ETSI/IQC Quantum Safe Cryptography Event

The hybrid bridge for migrating X.509 ecosystems to PQ

Co-authors:

Mike Ounsworth

Juan Carlos Fernández

ENTRUST

14/02/2023

“PQ/T HYBRID” TERMINOLOGY

- The word “**hybrid**” is incredibly overloaded in cryptography.
- *Flo Driscoll’s IETF draft* tries to untangle it:
  - **Post-Quantum/Traditional (PQ/T) Hybrid Scheme**:
    A cryptographic scheme *made up of two or more component algorithms* where at least *one is a post-quantum algorithm* and at least *one is a traditional algorithm*.
  - **PQ/T Hybrid Digital Signature**:
    A digital signature scheme *made up of two or more component digital signature algorithms* where at least *one is a post-quantum algorithm* and at least *one is a traditional algorithm*.
- **PQ/T hybrid KEMs**, **PQ/T hybrid PKE**, and **PQ/T hybrid digital signatures** are all examples of PQ/T hybrid schemes.

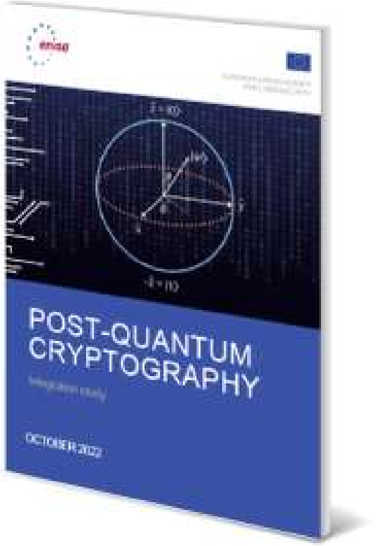
1: https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology

EUROPEAN REGULATORY LANDSCAPE

ENTRUST

ENISA (EUROPE)

- ENISA: Post Quantum Cryptography Integration Study - October 2022
  - *“the veridical paradox that by striving for quantum resistance using a PQC system we might be lowering security overall. Actually, there is **no guarantee that the post-quantum cryptosystems that survive the standardization process are secure**.”*
  - *“Furthermore, the complicated new ecosystem of post-quantum cryptographic software has **a clear risk of introducing bugs**. **A solution to this might be to augment, instead of simply replacing, current modern cryptosystems with PQC systems.**”*
  - *“Start with a system that encrypts and/or signs using elliptic-curve cryptography. Add an extra layer that also encrypts and/or signs using post-quantum cryptography.”*



POST-QUANTUM CRYPTOGRAPHY

Integration study

OCTOBER 2022

1: https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study, October 2022

BSI (GERMANY)

Federal Office
for Information Security

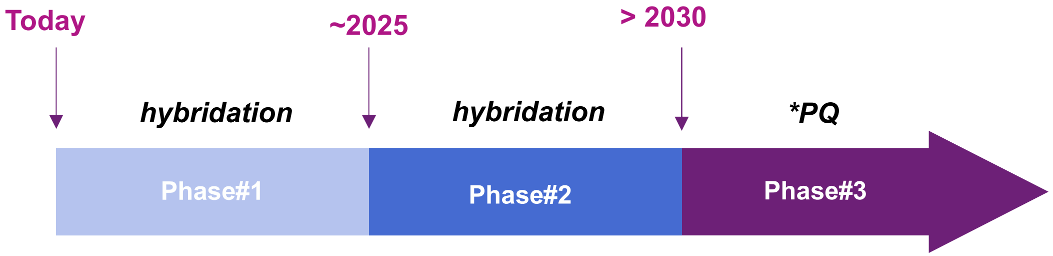
- Quantum-safe cryptography – fundamentals, current developments and recommendations - May 2022

  - *"At present, post-quantum cryptographic schemes are generally not yet trusted to the same extent as established cryptosystems since* ***they have not been equally well studied*** *in terms of* ***side-channel resistance*** *and* ***implementation security****, for example.*

  - *"The essential point, however, is that* ***post-quantum algorithms should generally not be used alone, but only in hybrid mode****, i.e. in combination with a classical procedure."*

1: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

ANSSI (FRANCE)



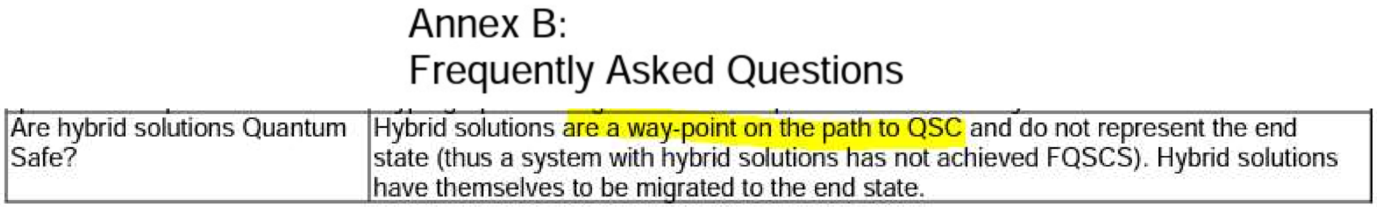
- ANSSI views on the Post-Quantum Cryptography transition - March 2022:
  - *"ANSSI emphasizes that* ***the role of hybridation in the cryptographic security is crucial and will be mandatory for phases 1 and 2 presented in the sequel****."*
    - *Phase 1 (today):* ***hybridation*** *to provide some additional post-quantum defense-in-depth to the pre-quantum security assurance.*
    - *Phase 2 (not earlier than 2025):* ***hybridation*** *to provide post-quantum security assurance while avoiding any pre-quantum security regression.*
    - *Phase 3 (probably not earlier than 2030): optional standalone post-quantum cryptography.*

[1] https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

ETSI

ETSI TR 103 619 V1.1.1 (2020-07)

- CYBER: Migration strategies and recommendations to Quantum Safe schemes – August 2020
  - *"NOTE 6: Recommendation ITU-T X.509 [i.4] specification for PKCs supports a number of modes that* ***allows for staged migration including hybrid modes****."*
  - *If backwards compatibility is required during a phased migration, then the PKI will have to support both classical and Quantum Safe signing algorithms, which can be handled either by using parallel classical and Quantum Safe certificate chains,* ***or by using hybrid certificate chains depending on the cryptographic agility of the existing relying parties****."*



Annex B:
Frequently Asked Questions

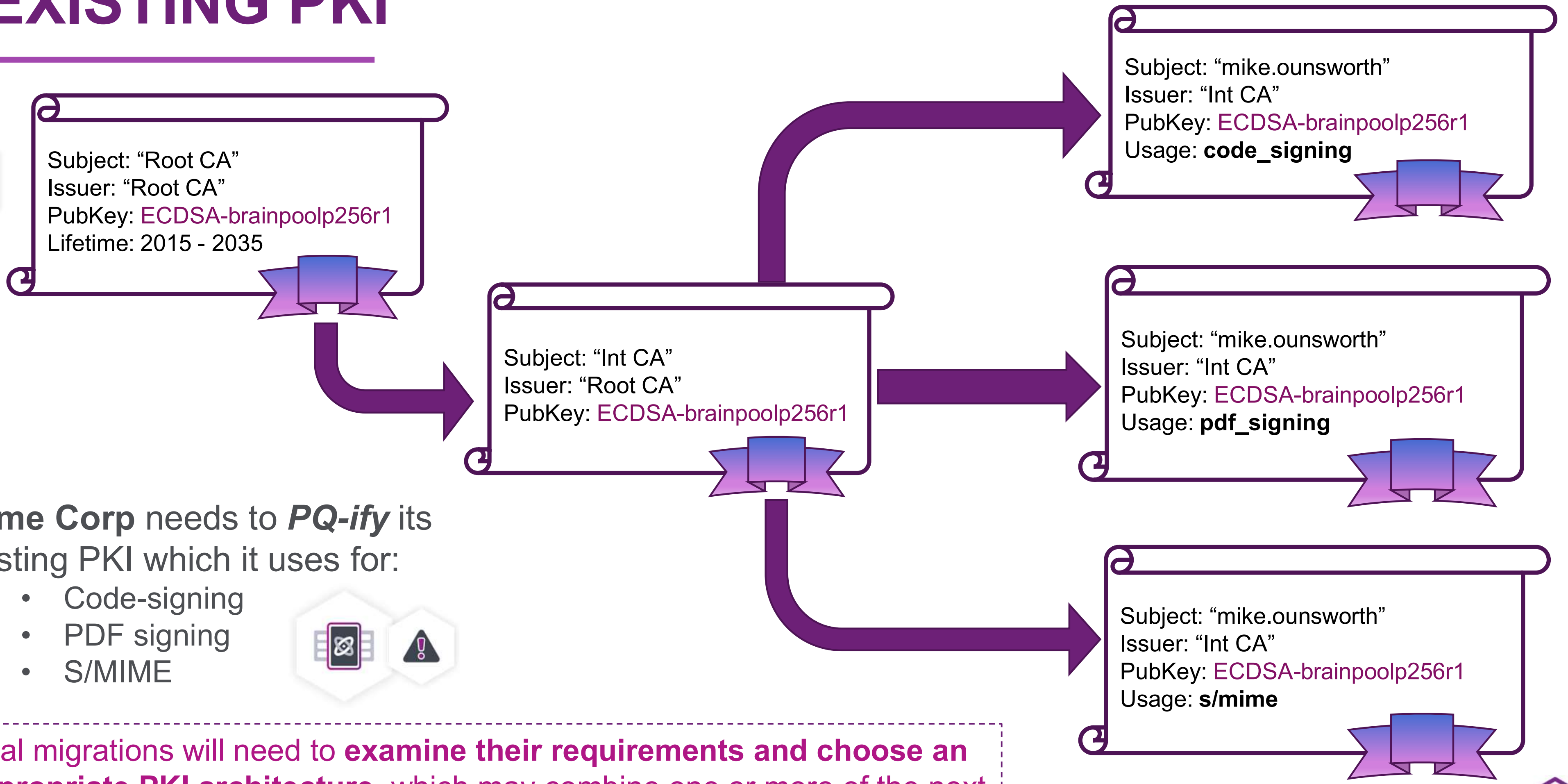
Are hybrid solutions Quantum Safe?	Hybrid solutions are a way-point on the path to QSC and do not represent the end state (thus a system with hybrid solutions has not achieved FQSCS). Hybrid solutions have themselves to be migrated to the end state.

1: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

EXAMPLE PQ/T HYBRID PKI MIGRATION

ENTRUST

EXISTING PKI



Subject: “Root CA”
Issuer: “Root CA”
PubKey: ECDSA-brainpoolp256r1
Lifetime: 2015 - 2035

Subject: “Int CA”
Issuer: “Root CA”
PubKey: ECDSA-brainpoolp256r1

Subject: “mike.ounsworth”
Issuer: “Int CA”
PubKey: ECDSA-brainpoolp256r1
Usage: **code_signing**

Subject: “mike.ounsworth”
Issuer: “Int CA”
PubKey: ECDSA-brainpoolp256r1
Usage: **pdf_signing**

Subject: “mike.ounsworth”
Issuer: “Int CA”
PubKey: ECDSA-brainpoolp256r1
Usage: **s/mime**

Acme Corp needs to ***PQ-ify*** its existing PKI which it uses for:

- Code-signing
- PDF signing
- S/MIME

Real migrations will need to **examine their requirements and choose an appropriate PKI architecture**, which may combine one or more of the next strategies (but not necessarily all)

ENTRUST

MIGRATION STRATEGY

Traditional ECDSA PKI

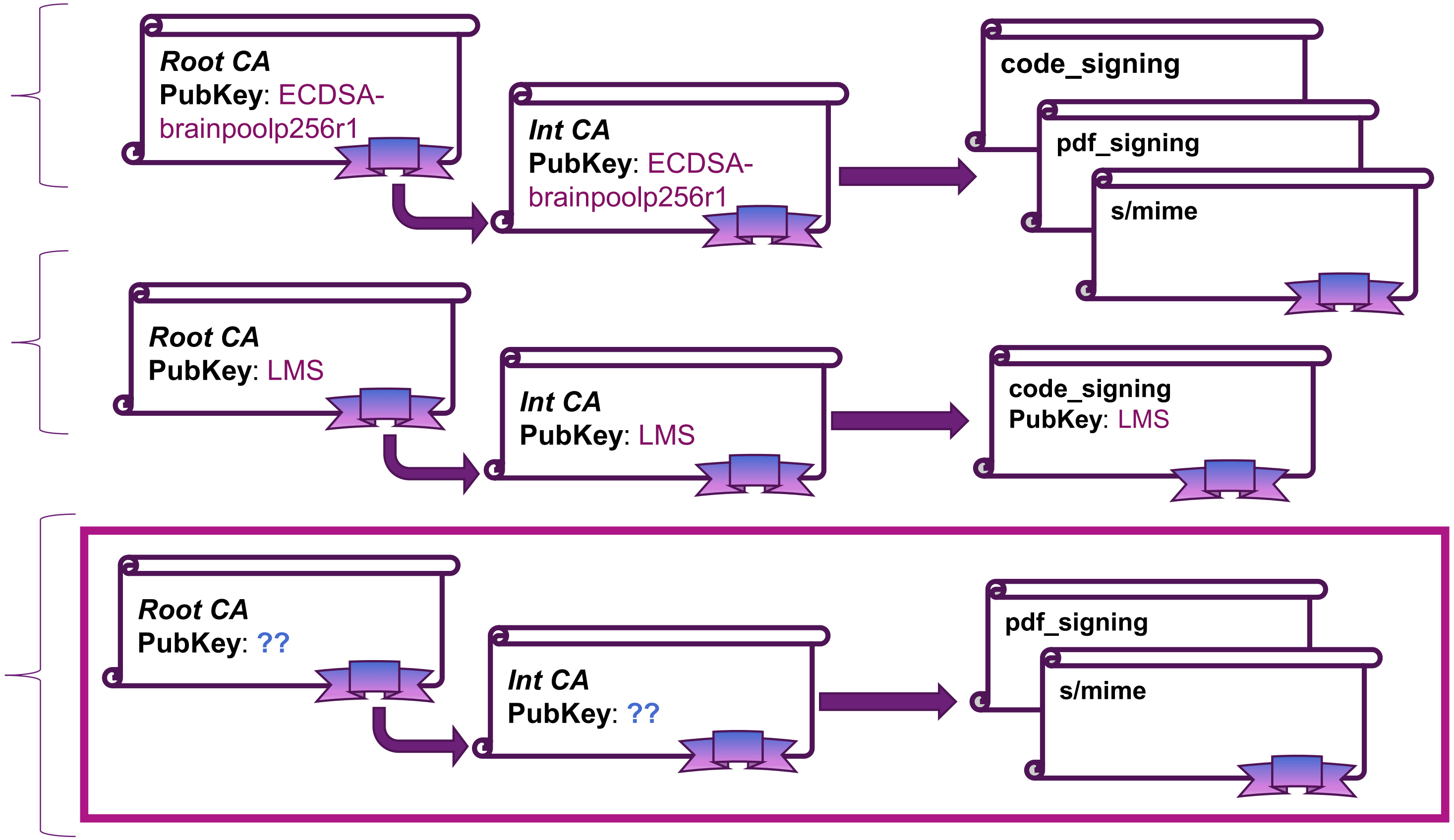
- Backwards compatibility
- Root already distributed
- ECDSA impl. is battle-hardened

LMS PKI for code-signing

- Standardized in 2020 (NIST SP 800-208)
- For long lifetime deployments
- **Hard** to manage pvk state (HBS)

What PQ resistant PKI do we use here?

Solution #1: Mixed PQ PKI
Solution #2: Composite PKI



Root CA
PubKey: ECDSA-brainpoolp256r1

Int CA
PubKey: ECDSA-brainpoolp256r1

code_signing

pdf_signing

s/mime

Root CA
PubKey: LMS

Int CA
PubKey: LMS

code_signing
PubKey: LMS

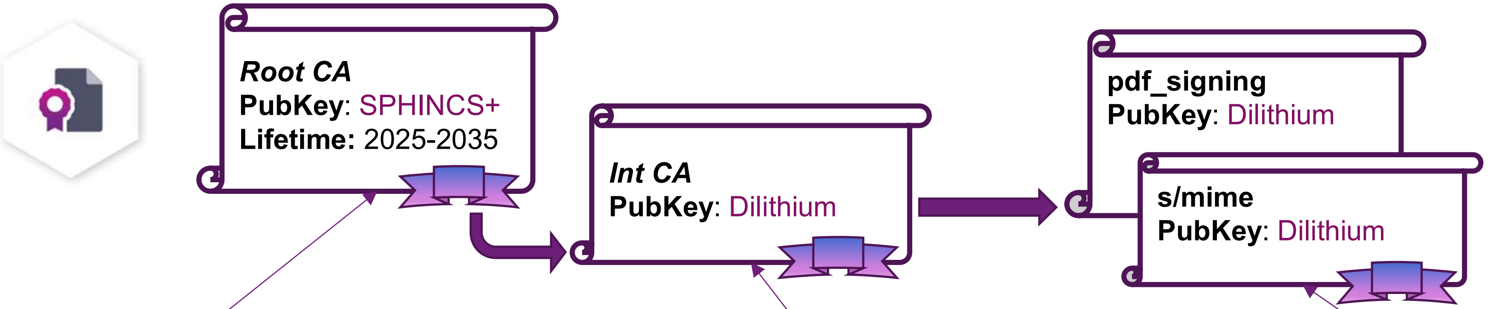
Root CA
PubKey: ??

Int CA
PubKey: ??

pdf_signing

s/mime

SOLUTION #1: MIXED PQ PKI



Root CA
PubKey: SPHINCS+
Lifetime: 2025-2035

Int CA
PubKey: Dilithium

pdf_signing
PubKey: Dilithium

s/mime
PubKey: Dilithium

We want a long lived **Root CA**, so use **HBS**.

Could use **LMS/XMSS**, but if regulation doesn't require it, use **SPHINCS+.**

SPHINCS+ is easier to manage removing pvk state.

Root and Int CAs certs will be **large** because of **SPHINCS+** signature.

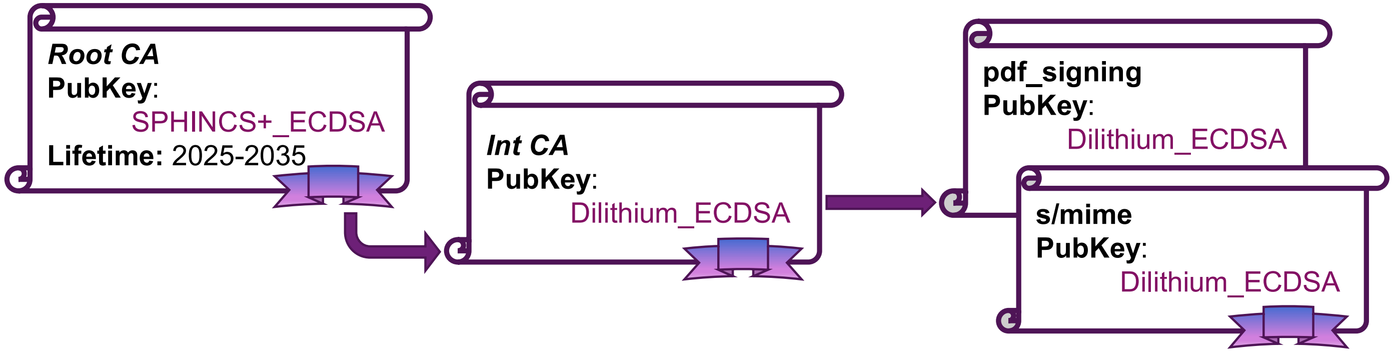
Root and Int CAs can be **cached** by the client and not sent over the network.

NIST is thinking about a **smaller SPHINCS+ parameter** (fewer lifetime signatures).

End Entity certs are **small** and **fast.**

1: https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/
1: https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-keys/
2: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

SOLUTION #2: COMPOSITE PKI



Root CA
PubKey: SPHINCS+_ECDSA
Lifetime: 2025-2035
Int CA
PubKey: Dilithium_ECDSA
pdf_signing
PubKey: Dilithium_ECDSA
s/mime
PubKey: Dilithium_ECDSA

- We are **not re-using** the keys from existing ECDSA PKI.
- Compared to the size and performance of **SPHINCS+** and **Dilithium**, **ECDSA goes unnoticed**.
- **PQ** algorithms are **not immune to implementation bugs**, even SPHINCS+.

(1) **Composite**

↑ **PQ protection**

↓ **Backwards compatibility**

Subject: Int CA
Issuer: Root CA
PubKey: Composite {Dilithium, ECDSA}
SigAlg: Composite {Dilithium, ECDSA}
Sig: {10100010…, 10001001…}

X.509 PQ/T Hybrid Syntax

Subject: Int CA
Issuer: Root CA
PubKey: ECDSA
X509v3Exts:
-**SubjectAltPublicKeyInfoExt**
Dilithium PBK
-**AltSignatureAlgorithmExt**
Dilithium
-**AltSignatureValueExt**
100100101
SigAlg: ECDSA
Sig: 10100010…

(2) **ISARA Catalyst**

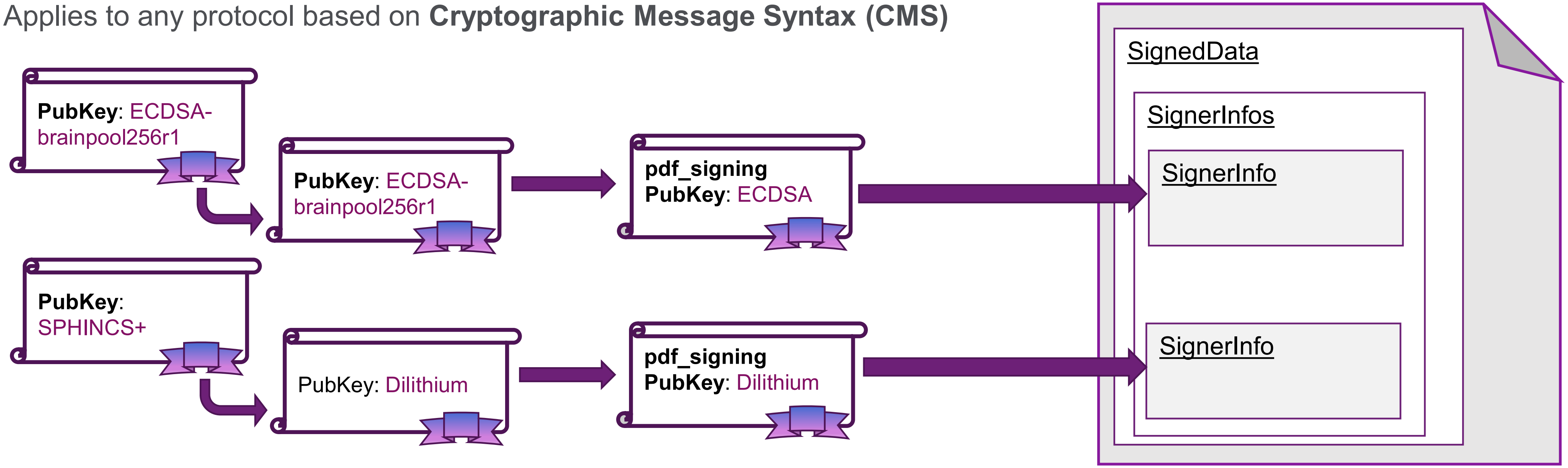
↑ **Backwards compatibility**

↓ **PQ protection**

ENTRUST

PQ/T HYBRID AT CMS LEVEL

Applies to any protocol based on **Cryptographic Message Syntax (CMS)**



PubKey: ECDSA-brainpool256r1

PubKey: ECDSA-brainpool256r1

pdf_signing
PubKey: ECDSA

PubKey: SPHINCS+

PubKey: Dilithium

pdf_signing
PubKey: Dilithium

SignedData

SignerInfos

SignerInfo

SignerInfo

- Backwards compatibility: CMS clients (code-signing, PDF, S/MIME) already handle multiple *SignerInfos* today.
  - So legacy clients ***should*** gracefully skip the PQ signature.
- Redundancy gives migration flexibility. PQ-aware clients can validate either:
  - PQ signature only, or
  - Both parallel signatures independently.

RFC5652 - SignerInfos:

"When the collection represents more than one signature, **the successful validation of one of the signatures** from a given signer ought to be treated as a successful signature by that signer..."

SUMMARY

European regulation is pro PQ/T Hybrid

- ENISA
- BSI
- ANSSI
- ETSI

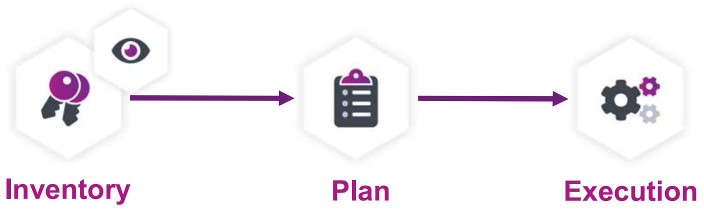
PQ/T Hybrid flexibility
Hybrid mechanisms give *flexibility* to *tune* the security and migration needs of your PKI.

Prepare your migration strategy

- Multiple PKIs
- Mixed PQ PKI
- Composite PKI

ENTRUST

The time to prepare for post-quantum is now!
Prepare your PQ/T Hybrid strategy.



Inventory

Plan

Execution

ENTRUST