Die Ausweisapp2 verspricht eine Revolution, doch Sie stellt auch höchste Ansprüche an den Datenschutz

22.03.2021 – München: Es ist nichts weniger als ein Quantensprung, den uns die digitale Ausweisapp2[1] – ein ambitioniertes und zugleich überfälliges Projekt des Bundes – verspricht. Die App ist zwar schon seit einiger Zeit verfügbar, doch bisher haben noch zu wenige Bürger von ihrer Existenz Notiz genommen, geschweige denn ihre Funktionen bereits genutzt.

Viel zu lange haben wir in Deutschland darauf warten müssen, eine praktische Lösung zur Identifikation im Internet an die Hand geliefert zu bekommen. Während digitale Vorreiter wie Estland bereits 99 Prozent ihrer Behörden-"Gänge" bequem über das Smartphone oder den PC abwickeln können[2], hinkt die deutsche Verwaltung bei der Digitalisierung noch deutlich hinterher. Immerhin hat sich der Bund im Jahre 2017 mit dem Onlinezugangsgesetz zur Digitalisierung der öffentlichen Verwaltung bis spätestens Ende 2022 verpflichtet[3]. Die Ausweisapp2 des Innenministeriums steckt zwar noch in den Kinderschuhen, doch sie legt auch den Grundstein für Behördengänge sowie Geschäftsabwicklungen im Internet.

Der digitale Identitätsnachweis ist der Schlüssel, auf den die Digitalisierung gewartet hat

Die deutsche Bevölkerung ist ihren Behörden in Sachen Digitalisierung bereits viele Schritte voraus und dürstet förmlich nach einem zügigen Ausbau der einheimischen digitalen Infrastruktur. Doch die öffentlichen Mühlen mahlen hierzulande leider etwas langsamer als andernorts, sowohl beim Glasfaserausbau als auch bei der Überwindung der öffentlichen Papierwirtschaft.

Im Zentrum aller offiziellen Onlineaktivitäten stehen die digitale Identität und die Möglichkeit ihres Nachweises. Jeder Vertragsabschluss setzt voraus, dass sich die Vertragspartner zweifelsfrei und rechtskräftig ausweisen können. Insofern verspricht die Ausweisapp2 der lahmenden Digitalisierung einen willkommenen Schub zu verpassen.

Die großen Chancen dürfen nicht durch Mängel beim Datenschutz aufs Spiel gesetzt werden

Zweifelsohne eröffnet ein digitaler Ausweis ungeahnte Möglichkeiten für die deutsche Bevölkerung und ihre Wirtschaft. Sie löst eine der letzten Bremsen, die einer Entfaltung der digitalen Gesellschaft bisher im Wege standen. Doch sind die damit verbundenen Risiken nicht minder gewichtig zu bewerten. Je mehr wir unseren Geschäften im Internet nachgehen, desto tiefgreifender sind die Konsequenzen eines Identitätsdiebstahls. Sollten Cyberkriminelle etwa die Kontrolle über eine fremde digitale Identität erlangen, so sind die Möglichkeiten für schwerwiegenden Missbrauch fast unbegrenzt. Angefangen bei Einkäufen auf Kosten des Opfers bis hin zu justiziablen Aktivitäten im Internet, kann ein krimineller Hacker immensen Schaden verursachen, sollte er sich aufgrund mangelhafter IT-Sicherheitsmaßnahmen den Zugriff auf die digitale Identität anderer verschaffen können.

Deshalb ist eine lückenlose und durchdachte IT-Sicherheitsstrategie der unverzichtbare Grundstein für das Gelingen einer jeglichen App zum digitalen Identitätsnachweis und sollte besonders in der Konzeptionsphase oberste Priorität erhalten.

---

[1] https://www.ausweisapp.bund.de/ausweisapp2/

[2] https://www.tagesspiegel.de/wirtschaft/digital-vorreiter-im-baltikum-behoerdendienste-erledigen-sich-in-estland-kuenftig-von-selbst/25385494.html

[3] https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html

Confidential Computing kann der digitalen Identität zum Durchbruch verhelfen

Daten können bei ihrer Speicherung und Übermittlung effektiv durch Verschlüsselung geschützt werden. Doch für ihre Verarbeitung ist es nach dem aktuellen Stand der Technik noch unumgänglich, sie zuvor zu entschlüsseln. Findige Cyberkriminelle sind sich dieser Tatsache bewusst und greifen gezielt jene Server an, auf denen die Datenverarbeitung stattfindet.

Um den Begehrlichkeiten, die durch die umfangreichen Missbrauchsmöglichkeiten einer Ausweisapp entstehen, einen Riegel vorzuschieben, kann man die Daten mit verschiedenen Lösungsansätzen vor einem unberechtigten Zugriff schützen. Drei Techniken haben sich dabei bewährt:

- Confidential Computing auf Prozessorebene: Die von Intel, Google & Co. entwickelte Technik ermöglicht es, Code vor seiner Verarbeitung auf gesonderte Speicherenklaven der speziell dafür ausgelegten Prozessoren auszulagern[4]. Dort ist er sicher vor Fremdzugriff geschützt.

- Confidential Computing auf Serverebene: Beim „Sealed Computing“ werden die Daten vor ihrer Verarbeitung auf einen versiegelten Server („Sealed Cloud“) übertragen[5]. Dort können Sie, sicher vor Fremdzugriffen, entschlüsselt und verarbeitet werden. Auf diese Weise sind Manipulation oder Diebstahl von vornherein ausgeschlossen.

- Zugriffsschutz mittels Blockchain: Dieser Ansatz wird beispielsweise beim geplanten digitalen Impfnachweis zum Einsatz kommen, indem die gesammelten und anonymisierten Daten verschlüsselt auf insgesamt fünf verschiedenen Blockchains hinterlegt werden[6].

Die Tatsache, dass die politischen Verantwortungsträger erkannt haben, dass lückenloser Datenschutz auch die verwundbare Datenverarbeitung abdecken muss, lässt darauf hoffen, dass auch künftige Projekte auf Bundesebene mit vergleichbaren Sicherheitsmaßnahmen versehen werden.

Gerade bei den zentralen personenbezogenen Daten und einem so mächtigen Instrument wie einer digitalen Ausweisfunktion sollten keine unnötigen Risiken eingegangen werden. Stattdessen sollten alle möglichen Vorsichtsmaßnahmen bedacht und die effektivsten Techniken zur Absicherung der digitalen Identität implementiert werden. Sollte das ambitionierte Projekt Ausweisapp2 zur Erfolgsgeschichte werden, könnte dadurch das empfindliche deutsche Vertrauen in öffentliche Digitalisierungsprojekte gestärkt und der mühsam erarbeitete Fortschritt für zukünftige Projekte gefestigt werden.

Weitere Beiträge rund um die Themen Datenschutz und Datensicherheit finden Sie unter www.privacyblog.de.

[4] https://confidentialcomputing.io/
[5] https://www.idgard.de/privacyblog/confidential-computing-und-sealed-cloud
[6] https://t3n.de/news/corona-blockchain-digitaler-impfpass-1364737/

uniscon – A member of TÜV SÜD

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons *Sealed Platform®* bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.

uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).

Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten *Sealed Cloud Technologie*, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design“ entwickelt.

Uniscon wurde 2009 gegründet und ist seit 2017 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Pressekontakt
uniscon GmbH, Wilhelm Würmseer
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20