Quantum Apocalypse Update.ical

State of Post-Quantum cryptography transition in 2026

STORMSHIELD

Yvan Vanhullebus - R&D Technical Leader

vanhu@stormshield.eu

Pass The Salt


WANTED
DEAD & ALIVE
SCHRÖDINGER'S CAT

Quantum computers (not really) explained

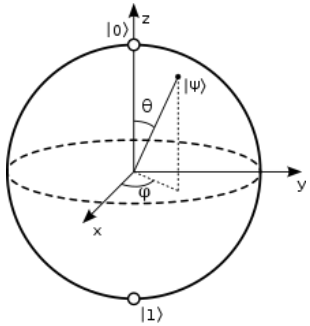
Don’t use intuition to try to understand them !

QuBit ???

Or Qu-bit, Qbit (/ˈkjuːbɪt/)

Different technologies: Superconducting, Trapped ion, Photonic, Silicon-based, Topological, Neutral atom, …

In very active research phase



Provides answers at amazing speeds !

Only for a very specific set of questions

Not 100% accurate

→ Check the answer, try again if needed

→ Runs thousands of times, take the most frequent answer

« Computes all possible values at the same time » ?

Not the way we would understand it.....

Quantum computers : metrics……..

Number of QuBits

« Mine has more than yours…….. »

« Raw » QuBits Vs « Stable » QuBits

(Vs « Stable but not the same way » QuBits

Vs Quantum Annealing Vs ……..)

Engineer’s stuff.....

Rare elements

Construction cost

.....

Coherence time

From far less than 1 second to at most some minuts today

Errors

Error rate

Errors correction

Errors tolerance

Everything in the same technology !

Each technology has strengths and weaknesses

Quantum Computers Vs Cryptography

The good news

Hashes algorithms: no known efficient attack

Some research on the subject

May change in the future ?

Move to 384 / 512 bits hashes for sensitive use cases ?

The (more or less) good news

Symmetric cryptography: Grover's algorithm

Research reduced to square root (ie « security bits / 2 »)

AES128 would become too weak with « 64 bits » of security

AES256 would still have 128 bits of security (same for ChaCha20)

Symmetric encryption key sizes increases over time

(I used to configure stuff with Blowfish40 / DES a long time ago.....)

Impact is quite moderate

There will be some kind of « AES512 » in the future(*)

Can Grover's algorithm really be implemented for AES / ChaCha20 ?

(*): AES « 256/256 » already in NIST process

The bad news

Asymmetric cryptography: Shor’s algorithm

Gets private key from public key very quickly !

- RSA
- Elliptic Curve Cryptography (ECC)
- Diffie-Hellman key exchanges

« Very quickly »: days, hours, minutes !

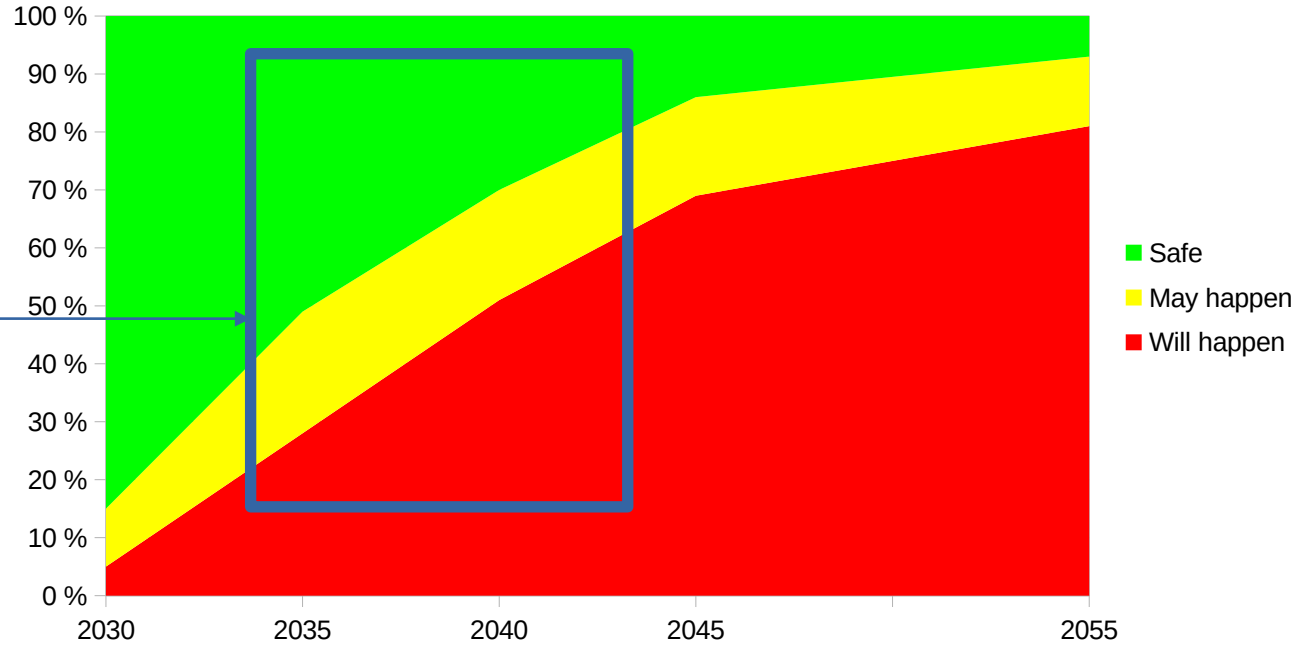
No, it does not « try all values simultaneously »: does a (fast) Quantum Fourier transform

When will they be broken ?

One day……..

Almost sure !

Risk increased since previous estimations



Expert’s estimates of likelihood of a quantum computer able to break RSA-2048 in 24 hours

Source: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

Consequences ?

Authentication: identity spoofing !

Certificates have limited lifetime (more or less 1 year?)

Signatures: sign bad data

Administrative documents

Software / firmware upgrades

Sensitive data

PKIs renewal to anticipate !

Worst case ?

Block user authentication ?

No more value for data signature ?

What about Web Of Trust ?

Consequences ?

Encryption: read unauthorized / sensitive data !

« Store now, decrypt later » attack:

Phase 1: collect encrypted data **now**, and store it……

Phase 2: wait for a way to be able to decrypt the data (can be a quantum computer or something else…….)

Phase 3: later, decrypt the data !

How much « later » is the data still expected to be unreadable ?

Phase 1 already started !

Mosca's Theorem

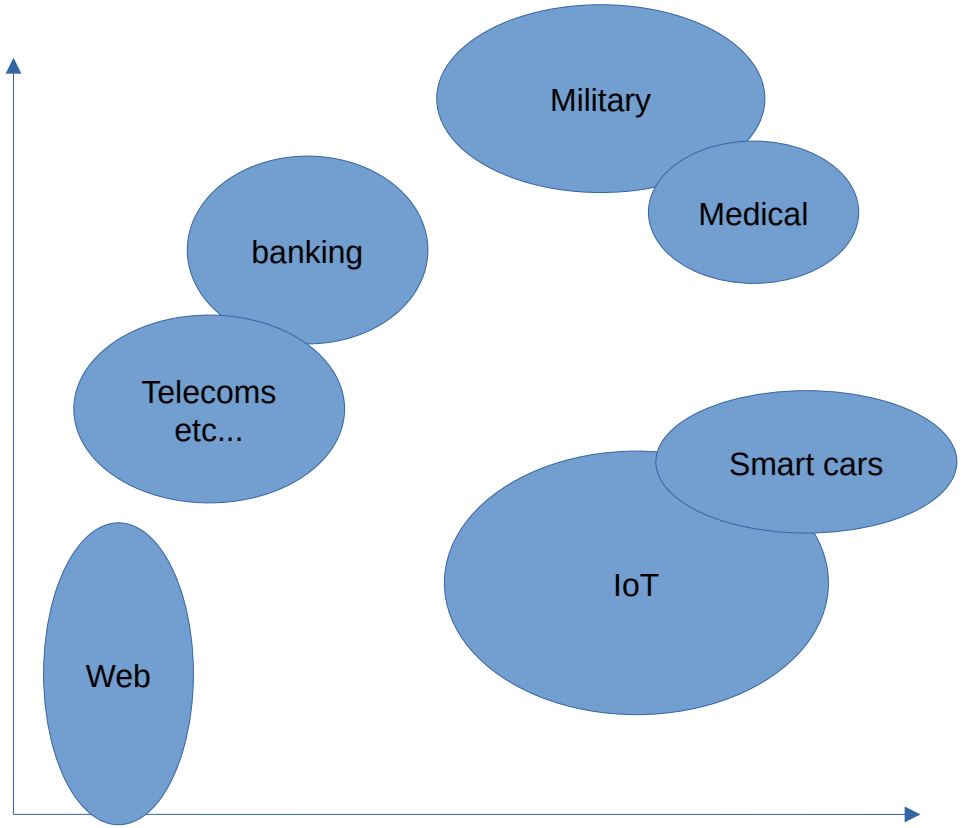
Y : Standardize + implement + deploy	X : Data expected to stay safe

Z :
Time before « Q day »

If X + Y > Z, then we have a major issue !

Various risk levels.....

Potential X
(expected data
confidentiality duration)



Post-Quantum Cryptography

How to avoid the quantum apocalypse ?

Various strategies.....

Good old Preshared keys !

Not vulnerable to quantum computers

Requires strong preshared keys

Applies only on specific use cases

Quantum Key Distribution

Out of scope today

Very specific constraints, very specific use cases

~~Increasing keys size~~

New algorithms

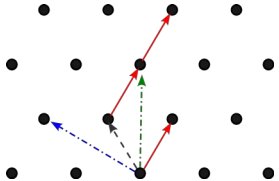
Other mathematical problems (Lattice-based, Code-based, Multivariate, Hash/Symmetric key based, Elliptic curve isogeny)

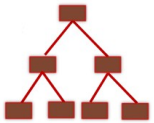
No known quantum attack (« post-quantum »)

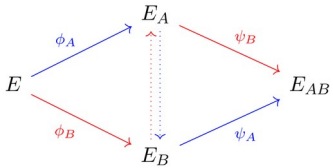
No known classical attack !

Runs on classic computer

$$G=[I\|P]=\begin{pmatrix}1&0&0&0&p1&p2&p3\\0&1&0&0&p4&p5&p6\\0&0&1&0&p7&p8&p9\\0&0&0&1&p10&p11&p12\end{pmatrix}$$







Post-quantum algorithms : standardization

Encrypt

NIST:

ML-KEM / FIPS-203 (formerly « CRISTALS-Kyber ») - Lattice

HQC (FIPS-xxx expected in 2027) - Code

FrodoKEM (ISO/IEC 18033-2:2006/Amd 2:2026) – Lattice

Classic McEliece

NTRU

BIKE

Sign / Authenticate

NIST:

ML-DSA / FIPS-204 (formerly « CRISTALS-Dilithium ») - Lattice

SLH-DSA / FIPS-205 (formerly « SPHINCS+ ») - Hashes

Falcon (still no FIPS-xxx) - Lattice

Mayo

MQOM

SNOVA

Ryde

LESS

Hawk

Cross

FAEST

SQIsign

(non exhaustive list)

Problems of the solutions……

How to use them

No DH like mechanism

Encrypt OR sign with a key pair / algorithm

Size

Private key

Public key

Encrypted / signed data

Mostly an issue for network protocols

Security level

Some mathematical problems are less studied than other

Some algorithms are more complex to implement properly

Secure implementations ? (timing attacks, side channel, ……)

Implementation requirements

CPU / Performance

Memory

(FPU)

No « Silver bullet »

Each post-quantum algorithm is at least

Quite bad in at least two aspects

or

Very bad in at least one aspect

To hybridize or not to hybridize ?

US / NSA: replace legacy with PQSafe

As soon as possible

Expected to be completed by 2035

Europe: hybridize

Most PQSafe algorithms are not still mature enough

Some may have vulnerabilities (and it happened to some candidates!)

No PQSafe alone for now (except for SLH-DSA and similar hash-based)

Hybrid approach : (RSA|ECC) + PQSafe

PQSafe only later (2030 ?)

Solutions for the problems of the solutions…….

Encryption

New algorithms

- How to use them in protocols (RFCs, ……)
- IANA numbers, …….
- Offline mode : how to ensure peers does know it ?

Bigger key / data size

- Not an issue for file / drive / etc… encryption
- Can be a big issue for network protocols : new RFCs…
- Latency impact expected at the beginning of negociations

No « DH Mode »

- Key Encapsulation Mechanism (KEM)
- Extend protocols to use KEM (RFCs, ….)

Hybrid mode

- Extend protocols (RFCs, ……)
- Latency impact expected at the beginning of negociations

Solutions for the problems of the solutions…….

Authentication / signature

New algorithms

- How to use them in protocols (RFCs, ……)
- IANA numbers, …….
- Offline mode : how to ensure peers does know it ?

Bigger key / data size

- Not an issue for file / drive / etc… protection
- Can be an issue for network protocols : new RFCs…
- Latency impact expected at the beginning of negociations

Hybrid mode

- Extend protocols (RFCs, ……)
- Latency impact expected at the beginning of negociations

Note : more data to carry than for encryption, but a little bit later in network negociations

Post-Quantum Cryptography

What to do NOW ?

Start to work on the subject…….

« Cryptocrastination »

« I don’t have strong secrets »

« It will happen late enough »

« Automagic migration » (variant : « IA will handle that »)

« I have other subjects to handle »

……

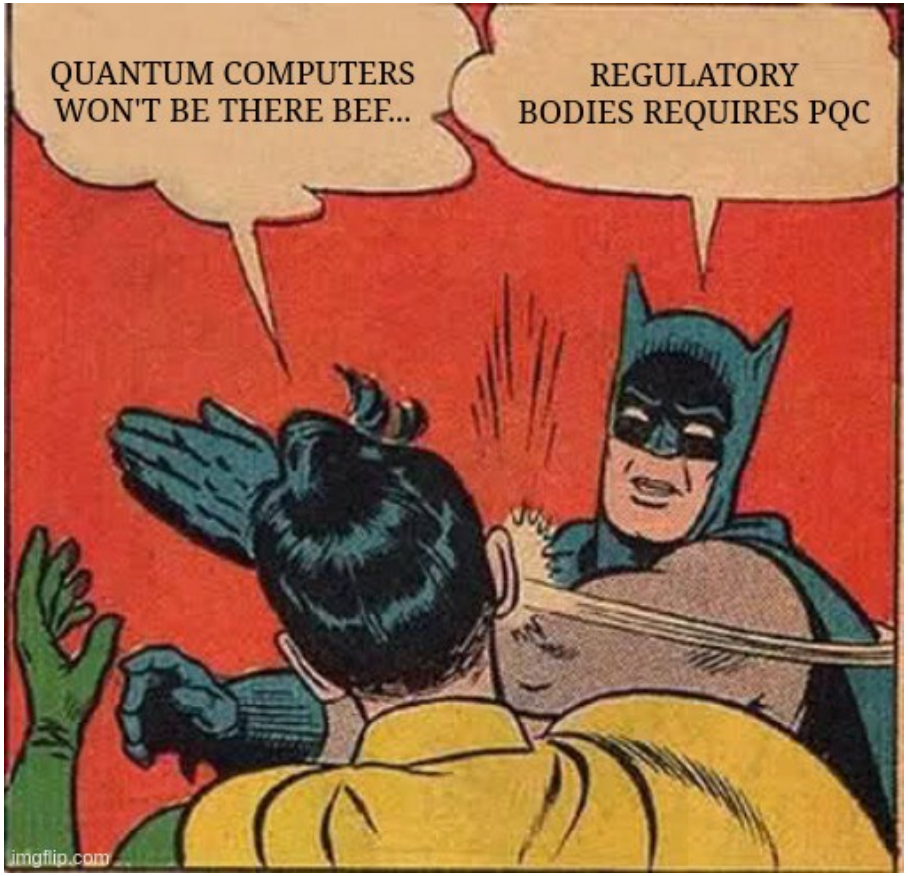
Start to work on the subject !!!

New « State Of The Art »

Will be mandatory for interoperability

Will be mandatory for compliance

- ANSSI, BSI, ENISA, …….
- NSA, FIPS, …….
- DORA, CRA, NIS2, ……..
- Common Criteria, NATO, ……
- ECCG
- (list far from being exhaustive)



Already done ?

Crypto inventory

Inventories ?

Use a dedicated tool ?

Also known as CBOM (Cryptographic Bill Of Materials)

Prioritize !

Do not wait a 100 % filled and prioritized inventory !

Crypto agility

Avoid / remove hardcoded secrets !

Crypto agility

Avoid / remove hardcoded algorithms !

Crypto agility

Automated / easy rotation of secrets

Crypto agility

Be ready to upgrade easilly and often your crypto stack(s)

Crypto agility

Handle transition period (negociation, backward compatibility, ...)

Crypto agility

One expression to cover so much various pains !

(list far from being exhaustive.....)

Prioritization quick HowTo

Encryption first

Store **NOW**, Decrypt Later

Sensitive data first

What will happen if someone can read that data in 5, 10 or 20 years ?

Heavy projects ?

Technical debt ?

Hardcoded crypto ?

…….

→ Plan and start a migration

Network first

More subject to « Store now » (especially if it goes through internet)

« Easier » :

- algorithm negociation in most protocols
- Ephemeral encryption keys in most protocols
- Protocols updates are more mature

Exceptions ?

Expected to be shut down / replaced soon ? (*)

Quick win opportunity ? (« fire and forget »)

Visibility / brand management / ….. ?

(*) : remember that it will take more time than expected to really shut it down…….

Network encryption : various layers…….

Not your perimeter ?

5G / 6G

Wifi ?

Some messaging services

Various proprietary stuff

……

→ Monitor the subject

→ Ensure crypto agility ?

→ Check the future of the solution

- Provider
- Dev community
- ……..

Mostly your perimeter

TLS (what you call « SSL »)

- Web / HTTPS
- Lot of other protocols

SSH

IPSec

Some other messaging services ?

……..

Network encryption : Global migration strategy

1: Prepare stuff…..

Get docs / infos

PoCs

…….

2: Upgrade stuff

Software / firmware / hardware

Still « Legacy » for now

Should be asynchronous

3: Add PQC algorithms

Should be asynchronous

In Hybrid mode for now (EU)

Legacy proposals still allowed

Check that everything still works……..

Network encryption : Global migration strategy

Adding algorithms ?

From…….	To…….	But not !
Legacy1	Legacy1+PQC	Legacy1
Legacy2	Legacy2+PQC	Legacy2
Legacy3	Legacy3+PQC	Legacy3
	Legacy1	Legacy1+PQC
	Legacy2	Legacy2+PQC
	Legacy3	Legacy3+PQC

(first match selection may choose Legacy1!)

Network encryption : Global migration strategy

4: PQC validation

Wait for all peers to be at step 3

Check that PQC encryption is used all the time

5: Remove legacy algorithms

Double check step 4 before !

Triple check step 4 before !

Can also be asynchronous : removing legacy algorithms on on side is enough

Wait for customer's call ……..

IPSec : the highest priority ?

Why IPSec first ?

Used to transport various other network protocols

Goes most of the time through Internet

Higher sensitive informations are transported via IPSec…..

Protocol extensions are ready (IKEv2)

Implementations are ready (at least Stongswan v6…..)

You HAVE TO do it mostly by yourself

(list more or less accurate also for other VPNs)

Migration strategy

See previous slide !

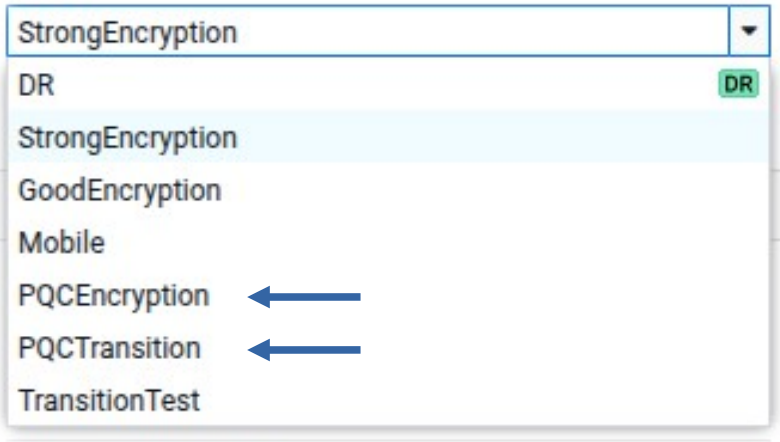
No « Big Bang »: migration can be done tunnel by tunnel

IKEv2 required !

Does someone still use IKEv1 ??????

IPSec : hints

Easy UI way ?



Manual configuration

Enable IKE Frag (RFC 7383)

Enable & Use Multiple Key Exchanges (RFC 9370)

Add a PQSafe KEM for both IKESA and ChildSAs

Order matters !

- RSA + ML-KEM ≠ ML-KEM + RSA !
- Use legacy (and smaller) algorithm first (before IKE Frag is available)
- Use that legacy algorithm first even if you don't need hybrid !

TLS : the easy migration ?

Just upgrade !

Draft-ietf-tls-ecdhe-mlkem (X25519MLKEM768)

Already in your browser

Already in your crypto stacks (*ssl, ...)

Already in lots of cloud servers

Enabled by default

You already use it !

Just so easy ?

Browsers: you should really be up to date !

Servers/others clients:

- are you really up to date ?
- Do you use default crypto configuration ?

Compatibility issues ?

TLS ClientHello can request more than 1 packet

Perfectly allowed by RFCs.....

Some implementations assumed ClientHello in 1 packet.....

May also happen on intermediate stuff (proxies, ...)

More details: https://tldr.fail

Mostly behind us ?

TLS : How to ensure PQC when needed ?

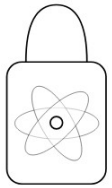
On client side

Browsers :

- no fine tunned configuration
- No exploitable logs
- Quantum lock icon ?

Others :

- Can enforce X25519MLKEM768
- Can produce logs



On server side

Can enforce X25519MLKEM768

How to ensure it won't break legitimate clients ?

Can produce logs

On the network ?

IDS, IPS, Proxy, ...

Quite easy to track / enforce PQC Key Exchange

Realistic ?

Can be done for your simple web server

Can be done for some other TLS things

What about most web sites with huge dependancies ?

SSH : somewhere between IPSec and TLS

Just upgrade !

OpenSSHv9 : sntrup761x25519-sha512

OpenSSHv10 : mlkem768x25519-sha256 (default)

Other SSH implementations ?

Windows 11 embedded OpenSSH without PQC ?

PQC can be enforced (client side / server side)

OpenSSHv10.1+

```
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
```

But.....

Server: do you use crypto default configuration ?

Client: who uses ~/.ssh/config for crypto config ?

Are you really up to date ?

How to ensure PQC is used when needed ?

Next steps !

Data encryption !

Files, mails, ……

Authentication / Signature !

Most encrypted stuff also needs authentication or signature……

Some other stuff also needs authentication or signature……

PQC PKI ?

Most of those use cases requires PKI or similar stuff

Hybrid support ?

Hardware support ? (HSMs, smartcards, TPMs, …..)

x.509 and hybrid ?????

X.509v3:

ONE algorithm

ONE public key

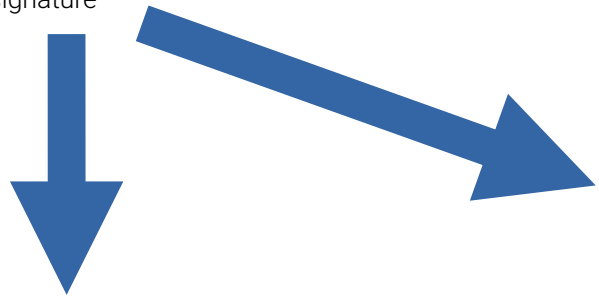
ONE signature

Multiple PKIs

Have a « legacy » PKI and a PQSafe PKI.....

Easy to set up

Hard to use: most protocols expect ONE certificate / identity



« Alt » / Catalyst / Chimera

x.509 is extensible !

AltAlgorithm, **Alt**Key, **Alt**Signature

Smooth transition if not set as « critical » (will be ignored)

But then, no way to ensure PQSafe !

Composite

New algorithms: RSA+ML-DSA, ECC+ML-DSA, ...

No changes to protocols

Peer MUST know those new « algorithms »

Rough transition, but PQSafe guaranteed

Other proposals

« Chameleon » certificates

Mixed PKI

Bridged PKIs

In some later future.....

Pure PQC transition

Legacy algorithms will be deprecated / removed in some future

New transition again !

New PQC Algorithms

Will ML-KEM / ML-DSA stay strong enough in the future ?

Will some use cases require other algorithms ?

Will pop from time to time……

TPMs

HSMs

Secure boot

Exotic protocols

Smartcards

(non exhaustive list)

(and this only covers direct IT subjects……..)

May happen at any time !

(CRQC : Crypto Relevant Quantum Computer)

Conclusion

This is a marathon !

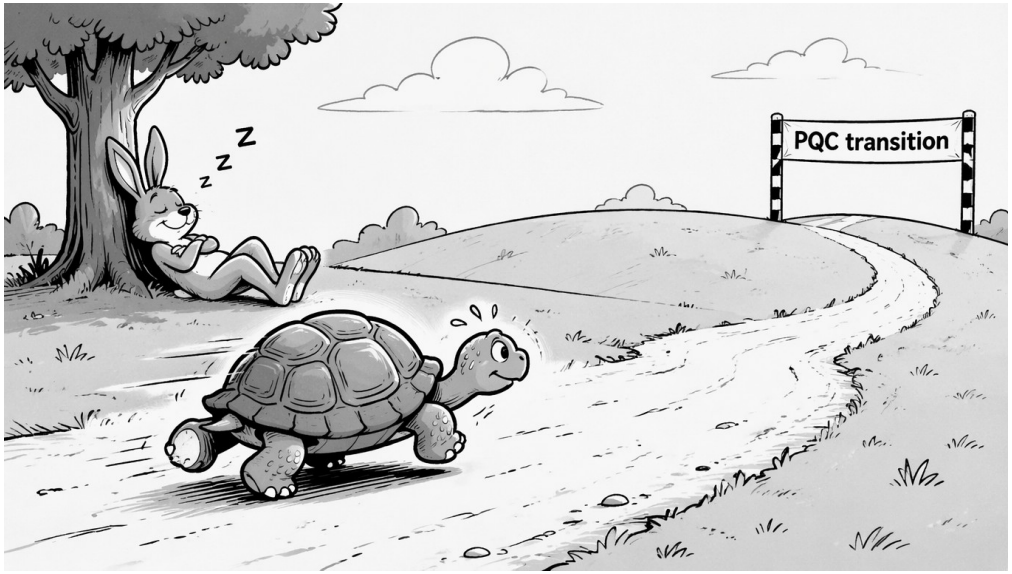
(at least…….)

It has already started !

Start you crypto inventory last year !

2026 focus: network encryption ?

Keep updated: agenda may change ?



(AI generated via creen.ai)

Questions ?

STORMSHIELD

(No cats were harmed during this presentation)

(Thanks to Victor and to imgflip.com)