Die Post-Quanten-Regulation kommt!

Doch wie gelingt der Umstieg?

Datum	20.01.2026
Ort	Omnisecure Berlin
Autoren	**Frank Morgner** (Bundesdruckerei GmbH) **Stefan-Lukas Gazdag** (genua GmbH)

Wer von IHNEN hat heute bereits PQC genutzt?

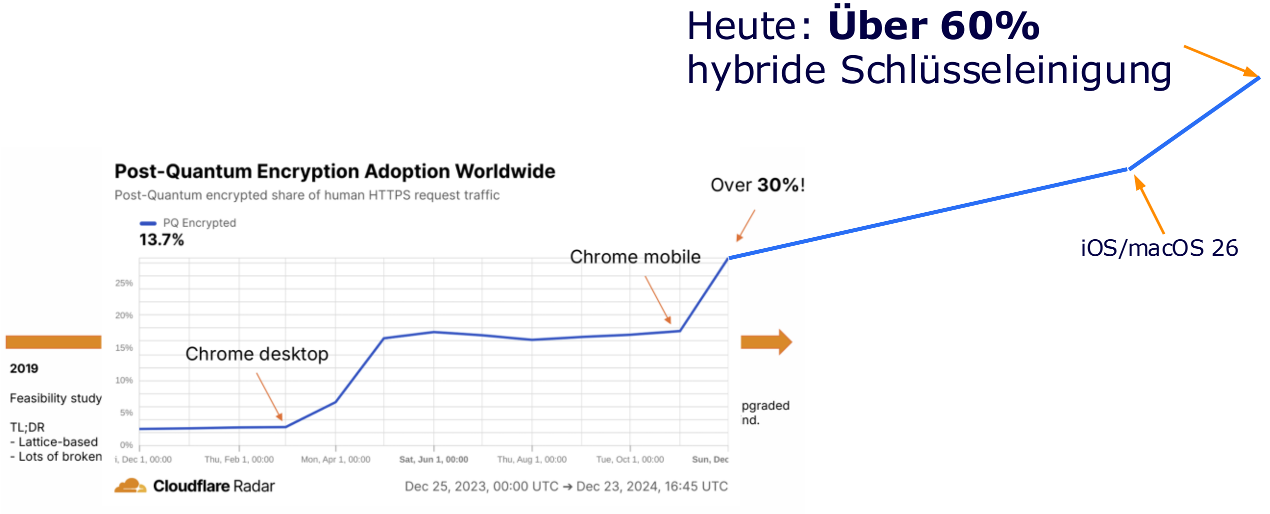
Alle nutzen Post-Quantum-Crypto!

Messenger haben PQC integriert

WhatsApp, Signal, iMessage haben Protokolle, Apps und Server angepasst, um hybriden Schlüsselaustausch mit ML-KEM zu unterstützen.

Große Teile des Web nutzen PQC

Chrome, Firefox, Safari,… nutzen standardmäßig hybriden Schlüsselaustausch mit ML-KEM. Auch CDN Cloudflare hat seine Serverinfrastruktur umgestellt. Derzeit sind etwa 60% des globalen Nutzer-generierten Datenverkehrs quantenresistent geschützt.



Heute: **Über 60%** hybride Schlüsseleinigung

Post-Quantum Encryption Adoption Worldwide

Post-Quantum encrypted share of human HTTPS request traffic

Cloudflare Radar

Dec 25, 2023, 00:00 UTC → Dec 23, 2024, 16:45 UTC

2025 Valenta: Why the Internet isn’t ready for Post-Quantum Certificates

Läuft die PQ-Migration also gut?

In vielen Fällen nicht so sehr…

Heterogene Systeme

Viele Anwendungen und Systeme hadern mit zahlreichen Anforderungen und Update-Zyklen.

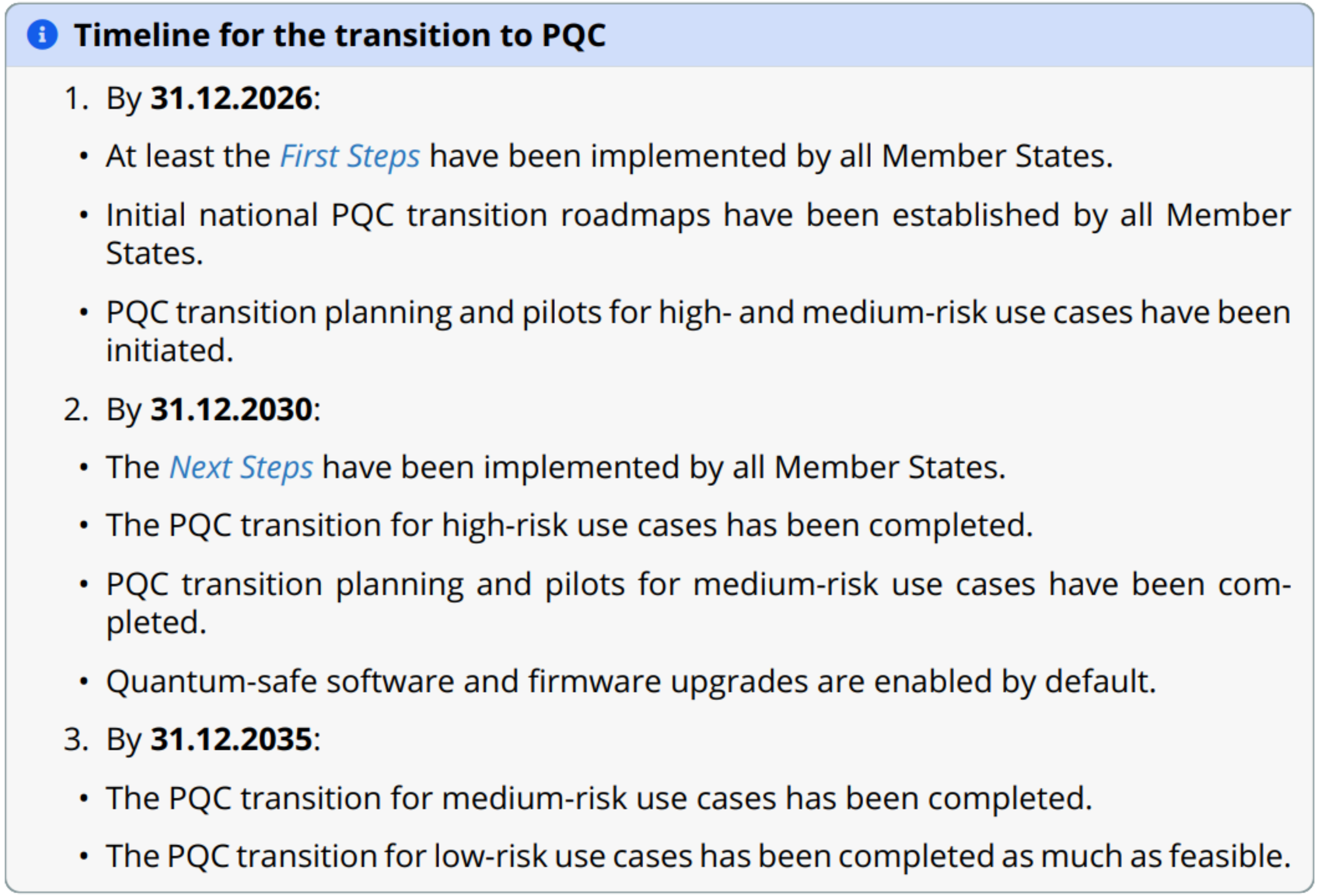
Protocol ossification

Obwohl in Protokollen vermehrt auf zukunftsfähige Designs geachtet wird, sind viele Protokolle und insbesondere Implementierungen sehr starr und schwierig anzupassen, ohne vermehrt Angriffsflächen und Fehler einzubauen.

Gemischte Signale und fehlende Anreize

Ständige Verbesserungen und Fortschritt verleiten zum Gefühl, dass PQC noch nicht ausgereift sei.

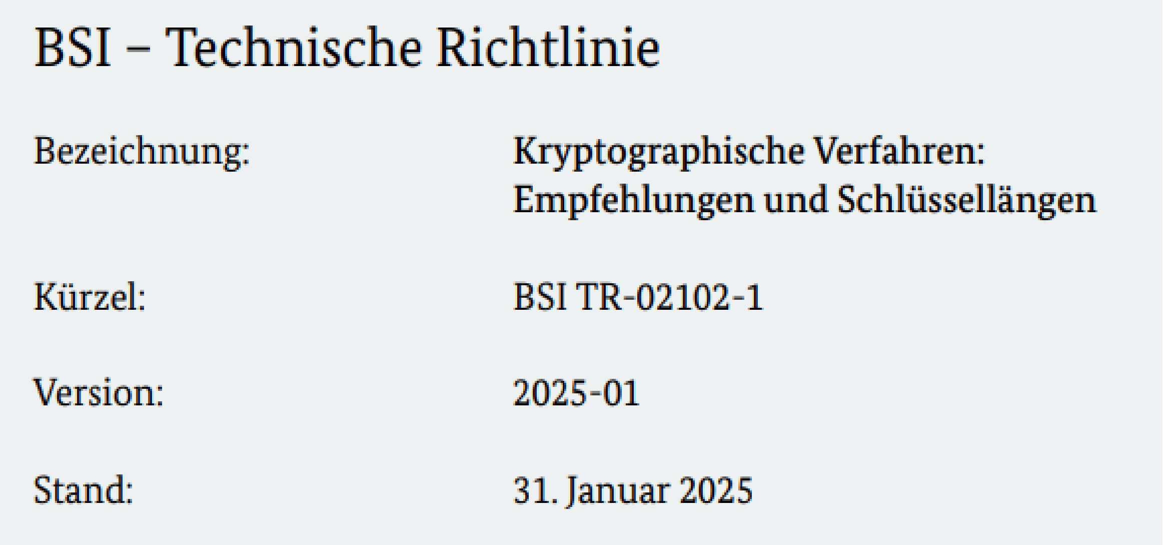
Die Regulation kommt



Timeline for the transition to PQC

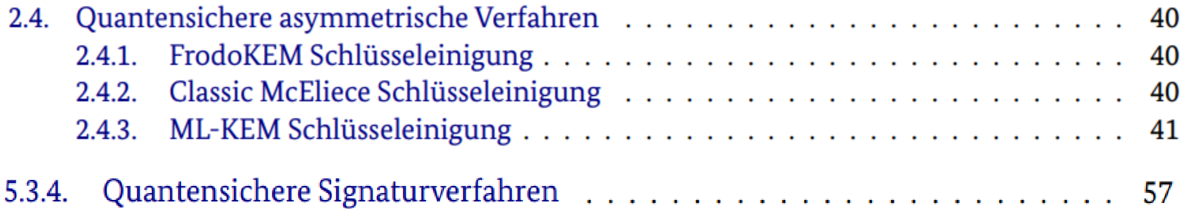
1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

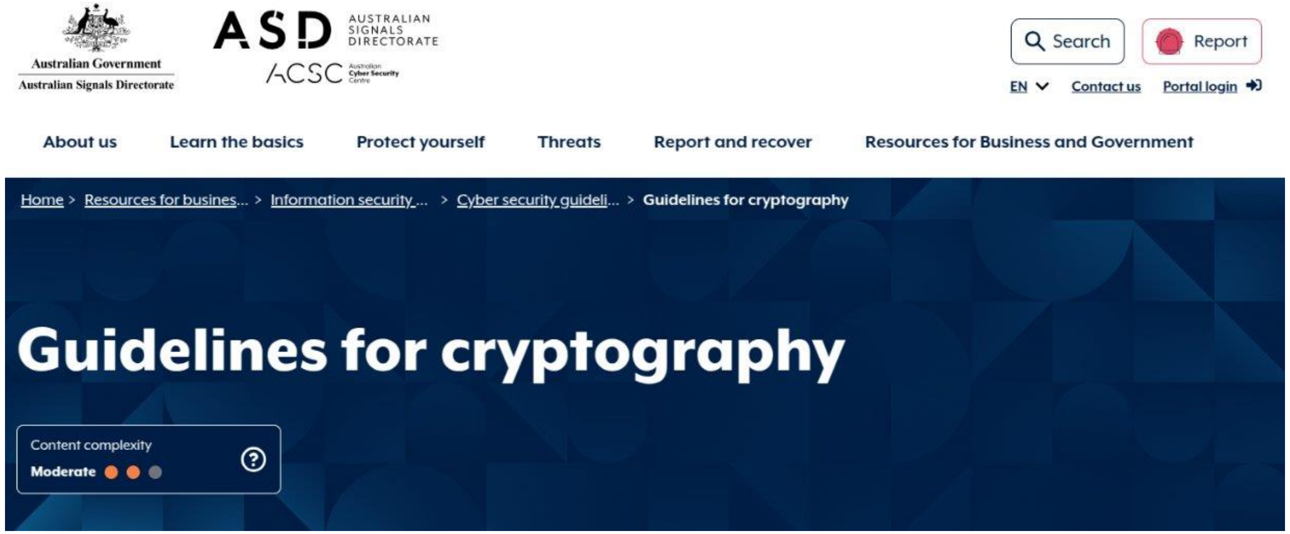
https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography



BSI – Technische Richtlinie

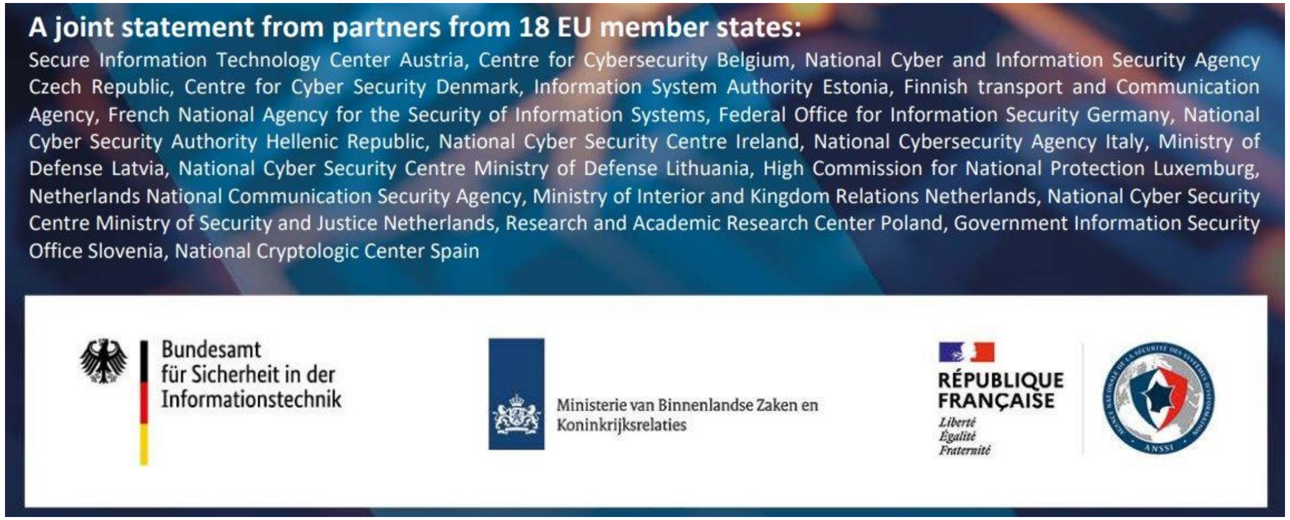
Bezeichnung:	Kryptographische Verfahren: Empfehlungen und Schlüssellängen
Kürzel:	BSI TR-02102-1
Version:	2025-01
Stand:	31. Januar 2025





Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Search
Report
EN
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government
Home > Resources for busines... > Information security ... > Cyber security guideli... > Guidelines for cryptography
Content complexity
Moderate

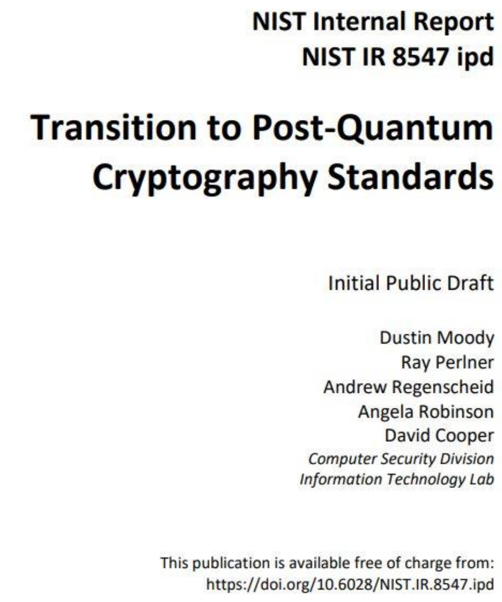
Guidelines for cryptography



A joint statement from partners from 18 EU member states:

Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain

Bundesamt für Sicherheit in der Informationstechnik
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ANSSI



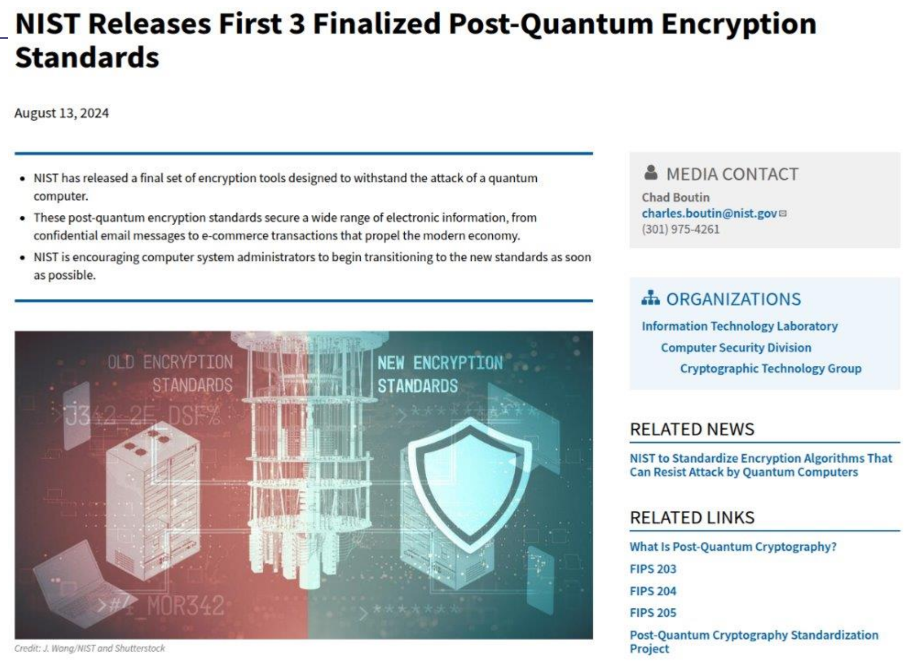
NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper
Computer Security Division
Information Technology Lab

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd



NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

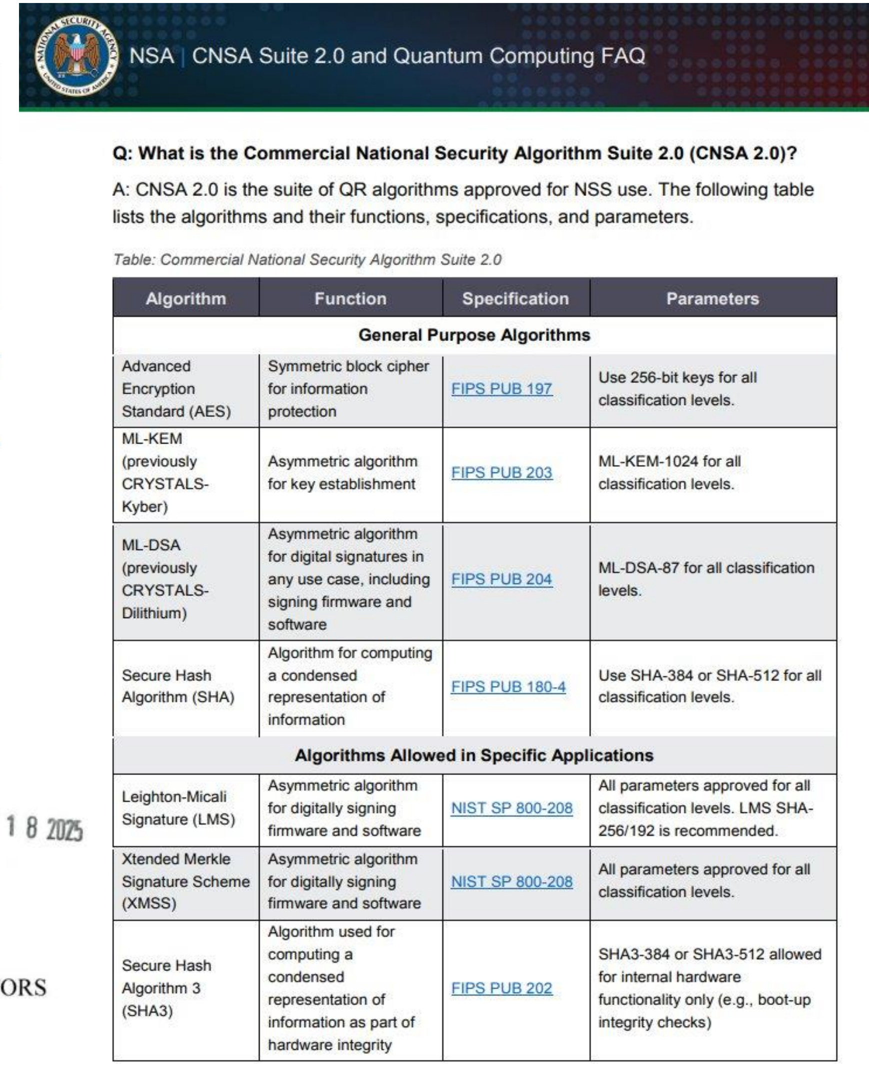
Credit: J. Wang/NIST and Shutterstock

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division
Cryptographic Technology Group

RELATED NEWS
NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers

RELATED LINKS
What Is Post-Quantum Cryptography?
FIPS 203
FIPS 204
FIPS 205
Post-Quantum Cryptography Standardization Project



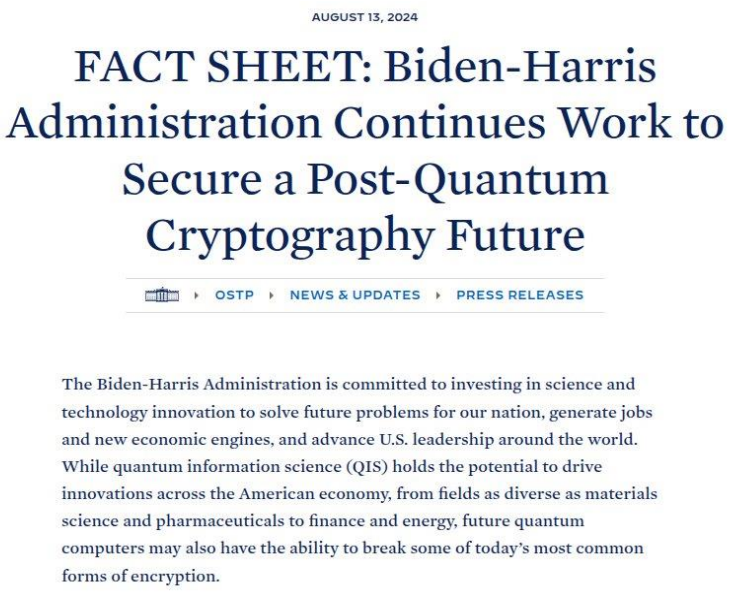
NSA | CNSA Suite 2.0 and Quantum Computing FAQ

Q: What is the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)?

A: CNSA 2.0 is the suite of QR algorithms approved for NSS use. The following table lists the algorithms and their functions, specifications, and parameters.

Table: Commercial National Security Algorithm Suite 2.0

Algorithm	Function	Specification	Parameters
General Purpose Algorithms			
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.
Secure Hash Algorithm 3 (SHA3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

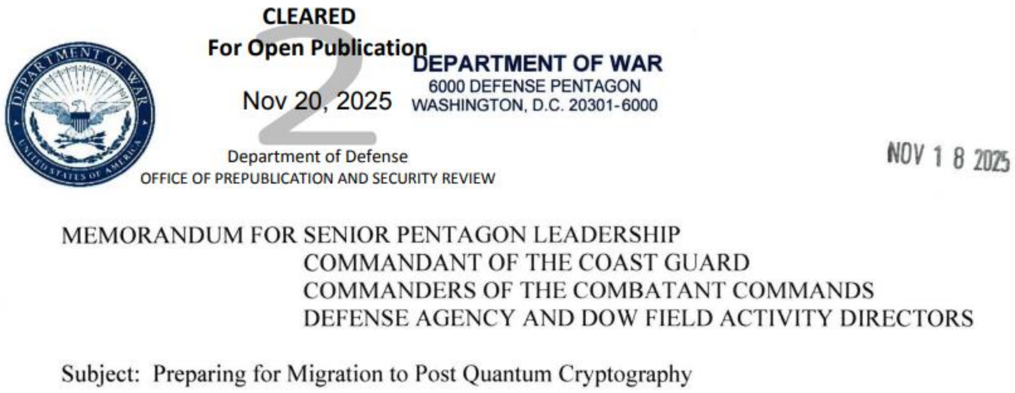


AUGUST 13, 2024

FACT SHEET: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future

OSTP › NEWS & UPDATES › PRESS RELEASES

The Biden-Harris Administration is committed to investing in science and technology innovation to solve future problems for our nation, generate jobs and new economic engines, and advance U.S. leadership around the world. While quantum information science (QIS) holds the potential to drive innovations across the American economy, from fields as diverse as materials science and pharmaceuticals to finance and energy, future quantum computers may also have the ability to break some of today's most common forms of encryption.



CLEARED
For Open Publication
Nov 20, 2025
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DEPARTMENT OF WAR
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NOV 18 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

Subject: Preparing for Migration to Post Quantum Cryptography

01

EU Projekt: PQCSA

Post Quantum Support
Action

Post Quantum Support Action

Gefördert von der Europäischen Union

DIGITAL- ECCC-2024-DEPLOY-CYBER-06-STANDARDPQC call in project 101190512 PQCSA

Projekt Partner

TU Eindhoven (NL),
Bundesdruckerei (DE),
CryptoExperts (FR),
KU Leuven (BE),
Trinity College Dublin (IRL)

PQCSA

Projektziele

PQC Standardisierung
PQC Migration Roadmaps
PQC Awarenes erhöhen

Wie wir arbeiten

SDOs: ISO/IEC, ICAO, IETF, GP, …
Events with Academia/Industry/…

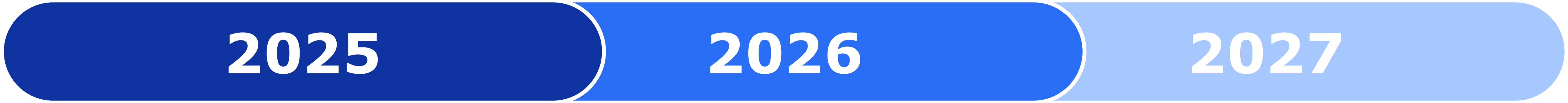
PQCSA Aktivitäten

Standardisierung (laufend)

- ISO/IEC (Kryptografie, Smartcards)
- ICAO (Reisedokumente)
- IETF LAMPS (Hybride Verfahren)
- Globalplatform (Secure Elements)
- CAB Forum, PKI Consortium (PKI Migration)

Geplant

- Co-located Events mit
  - FOSDEM'26 31.1.-1.2.2026
  - SDO von Krypto-Experten
  - CA Day für PKI Migration
- **https://pqcsa.eu/events.html**
  kostenfrei und offen für jeden



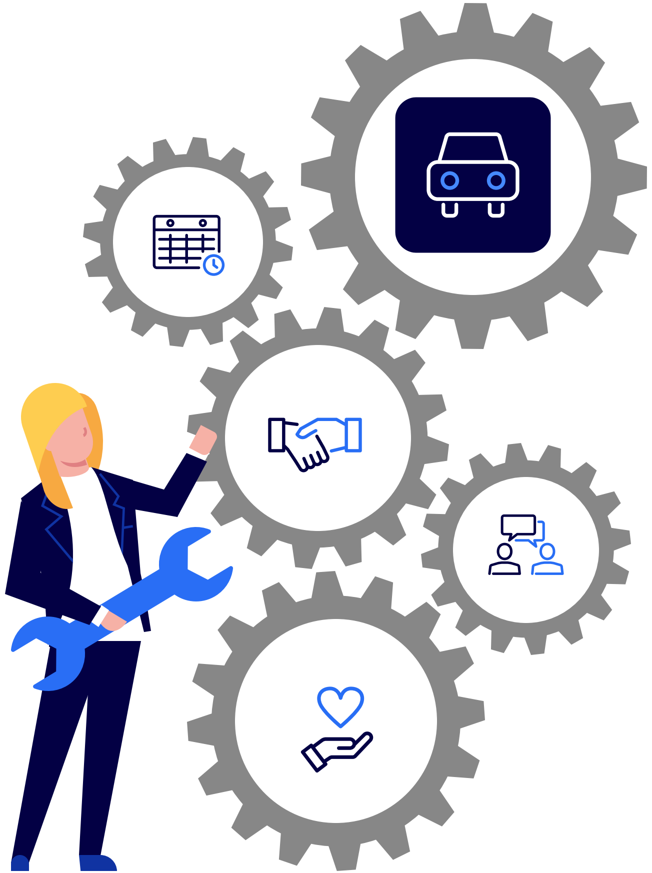
Workshops und Events

- PQCSA Summer School
- Workshop zu Migration
- PQC migration for automotive industry

Projekt Wrap-Up

Finalisierte Dokumente und Empfehlungen

Automotive und Krypto-Agilität?



Lebenszyklus

- Nutzungszeitraum eines Autos bis zu 30 Jahre
- Neue Produktreihen werden bis zu 8 Jahre vorbereitet
- Trotzdem kein Fokus auf PQC, wegen konkurierender Incentives

Heterogene Systeme

- Große Supply-Chain, gut orchestriert, ausgebaute Infrastruktur
- 100-300 Mikrocontroller geeignet für Software-Updates
- APIs und standards der Automotive-Industrie fehlt PQC

PQC Roadmap relevant, aber inwiefern?

- CRA relevant für Autos, NIS2 relevant für Online-Dienste
- Unklar ob “high” or “medium risk”
- Keine echte Verpflichtung zu PQC

Bessere Incentivierung

- UN Regulation No. 155: Cyber Security Management System, u.a. für Risiken wie “Using already or soon to be deprecated cryptographic algorithms”
- Ausphasen klassischer Verfahren hätte direkte Auswirkungen ohne weitere Regulierung (vgl. NIST IR 8547 ipd, 11/2024)

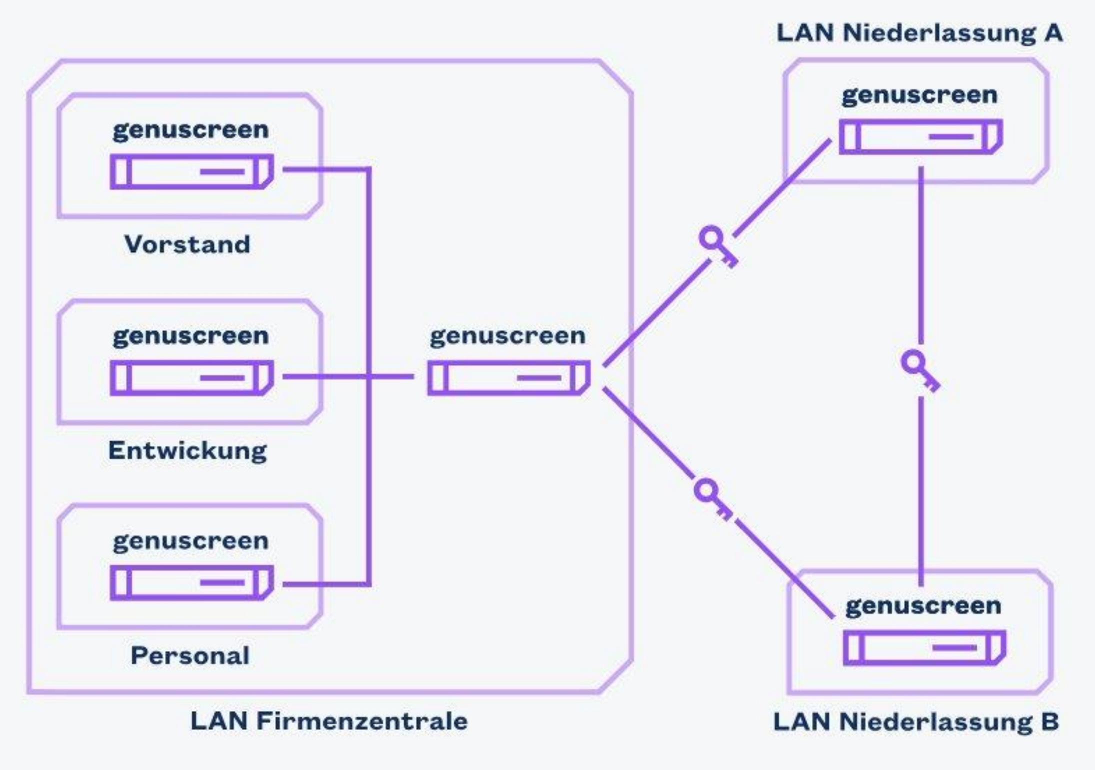
02

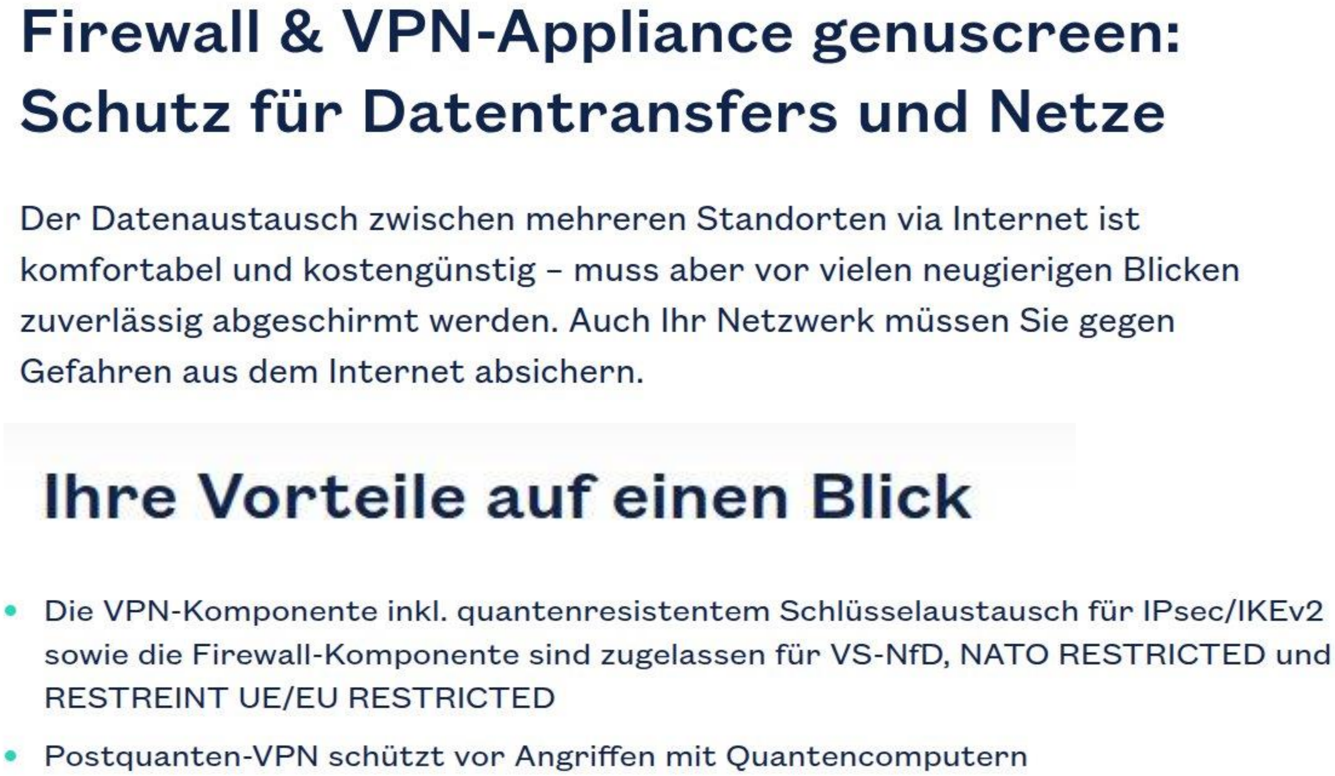
genuscreen

Firewall & VPN
Appliances

Migration der Produkte läuft

- Seit 2017: Zulassung (VS-NfD) für quantenresistente Software-Updates (nach Projekt squareUP)
- Seit 2024: Zulassung (VS-NfD) für quantenresistente VPNs (nach Projekt QuaSiModO)





Firewall & VPN-Appliance genuscreen: Schutz für Datentransfers und Netze

Der Datenaustausch zwischen mehreren Standorten via Internet ist komfortabel und kostengünstig – muss aber vor vielen neugierigen Blicken zuverlässig abgeschirmt werden. Auch Ihr Netzwerk müssen Sie gegen Gefahren aus dem Internet absichern.

Ihre Vorteile auf einen Blick

- Die VPN-Komponente inkl. quantenresistentem Schlüsselaustausch für IPsec/IKEv2 sowie die Firewall-Komponente sind zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/EU RESTRICTED
- Postquanten-VPN schützt vor Angriffen mit Quantencomputern

https://www.genua.de/it-sicherheitsloesungen/firewall-vpn-appliance-genuscreen

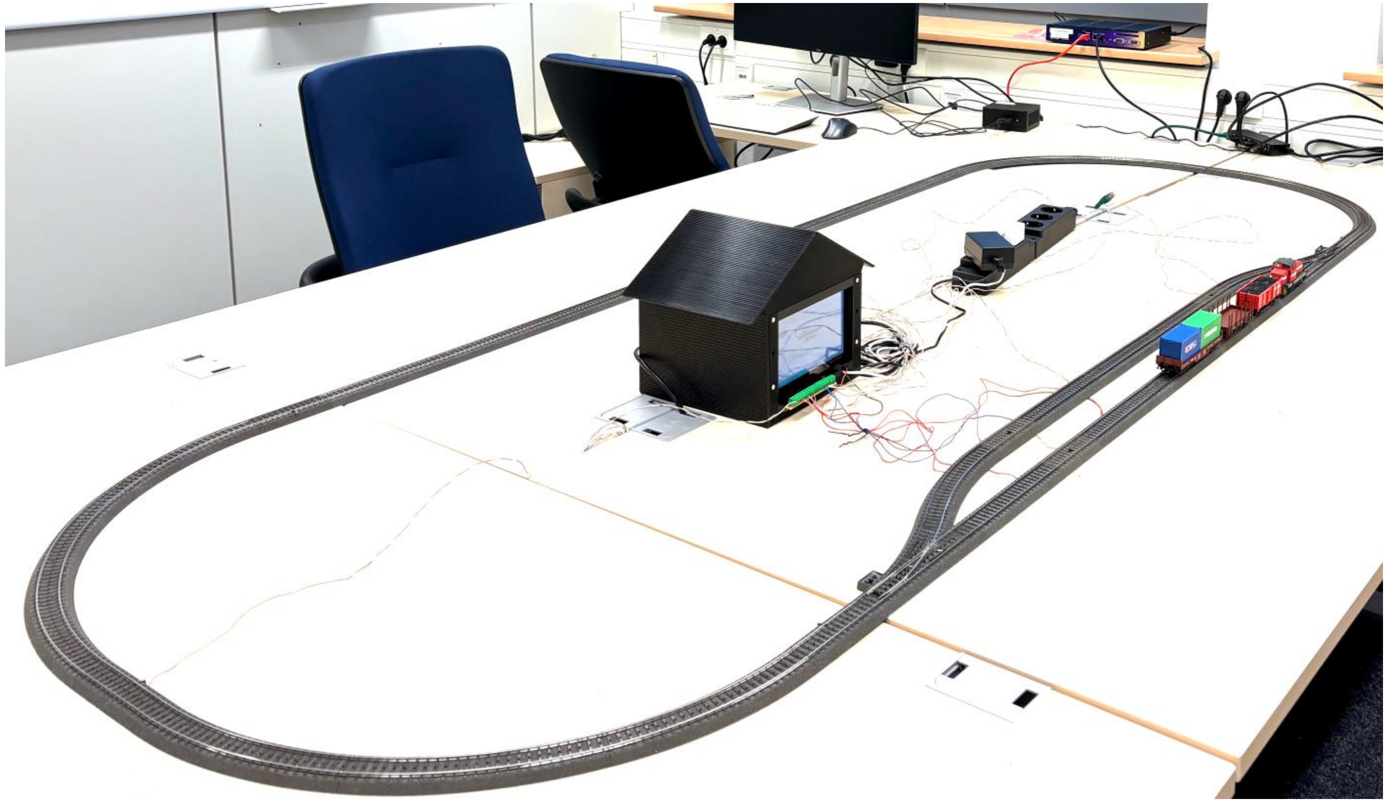
QUDIS

- Quantensichere Digitale Schiene
- Quantum Security im Safety-Kontext
- Projekt BMFTR-gefördert
- Partner: DB Systel, INCYDE GmbH, Hochschule RheinMain, Uni Regensburg, Uni Konstanz

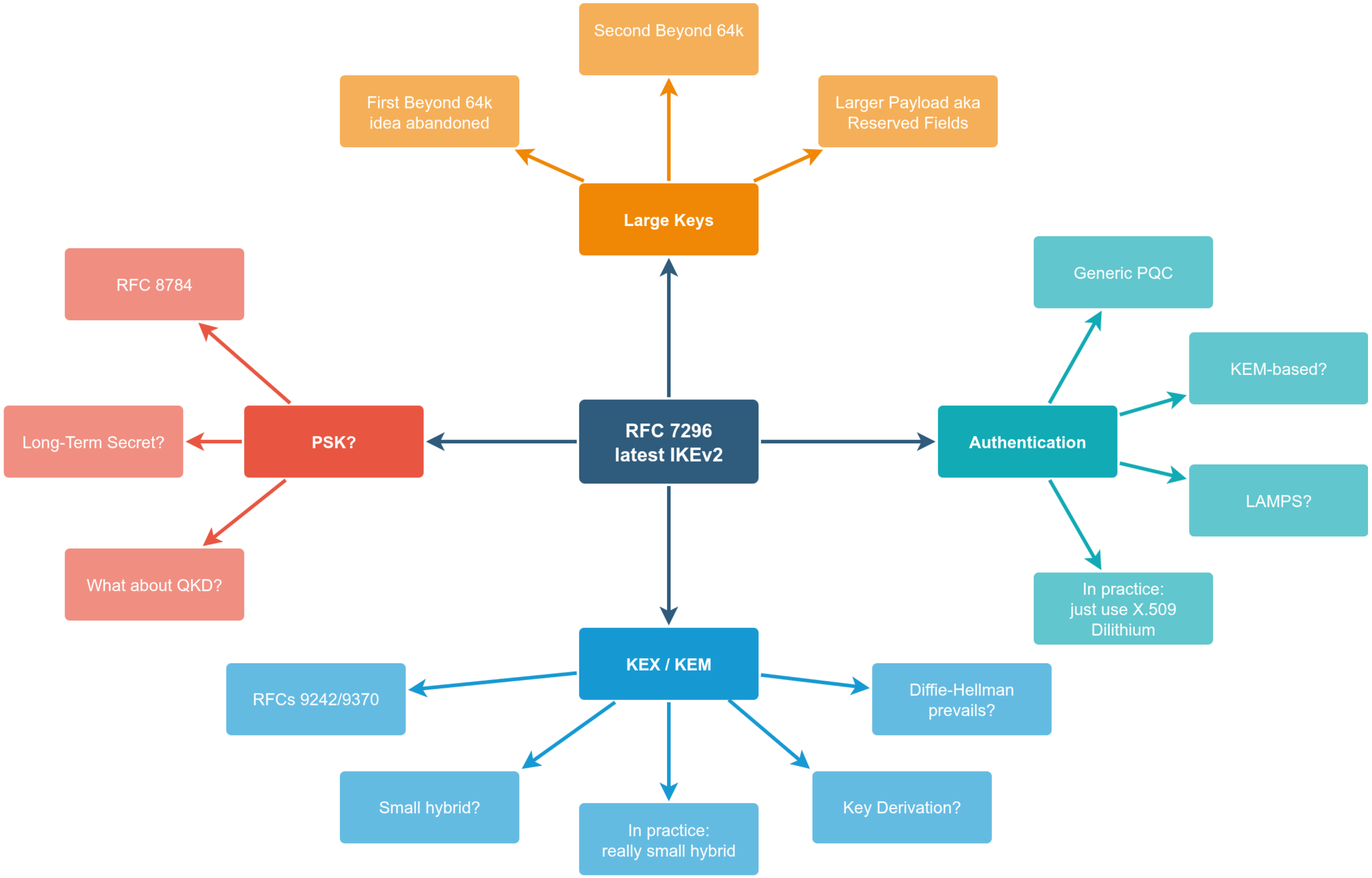
Gefördert durch:

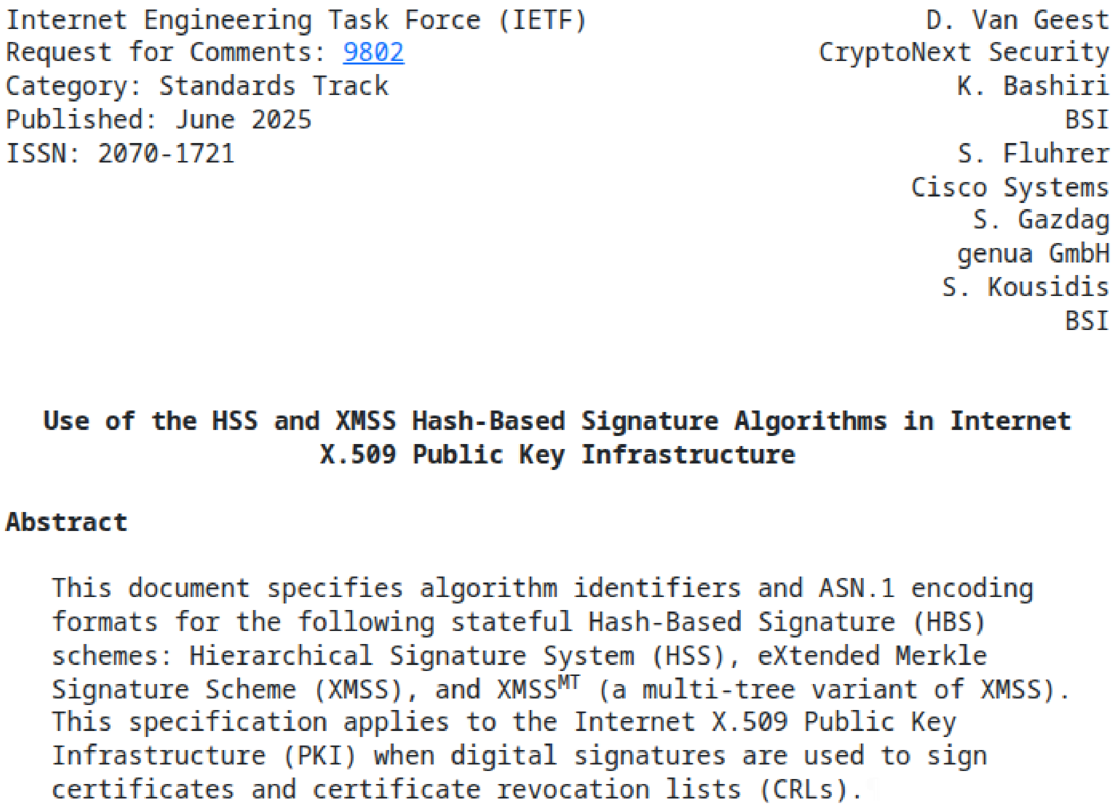
Bundesministerium
für Forschung, Technologie
und Raumfahrt

Grafik (zugeschnitten) mit freundlicher Genehmigung von Marc Stöttinger und Andreas Hellenbrand (Hochschule RheinMain)



https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qudis


Second Beyond 64k
First Beyond 64k idea abandoned
Larger Payload aka Reserved Fields
Large Keys
RFC 8784
Generic PQC
KEM-based?
Long-Term Secret?
PSK?
RFC 7296 latest IKEv2
Authentication
LAMPS?
What about QKD?
In practice: just use X.509 Dilithium
KEX / KEM
RFCs 9242/9370
Diffie-Hellman prevails?
Small hybrid?
Key Derivation?
In practice: really small hybrid

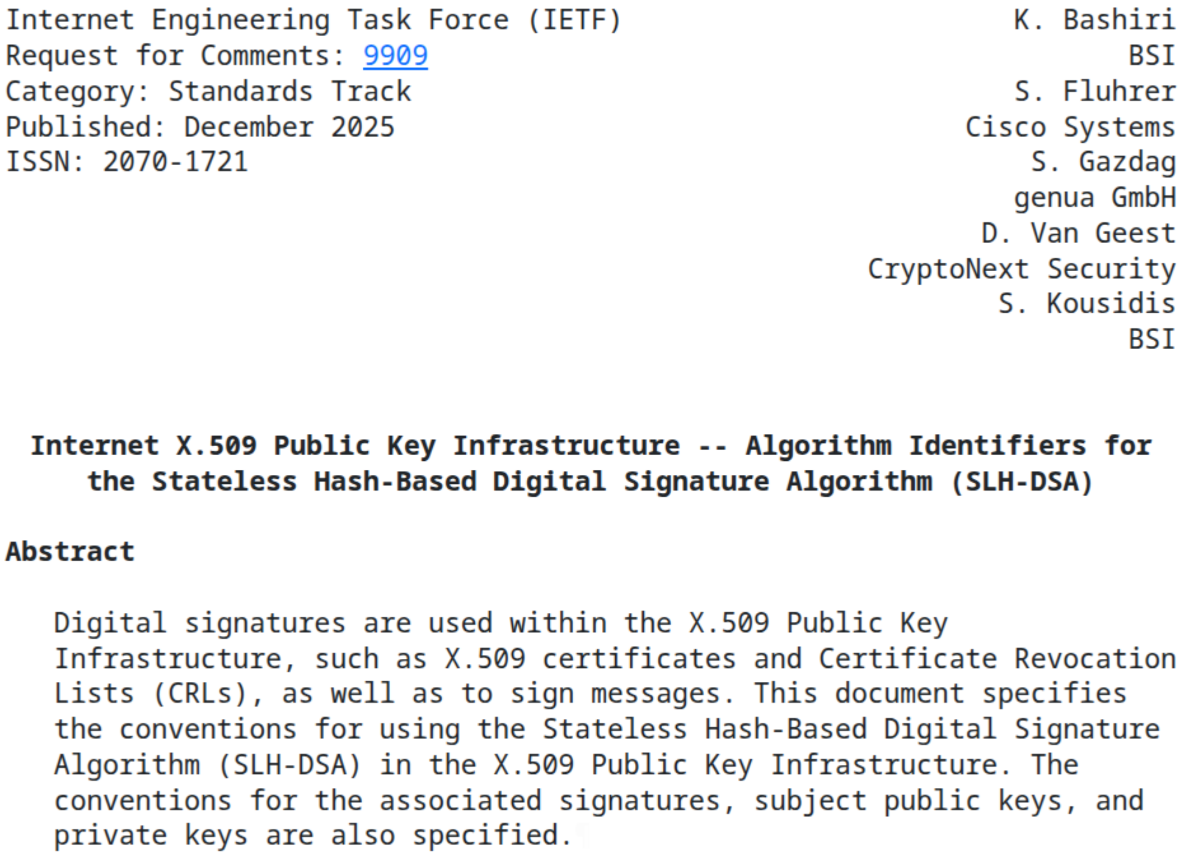


```
Internet Engineering Task Force (IETF)                D. Van Geest
Request for Comments: 9802                      CryptoNext Security
Category: Standards Track                                K. Bashiri
Published: June 2025                                            BSI
ISSN: 2070-1721                                          S. Fluhrer
                                                      Cisco Systems
                                                          S. Gazdag
                                                         genua GmbH
                                                        S. Kousidis
                                                                BSI
```

Use of the HSS and XMSS Hash-Based Signature Algorithms in Internet X.509 Public Key Infrastructure

Abstract

This document specifies algorithm identifiers and ASN.1 encoding formats for the following stateful Hash-Based Signature (HBS) schemes: Hierarchical Signature System (HSS), eXtended Merkle Signature Scheme (XMSS), and XMSS^{MT} (a multi-tree variant of XMSS). This specification applies to the Internet X.509 Public Key Infrastructure (PKI) when digital signatures are used to sign certificates and certificate revocation lists (CRLs).



```
Internet Engineering Task Force (IETF)                K. Bashiri
Request for Comments: 9909                                   BSI
Category: Standards Track                             S. Fluhrer
Published: December 2025                           Cisco Systems
ISSN: 2070-1721                                        S. Gazdag
                                                      genua GmbH
                                                    D. Van Geest
                                             CryptoNext Security
                                                     S. Kousidis
                                                             BSI
```

Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)

Abstract

Digital signatures are used within the X.509 Public Key Infrastructure, such as X.509 certificates and Certificate Revocation Lists (CRLs), as well as to sign messages. This document specifies the conventions for using the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) in the X.509 Public Key Infrastructure. The conventions for the associated signatures, subject public keys, and private keys are also specified.

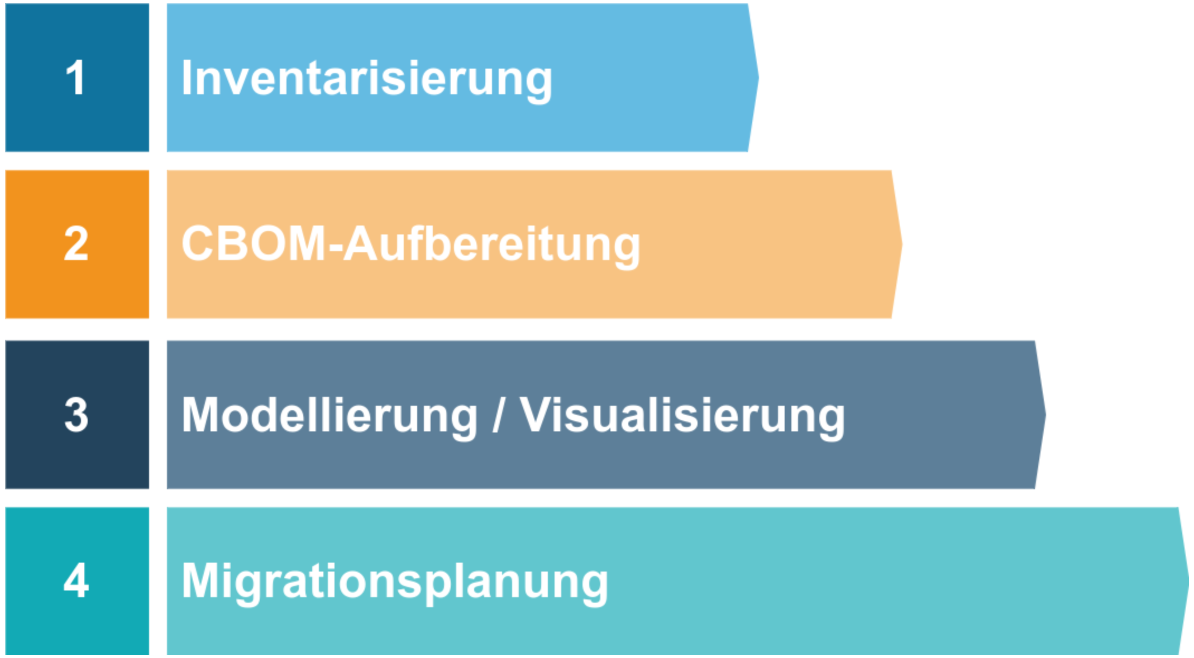
03

Migrationsplanung

Kryptoinventarisierung
& Priorisierung

AMiQuaSy

- Tooling für Kryptoinventarisierung
- Erstellung von Cryptographic Bills of Material (CBOMs)
- Migration gestützt durch graphbasierte Netzmodellierung
- Projekt BMFTR-gefördert
- Mit Xitaso GmbH und OTH Amberg Weiden



1 Inventarisierung

2 CBOM-Aufbereitung

3 Modellierung / Visualisierung

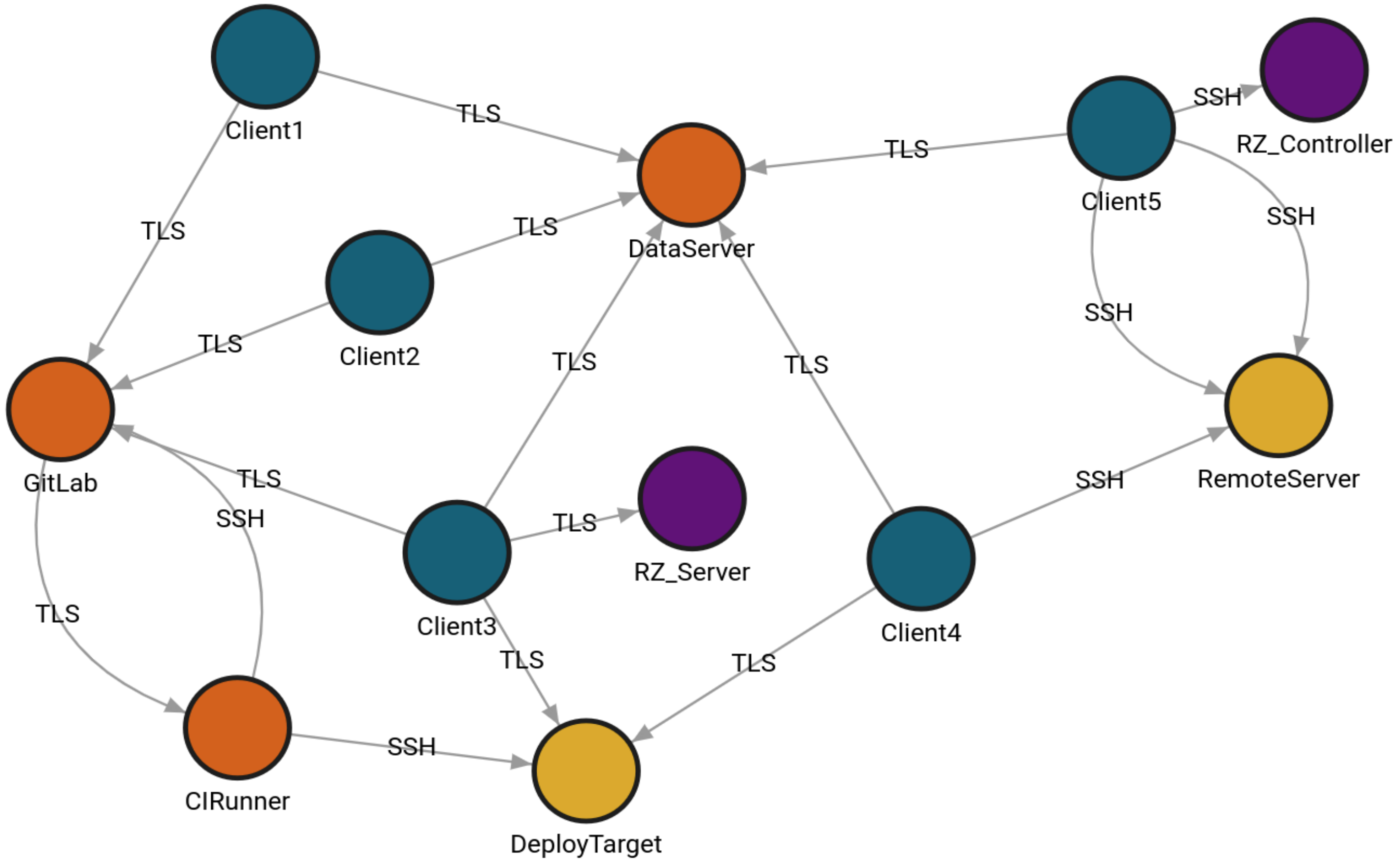
4 Migrationsplanung

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

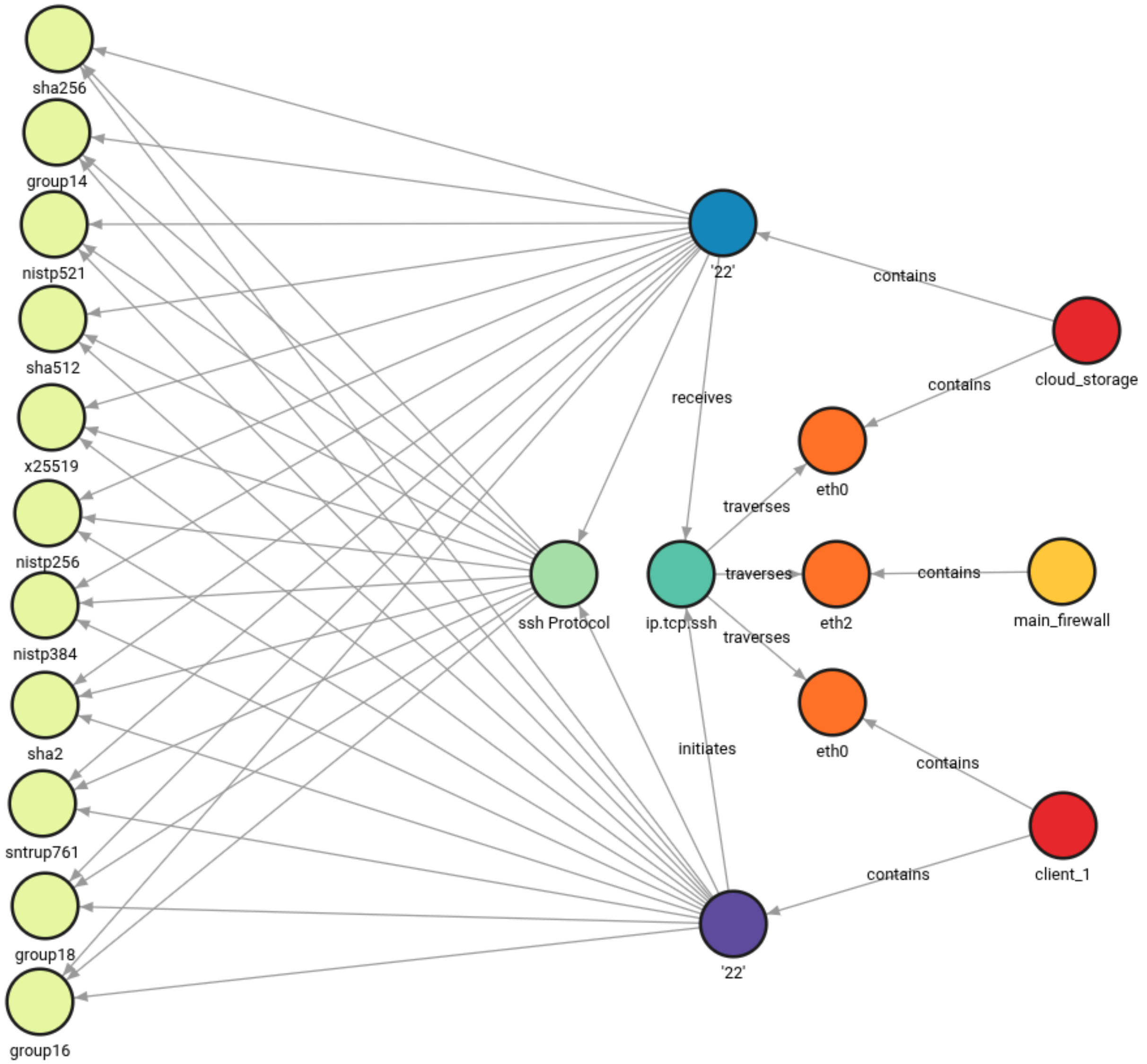
https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/amiquasy

AMiQuaSy



https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/amiquasy

AMiQuaSy

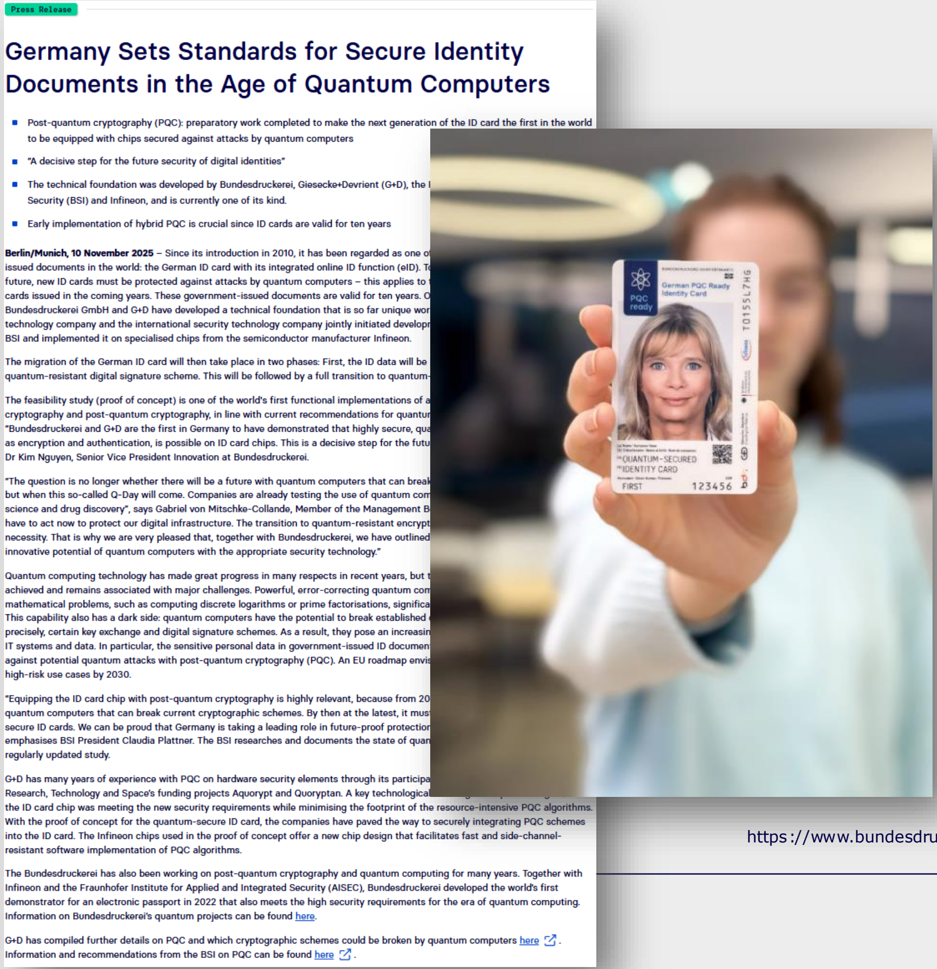


https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/amiquasy

04

Identity Documents

ID-Karte: PQC-ready



Press Release

Germany Sets Standards for Secure Identity Documents in the Age of Quantum Computers

- Post-quantum cryptography (PQC): preparatory work completed to make the next generation of the ID card the first in the world to be equipped with chips secured against attacks by quantum computers
- "A decisive step for the future security of digital identities"
- The technical foundation was developed by Bundesdruckerei, Giesecke+Devrient (G+D), the I
Security (BSI) and Infineon, and is currently one of its kind.
- Early implementation of hybrid PQC is crucial since ID cards are valid for ten years

Berlin/Munich, 10 November 2025 – Since its introduction in 2010, it has been regarded as one o
issued documents in the world: the German ID card with its integrated online ID function (eID). T
future, new ID cards must be protected against attacks by quantum computers – this applies to t
cards issued in the coming years. These government-issued documents are valid for ten years. O
Bundesdruckerei GmbH and G+D have developed a technical foundation that is so far unique wor
technology company and the international security technology company jointly initiated develop
BSI and implemented it on specialised chips from the semiconductor manufacturer Infineon.

The migration of the German ID card will then take place in two phases: First, the ID data will be
quantum-resistant digital signature scheme. This will be followed by a full transition to quantum-

The feasibility study (proof of concept) is one of the world's first functional implementations of a
cryptography and post-quantum cryptography, in line with current recommendations for quantu
"Bundesdruckerei and G+D are the first in Germany to have demonstrated that highly secure, qua
as encryption and authentication, is possible on ID card chips. This is a decisive step for the futu
Dr Kim Nguyen, Senior Vice President Innovation at Bundesdruckerei.

"The question is no longer whether there will be a future with quantum computers that can break
but when this so-called Q-Day will come. Companies are already testing the use of quantum com
science and drug discovery", says Gabriel von Mitschke-Collande, Member of the Management B
have to act now to protect our digital infrastructure. The transition to quantum-resistant encrypt
necessity. That is why we are very pleased that, together with Bundesdruckerei, we have outlined
innovative potential of quantum computers with the appropriate security technology."

Quantum computing technology has made great progress in many respects in recent years, but t
achieved and remains associated with major challenges. Powerful, error-correcting quantum com
mathematical problems, such as computing discrete logarithms or prime factorisations, significa
This capability also has a dark side: quantum computers have the potential to break established
precisely, certain key exchange and digital signature schemes. As a result, they pose an increasin
IT systems and data. In particular, the sensitive personal data in government-issued ID documen
against potential quantum attacks with post-quantum cryptography (PQC). An EU roadmap envis
high-risk use cases by 2030.

"Equipping the ID card chip with post-quantum cryptography is highly relevant, because from 20
quantum computers that can break current cryptographic schemes. By then at the latest, it mus
secure ID cards. We can be proud that Germany is taking a leading role in future-proof protectio
emphasises BSI President Claudia Plattner. The BSI researches and documents the state of quan
regularly updated study.

G+D has many years of experience with PQC on hardware security elements through its participa
Research, Technology and Space's funding projects Aquorypt and Quoryptan. A key technological
the ID card chip was meeting the new security requirements while minimising the footprint of the resource-intensive PQC algorithms. With the proof of concept for the quantum-secure ID card, the companies have paved the way to securely integrating PQC schemes into the ID card. The Infineon chips used in the proof of concept offer a new chip design that facilitates fast and side-channel-resistant software implementation of PQC algorithms.

The Bundesdruckerei has also been working on post-quantum cryptography and quantum computing for many years. Together with Infineon and the Fraunhofer Institute for Applied and Integrated Security (AISEC), Bundesdruckerei developed the world's first demonstrator for an electronic passport in 2022 that also meets the high security requirements for the era of quantum computing. Information on Bundesdruckerei's quantum projects can be found here.

G+D has compiled further details on PQC and which cryptographic schemes could be broken by quantum computers here ↗.
Information and recommendations from the BSI on PQC can be found here ↗.

Highlights und Eckdaten

- Proof-of-Concept Implementation mit Ziel der Seitenkanalresistenz
- eID und eMRTD Protokolle
- Hybride Kryptografie für Dokument und Terminal
- Kombination von LMS, ML-DSA/ECDSA, ML-KEM/ECDH
- PQC-Konformität zu ISO/IEC 7816 und IETF Drafts
- Hybrid Performance nahe der klassischen

Herausforderungen

- Internationale Standardisierung für PQC-Reisedokumente (ICAO) beginnt gerade erst
- Dokumente haben lange Laufzeit
- Heterogene Infrastruktur

try me

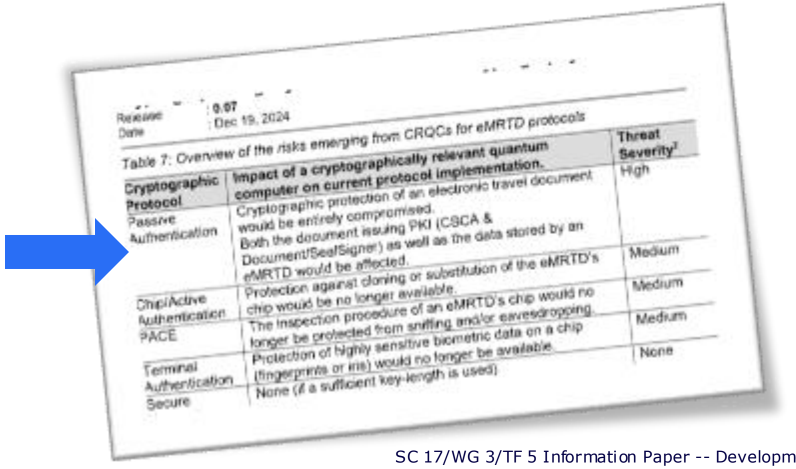
Karte und App am bdr-Stand

https://www.bundesdruckerei.de/de/newsroom/pressemitteilungen/deutschland-setzt-massstaebe-fuer-sichere-ausweisdokumente-im-zeitalter-der-quantencomputer#

Zweistufige Migration

1. **PQC-Light** – Absicherung der Passiven Authentisierung
   - PQC-sichere (hybrid) Signatur über die Ausweisdaten
   - Änderungen am zertifizierten Chip relativ klein
   - Potenziell großer Impact auf die Verifikationsinfrastruktur
   - Kurzfristig umsetzbar

2. **PQC-Chip** – Aktive PQC-Nutzung (CA, TA, PACE)
   - Nutzung von klassischer und quantensicherer Kryptografie (auch hybrid) für alle Parteien
   - Neue Chip-Architektur notwendig
   - Umsetzung ist mittel- und langfristig planbar

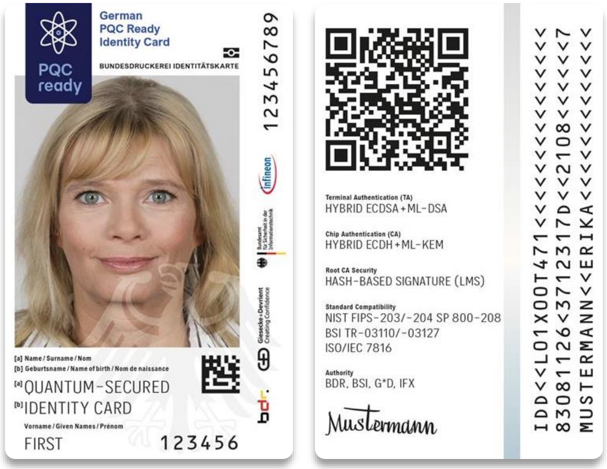


Release : 0.07
Date : Dec 19, 2024

Table 7: Overview of the risks emerging from CRQCs for eMRTD protocols

Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Threat Severity[1]
Passive Authentication	Cryptographic protection of an electronic travel document would be entirely compromised. Both the document issuing PKI (CSCA & Document/SealSigner) as well as the data stored by an eMRTD would be affected.	High
Chip/Active Authentication	Protection against cloning or substitution of the eMRTD's chip would be no longer available.	Medium
PACE	The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication	Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	Medium
Secure	None (if a sufficient key-length is used)	None

SC 17/WG 3/TF 5 Information Paper -- Developments regarding Cryptographic Agility and Post Quantum Cryptography for eMRTDs


PQC ready
German
PQC Ready
Identity Card
BUNDESDRUCKEREI IDENTITÄTSKARTE
123456789
Infineon
Bundesamt für Sicherheit in der Informationstechnik
Giesecke+Devrient Creating Confidence
bdr.
[a] Name / Surname / Nom
[b] Geburtsname / Name of birth / Nom de naissance
[a] QUANTUM-SECURED
[b] IDENTITY CARD
Vorname / Given Names / Prénom
FIRST
123456
Terminal Authentication (TA)
HYBRID ECDSA+ML-DSA
Chip Authentication (CA)
HYBRID ECDH+ML-KEM
Root CA Security
HASH-BASED SIGNATURE (LMS)
Standard Compatibility
NIST FIPS-203/-204 SP 800-208
BSI TR-03110/-03127
ISO/IEC 7816
Authority
BDR, BSI, G*D, IFX
Mustermann
IDD<<L01X00T471<<<<<<<<<<<<<<<
8308112<3712317D<<2108<<<<<<<7
MUSTERMANN<<ERIKA<<<<<<<<<<<<<

Zusammenfassung

- PQC-Awareness und Umstellung ist in vielen Bereichen zu finden
- PQC-Standards für einige Anwendungen noch nicht final
- Schrittweise Umstellung möglich per Risiko-basiertem Ansatz

→ **Incentive zur PQC-Migration stärken im Rahmen vorhandener Regulierung**

Risikobetrachtung durchführen und erste Schutzmaßnahmen durchführen

Contacts

Frank Morgner

Bundesdruckerei GmbH
Innovation
E-Mail: frank.morgner@bdr.de

Stefan-Lukas Gazdag

genua GmbH
Research & Innovation
E-Mail: stefan-lukas_gazdag@genua.de