

Preparing for the Quantum Era

R Rajeshkumar

Convener – ISO/IEC JTC1 SC17/WG3



The basis of Trust in eMRTDs

- eMRTDs use Asymmetric Cryptography (RSA or ECDSA) that rely on “one-way functions”.
- These are math problems that are simple to compute in one direction, but nearly impossible to reverse them

A simplified example

- Let us take two primes 823 and 941
- Product is 774,443
- If you know only the product 774,443 and are asked to find the factors, then you would have to try every prime number less than 880 (there are 150 prime numbers less than 880) to see if it is a factor of 774,443
- RSA 2048 key is 617-digits long. Number of primes that need to be tested is 130 followed by 295 zeroes:

[illegible]

- It would take billions of years for massive supercomputers to reverse it using current algorithms

Why are Quantum Computers a threat?

- Shor's algorithm details a method to reduce the number of computations that you need to do to do the factoring.
- This is achieved using a specific algorithm that removes the primes that are not a factor – Basically, weed out numbers that are not the solution – **Quantum computers are very good at doing that**
- This leaves a much smaller number of primes that we need to test – Hence, easier to do a brute force attack

Quantum computers – state of play

- To crack a 2048 bit keys, we will need at least 4096 logical qubits
- As of 2026, the highest number of viable qubits demonstrated is 96, which can crack a 48 bit key
- BUT, a lot of investment in research, so viable Quantum Computers could become a reality quite soon

What is Q-Day?

- Future moment when quantum computers become powerful enough to break today's asymmetric encryption.
- Threats:
 - **Harvest Now, Decrypt Later:** Hostile agents store today's encrypted communication and decrypt them when quantum computers are available
- Vulnerable Systems:
 - Internet traffic, online submission portals, email traffic, data transmission between data preparation systems and personalization systems

**This is outside the scope of Doc 9303 specifications,
but Issuers need to be prepared as soon as possible
to protect their Issuance Infrastructure**

Assymmetric Crypto in eMRTDs

- Assymmetric Cryptography is used in the following areas:
 - The CSCA is the root of trust in an eMRTD.
 - The Signer (DSC) protects the content of the chip
 - Secure messaging between reader and chip – used to protect against skimming and eavesdropping
 - Clone detection using Active Authentication or Chip Authentication

Threat levels

- If CSCA is compromised, all the eMRTDs are compromised – **HIGH**
- If DSC is compromised, all the eMRTDs signed by that DSC are compromised – **HIGH**
- Secure messaging is compromised – only that eMRTD will not be protected from skimming and eavesdropping – **LOW**
- Clone detection is compromised – only that eMRTD can be cloned - **MEDIUM**

So, current focus of work is on protecting Passive Authentication

Considerations

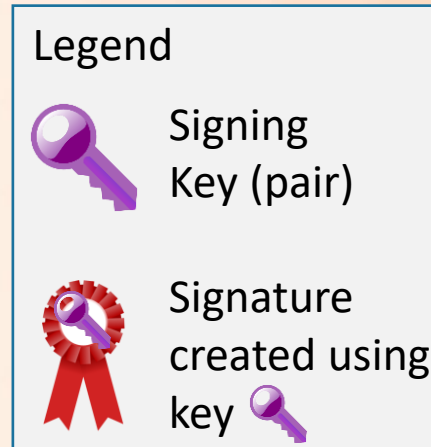
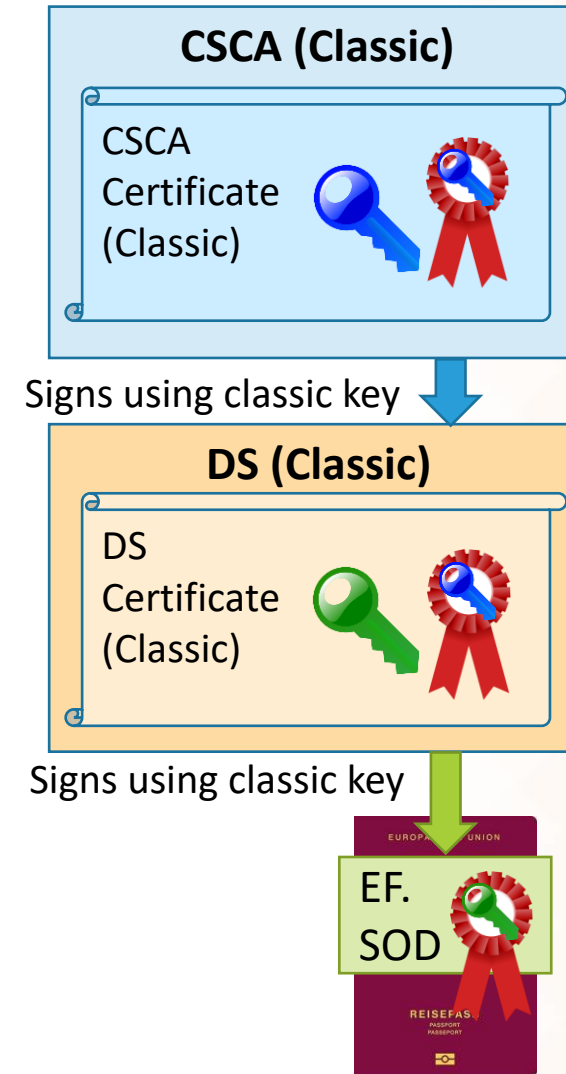
- A big bang change to Post Quantum (PQC) algorithms is not possible, as Issuers and border control systems will have to be updated
- Hence, a period of transition, where both classical and PQC are used
- Eventually, classical will be deprecated (made obsolete)

PKI Architectures

- Issuers will have to use both the classical and PQC algorithms to sign eMRTDs for at least a period of time
- There are different ways to implement these architectures

PKI Operation - today

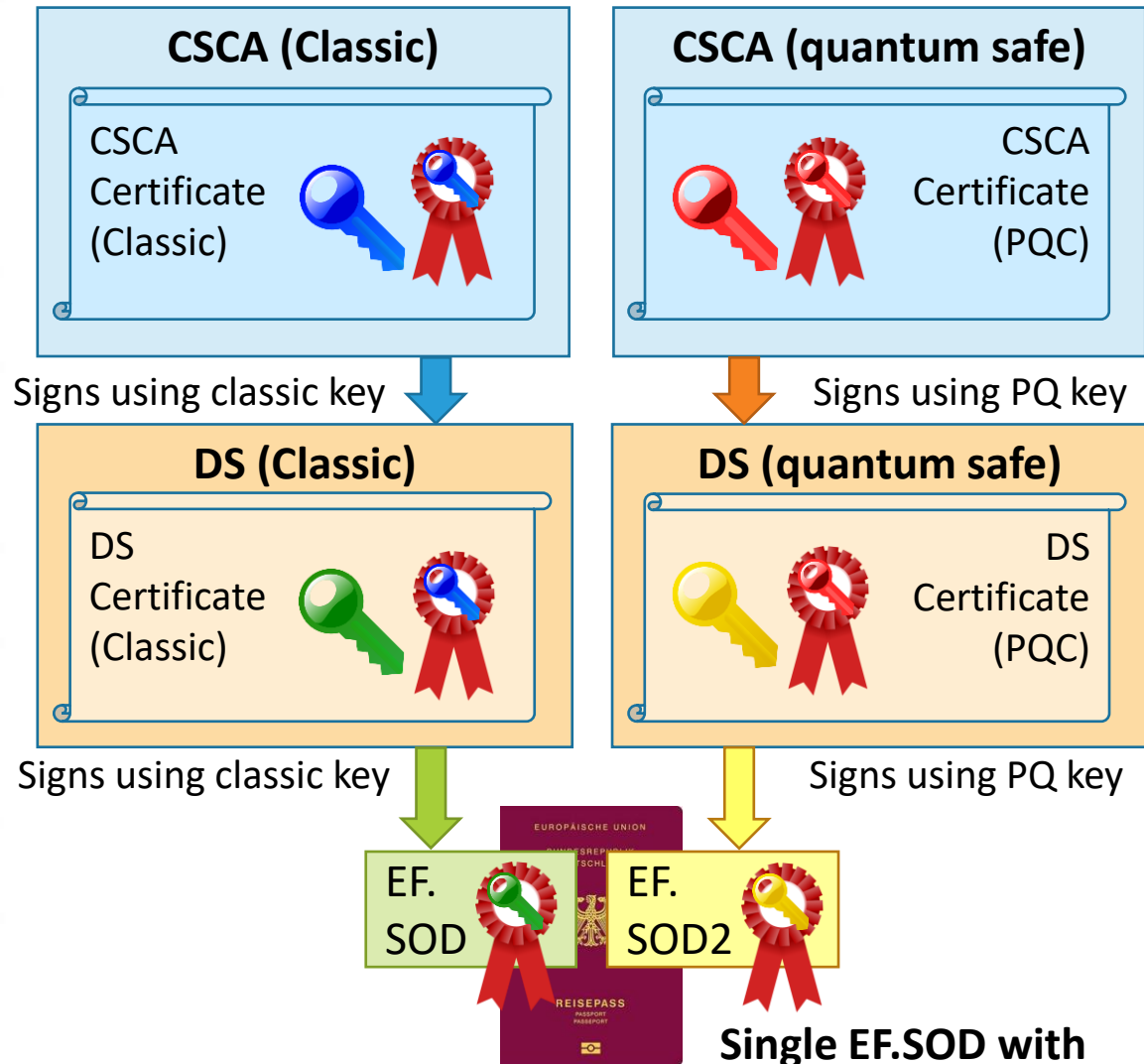
- Single branch PKI
- One CSCA per country



Source: Michael Hoppe, WG3/TF5

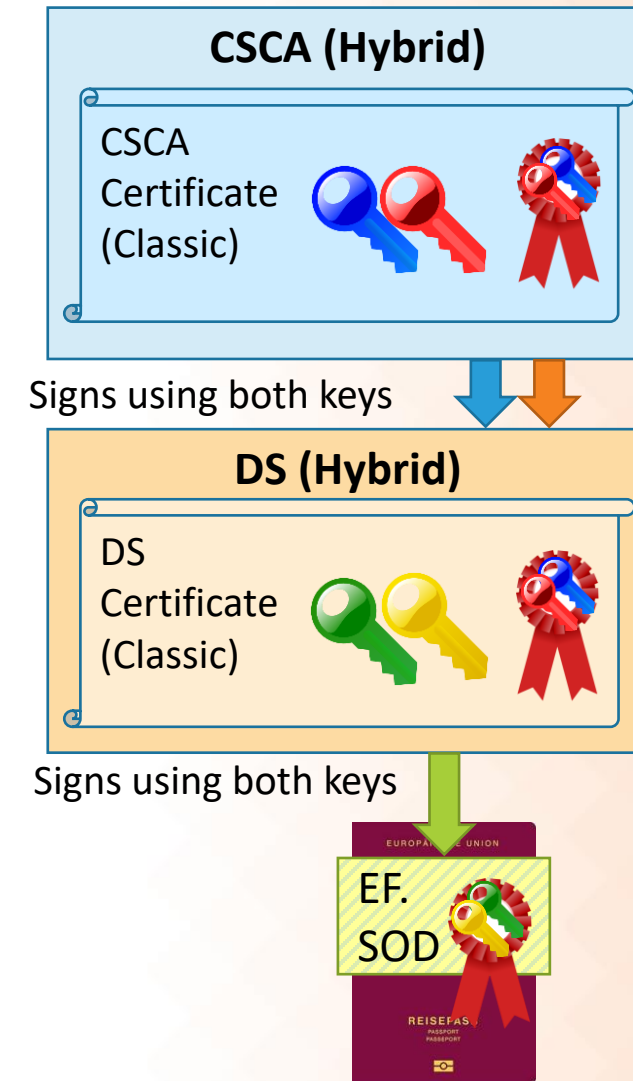
PKI Operation - tomorrow

Two
separate
PKI
branches



Single EF.SOD with
concatenated SignerInfos
is also possible

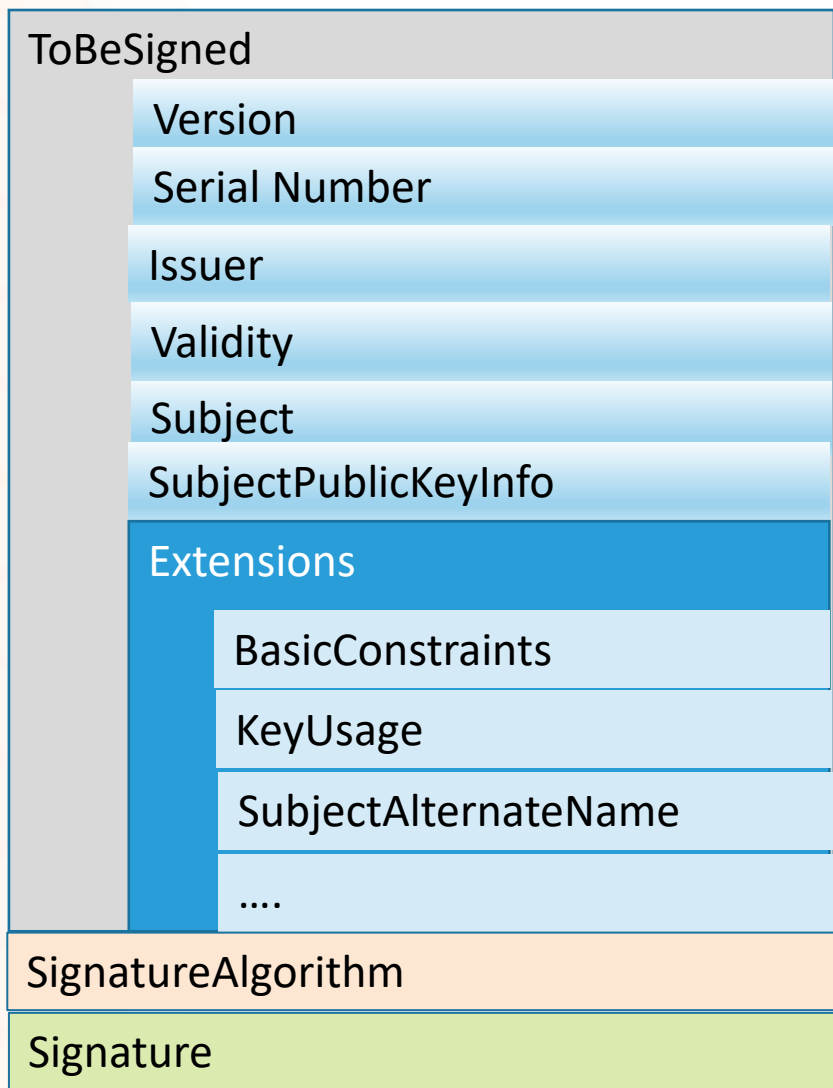
Linked
PKIs
issuing
hybrid
certificates



Source: Michael Hoppe, WG3/TF5

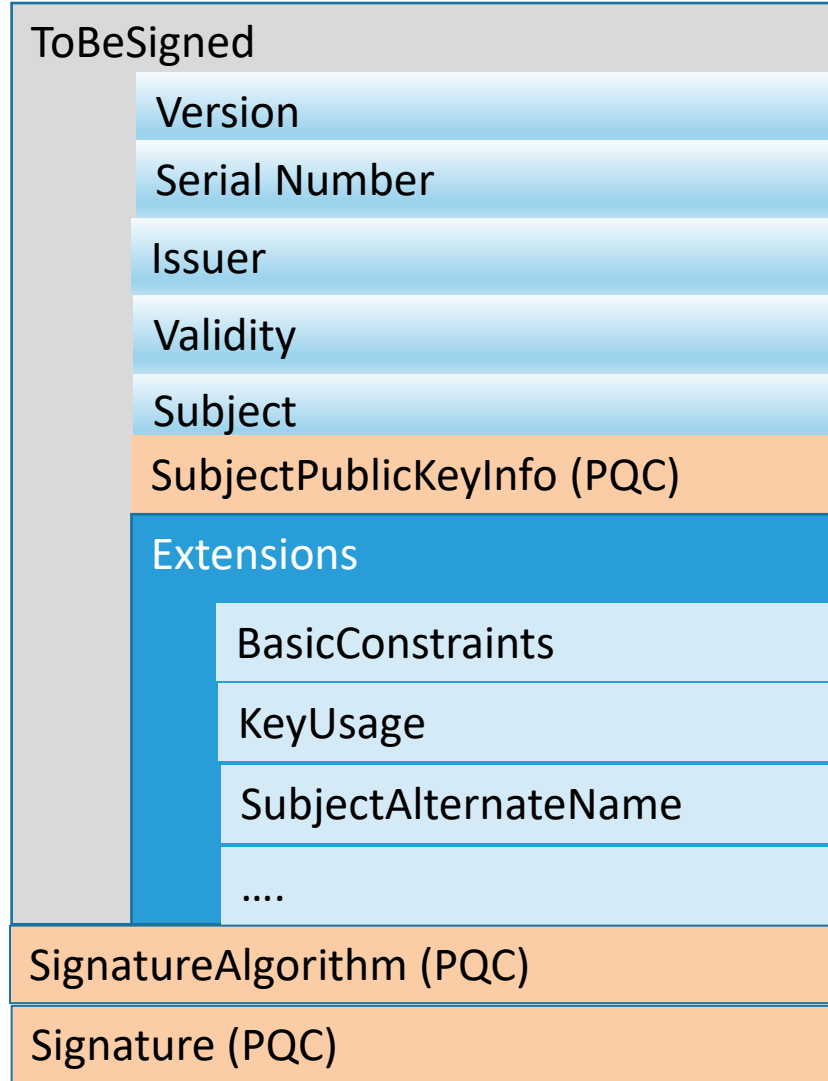
What is a Hybrid Certificate?

Anatomy of an X.509 Certificate



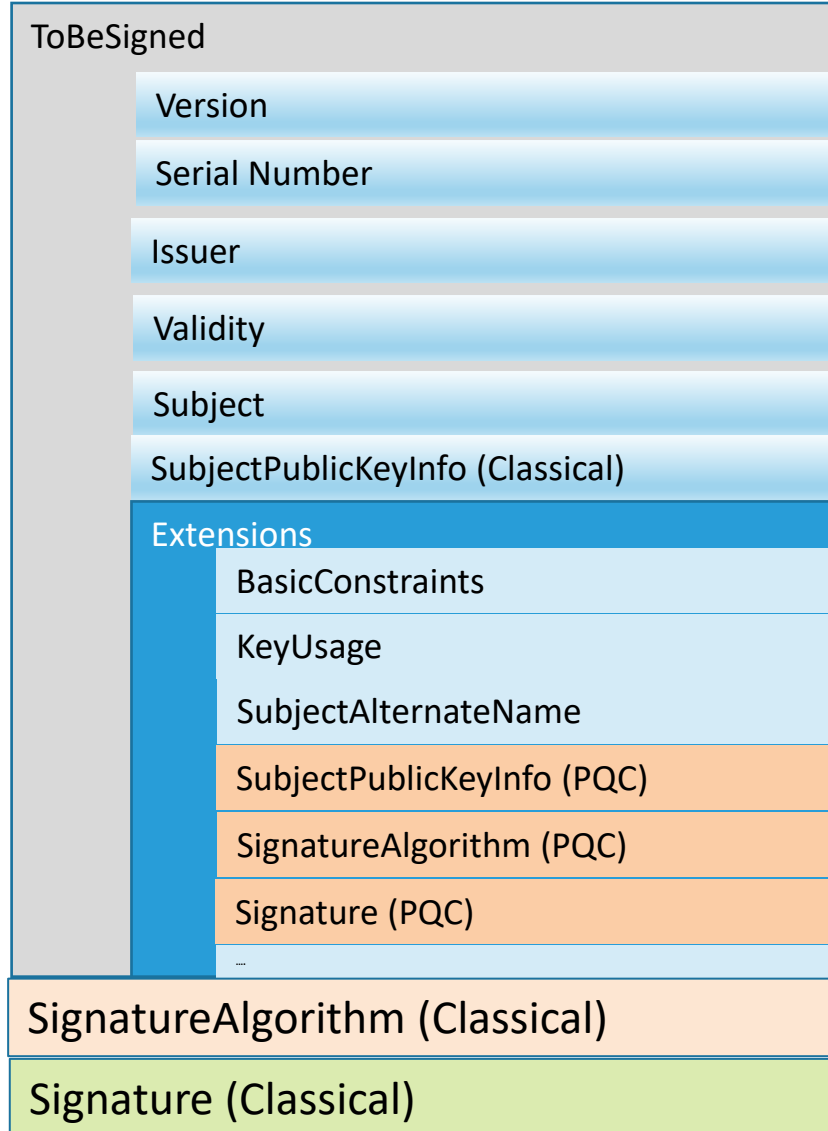
- Consists of three parts
 - Content to be Signed
 - Signature Algorithm
 - Signature
- ToBeSigned contains
 - Issuer
 - Validity
 - Public Key
 - Extensions
- When Inspection system encounters an extension it does not know, it checks if it is critical or non-critical
- If non-critical, it ignores it and continues.
- If critical, and IS does not know how to handle it, it should reject the certificate

Constructing a Hybrid Certificate – Step 1



- Create a certificate containing the PQC Public Key
- Use a PQC Signature Algorithm
- Create a PQC Signature and create an X.509 certificate

Constructing a Hybrid Certificate – Step 2



- Move the Publickey, signature algorithm and signature from step 1 as non-critical extensions of To Be Signed
- Use a classical Signature Algorithm to create a classical signature and an X.509 certificate
- Current Inspection Systems will ignore the extensions and continue to work
- Upgraded Inspection Systems know where to find the PQC algorithms and Signature

Pros and Cons

Dual Chain

- Specification possible using existing X.509 and CMS
- Backwards compatible
- Requires modification of SOD
- Operational Issues
 - For ease of use, both chains should have a common operational interface
 - For border, both trust chains have to be managed

Hybrid

- Specification for hybrid-X.509 and hybrid-CMS required – Major change to Issuers and Borders
- Backwards compatibility depends
- Only one PKI branch per country
- No modification to LDS of chip required.

Choice between Dual Chain and Hybrid

- Survey sent out by CASG of SC17/WG3 – responses equally split between the two
- Those advised by their National Cybersecurity Agencies choose Hybrid

Why do Cybersecurity agencies like Hybrid?

- For the internet, you cannot have two different PKI for the same transmission – so they would have to go “big bang” and switch to PQC algorithms
- There is some concern on the maturity of the PQC algorithms
 - WHY????????

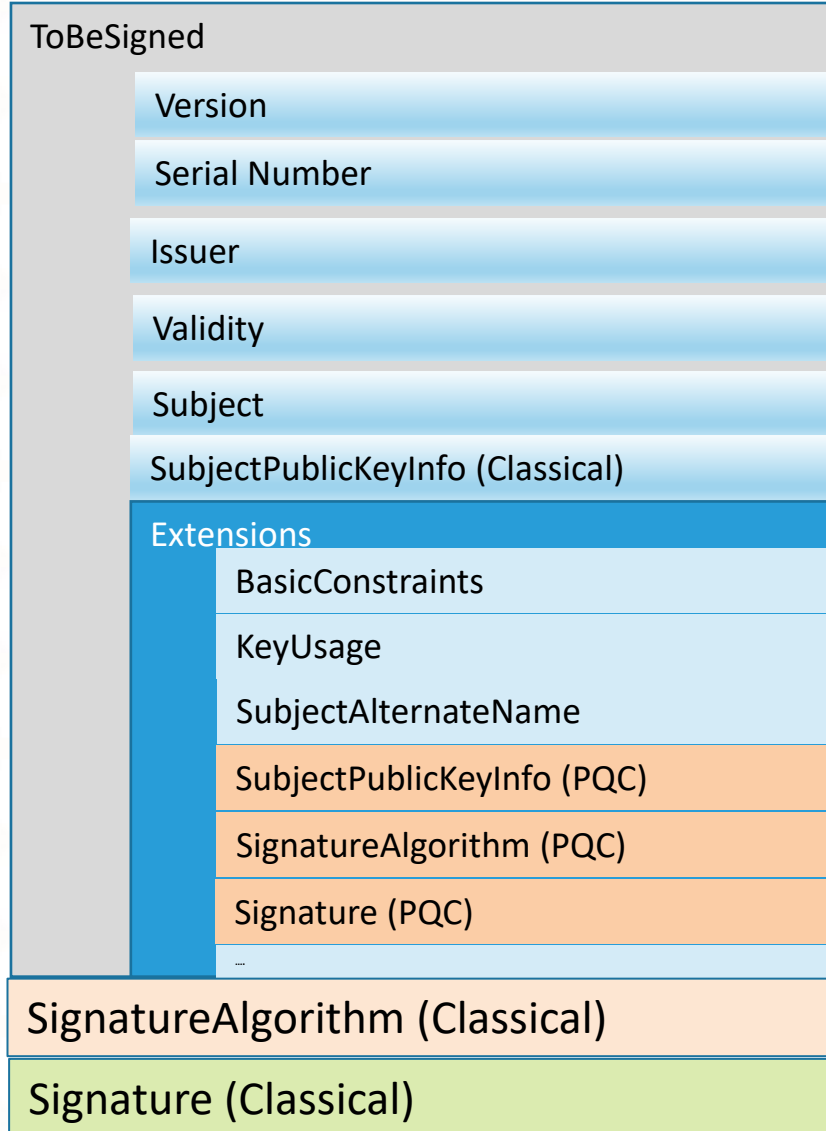
The story of SIKE

- On July 5, 2022, NIST announced four candidates for PQC Standardization Round 4 (Public Key Encryption/Key Encapsulation Mechanism – PKE/KEM)
 - Crystal – KIBER
 - BIKE - Bit Flipping Key Encapsulation
 - Classic McEliece
 - Hamming Quasi-Cyclic
 - **SIKE – Supersingular Isogeny Key Encapsulation**
- August 2022 – Paper from KU Lueven
- described a technique that uses complex mathematics and a single Pre-Quantum Computer (traditional PC) to recover the encryption keys protecting the SIKE-protected transactions.
- The entire process requires only about an hour's time

Reactions

- David Jao, University of Waterloo and evolutionQ, Inc. (principal submitter - SIKE)
 - In general there is a lot of deep mathematics which has been published in the mathematical literature but which is not well understood by cryptographers. **I lump myself into the category of those many researchers who work in cryptography but do not understand as much mathematics as we really should.** So sometimes all it takes is someone who recognizes the applicability of existing theoretical math to these new cryptosystems.
- Jonathan Katz, an IEEE Member and professor in the department of computer science at the University of Maryland
 - Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward

So, why is Hybrid popular?



- In hybrid structures, PQC algorithms are embedded in structures protected using classical algorithms
- For a hybrid structure, if PQC algorithm is broken first, we can fall back to classical algorithm
- If we used dual chain for eMRTD, we could simply ignore the PQC chain in such a case

Another important concept – Downgrade protection

- Two options:
 - We create a hybrid certificate and a hybrid SOD and put into chip
 - We use dual chain and create an SOD with two signers or two SODs
- Assume that the classical algorithm gets broken, then attacker will create a new certificate and SOD without the PQC algorithms
- Inspection Systems have no way of knowing whether the chip was supposed to contain PQC algorithms or not
- Called “**downgrade attack**”
- Will need an offline way of knowing whether the presented passport was supposed to have a PQC algorithm and signature – Could be through the PKD – Still a work in progress

An Unpleasant Surprise

- ECDSA will succumb to smaller quantum computers than RSA
- Example:
 - Breaking ECDSA-512 requires approximately 4,258 logical qubits
 - Breaking RSA-4096 requires approximately 8,194 logical qubits
- There is no curve stronger than ECDSA-512.
- RSA keylengths can be increased and can delay the threat:
 - 5120-bit RSA: 10,242 logical qubits
 - 6144-bit RSA: 12,290 logical qubits
 - 7168-bit RSA: 14,338 logical qubits
 - 8192-bit RSA: 16,386 logical qubits

Roadmap of specifications

- Crypto Agility Subgroup working on specifications for PKI infrastructure
- Will be discussed in the next NTWG in Miami
- The goal is to try and get it ready for TAG/TRIP in 2027
- Will allow for Issuers to start transitioning to support both classical and PQC algorithms from 2028
- At some sunset date, classical algorithms will be deprecated

Thank You

R.Rajeshkumar@auctorizium.com

RRaj88@gmail.com

www.linkedin.com/in/rraj88

