RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

PQC TRANSITION ANSSI VIEWS

Mélissa Rossi, ANSSI, France

National cybersecurity authority role of ANSSI in crypto

Advisory

Promote the use of state-of-the-art cryptographic standards.

- National guidelines on crypto
  « Guide des mécanismes cryptographiques »

- European guidelines on crypto (SOG-IS)
  Goal: harmonized crypto evaluation scheme
  « Agreed Cryptographic Mechanisms » (ACM)

Regulatory

Supervise the evaluation and delivery of security labels for cryptographic products.

VISA DE SÉCURITÉ — ANSSI

e.g. CC certificates

In the French scheme, security evaluations comprise cryptographic evaluation tasks.

Post-quantum cryptography

➢ The most promising avenue to thwart the quantum threat.

High academic and industrial interest in France (design, security of the primitives, cryptanalysis).

Key role of the ongoing NIST standardization process for PQC proposals as a catalyst.

- Strong involvement of the crypto research community
- Focus on a restricted number of KEMs and signatures while preserving the biodiversity.

Beyond the NIST objective to derive standards, the past three rounds of the standardization campaign **provide a variety of algorithms and solid (although recent) analysis**.

- A **fourth round** for extra analysis and new signature submissions seems relevant given the progress in several domains.

- Slight concerns about the distinction finalist/alternate. Both structured and unstructured lattices will be needed soon.
  - ➢ Why isn't FrodoKEM a finalist?

Post-quantum cryptography

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

- ≈ the maturity level of RSA in the mid 90's
- Multifaceted immaturity: difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols, secure implementations
- Immaturity will **not cease immediately with the publication of NIST standards**

Acknowledging this immaturity is important,

but it should not serve as an argument for postponing the first deployments.

Inital recommendations

No endorsement of any direct jump.

No drop-in replacement in the short/medium term

Single exception: hash-based signatures but the range of their potential applications are limited.

Hybridation.

Hybridation for KEMs and Signatures: post-quantum mechanisms constructed over a recognised pre-quantum scheme.

- Preservation of the pre-quantum security
- Extra protection against the quantum threat
- Low performance penalty over drop-in replacement

The sooner the better.

For security products aimed at offering a **long-lasting protection (after 2030) of information:**

➢ ANSSI encourages to start transitioning with hybrid mechanisms **as soon as possible.**

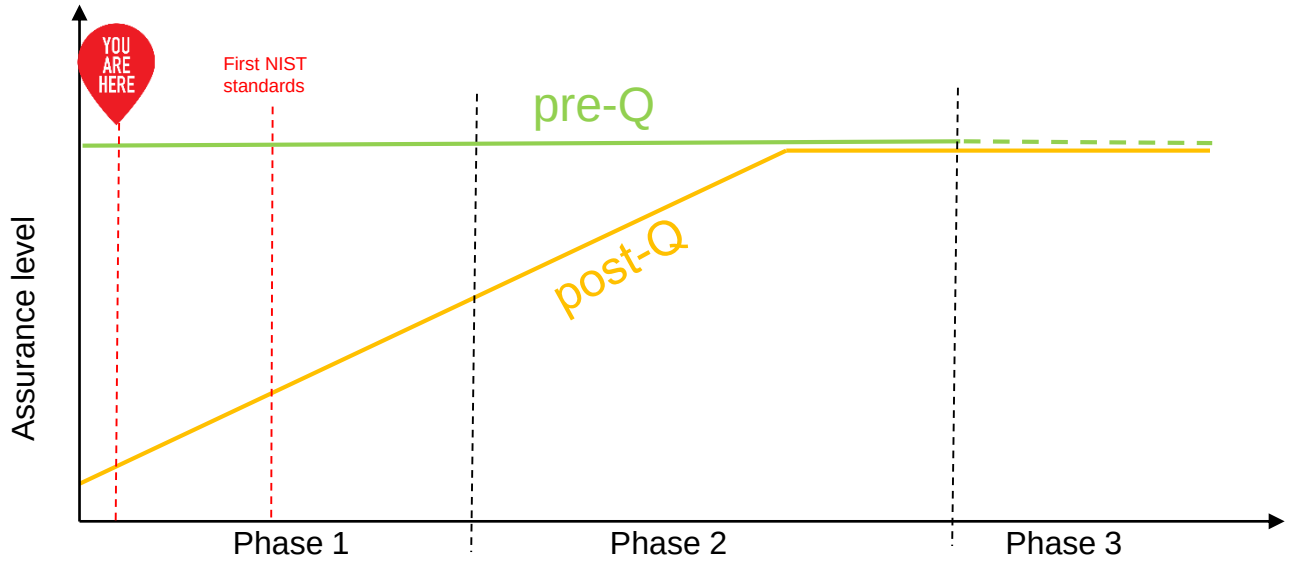
For all security products:

➢ ANSSI encourages crypto-agility.

More details in the next slide

3-phase transition

- A gradual overlap transition will progressively increase trust.
- It will be possible to better anticipate deployment problems.
- A learning phase will be beneficial before post-quantum crypto becomes mandatory.



Phase 1: Initialize the transition and best effort on PQ security

Existing guidelines **already allow** to ask for a security label for a product with a hybrid mechanism (post-quantum + recognized pre-quantum).

Important requirement: **no security regression**

i.e. at least equivalent to the security of the included pre-quantum scheme.

The post-quantum security is considered as an « in-depth defense » ≈ bonus security.

- **Relative freedom in the choice of the asymmetric PQ algorithm:**
  - **Stable and well-studied specifications** e.g. NIST finalists / trusted alternate.
  - **Conjectured post-quantum security level**: as high as possible for both asymmetric and symmetric algorithms preferably NIST level V ≈ AES-256.

Choosing **algorithms selected by NIST** for standardization is **not an absolute pre-requisite.**
Few exceptions are nevertheless expected in practice, at least for mainstream crypto.

➢ Example: a developer who wants a very conservative security can choose FrodoKEM even if NIST decides not to standardize it soon.

Phase 1 allows a learning period where implementors will be able to make early deployments.

Phase 2
Strengthen the requirements: PQ security assurance

- Continue to **systematically apply hybridation** (except for hash-based)

1. No more « in-depth defense »: post-quantum assurance as **integral part of the security labelization**.
   - ➢ Stronger requirement for the choice of the post-quantum primitives

Algorithm Restriction

ANSSI will identify **more restricted acceptability criteria for post-quantum algorithms** in the security products.

⇨ We do not guarantee that the set of acceptable algorithms will exactly match the set of NIST standards.

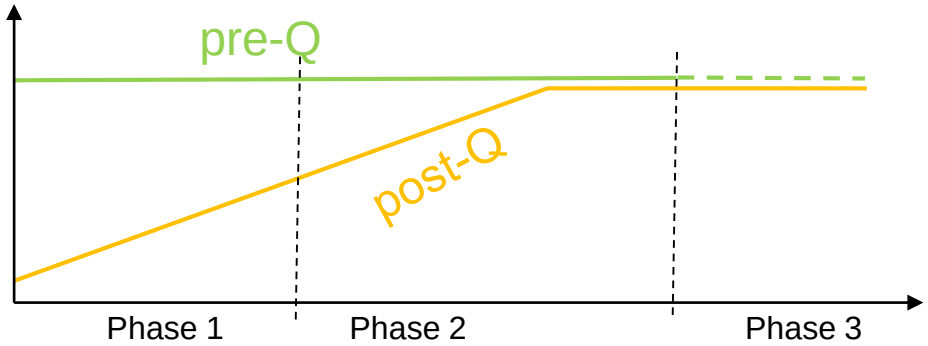
2. ANSSI will **stop delivering security labels for certain types of products claiming long-term security** if they do not offer PQ security.

Phase 3: Finalize the transition

Go

- Certain PQ schemes could optionally be used **without hybridation.**
- Post-quantum security will be mandatory for more and more types of products.

More details (timeline, examples…) will be available in a white paper that will appear before the end of the year on ANSSI's website.



➢ https://www.ssi.gouv.fr/en/