

Der Arbeitskreis Anwendung elektronischer Vertrauensdienste stellt die zentralen Thesen und Fragen seines Mitgliedertreffens hier in kompakter Form vor.

Leitfragen und Thesen: Vertrauensdienste und ihre Anbieter

Frage 1: Was braucht es, um für deutsche QTSPs in Europa ein level playing field zu schaffen?

Um für deutsche QTSPs in Europa ein level playing field zu schaffen, ist es notwendig, deutsche Sonderregeln im Bereich der Vertrauensdienste abzuschaffen, bzw. auf europäische Regelungen anzupassen. Dies gilt besonders für europäische Richtlinien, die nicht unmittelbar geltendes Recht in den Mitgliedsstaaten sind. So muss die NIS-Richtlinie einheitlich in nationales Recht umgesetzt werden, um die Gefahr von 27 unterschiedlichen europäischen Cybersicherheitsanforderungen zu vermeiden.

Ähnlich wie im Bereich der Identifizierung sollten Regelungen in Europa nur noch über gemeinsame Standards erfolgen. Hierbei ist eine enge Kooperation der Sicherheits- und Aufsichtsbehörden, Konformitätsbewertungsstellen und Standardisierungsgremien zwingend notwendig. So kann in der europaweiten Standardisierung ein gutes, zukunftsfähiges Konstrukt entstehen, das ein level playing field für alle schafft.

Der deutsche Föderalismus stellt hierbei eine besondere Herausforderung dar, da die unterschiedlichen Zuständigkeiten der Bundesländer eine einheitliche Umsetzung erschweren können. Diese Hürden gilt es gemeinsam mit Bund, Ländern, Kommunen und Unternehmen zu überwinden.

Frage 2: Wie erhöhen wir den Bekanntheitsgrad und das Vertrauen in den Einsatz elektronischer Vertrauensdienste?

Ein Hebel für die Akzeptanz von Vertrauensdiensten wird die Wallet sein. Eine Möglichkeit, diesen Hebel auch nutzen zu können, sind Awareness-Kampagnen. Diese wurden bereits im europäischen Ausland durchgeführt, um für die Nutzung von Vertrauensdiensten und nationalen Wallets zu werben.

Doch auch hier ist die Frage nach der Verantwortung durch den Föderalismus und den daraus entstehenden nationalen Flickenteppich entscheidend für den Erfolg. In Deutschland fehlt es an einer zentralen Leitung, die Länder und Kommunen bei der Implementierung von Vertrauensdiensten unterstützt. Hier bedingen sich Verwaltung und Wirtschaft gegenseitig: auf der einen Seite kann der Wirtschaft eine wichtige Rolle zukommen, da sie einen starken Impuls für die Nutzung liefern kann. Auch kann sie eine Art „Einsatzbeschreibung“ für Vertrauensdienste für die Verwaltung liefern, die ein klares

Ablaufschema und klare Nutzungsempfehlungen beinhaltet, um darüber aufzuklären, wofür welcher Vertrauensdienst genutzt werden kann.

Die Verwaltung andererseits kann, wenn sie auch nicht der Treiber sein wird, eine Initialzündung geben. In Österreich zum Beispiel wurden mit der Einführung der Handysignatur für die Erledigung von Amtsgängen millionenfach Signaturzertifikate verteilt – und damit der Schlüssel zu privaten Anwendungsfällen. Außerdem können Vertrauensdienste in der Entbürokratisierung von internen und externen Verwaltungsprozessen effizient eingebunden und so Bürgerinnen und Bürger an die verschiedenen Dienste herangeführt werden.

Dies wird jedoch auch bedingt durch eine einfache Möglichkeit für Bürgerinnen und Bürger, an diese Zertifikate und Dienste heranzukommen. Ein einfacher Zugang ist eine Grundvoraussetzung für die Verbreitung von Vertrauensdiensten und geht Hand in Hand mit einer durchdachten Kampagne sowie alltäglichen Use Cases.

Die Verwaltung kann eine Initialzündung für Vertrauensdienste geben, wenn sie auch nicht der Treiber sein wird.

These 1: Deutsche Vertrauensdiensteanbieter erhöhen unsere Souveränität.

Deutsche Vertrauensdiensteanbieter (QTSPs) agieren nicht in einem rein deutschen Kontext. eIDAS hat als ursprüngliches Ziel, den europäischen Vertrauensdienstemarkt zu harmonisieren und grenzüberschreitend gültige Regeln aufzustellen. Wenn wir über QTSPs sprechen, müssen wir also nicht nur national, sondern vor allem europäisch denken. Für die digitale Souveränität spielen europäische Vertrauensdiensteanbieter eine entscheidende Rolle. Deutsche QTSPs allerdings brauchen weniger, durch deutsche Sicherheits- und Aufsichtsbehörden aufgestellte, Hürden, um auf dem europäischen Markt agieren zu können. Dann erhöhen wir die Wettbewerbsfähigkeit deutscher Anbieter in Europa und stärken weiter die Souveränität Europas, die von allen europäischen QTSPs getragen wird – und die von Staat und Unternehmen kooperativ vorangetrieben werden muss.

Wenn wir über Qualifizierte Vertrauensdiensteanbieter sprechen, müssen wir also nicht nur national, sondern vor allem europäisch denken.

These 2: Wenn Vertrauensdienste in Gesetzen nicht erwähnt werden, werden sie nicht genutzt.

Wenn Vertrauensdienste nicht in den relevanten Gesetzen erwähnt und die Attribute ausstellenden Akteure nicht zur Digitalisierung verpflichtet werden, wird es für Vertrauensdienste sicher schwerer, sich flächendeckend durchzusetzen. In der Nutzung von elektronischen Signaturen und Attributzertifikaten hat der Staat eine Rolle, Schriftformerfordernisse auch digital abzubilden und Authentic Sources anzuhalten,

digitale Zertifikate zur Verfügung zu stellen. Dass sie jedoch nur mit regulatorischem Zwang in Deutschland genutzt werden, ist nicht zu befürchten.

Der Grund liegt in Europa: die eIDAS-Verordnung sieht bereits für bestimmte Sektoren wie Bildung oder Gesundheit den Einsatz digitaler Attributszertifikate vor, im Tourismus ist die Nutzung digitaler Tickets und Buchungsbelege schon länger gängige Praxis. Über die EUDI-Wallet sollen Nutzende außerdem qualifizierte elektronische Signaturen einfacher auslösen können. Spätestens durch die Wallet ist also ein Anstieg in der Nutzung von Vertrauensdiensten zu erwarten.

Ein solider und stringenter regulatorischer Rahmen für Vertrauensdienste ist also zwar ohne Zweifel eine starke Grundlage für ihre Verbreitung und, gesetzlich vorgeschriebene, Nutzung. Doch wie dieses Whitepaper zeigt, muss eine Vielzahl an Faktoren zusammenspielen, um Vertrauensdienste in die Breite zu tragen. Dazu gehören neben der Regulatorik vor allem ihre Bekanntmachung durch Kampagnen, eine vereinfachte Zugänglichkeit, sowie eine Wirtschaft, die mit der Bereitschaft zur Schaffung von Use Cases als Impulsgeber auftritt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. 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, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. 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 leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Clemens Schlepner | Referent Vertrauensdienste & Digitale Identitäten

T 030 27576-424 | c.schlepner@bitkom.org

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste

Copyright

Bitkom 2023

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.