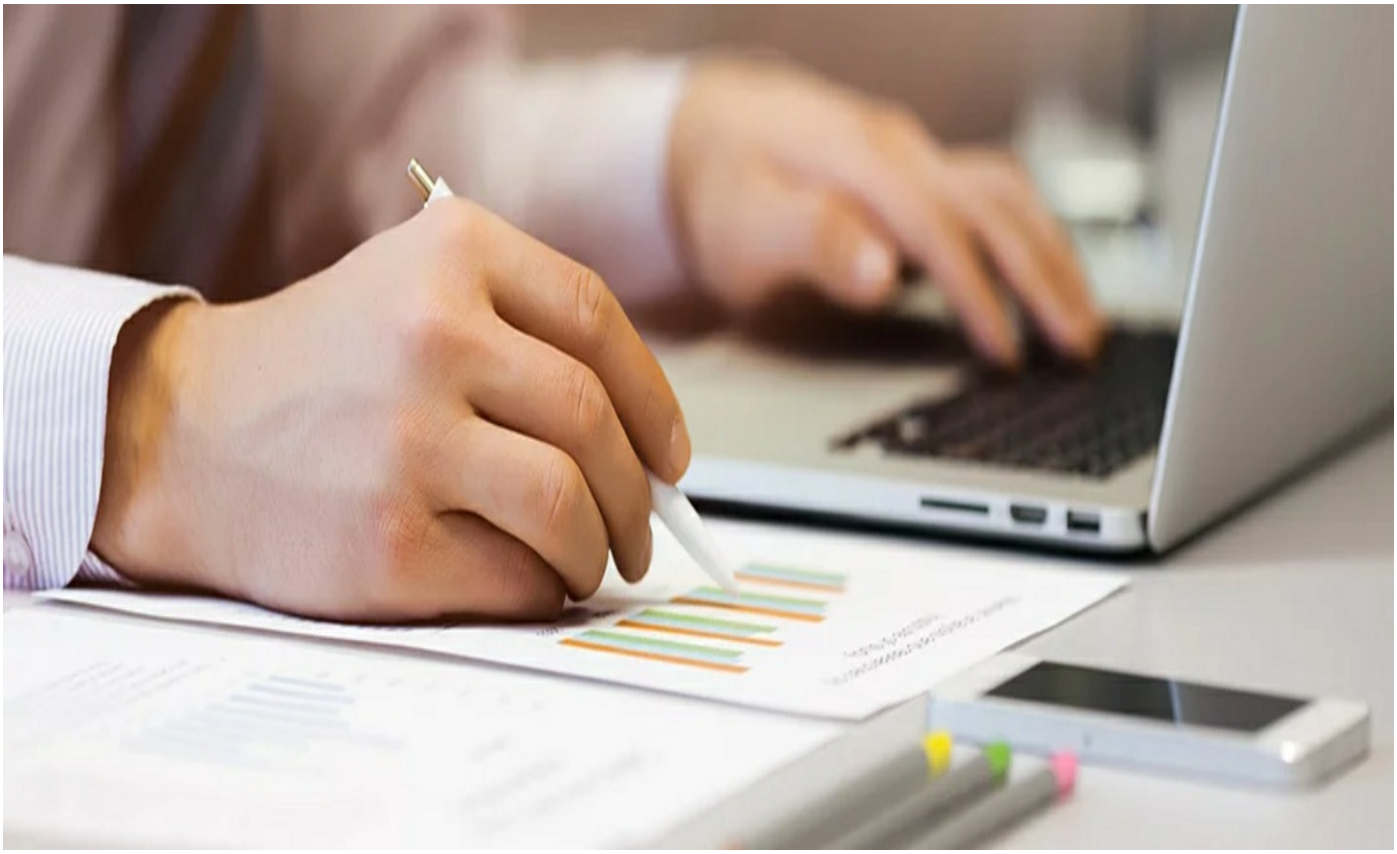

Deutschland setzt Maßstäbe für sichere Ausweisdokumente im Zeitalter der Quantencomputer

2025-11-10 | Berlin/München | Giesecke+Devrient

Seit seiner Einführung 2010 gilt er als eines der sichersten hoheitlichen Dokumente der Welt: der deutsche Personalausweis samt integrierter Online-Ausweisfunktion. Damit er auch zukünftig sicher bleibt, müssen neue Ausweise gegen Angriffe von Quantencomputern geschützt werden - das gilt für Hardware und Software aller Ausweise, die in den kommenden Jahren ausgegeben werden. Die hoheitlichen Dokumente sind zehn Jahre gültig. Eine weltweit bislang einzigartige technische Basis dafür haben die Bundesdruckerei GmbH und G+D in den vergangenen Monaten erarbeitet. Das Technologieunternehmen des Bundes und das internationale Sicherheitstechnologieunternehmen haben die Entwicklung des Demonstrators gemeinsam mit dem BSI initiiert und auf speziellen Chips des Halbleiterherstellers Infineon umgesetzt.

Die Migration des deutschen Personalausweises erfolgt dann in zwei Phasen: Zunächst werden die Ausweisdaten mit einem quantenresistenten Signaturverfahren gegen Fälschungen geschützt. Danach folgt die vollständige Umstellung auf quantensichere Technologie.

Die Machbarkeitsstudie (Proof-of-Concept) ist eine der weltweit ersten funktionalen Umsetzungen eines Personalausweises mit klassischer Kryptografie und Post-Quantum-Kryptografie, welche den aktuellen Empfehlungen für quantensichere Algorithmen entspricht. „Bundesdruckerei und G+D haben als erste in Deutschland nachgewiesen, dass hochsichere, quantenresistente Kryptografie, wie etwa Verschlüsselung und Authentisierung, auf Ausweis-Chips möglich ist – das ist ein entscheidender Schritt für die Zukunftssicherheit digitaler Identitäten“, sagt Dr. Kim Nguyen, Senior Vice President Innovations bei der Bundesdruckerei.

„Die Frage ist schon längst nicht mehr, ob es Quantencomputer geben wird, welche die aktuellen kryptografischen Verfahren brechen, sondern wann dieser sogenannte Q-Day kommt. Schon heute testen Unternehmen den Einsatz von Quantencomputern etwa bei der Material- und Medikamentenforschung“, sagt Gabriel von Mitschke-Collande, Mitglied der Geschäftsführung und Group CDO bei G+D. „Wir müssen jetzt handeln, um unsere digitale Infrastruktur zu schützen. Der Übergang zu quantenresistenten Verschlüsselungsverfahren ist keine Option, sondern eine Notwendigkeit. Deshalb freuen wir uns sehr, dass wir gemeinsam mit der Bundesdruckerei einen zukunftsfähigen Weg aufgezeigt haben, um das innovative Potenzial von Quantencomputern mit der entsprechenden Sicherheitstechnologie zu vereinen."

Die Technologie der Quantencomputer hat in den vergangenen Jahren große Fortschritte in vielen Details gemacht, allerdings ist eine echte Skalierung weiterhin nicht erreicht und mit großen Herausforderungen verbunden. Leistungsfähige und fehlerkorrigierende Quantencomputer könnten bestimmte mathematische Probleme, wie beispielsweise die Berechnung von diskreten Logarithmen oder Primfaktorzerlegungen, deutlich schneller lösen als klassische Computer. Diese Leistungsfähigkeit hat auch eine Schattenseite: Quantencomputer haben das Potential etablierte Kryptoverfahren zu knacken, genauer gesagt: einige Schlüsselaushandlungs- und Signaturverfahren. Damit sind sie eine zunehmend reale Bedrohung für die Sicherheit von IT-Systemen und Daten. Vor allem die sensiblen persönlichen Daten in hoheitlichen ID-Dokumenten müssen zukünftig vor möglichen Quantenangriffen geschützt werden – und zwar mit Post-Quanten-Kryptografie (PQC). Eine EU-Roadmap sieht die Umsetzung für kritische Anwendungsfälle mit hohem Risiko bis 2030 vor.

„Eine Ausstattung des Personalausweis-Chips mit Post-Quantum-Kryptografie ist äußerst relevant, denn wir müssen ab 2030 mit leistungsfähigen Quantencomputern rechnen, die aktuelle kryptografische Verfahren brechen können. Spätestens dann müssen quantensichere Ausweise ausgegeben werden können. Wir können stolz sein, dass Deutschland eine Vorreiterrolle bei der zukunftsfähigen Absicherung hoheitlicher Dokumente einnimmt”, betont BSI-Präsidentin Claudia Plattner. Das BSI erforscht und dokumentiert den Entwicklungsstand von Quantencomputern in einer regelmäßig aktualisierten Studie.

G+D hat langjährige Erfahrung mit PQC auf Hardwaresicherheitselementen durch seine Teilnahme an den Förderprojekten Aquorypt ■ und Quoryptan ■ des Bundesministeriums für Forschung, Technologie und Raumfahrt. Technologisch anspruchsvoll bei der Implementierung von PQC auf dem Ausweis-Chip war die Erfüllung der neuen Sicherheitsanforderungen und eine Minimierung des Footprints der ressourcenintensiven PQC-Algorithmen. Mit dem Proof-of-Concept zum quantensicheren Personalausweis haben die Unternehmen den Weg bereitet, die PQC-Verfahren sicher in den Ausweis zu bringen. Die im Proof-of-Concept genutzten Infineon-Chips bieten ein neues Chip-Design, das eine schnelle und seitenkanalresistente Softwareimplementierung von PQC-Algorithmen erleichtert.

Auch die Bundesdruckerei beschäftigt sich seit Jahren mit der Post-Quantum-Kryptografie und Quantencomputing. Gemeinsam mit Infineon und dem Fraunhofer-Institut für Angewandte und integrierte Sicherheit (AISEC) hat die Bundesdruckerei 2022 den weltweit ersten Demonstrator für einen elektronischen Pass entwickelt, der auch die hohen Sicherheitsanforderungen für die Ära des Quantencomputing erfüllt. Informationen zu den Quantenprojekten der Bundesdruckerei gibt es hier ■.



Weitere Details zu PQC und welche Kryptografie-Verfahren durch Quantencomputer gebrochen werden könnten, hat G+D hier zusammengestellt. Informationen und Empfehlungen des BSI zu PQC gibt es hier ■.

Über die Bundesdruckerei GmbH

Die Bundesdruckerei GmbH samt ihrer Tochtergesellschaft Maurer Electronics GmbH treibt technologische Entwicklungen in den Bereichen Identitäts- und Berechtigungsmanagement, Verwaltungsdigitalisierung, Datenanalyse und Künstliche Intelligenz sowie staatliche Zahlungsmittel und Werttransfersysteme an. Damit schafft sie die Basis für eine moderne und resiliente Gesellschaft.

Als Unternehmen der Bundesdruckerei-Gruppe und mit der Erfahrung von über 250 Jahren ebnet das Unternehmen den Weg in eine sichere digitale Zukunft. Die Bundesdruckerei GmbH besitzt aktuell über 5.400 nationale und internationale Patente, beschäftigt derzeit rund 3.090 Mitarbeitende und hat 2024 einen Umsatz von rund 940 Millionen Euro erzielt. Weitere Informationen unter www.bundesdruckerei-gmbh.de ■

Über Giesecke+Devrient

Giesecke+Devrient (G+D) ist ein weltweit tätiges Unternehmen für SecurityTech mit Hauptsitz in München. G+D macht das Leben von Milliarden von Menschen sicherer. Das Unternehmen schafft Vertrauen im digitalen Zeitalter, mit integrierten Sicherheitstechnologien in drei Geschäftsbereichen: Digital Security, Financial Platforms and Currency Technology.

G+D wurde 1852 gegründet und beschäftigt heute mehr als 14.000 Mitarbeiterinnen und Mitarbeiter. Im Geschäftsjahr 2024 erwirtschaftete das Unternehmen einen Umsatz von 3,1 Milliarden Euro. G+D ist mit 118 Tochtergesellschaften und Gemeinschaftsunternehmen in 41 Ländern vertreten.

Weitere Informationen: www.gi-de.com.