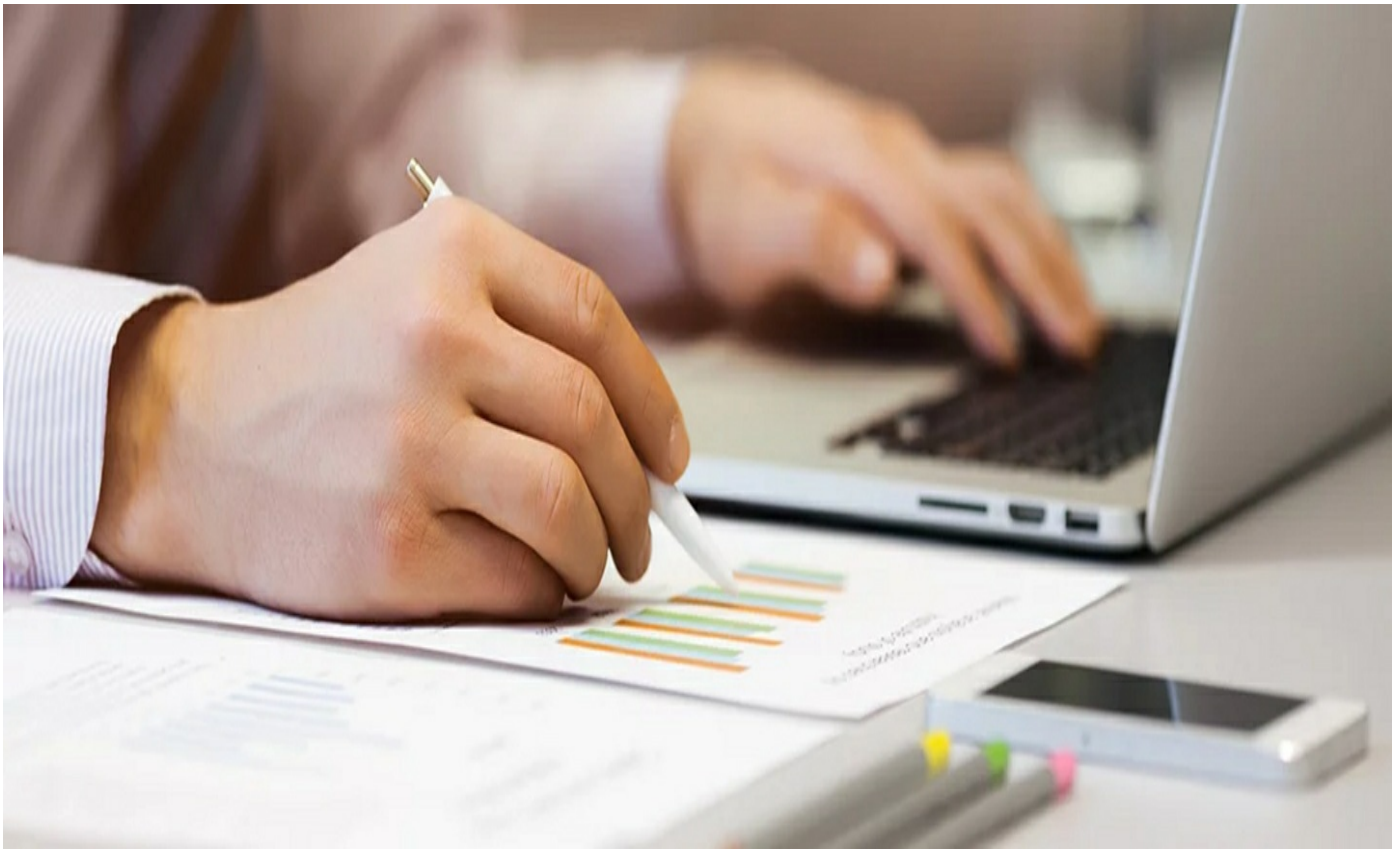

Germany Sets New Standards for Secure ID Documents in the Quantum Computing Era

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

Since its introduction in 2010, Germany's national ID card – with its integrated online identification feature – has been recognized as one of the world's most secure government-issued documents. To ensure that it remains secure in the future, the next generation of ID cards must be protected against potential quantum-computer attacks. This applies to both the hardware and software of all cards issued in the coming years, as each card is valid for ten years.

In recent months, Bundesdruckerei GmbH and G+D have established a unique technical foundation for this transformation. The federal technology company and the international SecurityTech leader jointly initiated the development of a demonstrator together with the German Federal Office for Information Security (BSI), implemented on specialized chips produced by semiconductor manufacturer Infineon.
Germany's transition to quantum-secure ID cards will occur in two stages. First, personal data will be protected from forgery using a quantum-resistant digital signature scheme. The second phase will involve a full transition to quantum-secure technology.
The proof of concept represents one of the world's first functional implementations of a national ID card that combines classical and post-quantum cryptography, following the latest recommendations for quantum-secure algorithms.
"Bundesdruckerei and G+D are the first in Germany to demonstrate that highly secure, quantum-resistant cryptography, covering both encryption and authentication, can be implemented on ID chips," said Dr. Kim Nguyen, Senior Vice President of Innovation at Bundesdruckerei. "This marks a decisive step toward ensuring the future security of digital identities."

“The question is no longer whether quantum computers capable of breaking current cryptographic methods will exist, but when this so-called Q-Day will arrive,” said Gabriel von Mitschke-Collande, Member of the Management Board and Group CDO at G+D. “Companies are already exploring quantum computing in areas such as materials science and pharmaceutical research. We must act now to protect our digital infrastructure. The transition to quantum-resistant encryption is not optional – it’s essential. That’s why we’re proud to have charted a path with Bundesdruckerei that combines the innovative potential of quantum computing with the right security technology.”
While quantum computing has advanced rapidly in recent years, true scalability has not yet been achieved and remains a major challenge. High-performance, fault-tolerant quantum computers could one day solve certain mathematical problems, such as the computation of discrete logarithms or prime factorizations, much faster than classical computers. That capability, however, comes with a downside: quantum computers could break established cryptographic systems – specifically key exchange and digital signature schemes. They pose an increasingly significant threat to IT systems and data security. Sensitive personal data stored in government ID documents must therefore be protected against potential quantum attacks using post-quantum cryptography. An EU roadmap calls for PQC adoption in critical and high-risk applications by 2030.
“Equipping ID card chips with post-quantum cryptography is essential, as we must assume that by 2030, quantum computers will be capable of breaking today’s cryptographic algorithms,” said Claudia Plattner, President of the BSI. “By then, governments must be ready to issue quantum-secure ID cards. Germany can be proud to take a pioneering role in protecting the future security of sovereign documents.” The BSI continues to study and document the progress of quantum computing in a regularly updated report.
G+D has extensive experience implementing PQC in secure hardware components through its participation in the German government’s funded projects Aquorypt and Quoryptan. One of the main technical challenges in deploying PQC on ID chips lies in meeting new security requirements while minimizing the computational footprint of resource-intensive PQC algorithms. With this proof of concept for a quantum-secure ID card, the companies have paved the way for safely integrating PQC algorithms into national identity documents. The Infineon chips used in the project feature a new design that supports fast, side-channel-resistant software implementation of PQC algorithms.

Bundesdruckerei has also been active in post-quantum cryptography and quantum computing for several years. Together with Infineon and the Fraunhofer Institute, the company developed the world’s first electronic passport demonstrator in 2022 that meets the stringent security standards of the quantum era. More information about Bundesdruckerei quantum projects can be found here.
Further details on PQC and the cryptographic algorithms at risk from quantum computers are available from G+D here. Information and recommendations from the BSI on PQC are available here.



Copyright: Bundesdruckerei

About Bundesdruckerei Gruppe GmbH

As a federal technology company, the Bundesdruckerei Group, with its digital and security expertise, contributes to the digital sovereignty of Germany and Europe. In doing so, it builds trust in society. Its individual companies offer identification systems as well as products and solutions related to cybersecurity and digitalization: for the public sector and sensitive areas of society and the economy.
The parent company, Bundesdruckerei Gruppe GmbH, includes Bundesdruckerei GmbH with its subsidiary Maurer Electronics GmbH, as well as D-Trust GmbH, genua GmbH, Xecuro GmbH, and iNCO Spółka z o.o. The group currently employs a total of around 4,620 people and generated sales of around €1.1 billion in 2024.

Bundesdruckerei Gruppe GmbH also holds shares in Veridos GmbH, DERMALOG Identification Systems GmbH, and Verimi GmbH. Further information is available at www.bundesdruckerei.de ■

About Giesecke+Devrient

Giesecke+Devrient (G+D) is a global SecurityTech company headquartered in Munich, Germany. G+D makes the lives of billions of people more secure. The company shapes trust in the digital age, with built-in security technology in three segments: Digital Security, Financial Platforms and Currency Technology.
G+D was founded in 1852 and today has a workforce of more than 14,000 employees. In the fiscal year 2024, the company generated a turnover of 3.1 billion euros. G+D is represented by 118 subsidiaries and joint ventures in 41 countries.
Further information: www.gi-de.com.