HAPKIDO

João Diogo Duarte

Introduction

- **H**ybrid **A**pproach for quantum-safe **P**ublic-Key **I**nfrastructure **D**evelopment for **O**rganisations (HAPKIDO)
- Dutch initiative, funded by NWO (overarching Dutch Research Organisation)
- Five-year project, seven involved parties (more on that later)
- Discussion on what exactly *hybrid* is to follow

HAPKIDO is a project that aims to investigate the complex task of migrating our 'classical' PKIs to **hybrid** quantum-safe PKIs.

Involved Parties

Coordination & PoC Development

Cryptographic Research

Governance

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Digital Government

PKI Management & Test Lab

Provider of Digital Identification & Signing Services

Moving to higher TRL (technology readiness level)

Introduction to the problem

Asymmetric Cryptography
Encryption and Decryption

pk: public key, belongs to Alice and is known to the public

sk secret key, belongs to Alice and only known to Alice

Idea: Encrypt your message m to Alice with their pk. Alice can decrypt your message with sk.

Decrypting with pk is not feasible.

TNO

Asymmetric Cryptography
Signing and Verifying

pk: public key, belongs to Alice and is known to the public

sk secret key, belongs to Alice and only known to Alice

Idea: Alice can sign a message with their sk and anyone can check its authenticity with Alice's pk.

Signing with pk is not feasible.

What are PKIs?

Public-Key Infrastructures (PKIs) are large, complex and interdomain systems that manage certificates (creation, distribute, revocation, usage...).

A **certificate** proves that a single public-key belongs to a specific entity.

Example of a certificate in next slide.

www.google.com | GTS CA 1C3 | GTS Root R1 | GlobalSign Root CA

Subject Name

Common Name	www.google.com

Issuer Name

Country	US
Organization	Google Trust Services LLC
Common Name	GTS CA 1C3

Validity

Not Before	Mon, 03 Apr 2023 08:25:07 GMT
Not After	Mon, 26 Jun 2023 08:25:06 GMT

Subject Alt Names

DNS Name	www.google.com

Public Key Info

Algorithm	Elliptic Curve
Key Size	256
Public Value	04:5A:CA:1B:EB:F2:A2:BA:24:73:8C:64:F3:90:92:E9:38:F3:37:11:29:17:58:59:0D:...

Where do quantum computers fit in?

Large-scale quantum computer will break currently-used asymmetric cryptography.

This will, naturally, affect PKIs:

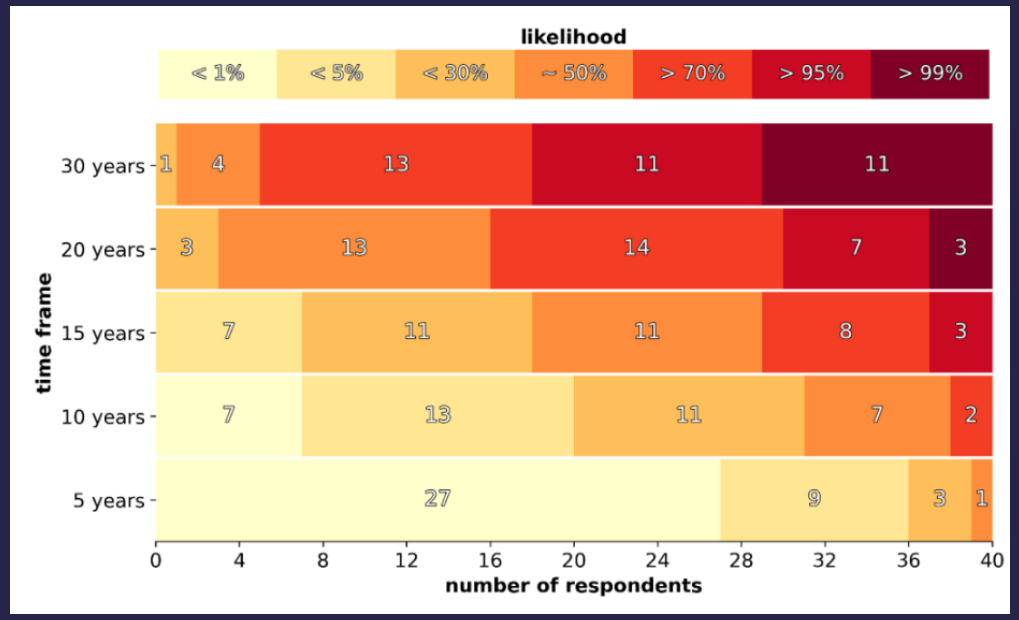
- Systems that rely on PKIs to manage their keys
- PKI functionalities (such as certificates)

Hence, we need to transition the cryptography involved in PKIs to quantum-safe cryptography!

When will quantum computers break crypto?

We don't know.

We can, however, look at experts' opinions from the 2022 Quantum Threat Timeline Report by evolutionQ for insight:



Hence, the average estimate from this graph is in **10-15 years**.

That sounds scary...

Yes...

On a positive note, we do have quantum-safe (specifically: post-quantum) candidates (NIST) and as we've seen action from major countries.

However, need to evaluate impact of migration: post-quantum schemes might have worse performance.

World on the move
NIST PQC Standardisation Competition

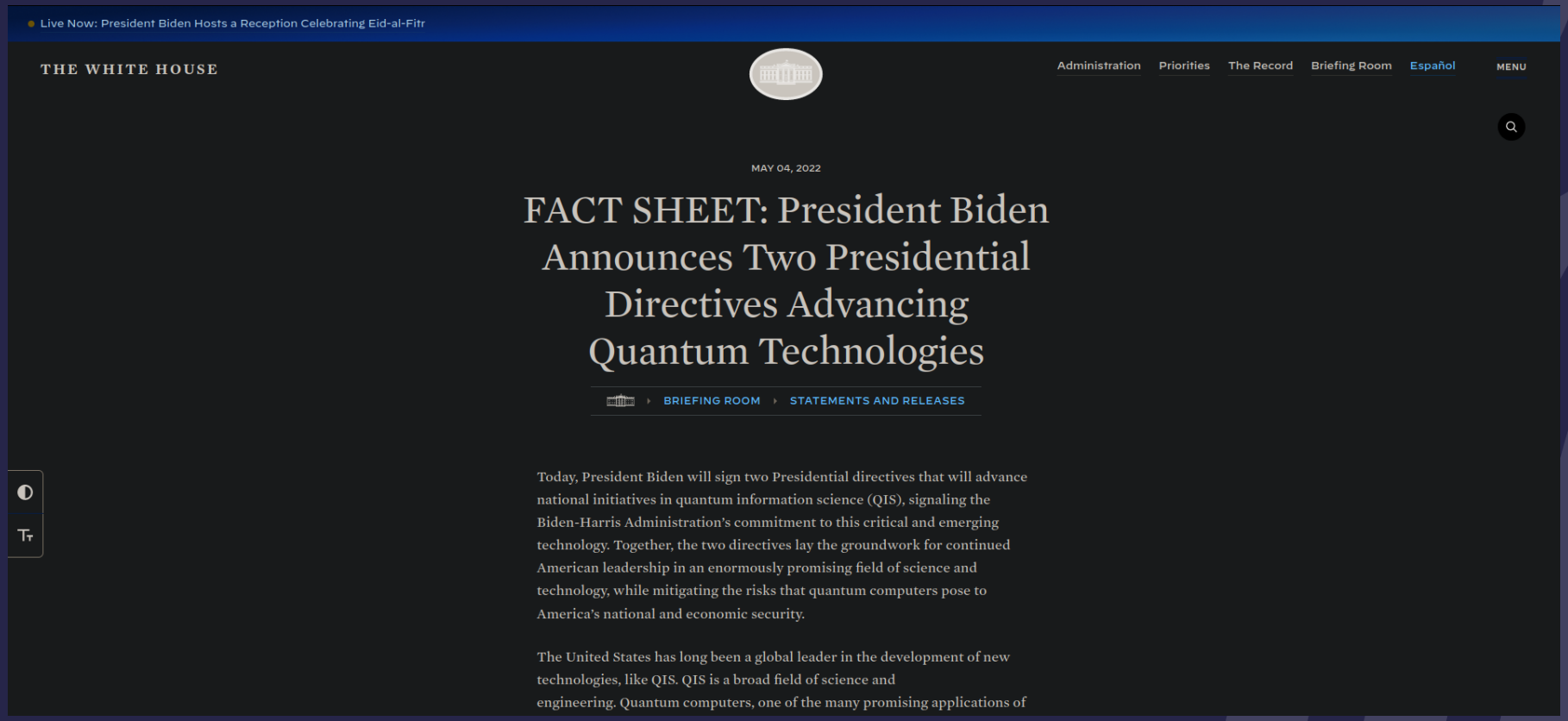
Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS$^+$

The following candidate KEM algorithms will advance to the fourth round:

Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
SIKE

World on the move
President Biden's Directives



Migration strategies
Big bang

Switching from classical to post-quantum in one go ("big-bang approach") not feasible

- Too many parties and systems involved: interoperability
- Insufficient trust in post-quantum building blocks (cf. Rainbow)

Migration strategies
Hybrid

Therefore: aim for systems that use both classical and post-quantum cryptography (**hybrid**)

- When interfacing with "legacy" party/system: ignore post-quantum part
- When possible, use both. System secure as long as one component secure

How would this look for PKIs?
Classical PKIs

How would this look for PKIs?
Hybrid PKIs

Seems simple? **Not at all!**

Challenges of the hybrid approach

This is **not trivial**:

- Details are complex, and security proofs are sometimes lacking
- Attack surface increases
- Need to "manage" both classical and post-quantum parties/systems
- No universally accepted and formal definition of this

Hybrid-OR vs Hybrid-AND?

Hybrid-OR: You can choose to use either classical quantum-unsafe cryptography or post-quantum cryptography

Hybrid-AND: You must use both classical quantum-unsafe cryptography *and* post-quantum cryptography.

In this field, hybrid can refer to both definitions.

When we refer to hybrid, we refer a mixture of both:

- Use both classical quantum-unsafe cryptography or post-quantum cryptography when possible.
- Only use classical if one of the parties does not support post-quantum cryptography

Problem may arise due to "downgrade attacks", policy matter?

Hybrid Certificates

Currently, certificates are constructed to only use classical cryptography. Naturally, this needs to change!

Challenge 1: Since post-quantum cryptography has very different properties (key sizes, generation time...), we need to construct certificates differently!

Challenge 2: If we want to use *both* classical and post-quantum cryptography (hybrid), we really need to further change the way we construct and handle certificates.

As there are multiple solutions to these challenges, multiple standards for hybrid certificates have been proposed.

Positioning HAPKIDO

Domains and Expterise

As we've seen, PKIs are complex ecosystems and their migration is going to be messy.

Hence, several levels involved:

1. Fundamental (cryptography)
2. Technical
3. Organisational
4. Legal
5. ...

Hence, connection between several domains and types of expertise needed

Desired Scientific and Societal Impact

- Fundamental results on quantum-safe cryptographic systems, for example, via the aforementioned cryptographic combiners.
- Understanding of technical & governance steps for migration
- Roadmap for transition to QS PKI
- Self-assessment Tools for organisations
- Awareness by public & stakeholders

Activities

Landscape of quantum-safe standardisation is very complex:

- Building blocks: NIST, ISO
- Protocols: IETF, GSMA, ETSI
- Certificates: ITU-T, IETF

Research initiatives:

- BSI in Germany (focus on “German PKIOverheid”)
- Proposals from number of TSP
- NIST NCCOE
- **AIVD PQC Migration Handbook**

PQC Migration Handbook

- Assists organisations with concrete steps and advice to mitigate to PQC.
- Aim of the handbook is to create awarenes and to enhance knowledge

Applies to any kind of organisation: Banks, insurers, government, telecom etc...

However, it does **not** discuss on PKIs.

PQC Migration Handbook and HAPKIDO

What are the differences between projects?

- HAPKIDO focuses specifically on PKIs (and as we seen, this is an incredibely complex topic)
- PKIs are out of scope of the handbook due to their complexity
- HAPKIDO has bigger ambitions and more deliverables that the handbook

Hence, HAPKIDO and the handbook can be seen as *complementing* each other.

Overview of activities and timeline

Where did we start?

The project started in October 2021.

Recap of first year:

- Plenty of preparatory work accomplished (methodology, literature, team building), first scientific output as well (2 articles)
- Website online https://www.tno.nl/hapkido, house style: done!
- Plenty of dissemination activities: HAPKIDO becoming famous

Where are we now?

Let's find out...

Overview of governance, SIA, serious gaming

Societal impact assessment

- Report soon to be finished

Governance

- Identified challenges in transition to QS PKI for public sector: https://dl.acm.org/doi/10.1145/3543434.3543644

Serious game to raise awareness

- Requirements identified, moving to next phase

Overview of cryptographic part

Focus on cryptographic combiners

- Combine several cryptographic schemes into one, having same functionality
- Secure if at least one component secur

A first result https://eprint.iacr.org/2022/773

- Compiler to turn adaptive oracle-based schemes into static ones, efficiently
- Consequence: construction of KEM combiner from PRF proven secure in Q-ROM

Overview of technical track

First PoC due end 2023

Some first observations:

- Hybrid certificates standardized by ITU-T since 3 years, but not yet commonly implemented in free certificate-management tools: need to pay or implement own tool
- Little crypto agility for e.g. of document-signing software: multiple schemes not taken into account
- Need to collaborate to upgrade standards

Future of HAPKIDO
Near future

In 2023:

- First PoC version
- Societal impact assessment, including dissemination video
- Requirement analysis
- Report on quantum-safe cryptographic combiners

Future of HAPKIDO
2024 and beyond

In 2024 and beyond:

- More PoCs with different applications
- Awareness-creation game
- Massive Online Open Course
- Self-assessment tool
- Enrich website

Thank you for listening!

Any further questions?