetzlichen Rahmenbedingungen.

Mit Self-Sovereign Identity, kurz SSI, wurde das digitale Identitätsmanagement neu erfunden. SSI liefert ein gänzliches neues Paradigma: Der Nutzer verwaltet und kontrolliert seine digitale Identität selbst, Fakten über den Nutzer stellen weiterhin Drittparteien aus, vertrauensstiftende Datenpunkte werden auf einer öffentlich zugänglichen, verteilten Datenbank (Distributed Ledger Technology, DLT) verankert und publiziert. Durch SSI entstand eine Situation, die durch die aktuelle eIDAS-Fassung nur unzureichend erfasst wurde und daher nicht adäquat abgedeckt werden konnte.

In einem öffentlichen Konsultationsverfahren zur eIDAS-Novellierung im Jahr 2020 wurde abgefragt, welche Verbesserungen und Optimierungen in die eIDAS-Verordnung - auch und insbesondere im Hinblick auf SSI - aufgenommen werden sollen. Diese Vorgehensweise wurde durch die zahlreichen SSI-Stakeholder und -Interessenvertreter intensiv genutzt. In der SSI-Gemeinschaft wird überaus positiv aufgenommen, dass der Vorschlag für eIDAS 2.0 eindeutig "SSI-freundlich" ist. Die eingereichten Vorschläge und Anmerkungen haben in weiten Teilen Anklang gefunden, sodass sie durch die Europäische Kommission berücksichtigt wurden.

Die eIDAS kennt nun explizit den Begriff "Self-Sovereign Identity" und dessen inhärenten Systematiken, d. h. ein dezentralisiertes Identitätssystem als elementaren Bestandteil, die Ausgestaltung mit Electronic Ledgers sowie die Digitale Wallet ("elektronische Brieftasche"). Tatsächlich werden eine "harmonised European Digital Identity Wallet" sowie eine "Toolbox for a European Digital Identity Framework" in Aussicht gestellt. Dies wird von TeleTrusT außerordentlich begrüßt.

SSI hat im Jahr 2021 ein enormes Momentum und hohe Sichtbarkeit erreicht. In vielfältigen hochkarätigen Initiativen in Deutschland und Europa wird darauf hingearbeitet, SSI in der Privatwirtschaft und der öffentlichen Verwaltung gleichermaßen in breiten Einsatz zu bringen. Die eIDAS-Novellierung liefert dazu flankierend Schub und die unabdingbare gesetzliche Grundlage.

Implementing Acts sind zu harmonisieren und möglichst viele sind zu implementieren, um ein "Level Playing Field" zu erreichen

TeleTrusT begrüßt die umfangreiche Anzahl verpflichtender Implementing Acts für die Europäische Kommission, wie sie derzeit im Proposal der neuen eIDAS enthalten sind. Im Sinne einheitlicher Vorgaben für den europäischen Binnenmarkt wird empfohlen, diese Anzahl nicht zu kürzen. Zudem sollten die Implementing Acts, wie im aktuellen Entwurf vorgesehen, auch auf europäische Standards und Normen verweisen. Nur so können gemeinsame technische Rahmenbedingungen, eine breite Umsetzung und vor allem Interoperabilität digitaler Identitäten und Vertrauensdienste gewährleistet werden.

Neben den aktuell vorgesehenen verpflichtenden Implementing Acts sollten diese auch bei Art. 20 und 24 eIDAS vorgesehen werden. Diese sollten auf europäische Standards hinsichtlich der grundlegenden Anforderungen an die Konformitätsbewertungsstelle im Allgemeinen (z.B. ETSI EN 319 403) sowie die grundsätzliche Konformitätsbewertung (qualifizierter) Vertrauensdienste im Besonderen verweisen (z.B. EN 319 401), um eine Vergleichbarkeit der Konformitätsbewertung in den Mitgliedsstaaten zu gewährleisten.

Darüber hinaus sollte auch Art. 45i um die Verpflichtung an die Europäische Kommission zum Erlass von Implementing Acts ergänzt werden. Electronic Ledger, im Kern DLT, bilden zum einen vielfach die technische Infrastruktur selbstsouveräner digitaler Identitäten (SSI), zum anderen schafft die European Blockchain

Service Infrastructure die technische Basis verteilter digitaler Ökosysteme in Europa auf Grundlage von DLT. Geprüfte wie vor allem vergleichbare und interoperable Vertrauenswürdigkeit elektronischer Ledger ist zur breiten Umsetzung und Anwendung von EBSI ebenso essentiell wie für das European Self-Sovereign Identity Framework (ESSIF). Umso mehr sollte mit verpflichtenden Implementing Acts, die wiederum auf europäische Standards und Normen verweisen (z.B. ETSI ESI, ETSI PDL, CEN JTC 19), ein gemeinsamer regulatorischer wie technischer Rahmen geschaffen werden, um eIDAS 2.0 im EWR erfolgreich umzusetzen.

Eine Umsetzungsförderung - auch der Kommunen - für Implementierung und Kommunikation sollte erfolgen

Der Erfolg der eIDAS 2.0 steht und fällt mit der Anwendung sicherer digitaler Identitäten und (qualifizierter) Vertrauensdienste. Der öffentlichen Verwaltung kommt hierbei eine Schlüsselrolle zu. Einerseits obliegt ihr die nationale Aufsicht und Verantwortung zur Informationssicherheit sowie die verpflichtende Akzeptanz bspw. des EU Digital Wallet oder aller mindestens fortgeschrittenen elektronischen Signaturen jedes qualifizierten Vertrauensdiensteanbieters. Andererseits umfassen G2B/G2C-Transaktionen einen wesentlichen Teil der Anwendungsfälle von eIDAS 2.0. In der ersten Fassung der eIDAS zeigte sich, dass Behörden zwar die Annahmepflichten umsetzten, nicht jedoch digitale Identitäten oder Vertrauensdienste selbst anwendeten. Ergebnis ist eine weiterhin begrenzte Digitalisierung der öffentlichen Verwaltung, was sich insbesondere in der Pandemie als nachteilig erwies. Um eine breite Anwendung der eIDAS 2.0 sicherzustellen, sollten öffentliche Stellen in Art. 6 und 27 eIDAS 2.0, neben den bestehenden Anerkennungsvorgaben, ebenso verpflichtet werden, digitale Identitäten und (qualifizierte) Vertrauensdienste verbindlich für die eigenen Anwendungsfälle einzusetzen. Unternehmen wie Bürger müssen die Möglichkeit erhalten jede digitale Identität, nur abhängig vom notwendigen Vertrauensniveau (LoA), jeden (qualifizierten) Vertrauensdienst bei einer Behörde einsetzen zu können und gleichzeitig darauf vertrauen zu können, dass öffentliche Stellen digitale Identitäten und (qualifizierte) Vertrauensdienste selbst einsetzen.

Zur Umsetzungsunterstützung sollten die Mitgliedsstaaten verpflichtet werden entsprechende Finanzmittel für die öffentlichen Stellen bereitzustellen und die Umsetzung digitaler Identitäten und (qualifizierter) Vertrauensdienste in öffentlichen Stellen gezielt zu fördern. Ebenso sollte eine verbindliche Umsetzungsfrist in eIDAS 2.0 definiert werden, um die zeitnahe Realisierung sicherzustellen.

EU Trusted List ist der Vertrauensanker für die Datenautobahn - sie ist eine Stärke der eIDAS und sollte der zentrale Vertrauensanker bleiben

Das übergeordnete Ziel der EU-Verordnung ist die Schaffung eines digitalen Binnenmarkts. Entsprechend sollen digitale Vertragsabschlüsse, Online-Dienstleistungen und elektronische Identitäten durch eIDAS gefördert und sicherer werden. Zu diesem Zweck definierte die Verordnung einen einheitlichen, europäischen Rechtsrahmen und vereinfachte bestehende Verfahren und Vorschriften, beispielsweise für die elektronische Unterschrift. Dabei verfolgt eIDAS einen für Innovationen offenen Ansatz und ist technologieneutral.

Ein wesentlicher Punkt ist die Schaffung der EU Trusted List auf der alle Vertrauensdienste in Europa mit ihren Vertrauensankern (beispielsweise CA-Zertifikate) gelistet sind. Die Liste ist sowohl menschenlesbar als auch maschinenlesbar. Somit wird auch technisch ermöglicht, alle Produkte die qualifizierte Vertrauensdiensteanbieter herausgeben, maschinell und kostenlos kryptographisch auf ihre Vertrauenswürdigkeit zu überprüfen. Ein praktisches Beispiel ist die Überprüfung der qualifizierten Signaturen durch den Adobe Reader, der die EU Trusted List unterstützt. Durch die offizielle Auflistung aller zugelassenen Vertrauensdienste mit ihren Vertrauensankern und der Möglichkeit diese zu jedem Zeitpunkt maschinell und kostenlos zu überprüfen, schuf die EU Kommission einen Vertrauensraum, in dem fast alle digitalen Dienste abgebildet werden können, wie z. B. DE-Mail, als sicherer E-Mail-Dienst, qualifizierte Signaturen und qualifizierte Siegel zur vertrauensvollen Sicherung von Dokumenten, natürlichen und rechtlichen Personen, nur um einige Beispiele zu nennen.

TeleTrusT fordert eine Aufnahme der Vertrauensanker der neuen Dienste wie qualified eletronic attestations of attributes (Artikel 3 (i) (45) oder qualified eletronic ledgers (Artikel 45 (i)) auf die EU Trusted List. Dies würde den bewährten Vertrauensraum auch auf die neuen Technologien erweitern und ein kostenloses öffentliches Vertrauen für neuen Technologien schaffen.

Die Verpflichtung, in Browsern Qualified Website Authentication Certificates (QWACs) anzuzeigen, wird unterstützt

Mit den eIDAS-Vertrauensdiensten ist ein Vertrauensraum entstanden, in dem Bürger, Behörden und Unternehmen sicher elektronisch kommunizieren können. Dazu gehört auch die Sicherheit, dass hinter einer Webseite eine echte und rechtmäßige Organisation steht. Zu diesem Zweck entwickelte die eIDAS-Verordnung sogenannte qualifizierte Webseiten-Zertifikate (QWAC). Technisch entsprechen sie den marktgängigen SSL-/TLS-Zertifikaten im Sicherheitsniveau und werden durch einen besonders sicheren Identifizierungsprozess von einem qualifizierten Vertrauensdiensteanbieter (qVDA) herausgegeben. Der Einsatz von QWACs wird jedoch leider bisher von den großen Browserherstellern nicht unterstützt, indem die Zertifikate weder als sicher akzeptiert oder im Browser angezeigt werden. Dies soll sich mit der eIDAS 2.0 ändern.

TeleTrusT begrüßt die Pflicht zur Anzeige der qualifizierten Webseiten-Zertifikate in Artikel 45.2. Dies fördert insbesondere den Verbraucherschutz, da es dem Verbraucher ermöglicht zu überprüfen, wem die Webseite gehört und beugt somit Phishing Attacken vor, wie eine Aachener Studie zeigt. So werden 99,6 Prozent der Phishing-Angriffe über Webseiten durchgeführt, die nicht mit EV-Zertifikaten gesichert sind. (EV-Zertifikate, sind SSL Zertifikate mit einem höheren Identifizierungsniveau, die jedoch auch nicht mehr seit 2018 von den Browsern angezeigt werden.)

Auch wäre der Missbrauch, der im April 2020 durch "Fake Corona Hilfen Antragsseiten" durchgeführt worden ist, nicht so einfach möglich gewesen, denn die Antragsteller hätten durch Verwendung von QWAC und ihrer Darstellung im Browser schneller feststellen können, dass sie sich auf einer betrügerischen Webseite befinden.

Eine Anzeige der QWAC-Zertifikate durch die Browser-Hersteller und eine Validierung dieser Zertifikate gegen die EU Trusted List, wie dies seit Jahren beim Adobe Reader üblich ist, würde die Digitalisierung ein ganzes Stück sicherer machen und Europa ein Stück digitale Souveränität zurückgeben, da nun die Rahmenbedingung der Identifizierung nicht mehr von den willkürlichen Änderungen der Bedingungen durch die Browserhersteller abhängen würden.

Europa hat positive Erfahrungen mit der Verwendung der QWAC-Zertifikate im Umfeld der Online-Zahlungsdienste (Payment Services Directive 2 - PSD2) gemacht. Hier wurde die Unterstützung durch QWAC ebenfalls vorgeschrieben und dies ermöglichte neue Geschäftsmodelle für FinTechs. Mit dem eIDAS Proposal und dem Artikel 45 (2) wird die vertrauensvolle Digitalisierung in einem neuen Marktsegment ermöglicht.

TeleTrusT empfiehlt die Strafbewehrung zur Durchsetzung der gesetzlichen Verpflichtungen aus der eIDAS Verordnung.