RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

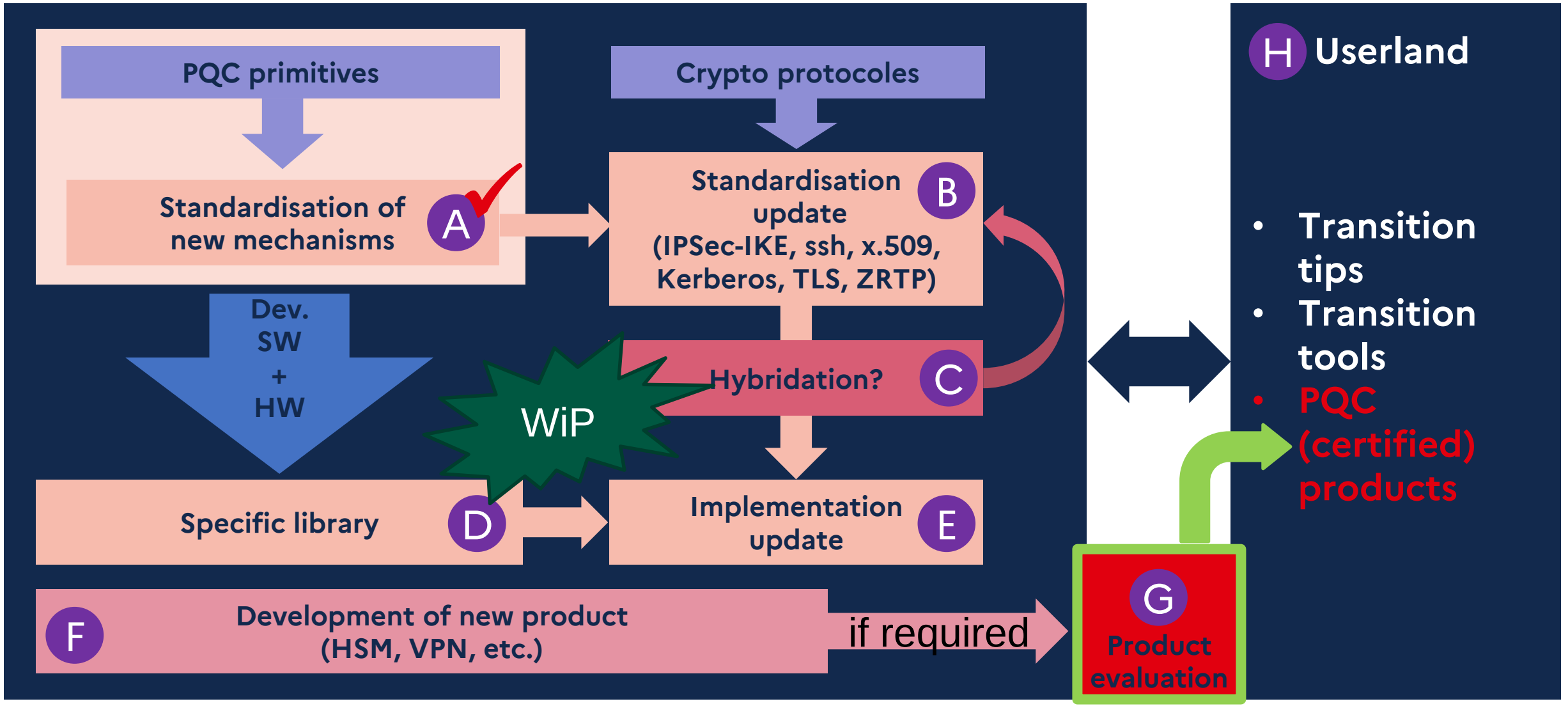
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

ANSSI PLANS FOR THE CERTIFICATION OF PRODUCTS USING PQC

ECW

RENNES 22/10/2024

POST-QUANTUM TRANSITION



RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

1. WORK IN PROGRESS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

PQC transition

Most cybersecurity agencies recommend transition:

- Massive investments in quantum computer technologies
- The potential threats have to be considered NOW

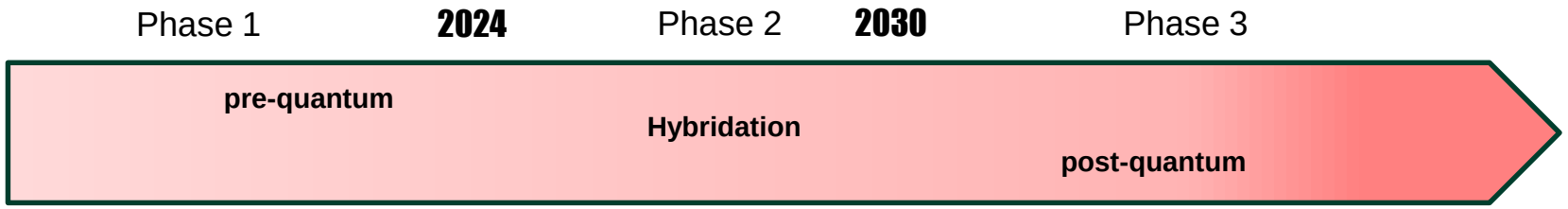
No longer excuse to wait:

- After an international consensus, **NIST published new PQC standards**
- PQC mechanisms are tested in wildly used application (OpenSSH)
- Protocols standardisation have begun the transition (TLS, IPSec)

ANSSI view on PQC transition

Significant strategic investments on the subject:

- Technical cryptographic recommendations (mechanisms, hybridation) available:
  - anssi-views-post-quantum-cryptography-transition
  - follow-position-paper-post-quantum-cryptography
- Contributor to European guideline (ACM)
- Willingness to participate in increasing the skills of the ecosystem



RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

2. SECURITY VISAS PROCESS

ANSSI security visas

ANSSI supervises the evaluation and delivery of **security visas** for security products:

- Security visas are required for governmental use (in particular, cryptography)

Accepted security visas are published online:

- certified-products
- produits-services-qualifies

Assessment of the products is performed by ITSEF companies

- CC evaluation or CSPN evaluation (First level security certification / French scheme)
- Include a theoretical analysis of cryptography used in the product
- Practical attacks (including side-channel)

ITSEF analyses (ETR = evaluation technical report) are reviewed by ANSSI

ITSEF licensing process

CCN (ANSSI certification body) supervise the licensing process (ANSSI-CC-AGR-P-01) with ANSSI's experts (licensed ITSEF list)

1. Preliminary audit
   - Technical review
   - Evaluation methodology review
   - (Selection of a "pilot project")
2. Selection and review of a "pilot project"
   - Implementation of technical knowledge and evaluation methodology
3. Final audit
   - Approval (or not) of the specific license

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

3. PQC PRODUCT EVALUATIONS

CCN feedbacks on PQC

2022 – Impact on security visa delivery included in technical papers (see previous slide)

2023 – ITSEF first review and first evaluation

2024 – Discussions with ITSEF (HW & SW) for approval PQC evaluations

– Need to **update licensing process for PQC**

2025 – First ITSEF approval

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Mechanisms based on “well-known” primitives

Hash based signatures:

- XMSS
- LMS
- SPHINCS+

Already used:

- Firmware
- PKI root key

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Upgrade of the cryptographic evaluation license

Cryptography is a specific license

For cryptographic licensing process, we add

- Hash-based signatures
- Hybridation mechanisms

For cryptography review we expect knowledge on

- XMSS/LMS, **RFC 8391** and **8554** (2018)
- NIST Standard **FIPS 205** (SLH-DSA, initially proposed as SPHINCS+)
- Hybridation mechanisms (ways to combine pre and post quantum algorithms)

Less wildly used so far

More or less new mechanisms:

- Code-based (Classic McEliece, BIKE)
- Lattice-based (NTRU, CRYSTALS)
- Isogeny-based (~~SIKE~~, CSIDE)
- Multivariate cryptography (GeMSS, ~~Rainbow~~)
- Braids group (~~WalnutDSA~~)

WARNING, less wildly study (so far)

- Cryptanalysis
- Fault attacks
- Side channel attacks

➢ **Countermeasure? Hybridation!**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

New PQC evaluation license

We have listed lattice-based mechanisms:

- **ML-KEM** (as describe in the **FIPS 203** standard)
- **ML-DSA** (as describe in the **FIPS 204** standard)
- **FrodoKEM** (ISO standardisation in progress)
- **FN-DSA Falcon (alias Falcon** for now, NIST standardisation in progress**)**
- **NTRU Prime** (available in OpenSSH)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

What do we require during an audit

- Basic knowledge of lattice-base primitives (SVP, LWE, etc.)
- Knowledge of lattice-based mechanisms (ML-*, Frodo, etc.)
- State of the art for generic attacks
- Tools for conformity test
- State of the art on implementation mistakes
- State of the art for fault attacks and side channel attacks (for HW ITSEF)
- An evaluation’s methodology

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Otherwise

Non-hash-based or non-lattice-based PQC-mechanism

- ➢ Follow the “unusual crypto-mechanism” analysis
- It is possible to evaluate the product via ANSSI’s experts for instance
- By now, there are no other special evaluation licenses
- Stay in touch! Don’t hesitate to ask!

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

THANK YOU!