PQC migration

a systems point of view

Berg, S.H.M. (Stefan) van den |

whoami

- Stefan van den Berg
  - Master in Information Security Technologies and Embedded Systems

- Cyber security researcher at TNO
  - Post Quantum Cryptography
  - Formal verification
  - Software testing

Current situation

- Cryptography is used for:
  - Authentication, Confidentiality and/or Integrity

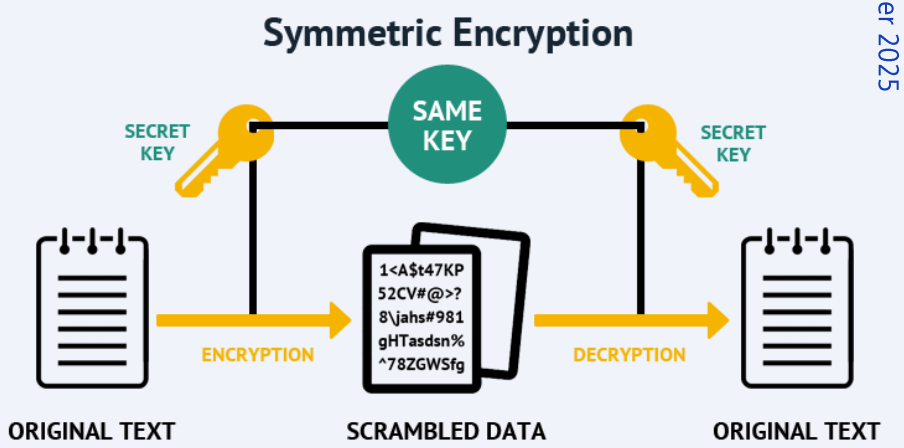
- Either directly used by an application/system or as a dependency

- Use-cases:
  - Over The Air-updates (firmware signing)
  - TLS connections
  - Sensitive data at rest
  - ...

Cryptography – Two Categories

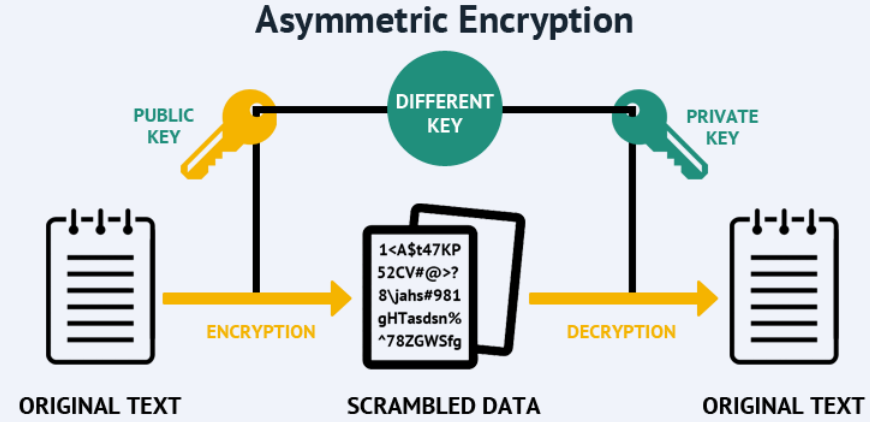
Symmetric Cryptography

- One key for both encryption and decryption
- Requires pre-arranging a shared secret key
- Examples: *Caesar, Vignère, Enigma, AES, DES, Blowfish, Salsa20, ChaCha20*



Asymmetric ("Public-Key") Cryptography

- Different keys for encryption (*public key*) and decryption (*private key*)
- Security based on mathematical "hard" problems
- Often used for exchanging/establishing symmetric key
- Examples: *RSA, ECDSA, Diffie-Hellman*

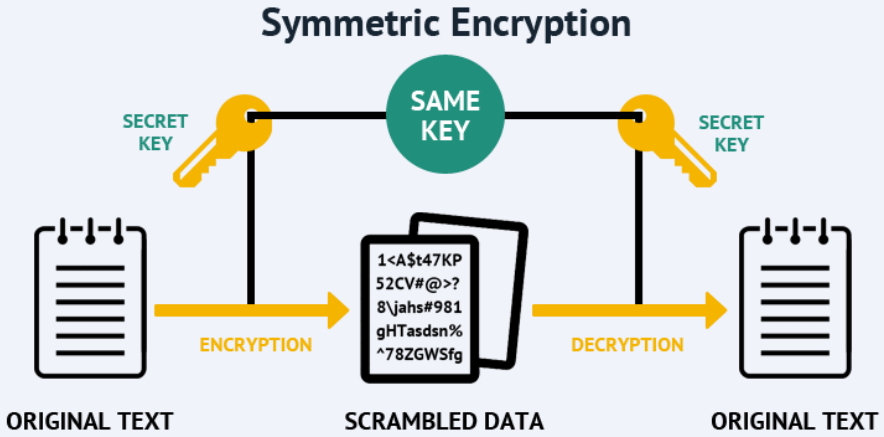


Cryptography – Two Categories

Symmetric Cryptography

- One key for both encryption and decryption
- Requires
- Examples: *Caesar, Vignère, Enigma, AES, DES, Blowfish, Salsa20, ChaCha20*

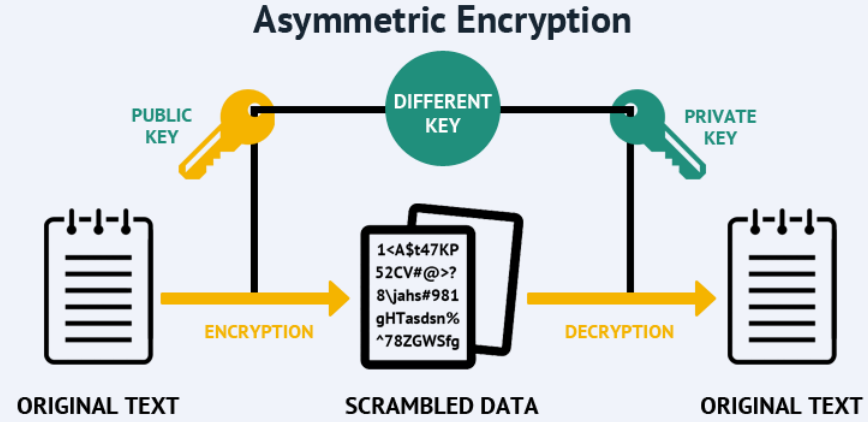
Weakened by quantum attacks (Grover's algorithm)



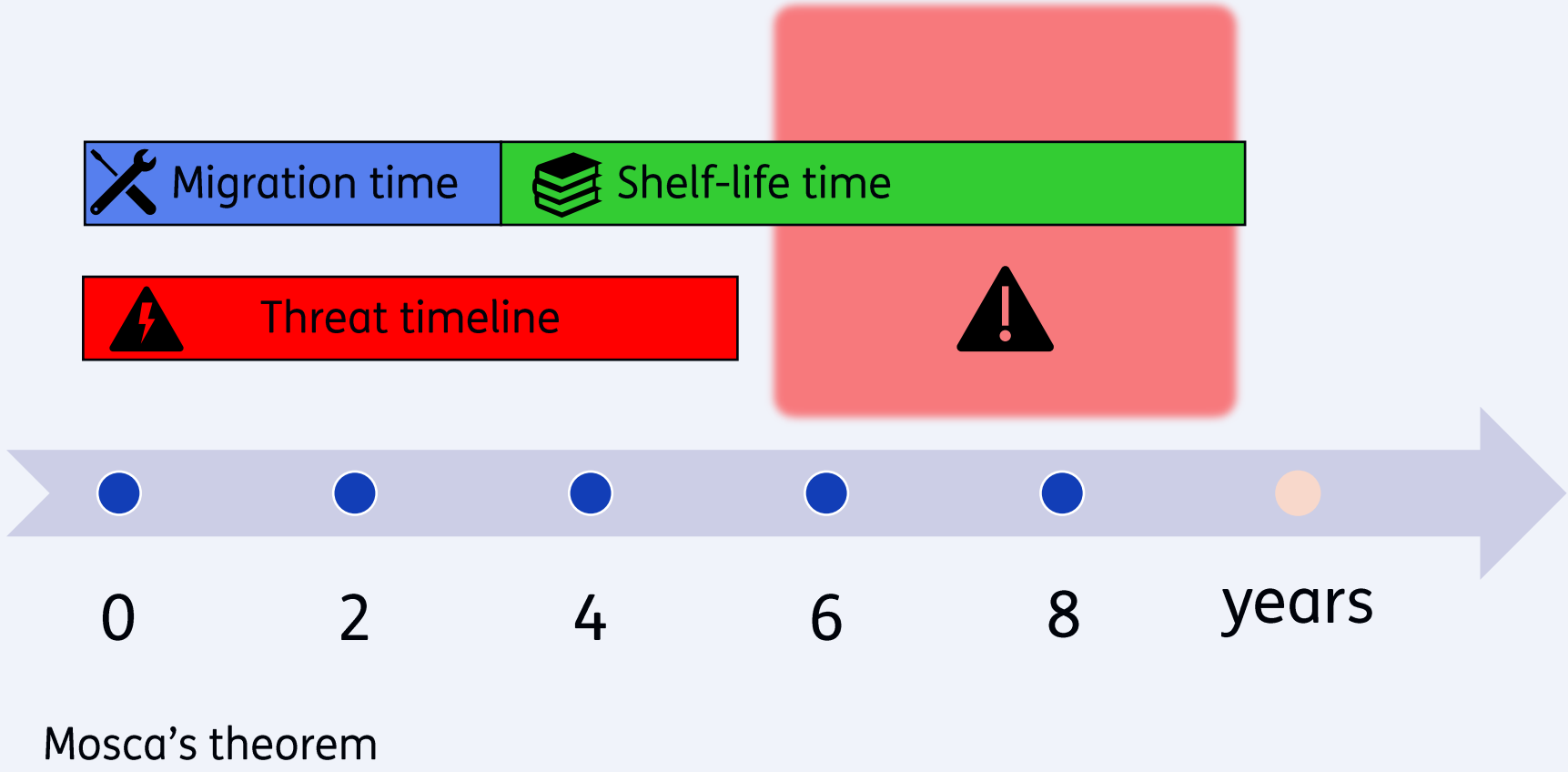
Asymmetric ("Public-Key") Cryptography

- Different keys for encryption (*public key*) and decryption (*private key*)
- Security based on mathematical "hard"
- symmetric key
- Examples: *RSA, ECDSA, Diffie-Hellman*

Completely broken by quantum attacks (Shor's algorithm)



Quantum risk and cryptography



Mosca's theorem

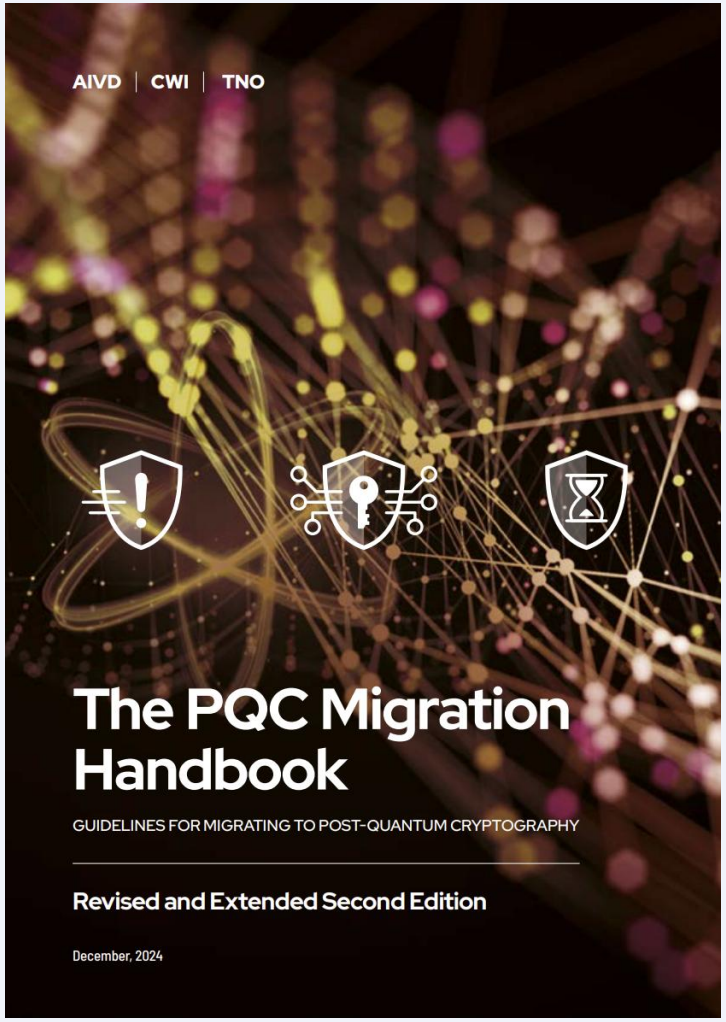
Recap quantum risk and cryptography

- Broken **asymmetric encryption** (key exchange)
  - If confidentiality is gone, it is not recoverable (re-encrypt is not going to help)
  - Store now decrypt later urgency

- Broken **asymmetric signature** -> authentication
  - Enables impersonation after q-day
  - Authentication is often short-lived, but not always! (IDcard)
  - Can have major impact (Diginotar example)
  - Reissuing authentication with PQC signature keys can solve treat, as long as authentication using the old keys are not accepted anymore afte q-day

- Broken **asymmetric signature** -> non repudiation, integrity and authenticity
  - Enables forging/manipulation (malicious software updates, hacking, DOS, physical attacks) after q-day
  - Signatures can be valid (accepted) for a long time. Document signatures, software updates, secure boot.
  - Reissuing document/messages with PQC signatures can solve treat, as long as the old signature is not accepted anymore after Q-day

PQC migration handbook



https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

Timelines

- NIST
  - 2030 deprecation of vulnerable algorithms
  - 2035 full phase-out of classical crypto
- EU roadmap PQC
  - End of 2026:
    - Start planning and pilots for high- and medium-risk use-cases
    - National PQC transition roadmaps
  - End of 2030:
    - High risk use-cases completed;
    - pilots for medium use-cases completed;
    - QS software updates by default
- BigTech
  - Google 2029
  - Cloudflare 2029

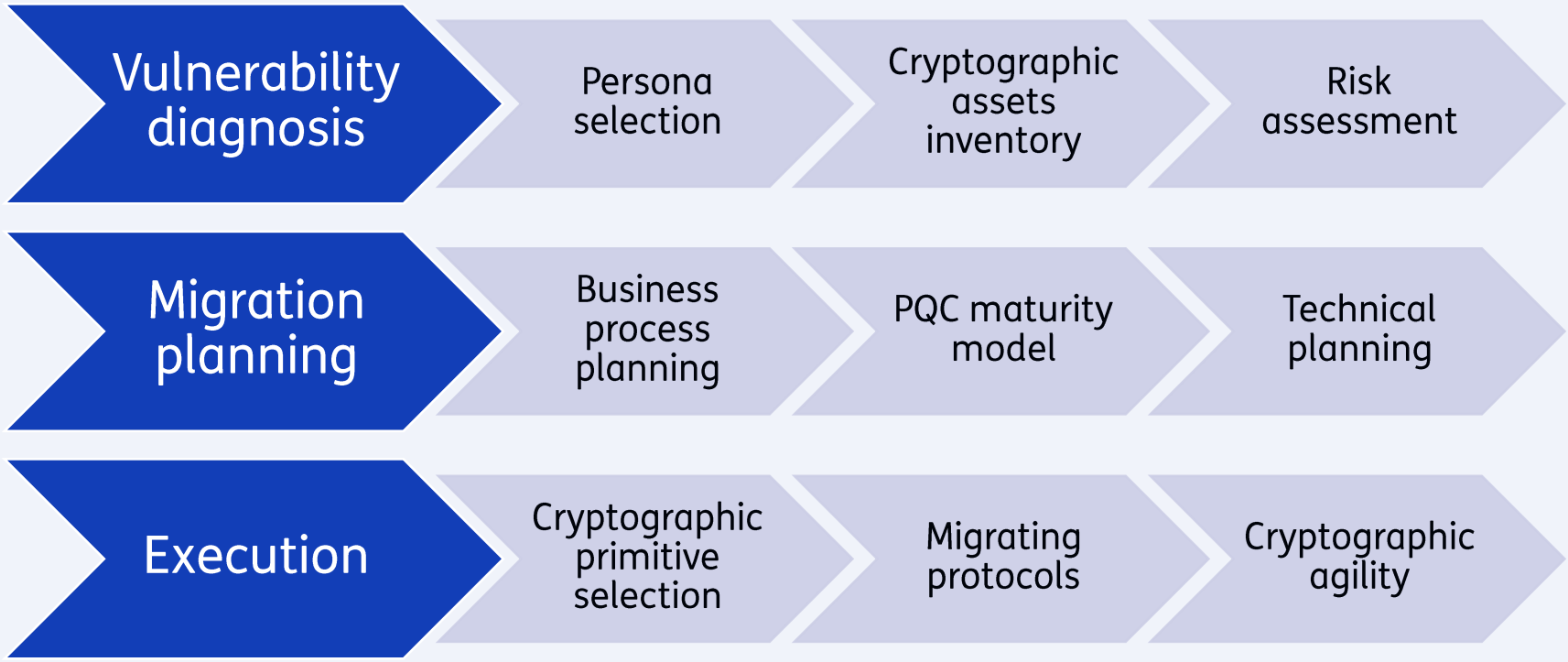
IR 8547, Transition to Post-Quantum Cryptography Standards | CSRC

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future

Google's timeline for PQC migration

Cloudflare targets 2029 for full post-quantum security

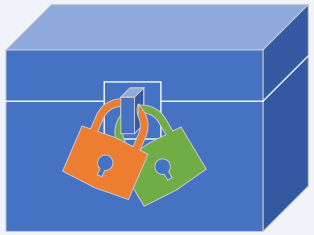
Migration steps



Migration to PQC

- Swap for PQC algorithm
  - Protects against quantum computer
  - PQC uses complex math, less experience with side channel protection
  - PQC sizes are currently quite large (work being done on better alternatives)

- Hybrid approach
  - Two layers of protection (One ECC, because fast and small, one PQC)

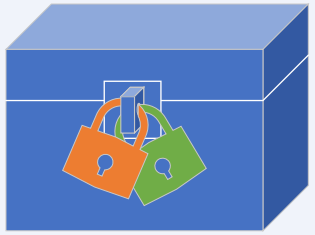


What are the countries opinions?

- **USA** (IR 8547):
  - “The migration to post-quantum cryptography **may initially include hybrid”.**
  - “When used, hybrid solutions are typically expected to **be temporary measures** that lead to a **second transition** to cryptographic tools that use only PQC algorithm”
- **UK** (NCSC-UK)
  - “If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an **interim measure**, and it should be used within a flexible framework that enables a straightforward migration to **PQC-only** in the future.”
- **EU**: recommends hybrid:
  - “When migrating to post-quantum cryptographic solutions, it is **recommended** to use standardised and tested **hybrid** solutions, **whenever feasible** and **suitable**”
- **NL** (handboek): promotes hybrid use
  - “De belangrijkste aanbeveling voor **bijna alle protocollen** is om een **hybride** oplossing te gebruiken”
- **DE**: Actively recommends hybrid, even after q-day
  - “Post-quantum schemes should **only** be used **in combination with** classical schemes ("**hybrid**") if possible. Due to the previously mentioned point, a hybrid approach (with two or more post-quantum schemes) is a possible solution even after the development of cryptographically relevant quantum computers.”

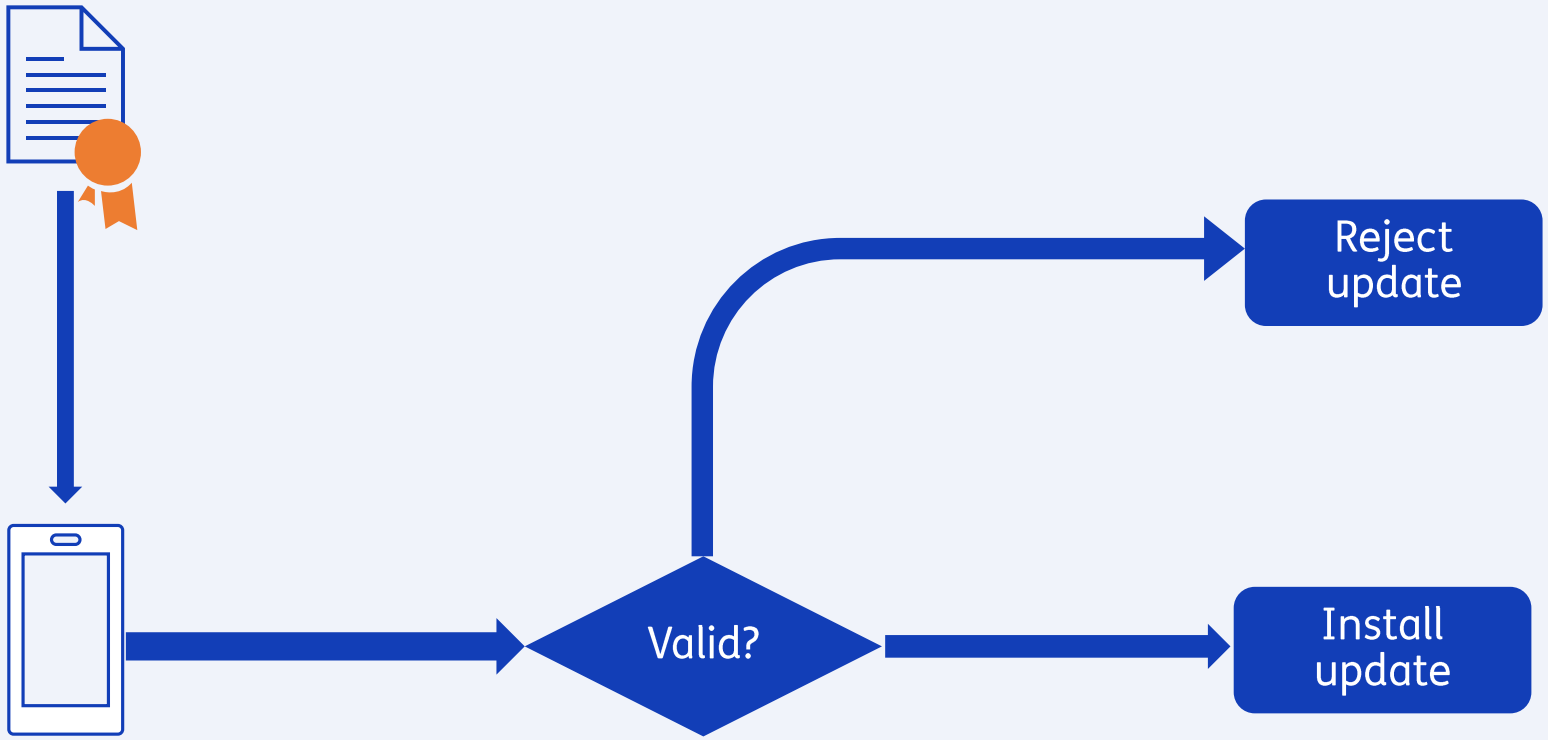
Hybrid what?

- Hybrid key exchange
  - 2 key exchanges, resulting keys are combined with a **secure combiner** into one result
  - The resulting key is used in rest of the protocol (often by symmetric algorithms)

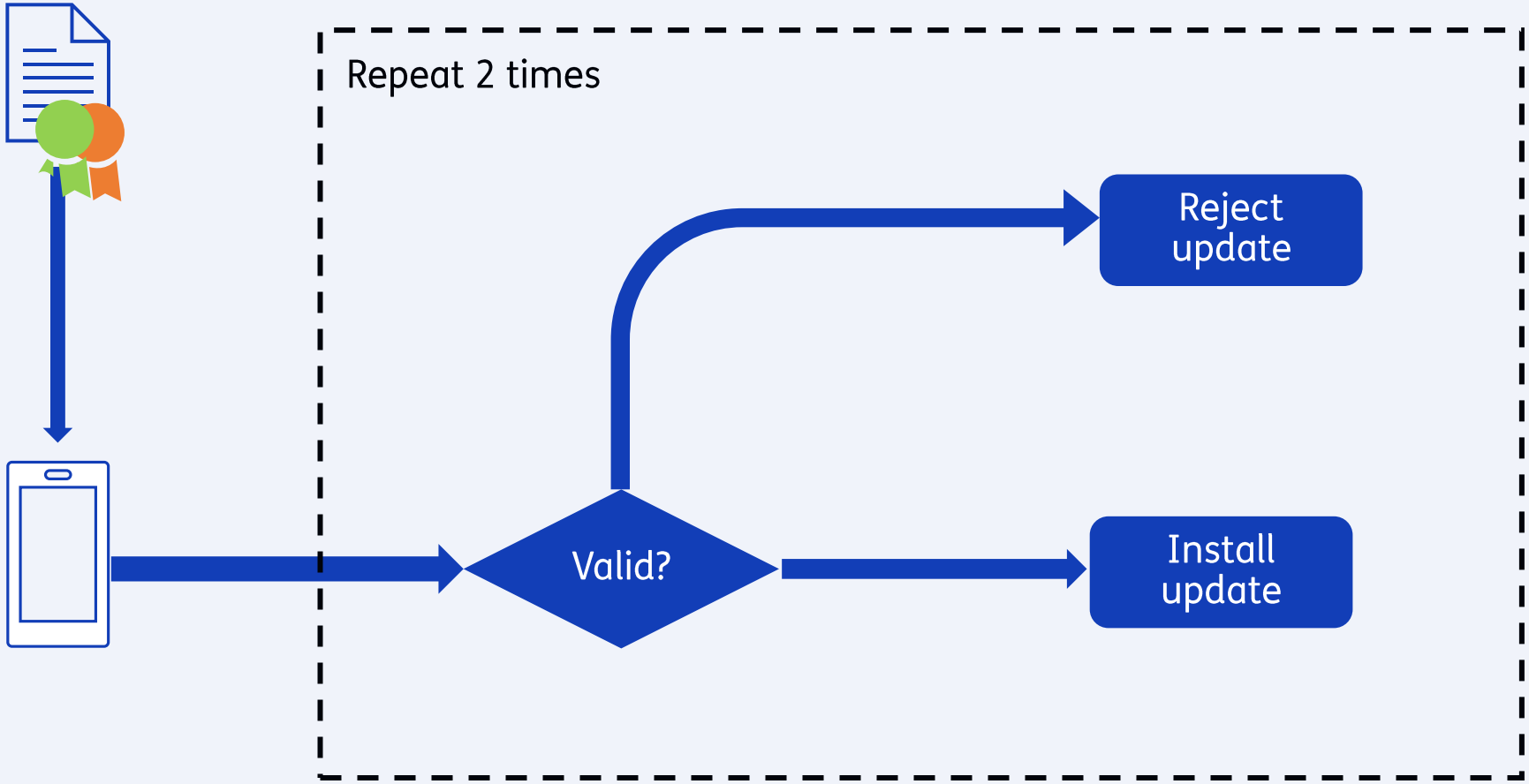


- Hybrid signatures
  - 2 signatures are made on the message, verification only succeeds if both are valid

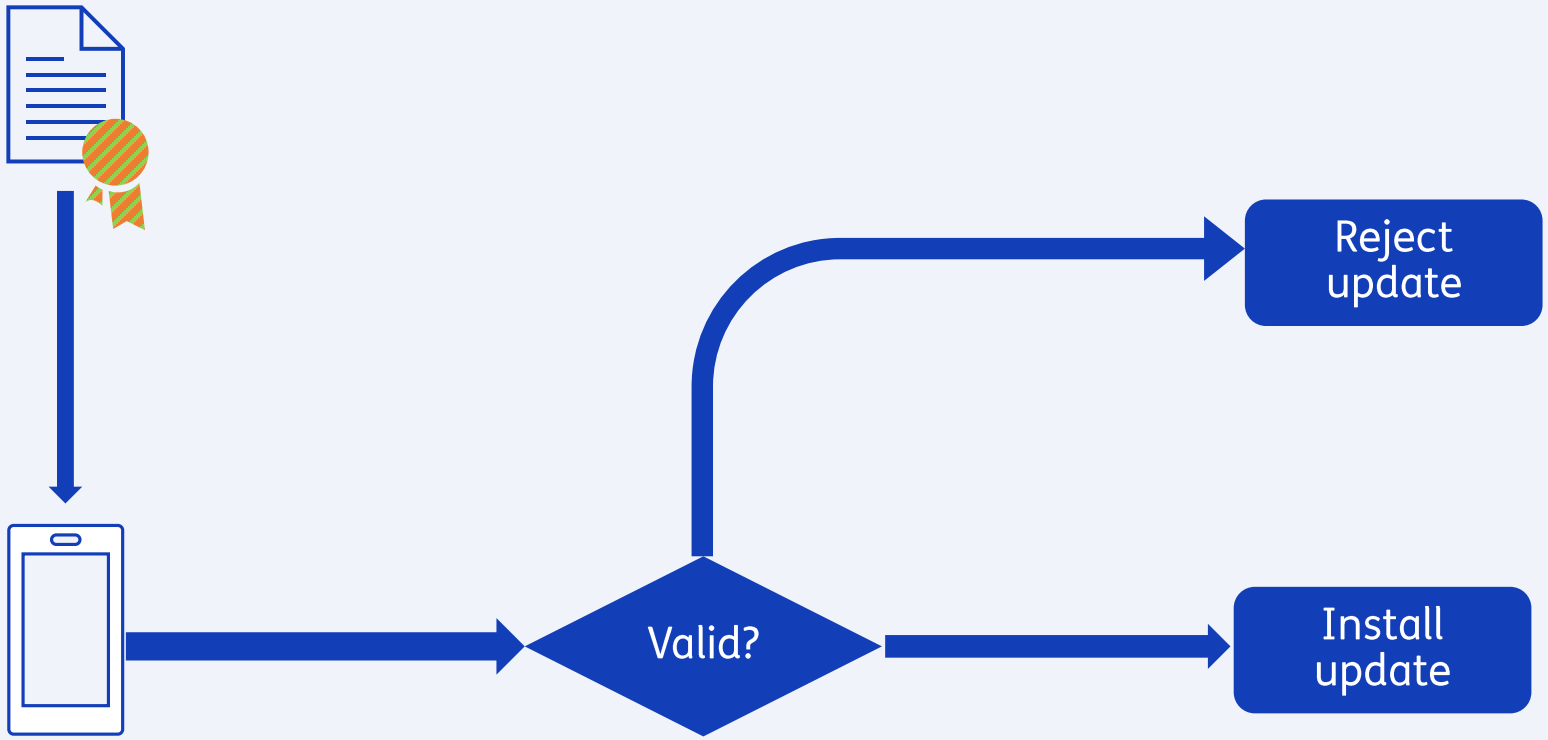
Over-the-air update



Over-the-air update



Over-the-air update



Where to do hybrid

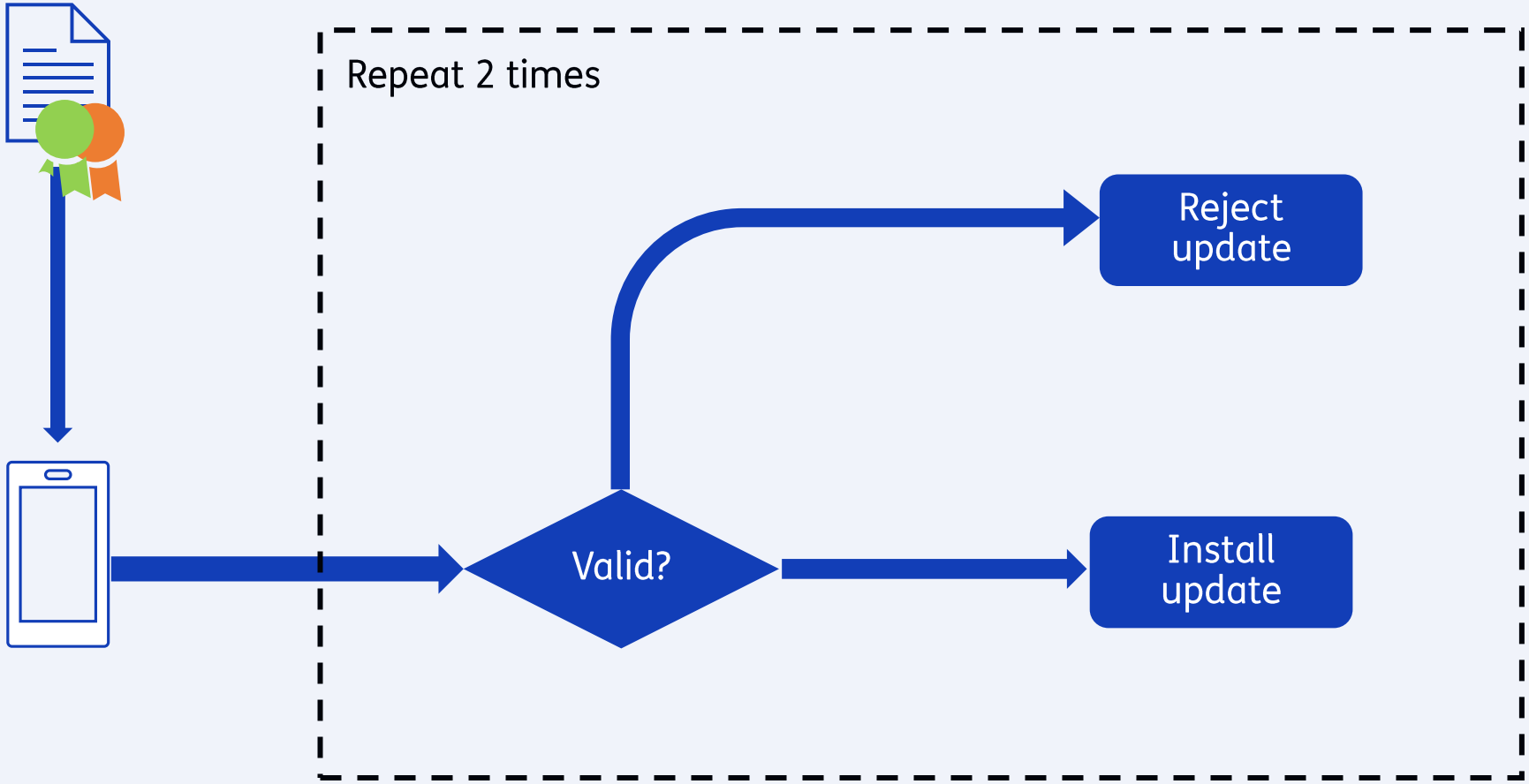
At the place where the crypto is used

- Developer/admin/engineer has a choice *which algorithms* to combine
- Has choice *how* to combine
- ➢ Complexity at the implementation side
- ➢ Room for errors and misconfiguration
- Adjustment needed in the protocol/software for two keys/signatures/verifications
- ➢ A lot of protocols and software needs to be adjusted

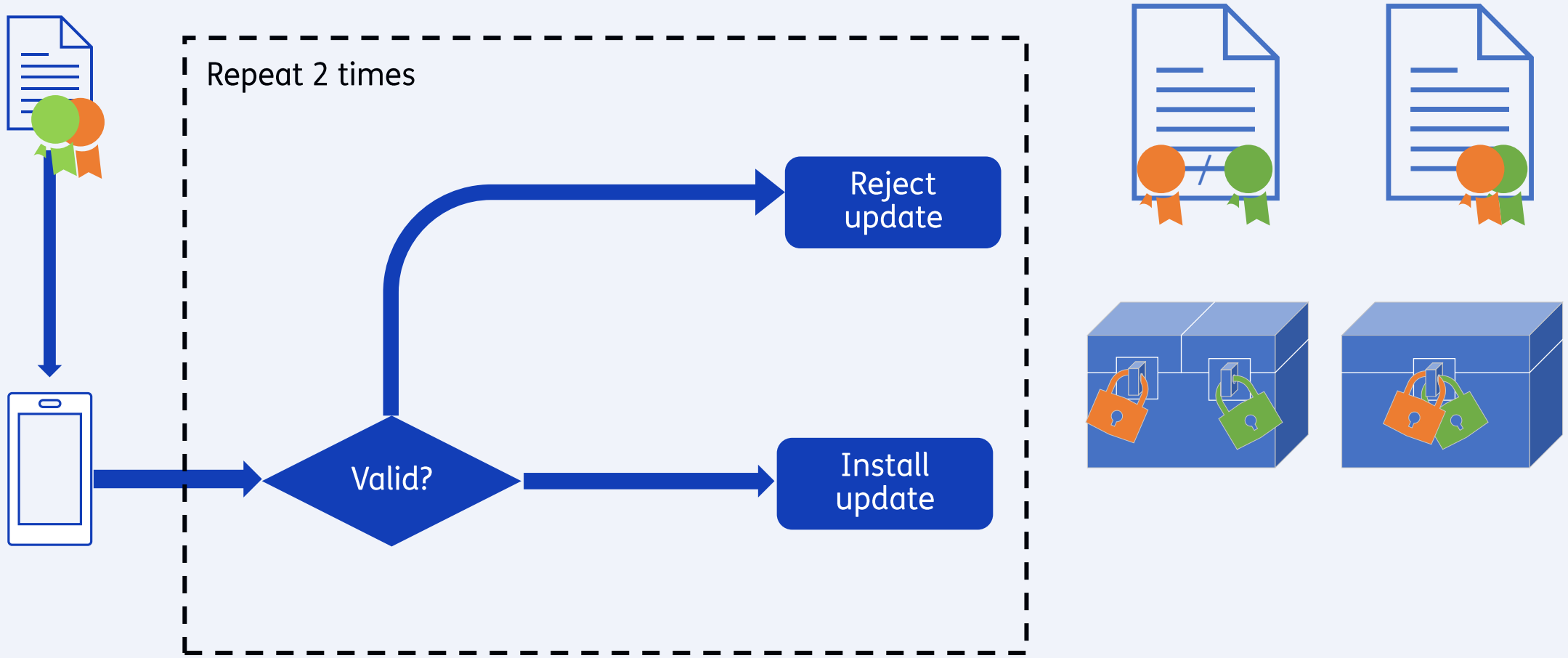
As a new hybrid algorithm

- Cryptographers choose combinations & correct combiner
- No additional complexity for develop/admin/engineer: “just a new algorithm”
- Less room for error
- Protocols only need to add a new algorithm, not change logic.
- ➢ Standardising a new algorithm will be less work than adjusting everything that used cryptography

Over-the-air update



Over-the-air update



Hybrid options for PKI certificates

- Both flavors have been proposed:

Composite

Naam houder: tno.nl
Algoritme publieke sleutel: **RSA_ML-DSA**
Publieke sleutel: **AD:0F:B0…,F3:3E:04…**

Geldigheid:
Geldigheid: 1-3-2026 tot 1-7-2026

Extensies:
….

Naam uitgever: CA123
Handtekeningalgoritme: **MLDSA-ECDSA**
Handtekening CA: **38:D8:95..,5B:F5:4E:…**

Catalyst

Naam houder: tno.nl
Algoritme publieke sleutel: RSA
Publieke sleutel: AD:0F:B0:04…

Geldigheid: 1-3-2026 tot 1-7-2026

Extensies:
- altPubSleutelAlg: **ML-DSA**
- altPubSleutel: **15:A0:B5…**
- altHandtekeningAlg: **ML-DSA**
- altHandtekening: **5B:F5:4E...**

Naam uitgever: CA123

Handtekeningalgoritme: ECDSA
Handtekening CA: 38:D8:95:F5...

Proposal delta/chameleon certificates

Chameleon certificate (delta)

Naam houder: tno.nl
Algoritme publieke sleutel: RSA
Publieke sleutel: AD:0F:B0:04…

Geldigheid: 1-3-2026 tot 1-7-2026

Extensies:
DCD: 11001010100

Naam uitgever: CA123

Handtekeningalgoritme: ECDSA
Handtekening CA: 38:D8:95:F5..

Genereert

Naam houder: tno.nl
Algoritme publieke sleutel: **ML-DSA**
Publieke sleutel: **15:A0:B5…**

Geldigheid:
Niet voor: 1-3-2026
Niet na: 1-7-2026

Extensies:
…

Naam uitgever: CA123

Handtekeningalgoritme: **ML-DSA**
Handtekening CA: **5B:F5:4E...**

Please do not mix optional and mandatory hybrids!

- Confusion
- Competition
- Delay

- Providing choice which of the algorithms to use can be dangerous
- ➢ Downgrade attacks

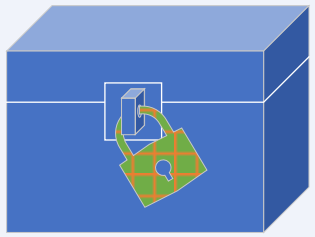
A short history on supporting multiple ciphers in TLS

- SSL 2.0 / 3.0 (1995–1999)
  - Introduced *cipher suite negotiation* to support multiple algorithms (export ciphers, RC4, DES).
  - → **Downgrade risk**: attackers could force weak/export ciphers.
  - → A**ttacks:** POODLE exploited SSL 3.0's weak CBC padding.
- TLS 1.0 / 1.1 (1999–2006)
  - Continued cipher agility (CBC, MAC-then-Encrypt) for backward compatibility.
  - → **Downgrade risk**: protocol version rollback to SSL 3.0.
  - → **Mitigation:** client/server version checks, but optional and inconsistent.
- TLS 1.2 (2008)
  - Added stronger suites (AEAD, SHA-256, ECDHE) while still allowing legacy ciphers.
  - → **Downgrade attacks:** BEAST, FREAK, Logjam exploited fallback and weak DH parameters.
  - → **Mitigation**: `TLS_FALLBACK_SCSV` to signal intentional downgrades.
- TLS 1.3 (2018)
  - Removed insecure cipher suites and renegotiation; only modern AEAD + PFS allowed.
  - → **Downgrade protection**: built-in via `supported_versions` and server-signed downgrade markers.
  - → **Result:** cipher agility preserved, downgrade attacks structurally prevented.

Key takeaway:
Cipher suite flexibility enabled cryptographic evolution, but without strict downgrade protection, lead to attacks.
TLS 1.3 keeps agility while cryptographically enforcing the secure cipher negotiation.

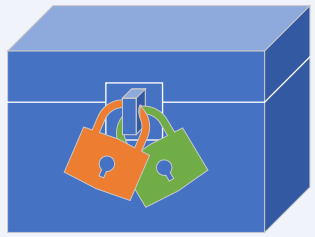
Hybrid as an algorithm

- Reduces risk of PQC vuln.
- Determines which choices are allowed
- Abstracts the hybrid away
- No extra complexity
- Less work to implement



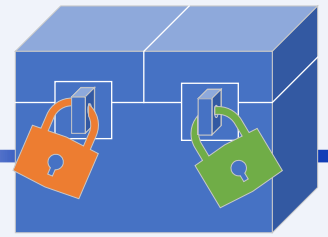
Hybrid in protocols /software

- Reduces risk of PQC vuln.
- Provides choice which algorithms to combine
- Creates more complexity
- Requires adjustment of logic in all crypto consuming protocols and software



“Optional” hybrid

- Does not reduce PQC risk
- Provides choice on algorithms to use
- Might help for backwards compatibility?
- Might introduces downgrade attack risk
- Is not the hybrid that the EU wants



Contact me

Mail to: stefan.vandenberg@tno.nl

Other resources

- PQC Handbook
  QSC migration manual for industry
- HAPKIDO
  QSC migration for public-key infrastructures
- DITM
  critical energy/automotive infrastructure
- PQChoiceAssistant
  advising which QSC scheme to use
- Confidential-6G
  QSC in context of (future) 6G networks
- SCARI
  Cryptographic inventory and quantum risk methodology