

Auf einen Blick

eIDAS Review & EU Digital ID

Ausgangslage

Die EU Kommission stellte am 3. Juni 2021 den Verordnungsvorschlag für die EU Digital ID und den Review der eIDAS Verordnung vor. Der Vorschlag soll die Nutzung der digitalen Identität fördern und beinhaltet unter anderem die Einführung der ID-Wallet, mit der Bürger sich digital ausweisen und ihre Identitätsdaten und amtlichen Dokumente in elektronischer Form speichern und verwalten können.

Bitkom-Bewertung

Geht in die richtige Richtung: Der Vorschlag zur Schaffung der EU ID und Wallet ist ein wichtiger Schritt.

Unsere Ziele sind eine hohe Akzeptanz, Marktoffenheit, europäische Harmonisierung sowie europaweite Anwendungsmöglichkeiten.

Das Wichtigste

Im Detail lässt der Vorschlag noch Fragen offen und bedarf der Nachbesserung, insbesondere bezüglich folgender Punkte:

- **Technische Details, Standardisierung und Wechselwirkungen mit weiterer Regulierung**

Technische Details des Designs der Wallet und die zugrundegelegten Standards sind noch nicht abschließend geklärt und müssen gemeinsam mit der Industrie konsultiert und entwickelt werden. Außerdem ist Kohärenz im Regulierungsrahmen unbedingt sicherzustellen.

- **Erfolgreiche Durchsetzung im Markt**

Für erfolgreichen Wettbewerb mit bestmöglichen Lösungen und einer erfolgreichen Durchsetzung der Wallets sollte sich die EU aus unserer Sicht dafür einsetzen, dass mehrere zertifizierte Wallets nebeneinander im Markt existieren können. Die Anforderungen an die Zertifizierung sollten einheitlich, realistisch und praxisnah von der EU vorgegeben werden.

- **Incentivierung der Anwendung ohne pauschale Verpflichtung**

Wir sind der Überzeugung, dass die EU die Mitgliedstaaten ermutigen sollte, digitale Lösungen anzubieten, die für Nutzer attraktiv und überzeugend genug sind, um sie anzunehmen. Eine pauschale, undifferenzierte Verpflichtung bürdet Unternehmen der Privatwirtschaft unnötige Anstrengungen, hohe Verunsicherung und Kosten auf.

eIDAS Review & Digitale Identitäten

September 2021

Seite 2

Zusammenfassung

Bitkom begrüßt den Entwurf der EU-Kommission, da dieser einen weiteren wichtigen Grundstein für sichere digitale Identitäten und Vertrauensdienste in der Europäischen Union legt. Die digitale Souveränität Europas wird gestärkt, indem digitale Identitäten etabliert und diese von EU-Bürgern EU-weit selbstbestimmt genutzt werden können. Bitkom bedankt sich für die Möglichkeit im Rahmen des Konsultationsprozesses Stellung zu nehmen.

Die Europäische Kommission hat zurecht erkannt, dass die digitalen Identitäten weiterhin unter der Hoheit der Mitgliedstaaten bereitgestellt werden sollten. Auch die Einführung neuer Vertrauensdienste ergänzt das europaweit aufgespannte Netz von Vertrauensdiensten sinnvoll. Zudem ist es erfreulich, dass insgesamt ein eID-Ökosystem mit entsprechender Anschlussfähigkeit an weitere europäische Initiativen (wie den Digital Markets Act (DMA) und den Digital Services Act (DSA)) angestrebt wird. In diesem Zusammenhang ist insbesondere die Verpflichtung zur verbraucherfreundlichen Darstellung von qualifizierten Website-Zertifikaten (QWACs) positiv hervorzuheben.

Im Detail bedarf der Vorschlag aus unserer Sicht jedoch noch der Anpassung um flächendeckende Durchsetzung, Nutzerfreundlichkeit und Akzeptanz zu erzielen. Dies kann aus unserer Sicht nur durch transparente und breite Beteiligung der Industrie bei der Entwicklung, dem Design, Standardfestlegung und weiterer Anforderungen an die Wallet und ihre Nutzung erreicht werden. Kohärenz im gesamten Regulierungsrahmen ist dabei ebenso sicherzustellen. Wir sind außerdem der Überzeugung, dass die EU die Mitgliedstaaten ermutigen sollten, digitale Lösungen anzubieten, die für Nutzer attraktiv und überzeugend genug sind, um sie anzunehmen. Eine pauschale, undifferenzierte Verpflichtung bürdet Unternehmen der Privatwirtschaft unnötige Anstrengungen, hohe Verunsicherung und Kosten auf.

Für erfolgreichen Wettbewerb mit bestmöglichen Lösungen und einer erfolgreichen Durchsetzung der Wallets sollte sich die EU ebenfalls dafür einsetzen, dass mehrere zertifizierte Wallets nebeneinander im Markt existieren können. Die Anforderungen an die Zertifizierung sollten einheitlich und praxisnah von der EU vorgegeben werden.

Detailbewertung

Im Folgenden gehen wir auf die aus unserer Sicht relevantesten Details zum Verordnungsvorschlag ein.

1) Referenzen auf natürliche und juristische Personen

Bitkom begrüßt, dass die Wallets auch für jur. Personen eingeführt werden. Es sollte aber in den Kapiteln I-III klargestellt werden, welche Regelung sich jeweils auf nat. und/oder juristische Personen bezieht. Selbiges gilt für "personenbezogene Daten" und "Personenidentifizierungsdaten".

Die eIDAS 2.0 sollte daneben klarstellen, dass sowohl die EU-Digital Wallet, also auch die staatlichen wie privaten eID Schemes sowie die damit zusammenhängenden Regelungen für juristische und natürliche Personen gelten, sofern nicht für einzelne Regelung eine spezielle Ausrichtung notwendig ist.

2) Zu Artikel 3d): Aufnahme von Identifizierungsdiensten in die Liste der Vertrauensdienste

„Identifizierungsdienste“ nach Art. 24 sind ein zentraler Aspekt der Vertrauensdienste und sollten als eigenständiger Vertrauensdienst reguliert werden. Es sollte die Möglichkeit ergänzt werden, dass Identifizierungsdienste auch als qualifizierte Vertrauensdienste geprüft und gelistet werden. Dies würde für eine Harmonisierung der unterschiedlichen Niveaus bei den Identifizierungsverfahren und für eine Angleichung der Sicherheitsniveaus sorgen. Aktuell gibt es stark abweichende Regelungen, was zu einer Wettbewerbsverzerrung führt.

Bei der Prüfung sollten geeignete technische Standards wie beispielsweise der ETSI TS 119 461 zur Einstufung des Vertrauensniveaus herangezogen werden.

Alternativ zu einer Regulierung als eigenständiger Vertrauensdienst sollte zumindest sichergestellt werden, dass eine Harmonisierung auf europäischer Ebene sowohl auf technischen Standards beruht als auch durch eine Harmonisierung der Zertifizierungsanforderungen der Konformitätsbewertungsstellen erfolgt.

3) Zu Artikel 6a (Einführung einer European Digital Identity Wallet)

Für erfolgreichen Wettbewerb mit bestmöglichen Lösungen und einer erfolgreichen Durchsetzung der Wallets sollte sich die EU dafür einsetzen, dass mehrere zertifizierte

Wallets nebeneinander im Markt existieren können. Die Anforderungen an die Zertifizierung sollten einheitlich und praxisnah von der EU vorgegeben werden

Weiterhin sollte in Art. 6a Abs. 3 b) klargestellt werden, dass neben der qualifizierten elektronischen Signatur auch das Unterzeichnen mit qualifizierten elektronischen Siegeln aus der Wallet heraus möglich ist.

Mit Bezug auf Artikel 6a Absatz 3 Buchstabe b) ("European Digital Identity Wallets shall enable the user to: [...] (b) sign by means of qualified electronic signatures") sollte gewährleistet werden, dass das Wallet als Identifizierungs- und Authentisierungsinstrument für die Verwendung eines qualifizierten elektronischen Zertifikats für eine qualifizierte elektronische Signatur dient, das von einem QTSP ausgestellt wurde, der vom Eigentümer des Wallets (bzw. je nach Prozess und Anwendungsfall, von der Relying Party) *frei gewählt* wurde. Anderenfalls besteht die Gefahr, dass wenn der Walletanbieter selbst als QTSP tätig ist, diese freie Wahl „eingeschränkt“ werden könnte (mit negativen Auswirkungen auf den fairen Wettbewerb im digitalen Binnenmarkt bzw. Erleichterung von Monopolen bzw. marktbeherrschende Stellungen).

Für den Erfolg der EU-Wallet muss sichergestellt sein, dass alle verifizierbaren Attribute über die EU-Wallet abgebildet werden können, wie z.B. in Registern hinterlegte Vertretungsbefugnisse. Ein Ausschluss würde die Anwendungsszenarien und damit den Erfolg der EU-Wallets unnötig einschränken.

4) Zu Artikel 6b) Anforderungen an relying partys

Juristische Personen sollten die EU-Digital Wallet möglichst umfassend aktiv einsetzen. Daher sollten juristische Personen, welche sich als relying party registrieren, selbst zur Nutzung einer EU-Digital Wallet verpflichtet sein.

Die Anforderungen an die von den relying parties angewandten Verfahren und die durchzuführenden Prüfungen müssen jedoch noch näher definiert und Begrifflichkeiten klargestellt werden.

5) Neue Zertifizierungsanforderungen für die Wallet (Art. 6c)

Art. 6 der eIDAS-VO von 2014, der eine gegenseitige Anerkennung von eIDs vorsah, wurde durch neue Regelungen zur EU Digital Identity Wallet (Art. 6 a-d) ersetzt. Die Wallets müssen – wie auch andere elektronische Identifizierungsmittel – von den Mitgliedstaaten anerkannt werden (Art. 12b und c). Zugleich werden Zertifizierungsstandards festgelegt (Art. 6c (4)), welche die Wallets erfüllen müssen.

Wir begrüßen die vorgesehenen Durchführungsrechtsakte (Art. 6c (1)). Sie führen zu einer stärkeren Harmonisierung der Anforderungen. Auf diese Weise wird den EU-Bürgern die Nutzung erleichtert und die Reichweite erhöht.

6) zu Artikel 10a (Auftreten von Sicherheitslücken)

Wenn eine Sicherheitslücke auftritt, soll nach dem Vorschlag der Kommission die Ausstellung und Gültigkeit der digitalen Briefftasche ausgesetzt werden.

Wir halten hier Klarstellungen für erforderlich. Die Bereitstellung von ID-Wallets ist sowohl im hoheitlichen als auch im wirtschaftlichen Bereich von eminenter Bedeutung. Hier bedarf es einer „Resilienz“-Ergänzung, die sicherstellt, dass bei einer Kompromittierung des Systems der weitere Betrieb (notfalls analog) gesichert ist.

7) Zu Artikel 11 a (2): Eine eindeutige und dauerhafte Kennung muss auch an juristische Personen vergeben werden.

Wir unterstützen die Anforderungen zur Bereitstellung einer eindeutigen und dauerhafte Kennung an natürliche und juristische Personen und fordern, dieses Identifizierungskennzeichen angelehnt an internationale Spezifikationen, z.B. nach ETSI auszugestalten. Vgl. Kapitel 5.1.4 ETSI EN 319 412-1 (2020-07)

Mit Bezug auf die juristischen Personen wäre ein Hinweis auf die Möglichkeit des Einsatzes von LEI (Legal Entity Identifier: <https://www.gleif.org/de/about-lei/introducing-the-legal-entity-identifier-lei>) wünschenswert.

8) Zu Artikel 12b: Akzeptanz der Wallet

Der Kommissionsentwurf sieht vor, dass mit dem neu einzufügenden Artikel 12b, neben den großen Plattformbetreibern („very large online platforms“ wie im Digital Service Act definiert) auch zahlreiche privatwirtschaftliche Branchen per se zur Akzeptanz der European Digital Identity Wallet verpflichtet werden (siehe Artikel 12b (2) im Entwurf). Hierbei wird offensichtlich das Ziel einer möglichst durchgängigen Verbreitung des European Digital Identity Wallet verfolgt. Eine Verpflichtung ganzer Branchen, ohne konkreten Bezug zu definierten relevanten Anwendungsfällen für die Bürger*innen, ist zu pauschal. Die Kommission schlägt vor, dass Stakeholder aus zahlreichen Branchen verpflichtet werden sollten, EU Digital Identity Wallets zu akzeptieren, bei denen eine starke Benutzerauthentifizierung für die Online-Identifizierung durch nationales Recht oder EU-Recht oder durch vertragliche Verpflichtung erforderlich ist. Wir sind der Überzeugung, dass die EU Institutionen die Mitgliedstaaten ermutigen sollten, digitale Lösungen anzubieten, die für Nutzer attraktiv und überzeugend genug sind, um sie anzunehmen. Eine pauschale,

undifferenzierte Verpflichtung bürdet Unternehmen der Privatwirtschaft unnötige Anstrengungen, hohe Verunsicherung und Kosten auf. Ohne klare Rahmenbedingungen, wann ein Unternehmen von der Verpflichtung betroffen sein soll, zeitlich ausreichende und nutzerzahlabhängige Übergangsfristen, sowie eine strenge Begrenzung auf die Regulierung der wirklich relevanten Anwendungsfälle, ist mit fehlender Akzeptanz durch die Privatwirtschaft zu rechnen.

9) zu Art. 24c (Harmonisierung bei der Zertifizierung von Vertrauensdiensten)

Die Europäische Kommission wird deutlich mehr Durchführungsrechtsakte erlassen, die auf internationale technische Standards referenzieren werden, die z.B. durch CEN und ETSI erlassen werden. Durch diese Durchführungsrechtsakte können die Anforderungen an die Zertifizierung von Vertrauensdiensten stärker harmonisiert werden. Für Art. 24c wurde durch die ETSI bereits ein neuer Standard ETSI TS 119 461 veröffentlicht, welcher durch die Kommission akzeptiert werden sollte.

Wir begrüßen das Bestreben der Europäischen Kommission, die Zertifizierung von Vertrauensdiensten weiter zu harmonisieren. In diesem Zusammenhang könnten die bisher zugelassenen Systeme auf Basis „vergleichbarer Sicherheit“ mittelfristig nicht mehr zulässig sein. Für diese Fälle wäre es sinnvoll und wünschenswert, eine Übergangsfrist vorzusehen.

10) zu Art 45. a-f

a) Neue Vertrauensdienste

Neue Vertrauensdienste sollen den EU-weit aufgespannten Vertrauensraum ergänzen. Dazu gehören Vertrauensdienste zur elektronischen Archivierung und elektronischen Attestierung von Attributen, zur Verwaltung von elektronischen Fernsignatur- und Siegelerstellungsgeräten oder elektronische Ledger.

Die neuen Vertrauensdienste bieten aus unserer Sicht große Chancen für den digitalen Binnenmarkt.

b) Spezifikationen notwendig

Dies gilt auch für die Einführung des im Entwurf enthaltenen neuen qualifizierten Vertrauensdienstes „electronic attestation of attributes“ den wir prinzipiell begrüßen. Denn durch den Vertrauensdienst, aufgeführt im neuen Sektor 9 des Verordnungsentwurfs (Artikel 45 a-f), folgt die logische Ergänzung um reine Identitätsdaten der Bürger*innen. Aus dem Entwurf wird jedoch nicht deutlich, wie ein

solcher Vertrauensdienst über alle EU-Mitgliedsstaaten hinweg funktionieren soll. Viele dringend notwendige Spezifikationen werden, aus nicht nachvollziehbaren Gründen, auf spätere Implementing Acts verschoben.

Darüber hinaus werden in dem Entwurf die unterschiedlichen Verantwortlichkeiten zwischen den Nationalstaaten und den Vertrauensdiensteanbietern nicht ausgearbeitet. Es wird zum Beispiel nicht deutlich, unter welchen Umständen designierte Intermediäre als Quelle auftreten können oder wann es sich um eine nationale Quelle handeln muss. Somit bleibt unklar, wer zum Beispiel in föderalen Verbänden oder zentralstaatlich die geforderten Möglichkeiten zum elektronischen Zugriff auf die „öffentlichen Quellen“ zu schaffen hat. Vielmehr muss genau spezifiziert werden, wie eine Vertrauenswürdigkeit der Quellen hergestellt und dauerhaft gewährleistet werden kann.

Nicht nachvollziehbar erscheint der Entwurf auch mit seiner Forderung in Artikel 45f (4), wonach ein Vertrauensdienst nur in einer separaten Rechtseinheit betrieben werden darf. Wie ist dieses zu begründen? Worin unterscheidet sich die „Qualität“ dieses Vertrauensdienstes von anderen, bei denen diese Forderung nicht aufgestellt wird. Es muss aus unserer Sicht dringend unterschieden werden zwischen Wallet Providern sowie den Providern der verschiedenen qualifizierten Attribute in der Wallet. Demnach sollte die unter Artikel 45f (4) aufgeführte Forderung lediglich für Wallet Provider gelten, nicht jedoch für die Zulieferer der Attribute. Die Gründung einer ausgelagerten Rechtseinheit würde eine zusätzliche Hürde für die Anbieter von Vertrauensdiensten zur Folge haben.

Ein Sicherheitsgewinn durch eine rechtliche Trennung erschließt sich lediglich für den Anbieter und Betreiber des Wallets als Datenintermediär, bei dem eine Weiterverwendung gewonnener Daten ausgeschlossen werden muss. Wir halten für mehr Transparenz und Sicherheit eine europäische Vertrauensliste, in der die Quellen der qualifizierten Attribute einheitlich eingetragen sind und analog der *European Trustlist* zur Validierung öffentlich für alle herangezogen werden können für sinnvoll.

c) QWACs

Die vorgeschlagene Visualisierung von QWACs ist ein Meilenstein für den digitalen Binnenmarkt und stärkt den europäischen Verbraucher- und Datenschutz. Die Visualisierung der QWACs ist eine wichtige Maßnahme, die zu mehr Transparenz und Datenschutz in der digitalen Welt führt.

11) Zu Art. 45 f: Zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen

Beschränkung des personenbezogenen Profilings werden zur Zeit intensiv diskutiert, sind aber auch bereits gesetzlich adressiert. Die aktuelle Formulierung geht in jedem Fall über die Anforderungen der DS-GVO hinaus.

Wir schlagen vor, Artikel 45f komplett zu streichen und die Anforderung in Artikel 6a 7) durch einen Hinweis auf die geltende DS-GVO zu ersetzen.

12) Backup Möglichkeiten

Es muss berücksichtigt werden, dass die Bürger ihre Smartphones häufig wechseln oder auch verlieren. Diesem Umstand ist Rechnung zu tragen und die Notwendigkeit eines verschlüsselten Backups daher sehr wichtig. Im VO Entwurf wird nicht deutlich, wie eine Lösung aussehen kann.

Sinnvoll erscheint uns hier z.B. ein HSM-gestütztes serverseitiges Backup. Solche Systeme können so implementiert werden, dass selbst der Anbieter keine Möglichkeit hat, auf die Daten zuzugreifen, während gleichzeitig die notwendige starke Kundenauthentifizierung (2-Faktor) zur Wiederherstellung des Backups gewährleistet ist.

13) Tool Box

Die Expertengruppe welche die Toolbox ausarbeitet sollte auch mit Vertretern von Verbänden und privaten Anbietern ergänzt werden. Auch dieses Know-How und die dortigen Interessen müssen vertreten sein, um insb. Auch Aspekte rund um internationale Standards, geistiges Eigentum, Daten- und Know-How-schutz einfließen zu lassen. Wenn das Ziel ein offenes Ökosystem ist müssen auch die Expertengruppen entsprechend offen und transparent gestaltet sein.

14) Authentifizierung / Biometrie

Die Verbreitung der EU eID Wallet wird wesentlich von der Usability abhängen. Ein alleinige Nutzung einer PIN hat sich als nicht sicher und nicht nutzerfreundlich gezeigt. Biometrie als Authentifizierungsverfahren sollten möglich gemacht werden. Dahingehend sollte ebenso auf ein Zertifizierungsprogramm für das Sicherheitsniveau der biometrischen Sensoren abgestellt werden.

15) Offenes Ökosystem / Wahlfreiheit

Um das Ziel eines offenen Ökosystems zu erreichen ist ein besonderer Fokus auf die Interoperabilität und Übertragbarkeit der Identitäten und Attribute in den Wallets zu legen. Um ein europäisches Ökosystem zu etablieren sollte es beispielsweise möglich sein, die Identität eines deutschen Bürgers in die Wallet eines anderen Mitgliedsstaates zu legen (z.B. eine französische EU eID Wallet). Ebenso muss die Wahlfreiheit der Bürger gewährt bleiben und sichergestellt werden, dass der VO Entwurf die Möglichkeit eröffnet, dass der Bürger seine Identität aus zwischen zwei zertifizierten Wallets transferieren kann. Dies ergibt sich auch aus der Notwendigkeit Backups zu ermöglichen: Hier muss ein Transfer auf ein neues Gerät möglich sein sowie ein verschlüsseltes Backup möglich sein.

16) Datenschutz und Cybersicherheit (insb. im Kontext der NIS2-RL)

Datenschutz, Digital Trust und Cybersicherheit sind die drei Säulen der digitalen Welt, und Europa gibt mit der DSGVO, der eIDAS-Verordnung und der NIS-Richtlinie(n) den Weg für ihre Regulierung vor. Der Vorschlag unterstreicht die Notwendigkeit, dass Digital Wallets, QTSPs und Vertrauensdienste ein Höchstmaß an Sicherheit gewährleisten, und schreibt in Artikel 24 a) vor, dass QTSPs Artikel 18 der NIS-2-Richtlinie einhalten müssen. Obwohl wir dem Prinzip zustimmen, müssen wir darauf hinweisen, dass dies das Risiko möglicher zukünftiger Abweichungen zwischen den Sicherheitsanforderungen für QTSPs in verschiedenen Mitgliedstaaten birgt, was die Harmonisierung beeinträchtigt. Da es sich bei der NIS 2 um eine Richtlinie handelt, kann jeder Mitgliedstaat nämlich bei der Umsetzungsphase eine unterschiedliche Auslegung unterstützen; wenn wir außerdem bedenken, dass sich die NIS-Aufsichtsstellen von den eIDAS-Aufsichtsstellen unterscheiden könnten, besteht die Möglichkeit von Konflikten, die Auswirkungen auf die Harmonisierung und die Kosten für die Bereitstellung ähnlicher Vertrauensdienste in der EU haben könnten. Eine strikte Koordination zwischen der Kommission, der ENISA, dem Kooperationsnetzwerk und den NIS-Aufsichtsorganen ebenso wie klare Richtlinien für QTSPs, wie sie die Anforderungen erfüllen sollen, für die Aufsichtsorgane, um den Überwachungsprozess zu leiten, und für die CAB, um die Ansätze während der Audits zu harmonisieren sind daher sehr wichtig, um dieses Problem zu verhindern.

Der eIDAS-Vorschlag führt in Artikel 3 Nr. 53) die Definition des „electronic ledger“ ein („tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering“). Die Definition ist sehr offen und selbst mit Hilfe von Präambeln und anderen Verweisen ist es nicht klar, was das Ziel der Verordnung zu diesem Thema

ist, und auch nicht, was „electronic ledger“ nach diesem Artikel tatsächlich ist. Es könnte sinnvoll sein, die folgenden Punkten besser zu verdeutlichen:

a) Ziel der Verordnung: gemäß Präambel 34 soll ein qualifiziertes electronic ledger einen Governance-Rahmen und SSI ermöglichen. Die derzeitige eIDAS-Verordnung verfolgt bereits einen zentralisierten Ansatz in Bezug auf die Identität, aber wenn das Ziel des neuen Vorschlags darin besteht, zu einer stärker dezentralisierten Lösung überzugehen, sollte dies deutlicher zum Ausdruck gebracht werden.

b) Definition von „electronic ledger“: angesichts der Definition könnten heute viele Instrumente die Unveränderbarkeit und Zeitstempelung von Daten gewährleisten - und werden auch dafür verwendet. Es könnte nützlich sein, mehr Details hinzuzufügen, um zu verstehen, worin der Wert eines neuen qualifizierten Vertrauensdienstes besteht, und um hervorzuheben, welche Aufgaben ein „electronic ledger“ besser erfüllen kann als die bestehenden Vertrauensdienste. Diese Klarstellung wird auch eine Doppelregulierung des Themas vermeiden: viele der heute von Regierungen und Unternehmen genutzten elektronischen Ledger sind bereits in den Mitgliedstaaten reguliert.

17) Aktive Teilnahme von Behörden

Anknüpfend an den EU Vorschlag sollte die Gesetzgebung der Mitgliedsstaaten Behörden in allen relevanten Fachgesetzen durchgängig dazu verpflichten, in den verschiedenen Rollen am Ökosystem teilzunehmen und existierende Trust Services (z.B. elektronische Siegel und neu entstehende Mittel (electronic means/attestations) auch aktiv einzusetzen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.