RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Transition to post-quantum cryptography (PQC) : Industrial and market challenges

Geoffroy Hermann
Head of « Industry and technologies » Division
French cybersecurity agency (ANSSI)

ANSSI'S WORK ON PQC

The transition to PQC will last more than ten years. It will impact the entire digital ecosystem and will probably require significant financial support.

Objective : support and accelerate the transition to PQC in France

On-going work on a plan for the transition to PQC :

- Working on scientific and technical aspects (currently : integration in protocols) ;
- Working on risk analysis and use case prioritization ;
- Offering PQC-related training course ;
- Working on certification and approval schemes ;
- Following standardization processes ;
- Working at EU level :
  → Joint position papers with other EU NCSA ;
  -> Co-chair of the new PQC workstream of the NIS cooperation group ;
  -> Following Horizon Europe and Digital Europe programs via ECCC.

PQC : CHALLENGES FOR THE MARKET

Objectives :

User side

- Migrating on time (including retroactive attacks).
- Making a successful migration (no loss of availability or integrity).

Supplier side

- Offering trusted products and services.
- Maintaining EU strategic autonomy.
- Turning the technological challenge into an economic opportunity.

MARKET STUDIES CONDUCTED BY ANSSI

- ✓ **3 studies** conducted between July 2023 and January 2024.
- ✓ To be published soon.

Who?

- Cryptographic solution providers (18)
- Final users under ANSSI's scope (50+)
- Services providers (34)

Survey

What?

- Awareness/knowledge
- Migration obstacles
- Needs and expectations

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

1/3

CRYPTOGRAPHIC SOLUTION PROVIDERS

CRYPTOGRAPHIC SOLUTION PROVIDERS

= developers of security products using cryptography

- ✓ Those who implement algorithms based on post-quantum primitives : **crypto « specialists ».**
- ✓ Those who use post-quantum algorithms to integrate them into the protocols of their products.

- **Knowledge and maturity on PQC**
  - Good for crypto specialists and manufacturer of encryption products
  - Note the case for cyber products suppliers
- **Migration obstacles**
  - Lack of standardization (algorithms, protocols and hybridization)
  - Lack of immediate market
  - Unclear impacts on performance and systems
- **Needs and expectations**
  - Implementations of reference for post-quantum algorithms
  - Migration plan (with firmer timeline)
  - Awareness of decision-makers and customers

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

2/3

FINAL USERS

FINAL USERS

= organisations within ANSSI's scope that implement/use crypto

- ✓ Public institutions
- ✓ Regulated operators (public and private) of the following sectors: education & research, defence, industry, health, finance, space, telecom

- **Knowledge and maturity on the subject**
  - >50% are at risk for retroactive attacks
  - No migration plan
  - Strong need for support and advice
- **Migration obstacles**
  - Poor understanding of the issues
  - Lack of resources (financial/human)
  - Lack of consulting services to help with the migration
  - No regulatory obligation
- **Needs and expectations**
  - Awareness on the quantum threat (also for decision-makers)
  - Visibility on the timeline
  - Quantum "generic" risk analysis listing priority use cases

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

3/3

CYBER SERVICES PROVIDERS

SERVICES PROVIDERS

= those who will support organizations in their migration

- ✓ Qualified information systems security audit service providers (PASSI)
- ✓ Security consulting providers (PACS) in a qualification process
- ✓ Cyber products/services evaluation centres (ITSEF)

- **Knowledge and maturity on the subject**
  - Very immature consulting offers (70% have no offer)
  - BUT good knowledge of the threat and challenges
  - AND ready to set up service offers in <2 years.
- **Migration obstacles**
  - No customer demand, no mission carried out yet
  - No perceived interest or urgency among customers
  - No regulatory obligation
- **Needs and expectations**
  - Technical recommendations
  - More awareness
  - Binding regulatory framework
  - Community animation (structuring the community of service providers/consulting companies)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

EXPECTATIONS FOR THE CYBERSECURITY ECOSYSTEM

→ On the industrial side : exchange on industrial roadmaps to refine technical guidelines, provide realistic timeframe.

-> On the user side : inventory of current POCs and advanced users.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

THANK YOU

CONTACT : INDUSTRIES@SSI.GOUV.FR