



September 14, 2023

# Security TF PQC Migration

Olivier Van Nieuwenhuyze

Incorporating Flexibility and Agility into Automotive Solutions: Post Quantum Crypto Migration

# Agenda

Introduction

Solutions

GlobalPlatform

# GlobalPlatform Policies

Please be aware that this meeting is being held in accordance with **GlobalPlatform's Bylaws and GlobalPlatform policies issued thereunder**, including but not limited to:

- **Antitrust Policy**
- **IPR Policy**
- **Member Confidentiality Requirements**
- **Meeting Protocol and Guidelines**

## Patent Call

*“Please be aware that this meeting is being held under the GlobalPlatform Intellectual Property Rights Policy. If you do not have a copy of this policy, please contact (or inform) the chairperson during this meeting. You may also view and download a copy of the policy at the Membership section of the GlobalPlatform Website.*”

*At this time, each person in attendance is required to inform the chairperson if they are personally aware of any claims under any patent applications or issued patents which would be likely to be infringed by an implementation of any specification or other work product which is the subject of this meeting. You need not be the inventor of such patent or patent application in order to inform GlobalPlatform of its existence, nor will you be held responsible for expressing a good faith belief which proves to be inaccurate.”*



# Introduction

Quantum Computing Threat

# The Quantum Computer



# QUBIT

**BIT**

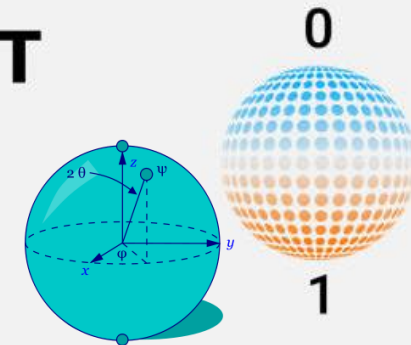
Classical Computing

0 

1 

**QUBIT**

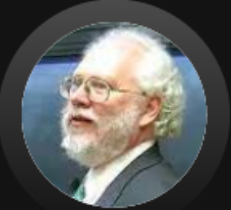
Quantum Computing




# How Quantum Computer Impacts Cryptography?

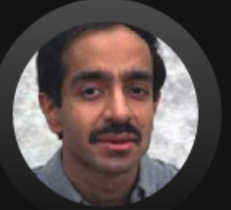
CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	<b>No longer secure</b>
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			
CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	e.g. longer keys needed
SHA-2, SHA-3	-----	Hash functions	e.g. larger output needed

Peter SHOR





Lov GROVER

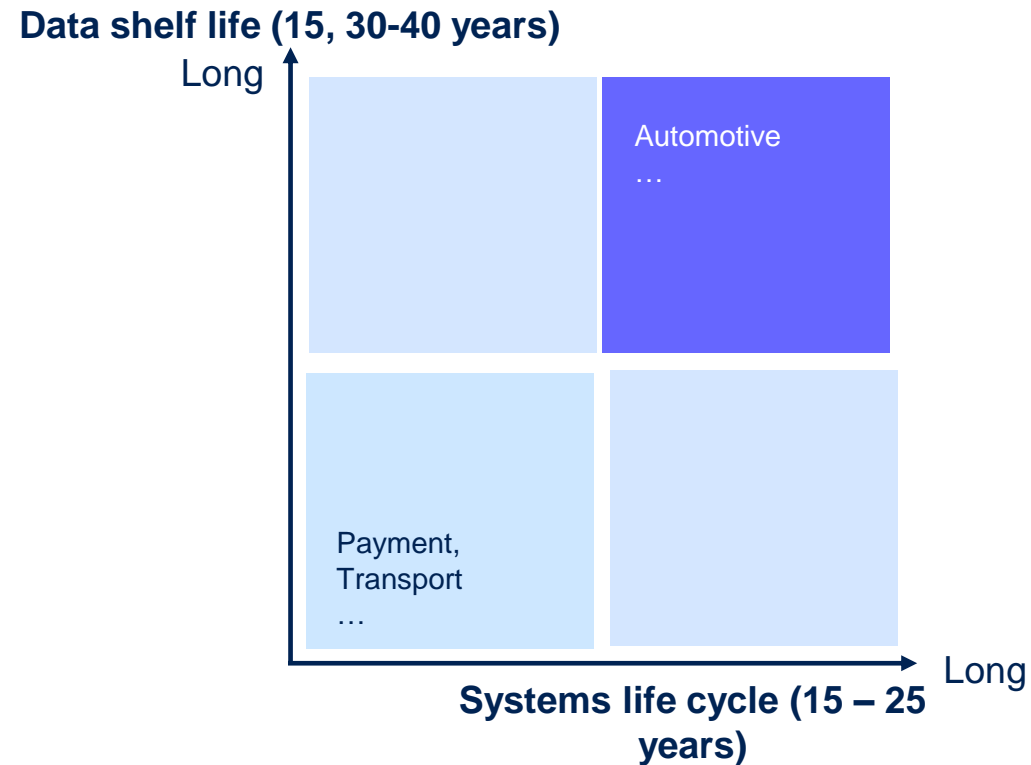


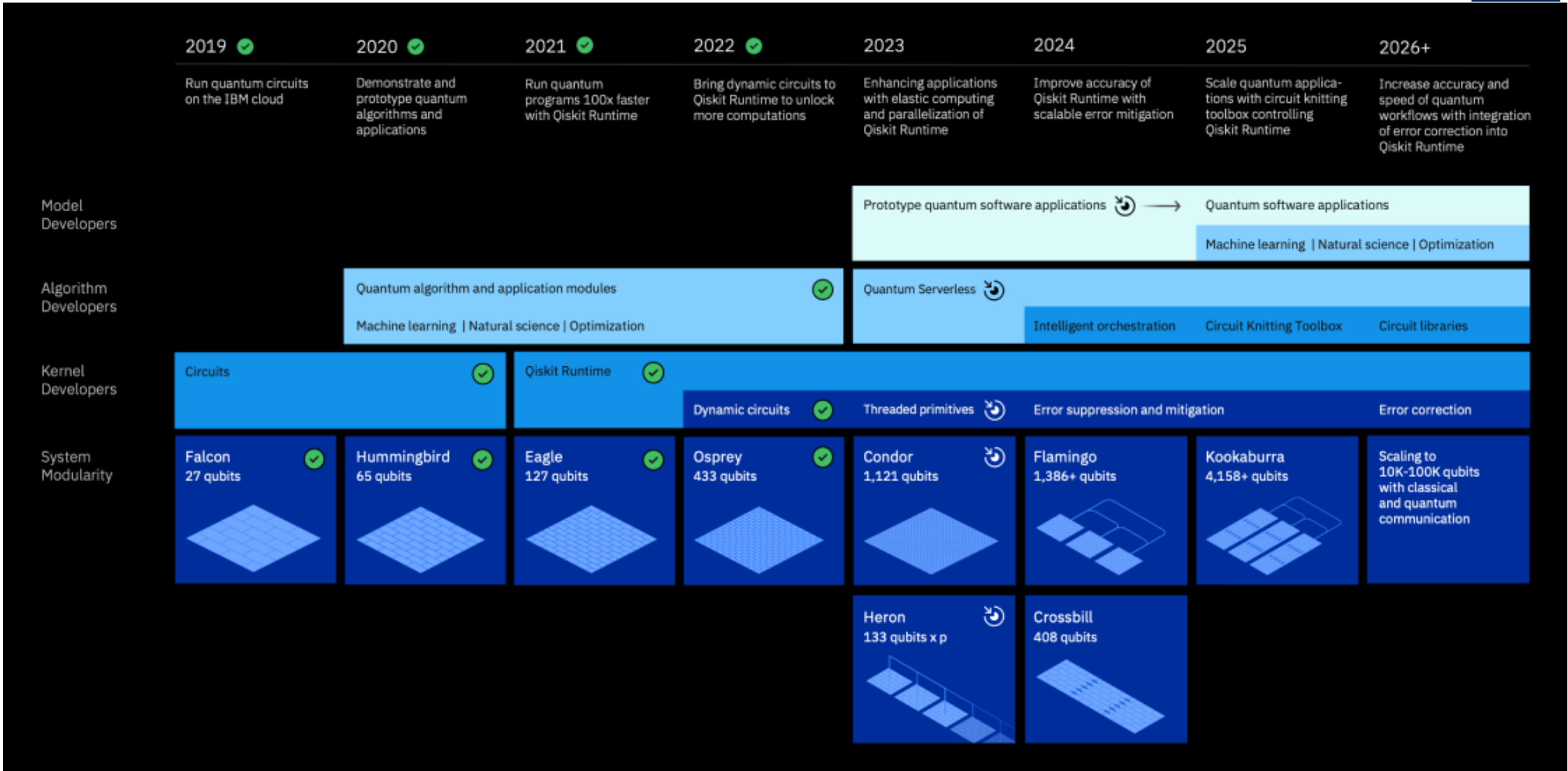
# Is this really a problem ?

Significant effort to find solution

Time & difficulty to migrate/deploy the solution

Challenge start today as “*Store now, Decrypt later*” attack



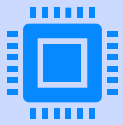




## How long to break RSA 2048 bits ?



Classic computer : 300 trillions years



A “perfect” Quantum computer with 4099 bits will take 10 seconds

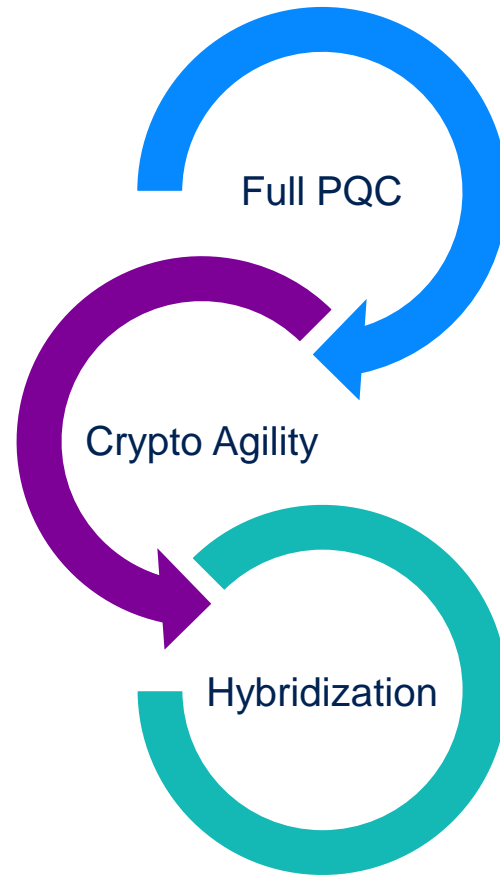


A Quantum computer with 20 million “noisy” qubits will take 8 hours.



# Solutions

# Solutions



# Organizations Standardizing PQC algorithms

## Mainly

- NIST (See next slides)
- ISO SC27
- (ETSI CYBER QSC)

China organized a separated competition and already select several post-quantum algorithms.

- LAC and Aigis-Sig won the first prize in 2020.
- <https://www.cacrnet.org.cn/site/content/854.html>

Russia seems to have its own selection process too.

- No information.

# NIST PQC Status

## Final selection for standard (July 2022)

- **Crystals-Dilithium** for signature is the recommendation (strong security and excellent performance)
- **Falcon** (to be used when Dilithium signatures are too large) and **Sphincs+** (hash-based)
- **Crystals-Kyber** for KEM (strong security and excellent performance)
- Draft standards available (summer 2023), first PQC standards should be published in 2024 (FIPS & SP)

## 4th Round candidates for KEM, already including

- **BIKE** (most competitive performance) and **HQC** (strong security assurance, larger key size than BIKE), both based on structured codes, one of which could be standardized
- **Classic McEliece** (secure but too large public key size),
- and **SIKE** (small key and ciphertext sizes). INSECURE

# NIST PQC Status Cont.

## Additional signature post-quantum signature scheme

- Purpose
  - Not based on structured lattices (to diversify the portfolio)
  - For certain applications, need of short signatures and fast verification
- Status
  - 50 submissions
  - 40 submissions considered as complete and proper
  - Process might take several years

# What Is Crypto Agility?

Introduced by

- ETSI in its 2014 white paper on quantum-safe cryptography and security
- as well as The National Institute of Standards and Technology (NIST) in its 2016 report on post-quantum cryptography.

Crypto agility allows for a system or application to migrate to alternate cryptographic algorithms without causing a significant disruption to the infrastructure, allowing security updates to be quickly deployed to fix broken algorithms or replace vulnerable ones.

**In short, crypto agility offers the flexibility to meet the changing security needs of our connected world.**

The Holy Grail!

# Hybrid Cryptography

Hybrid cryptography, sometimes called composite cryptography,

- is a combination using one algorithm from the pre-quantum era, e.g.: RSA, and another algorithm from the post-quantum era, e.g.: one of the signature PQC algorithm from NIST PQC project.
- Thanks to this combination, the security is guaranteed by the security of each algorithm in its proper attack model.

The maturity level of the post-quantum algorithms should not be overestimated.

- This level is comparable to the maturity level of RSA in the mid 90's

**PQC will not become mature with the publication of NIST standards**

Hybridization should facilitate the migration and keep backwards compatibility

Different approaches have been proposed and different view from National Agencies

- Hybrid solutions are requested by ANSSI (France) and BSI (Germany)
- Hybrid is encouraged by ENISA (EU) and ETSI (EU)
- Hybrid is discouraged by NSA (US), NCSC (UK) and CSE (Canada)





# GlobalPlatform

# Crypto Algorithms Recommendation – June 2021

**Deprecated  
80 bits (or less)**

**DES  
3DES with 2 keys  
SHA-1  
RSA-1024  
ECDSA-160  
TLS 1.0 and TLS 1.1**

**Legacy use  
112 bits  
until 2023**

**3DES with 3 keys  
SHA-224  
RSA-2048  
ECDSA-224**

**Recommended  
128 bits**

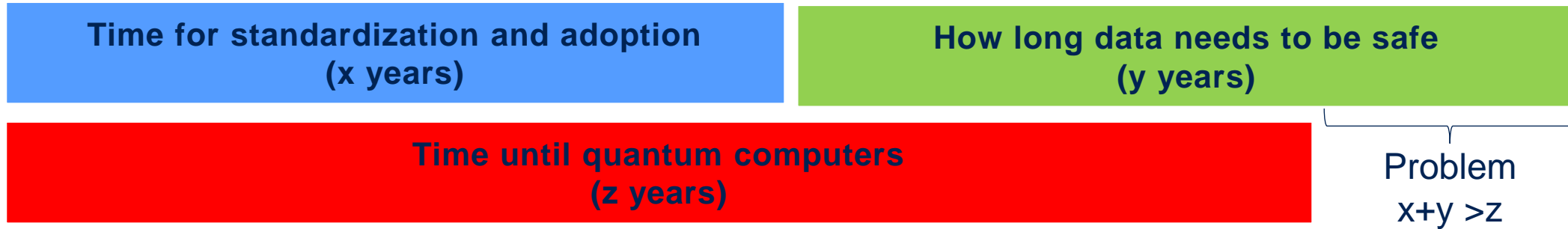
**AES-128  
SHA-256  
RSA-3072  
EdDSA  
ECDSA-256  
TLS 1.2 and TLS 1.3**

**Under scrutinization**

**Reco for PQC  
128 /256 bits?  
(unknown date)**

**AES-128 /256?  
SHA-256 /384?  
??  
??**

# Migration strategy – When ?



Can we extrapolate x, y and z?

- x roughly 2030
- y depends on the use case (telecom < bank < government ~ automotive < defense...) health?
- z? 2040 – 2050 ?



# Secure Components

## Secure Element

**Only lattice-based algorithms  
are practical on current SE!**

**Good news, this is what is being  
standardized by NIST:**

**Dilithium and Kyber**

## Trusted Execution Environment

**GP TEE is enabling  
all the NIST final candidates  
in TEE Internal Core 1.4 specification.**

**Memory size is typically not an issue in a TEE,  
but PQC will be slower than  
their classic cryptographic equivalents ....**

# A strategy for GP, discussion on-going

Hybrid cryptography, sometimes called composite cryptography,

Symmetric Cryptography

- SCP03 : OK, but envisage to double the Key Size

Asymmetric Cryptography needs to evolve

- SCP11 : NOK
- In principle, follow the NIST recommendation
- but also, other algorithms if needed (e.g.: country regulation)

The maturity level of the post-quantum algorithms should not be overestimated.

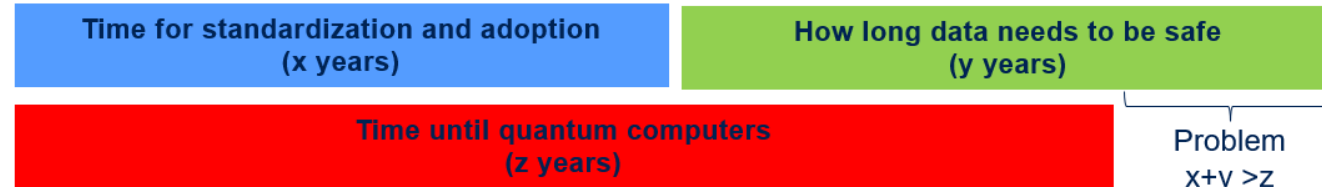
Having Crypto Agility and OS Update

- **SCP 04 is OK**
- Be able to download new keys/algorithms with sufficient protection (e.g. to load AES-128 keys Need of 256 bits).

# A strategy for GP, discussion on-going Cont.

What is our y?

- Think about lifetime of product, but also development time and certification duration



Support Hybrid Algorithm

- Full PQC
- Or Hybrid PQC (required by some countries)
- Whatever the case and our choice, the device must embed all solutions (classic and PQC), to be able to communicate with the other elements of the ecosystem until all are migrated. This will also ease use of hybridization.



# Global Platform™

The standard for  
secure digital services  
and devices

→ [globalplatform.org](https://globalplatform.org)