Bundesdruckerei/G+D

Zukunftssichere digitale Identitäten

[14.11.2025] Bundesdruckerei und G+D haben gemeinsam mit dem BSI einen Demonstrator für einen quantensicheren Personalausweis entwickelt. Der Ausweis soll künftig Post-Quantum-Kryptografie nutzen, um persönliche Daten vor Angriffen durch Quantencomputer zu schützen.

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. Dafür haben die Bundesdruckerei sowie Giesecke+Devrient in den vergangenen Monaten eine innovative technische Basis erarbeitet. Das Technologieunternehmen des Bundes und das internationale Sicherheitstechnologieunternehmen haben die Entwicklung des Demonstrators gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) initiiert und auf speziellen Chips des Halbleiterherstellers Infineon umgesetzt.

Einzigartige technische Basis

Die Migration des deutschen Personalausweises soll dann in zwei Phasen erfolgen: 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 Kim Nguyen, Senior Vice President Innovations bei der Bundesdruckerei.

Post-Quanten-Kryptografie bis 2030

Die Technologie der Quantencomputer hat in den vergangenen Jahren große Fortschritte in vielen Details gemacht. Eine echte Skalierung ist derzeit aber noch nicht erreicht und mit großen Herausforderungen verbunden. Leistungsfähige Quantencomputer könnten bestimmte mathematische Probleme deutlich schneller lösen als klassische Computer und haben damit auch das Potenzial, etablierte Kryptoverfahren zu knacken. Vor allem die sensiblen persönlichen Daten in hoheitlichen ID-Dokumenten müssen zukünftig vor möglichen Quantenangriffen geschützt werden – 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“, betont BSI-Präsidentin Claudia Plattner.

(sib)

Stichwörter: Digitale Identität, Giesecke+Devrient, Bundesdruckerei, Quantencomputing