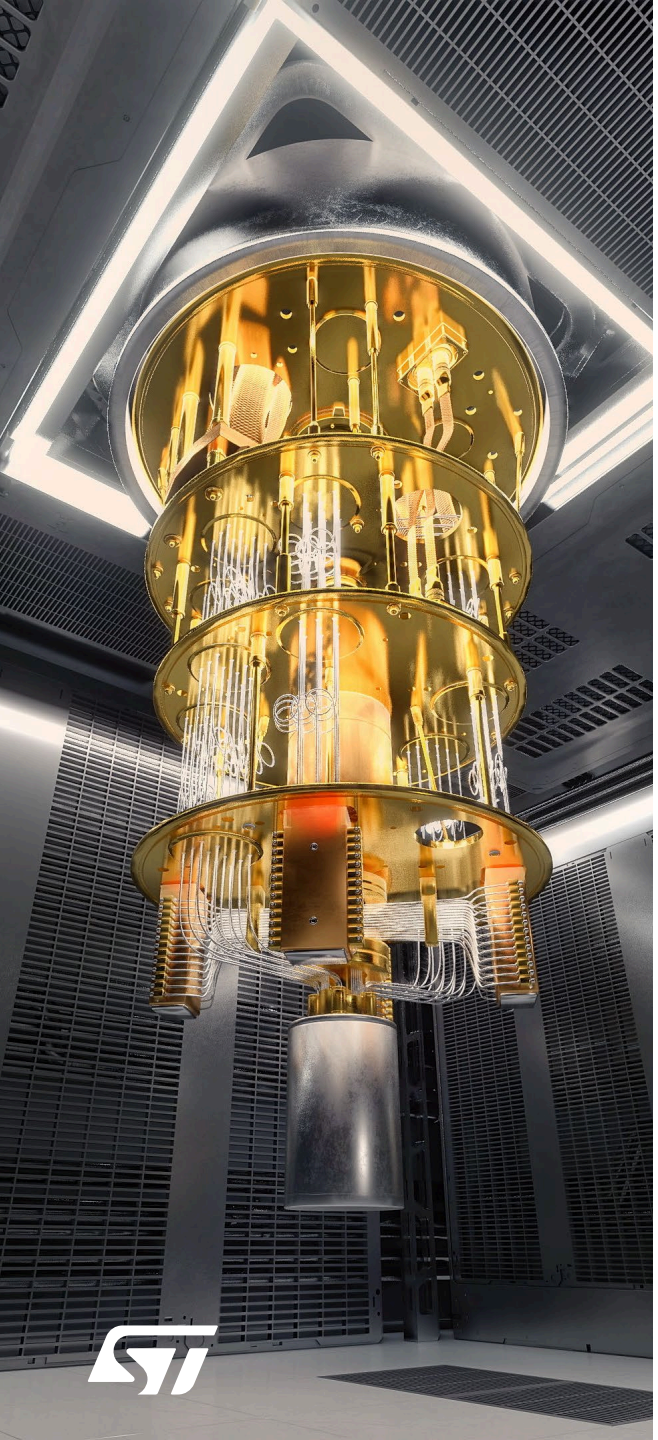
Post-quantum cryptography

From risk to opportunity



What is post-quantum cryptography?

PQC runs new cryptographic algorithms designed to **resist quantum attacks.** It is set to **replace vulnerable** public-key algorithms.

What you need to know

PQC will replace **RSA / ECC** for key exchange and digital signatures
Main standardized PQC algorithms:

- **ML-KEM** for key encapsulation
- **ML-DSA** for digital signatures
- **SLH-DSA** for specific signature use cases

Why PQC matters?

- Quantum computers may eventually **break today's** public-key cryptography
- Encrypted data can be **stolen now, and decrypted later**
- Long-life devices and **sensitive data** are the most exposed
- Now, a security and compliance priority

The **transition starts TODAY,** before the risk turns real.

Why migrating to PQC is challenging?

Top 4 challenges

- Bigger keys and signatures
- More memory and computation
- Need to update devices, software, and infrastructure
- Long-term certification and integration cycles

PQC migration
How much time do you have?

Hybrid
Near-term
(2025-2027)

NIST publication 2024
FIPS-203 (ML-KEM)
FIPS-204 (ML-DSA)
FIPS-205 (SLH-DSA)

USA: New acquisition must be CSNA 2.0 compliant by January 2027

EU: Joint statement on migration phase up to 2030 using hybrid crypto systems

US
(NSA)
Europe
(BSI, ANSSI)

Full Migration
Mid-term
(2030-2031)

RSA & ECC algorithms will be phased out

USA: All equipment not CSNA2.0 must be phased out

EU: full migration required

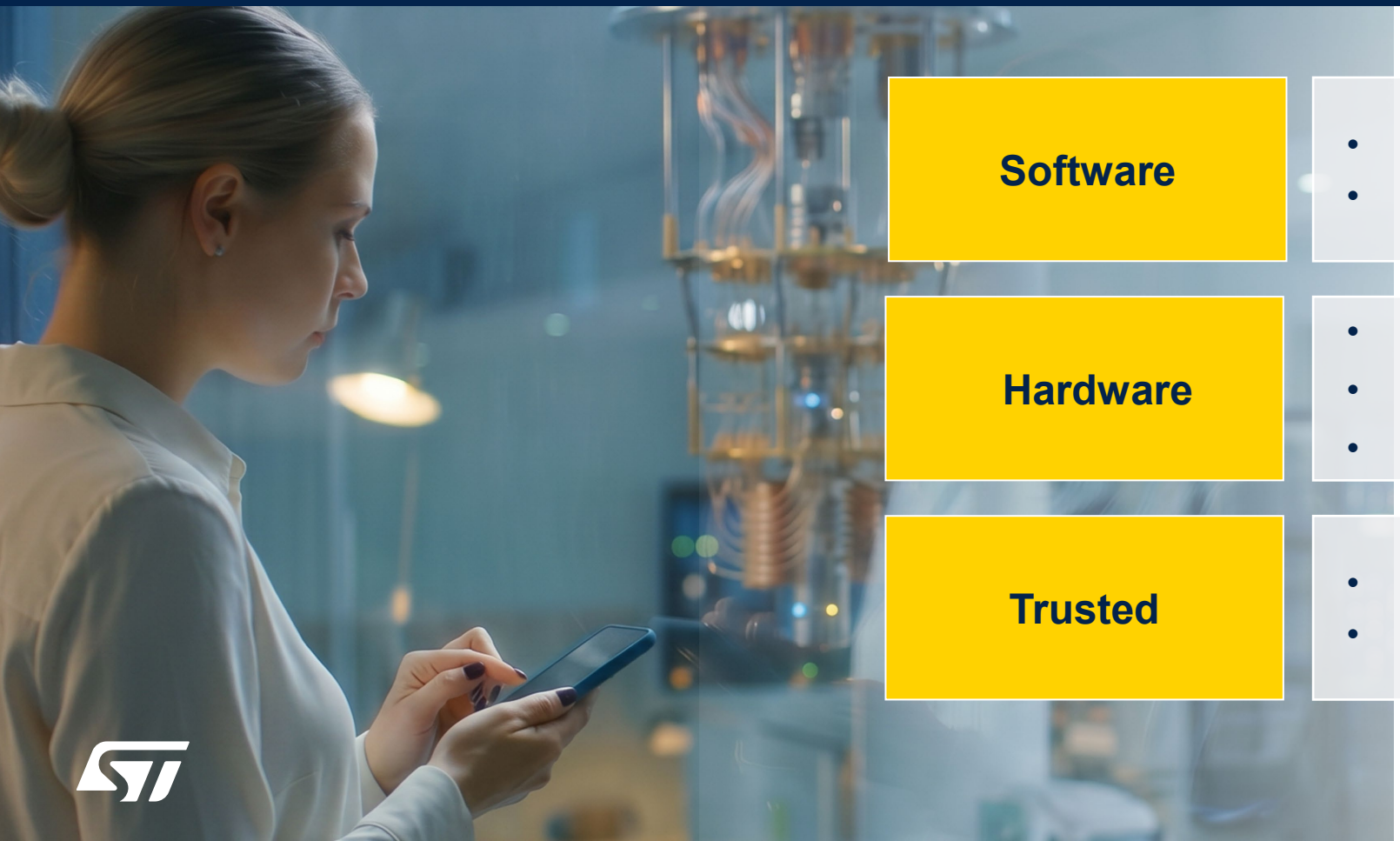
US
(NSA)
Europe
(BSI, ANSSI)

Classical asymmetric algorithms phase-out target: 2035

RSA & ECC algorithms will be phased out

Smooth and reliable PQC transition

We make PQC practical and ready for deployment in real-world applications with ML-KEM and ML-DSA algorithms.



Software

- PQC libraries for STM32
- Certified PQC libraries for secure elements

Hardware

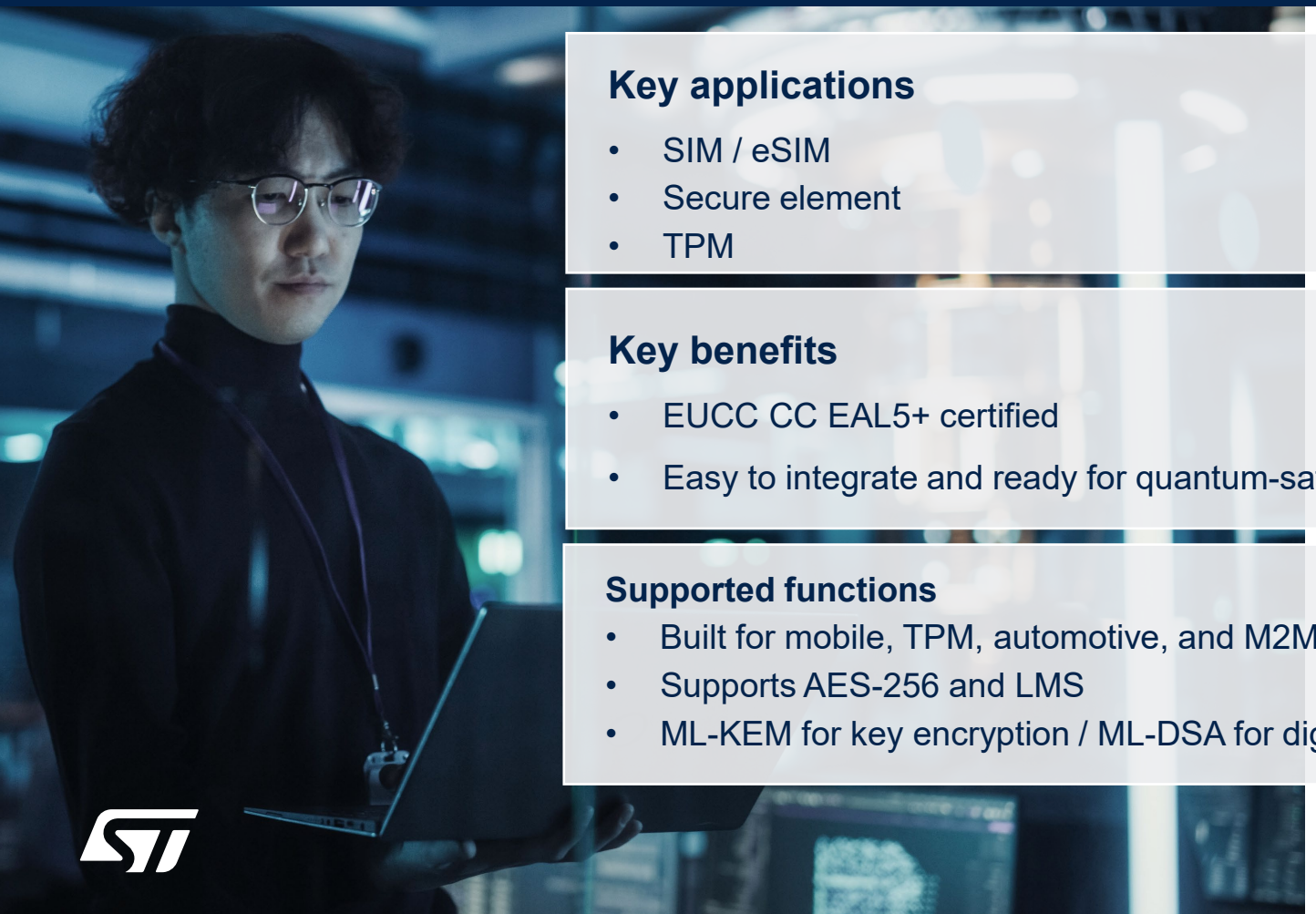
- Hardware accelerator
- Enhanced NFC capability
- Multiple applications support

Trusted

- Security certifications
- Side-channel & fault injection attack protection

PQC-ready software libraries

Certified NesLib-PQML library for ST33K1M5 secure MCU



Key applications

- SIM / eSIM
- Secure element
- TPM

Key benefits

- EUCC CC EAL5+ certified
- Easy to integrate and ready for quantum-safe use cases

Supported functions

- Built for mobile, TPM, automotive, and M2M
- Supports AES-256 and LMS
- ML-KEM for key encryption / ML-DSA for digital signatures

EUCC CC EAL5+ certified
Supports all
ML-KEM key sizes
Supports all
ML-DSA key sizes
Low RAM footprint
Optimized performance

Secure mobile chip with PQC for next-gen connected services

PQC hardware accelerator inside an NFC/eSE/eSIM combo

Post quantum cryptography

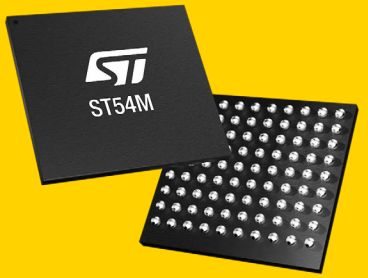
- Withstand quantum computing attacks in the coming years
- Larger memory & higher computer power

More services

- Driving license, national ID, Japan PKI, Healthcare
- eSIM pervasion with MEP

Enhanced RF front end with 3 W output power

- Improve performance with flexible antenna form factor
- Ensure a stable user experience in RW mode
- Support new use cases (mPOS, wireless charging)



Integrated DC-DC
and output power **up to 3W**

I3C interface

Arm® Cortex® M35P **200M Hz**

NVM **2.5 to 4.5 Mbytes**

RAM cache **16 Kbytes**

System RAM **150 Kbytes**

Our technology starts with You

Find out more at www.st.com/ST54M