

Quantum risks and cryptography rules: act now, but how?

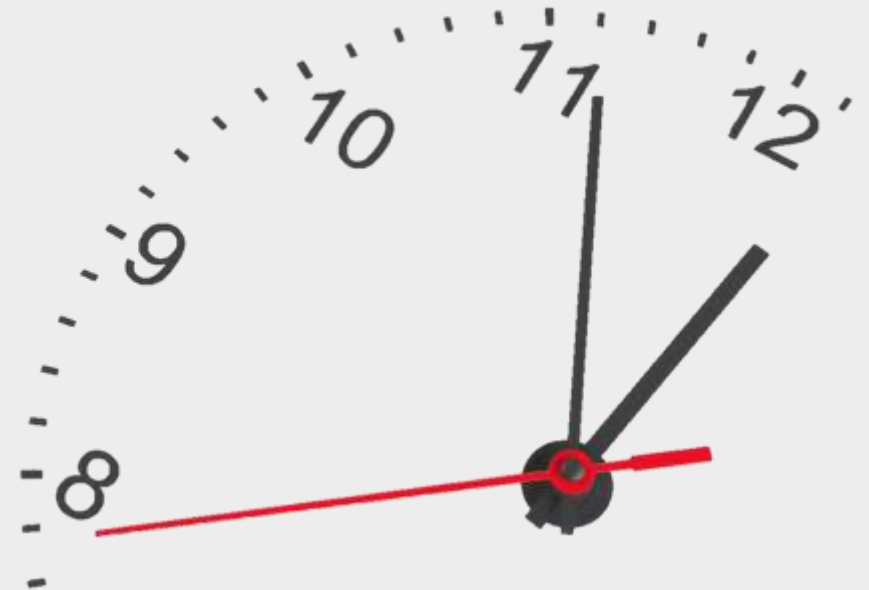
Luuk Danes & Sander Dorigo

ISACA Risk Event
12 November 2025



Q-day is coming

... and some applications
are already vulnerable





Source:

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

i 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.



Crypto Procrastination



Luuk Danes

 CRYPTOGRAPHY
IN CONTEXT





Why do we (crypto) procrastinate?

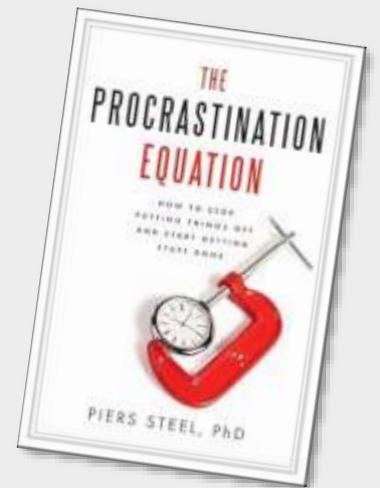
How can we overcome it?

Three ways to start today



$$\text{Motivation} = \frac{\text{Expectancy} \times \text{Value}}{\text{Impulsiveness} \times \text{Delay}}$$

Source: Piers Steel, The Procrastination Equation
Based on the temporal motivation theory (TMT):
Steel, P.; Konig, C. J. (2006). "Integrating Theories of Motivation"





Motivation

increases

if you believe you can succeed

and

if you believe the task is valuable



Motivation

decreases

if you're easily distracted

or

if the reward is far away



Make your organisation quantum-safe!



Make your presentation tum-safe!



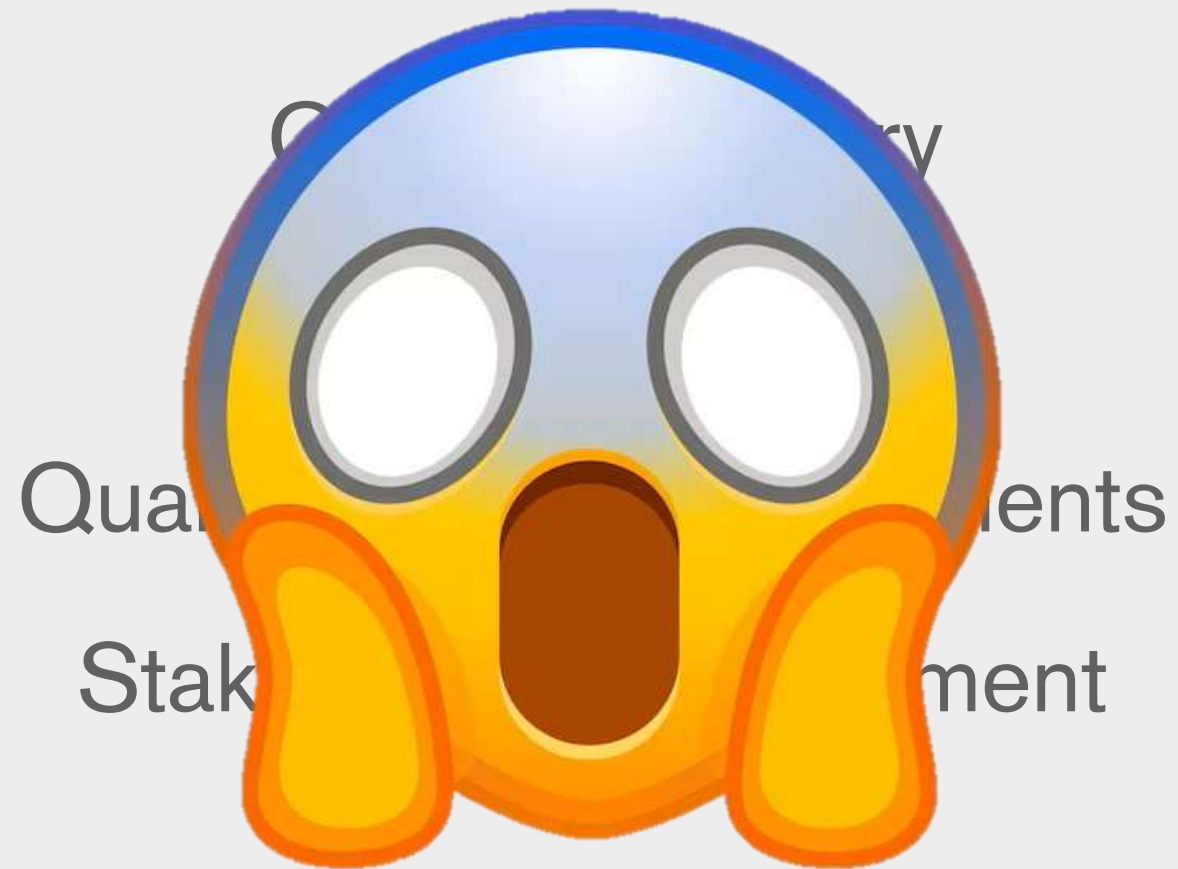


Crypto Inventory

PQC Roadmap

Quantum Risk Assessments

Stakeholder Engagement





Boost your motivation



**Just take the first step
towards a quantum-safe future ...**



... but make sure it has:

High chance of **success**

Value beyond quantum-safety

Concrete actions

Short-term results



You must **inventory all cryptography**
before addressing quantum risks



~~You may not know the topography
before taking on risks~~



You can only start
once the **standards are finalised**



once the process is finalised



You need to
understand quantum mechanics
or use quantum technology



~~You need to understand quantum mechanics~~



You must know where and how you're using
(quantum-safe) cryptography



YES

You must know where and how you're using
(quantum-safe) cryptography



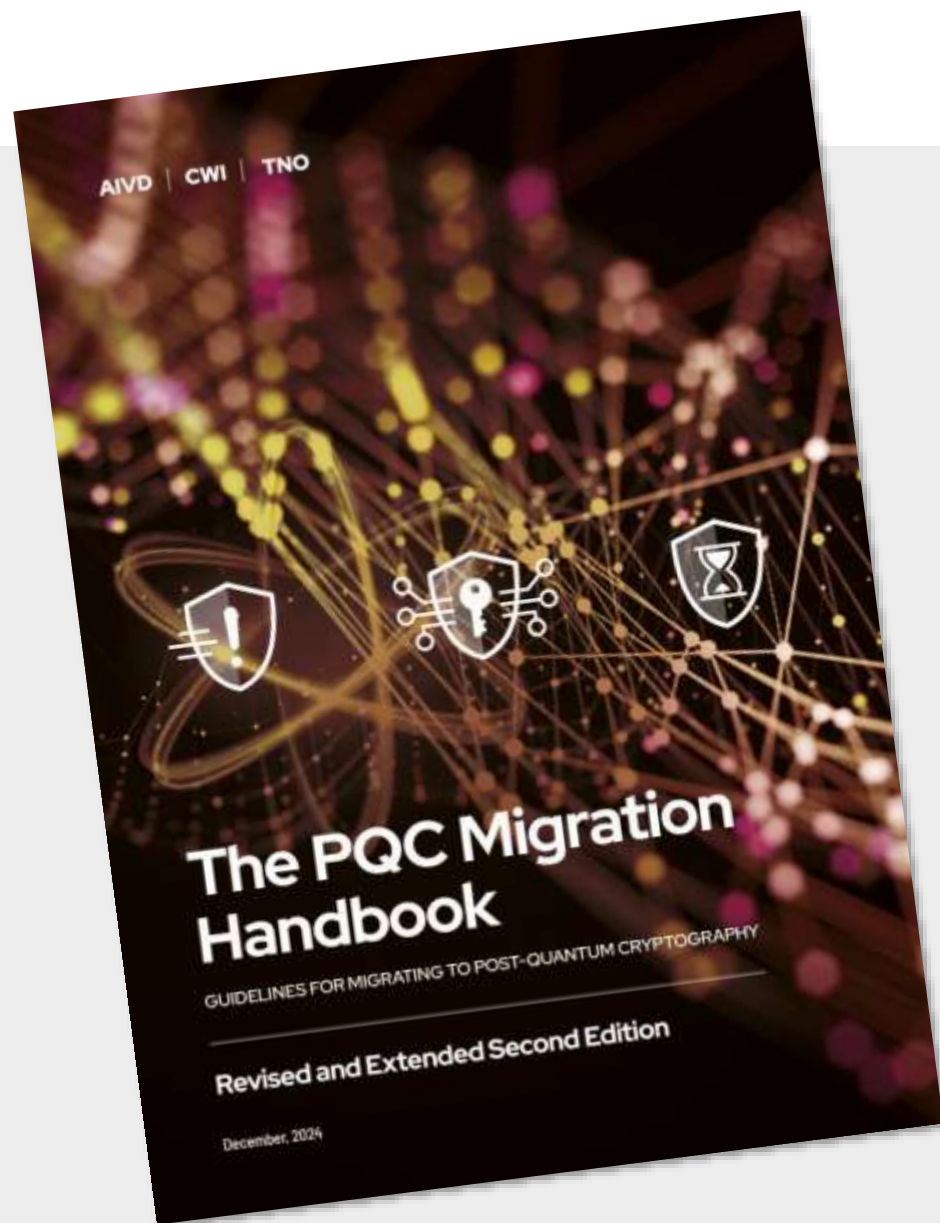
Plan a Learning & Sharing Activity

☐ Success | ☐ Value | ☐ Concrete | ☐ Short-term



Visualise Business Impact

□ Success | □ Value | □ Concrete | □ Short-term



The PQC Migration Handbook

AIVD, CWI & TNO / 2nd edition



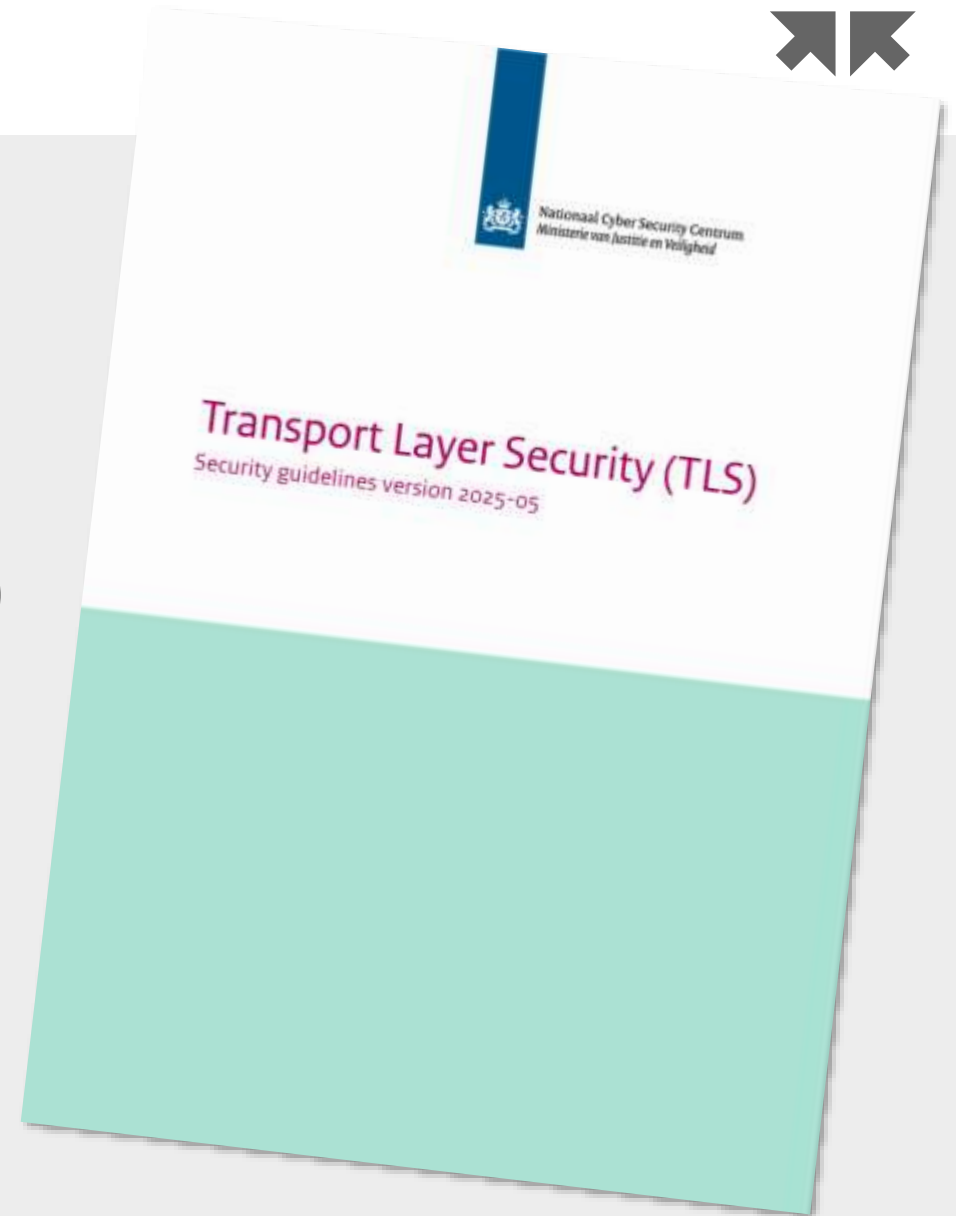
Future-proof your TLS

□ Success | □ Value | □ Concrete | □ Short-term



Transport Layer Security (TLS) Security guidelines

NCSC / version 2025-05



Quantum risks and cryptography rules: act now, but how?

Sentyron



1948

Nederlandse
Seintoestellen
Fabriek

1957

Philips USFA
(Ultrasonie
fabriek)

1990

Philips Crypto

2003

Fox Crypto

2025

Sentyron





PUBLIC













PUBLIC



PUBLIC



FIPS 203

ML-KEM

General encryption



FIPS 204

ML-DSA

Digital signatures



FIPS 205

SLH-DSA

Digital signatures



FIPS 206

FN-DSA

Digital signatures





PUBLIC



TLS 1.3



SSH

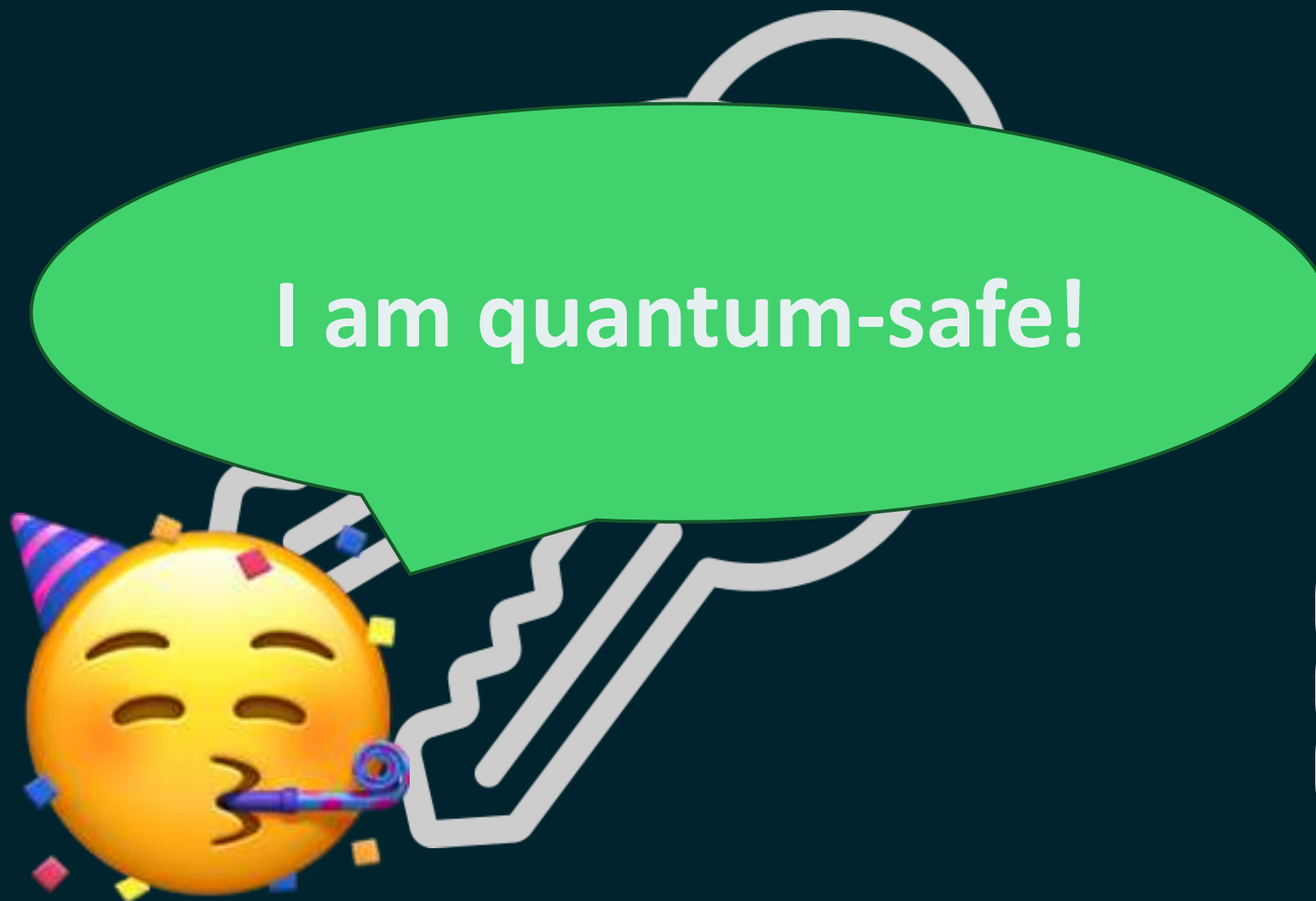


S/MIME



Signal







PUBLIC



Hybrid: contains both quantum-safe and classic key + signature





Hybrid: contains both quantum-safe and classic key + signature



Chameleon: contains the same, and other metadata
Can be used to generate a “new” certificate





Hybrid: contains both quantum-safe and classic key + signature



Chameleon: contains the same, and other metadata
Can be used to generate a “new” certificate



Composite: the certificate contains a mixed key and signature,
making it quantum-safe





Hybrid: contains both quantum-safe and classic key + signature



Chameleon: contains the same, and other metadata
Can be used to generate a “new” certificate



Composite: the certificate contains a mixed key and signature,
making it quantum-safe



+



Merkle Tree: the certificate contains very little data,
all relevant information can be found online



Securing the digital frontier

- Quantum-safe technology exists and can be safely integrated
- Quantum-safe algorithms and protocols will make you secure against “steal now, decrypt later” attacks
- Having a vision and ambition impresses auditors and certifying organisations ;-)



Act now!

It is both necessary
and possible to start
becoming quantum-safe

sander.dorigo@sentyron.com
www.sentyron.com



PUBLIC

But how?

Take your first step!

And aim for:

High chance of **success**

Value beyond quantum-safety

Concrete actions

Short-term results

luuk.danes@cryptoincontext.nl
www.cryptoincontext.nl

