IBM MQ et PQC
(Post Quantum Cryptography)

Une production : Demey Consulting

Version 1.02 – Mars 2025

Chiffrement classique

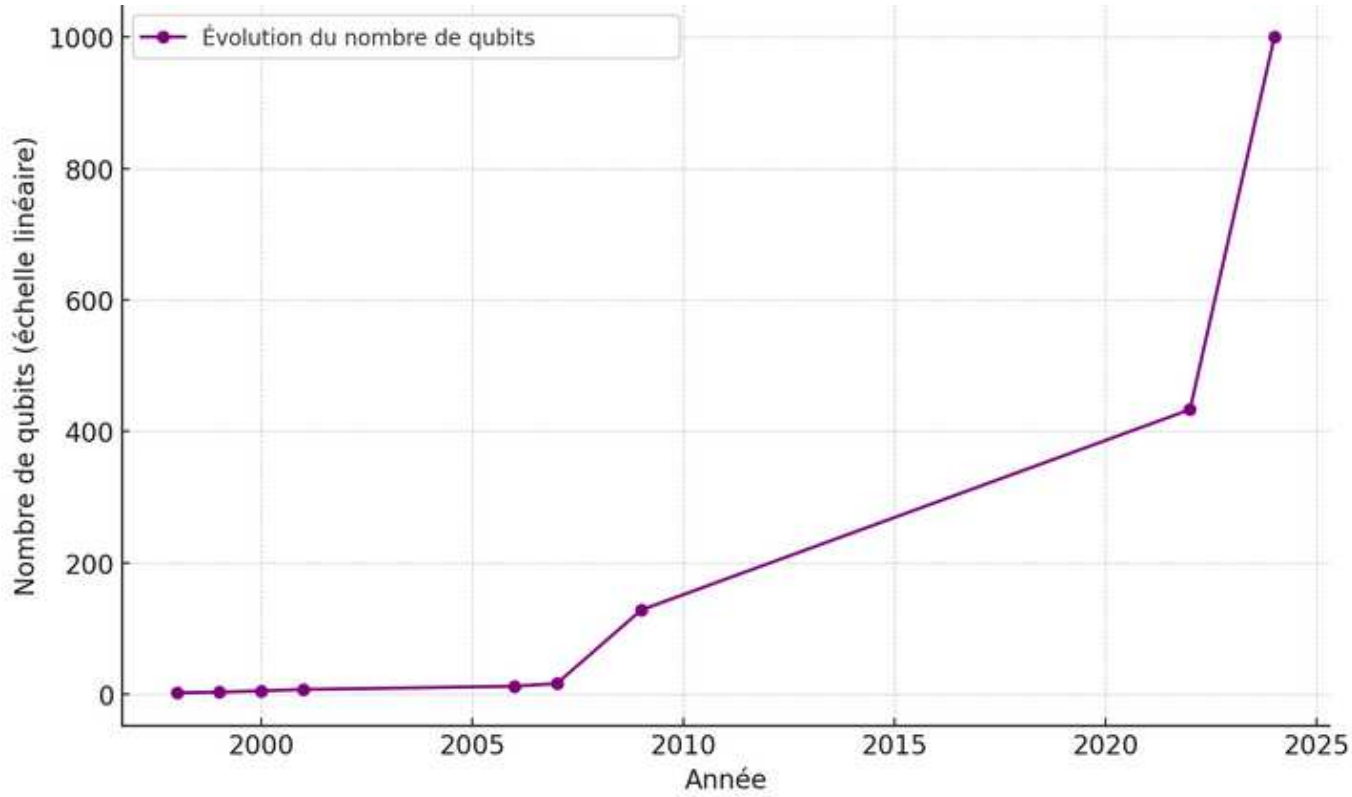
- Aujourd'hui : RSA
  - Clés de 1024 à 4096 bits
  - Standard : 2048 bits
- Repose sur la difficulté de factoriser un grand nombre en deux nombres premiers
- A priori incassable : 1 milliard d'années pour « casser » du RSA 2048 avec des moyens traditionnels

Informatique quantique

- Au stade exploratoire
- Quantum bits or qubits
- Capacité de calcul hautement parallèle
- 1994 : algorithme de Shor
  - Définit comment casser une clé RSA avec un ordinateur quantique
  - Peter Shor, mathématicien américain, montre qu'il est possible de factoriser des grands nombres dans un temps raisonnable à l'aide d'un calculateur quantique
  - Exponentiellement plus rapide que le meilleur algorithme connu tournant sur un ordinateur classique

Evolution du nombre de qubits dans les ordinateurs quantiques

Année	qubits
1998	2
1999	3
2000	5
2001	7
2006	12
2007	16
2009	128
2022	433
2024	1000
2025	?



Impact sur le chiffrement RSA

- On considère qu'il faut 4000 qbits(*) pour casser une clé RSA en 100 secondes
- Cette capacité sera probablement disponible hors des labos vers 2030/2035
- Et un chiffrement RSA-2048 pourra être cassé en quelques heures, voire en quelques minutes

(*) suivant les sources et le type de qubit

Conséquences

- Evolution des algos de chiffrement
  - Passer au chiffrement « post quantique » (PQC)
- Dead line :
  - 2030, 2035, … ?
  - Ou avant ….

Données chiffrées : Durée de protection

Question : Pendant combien de temps les données doivent rester protégées par un chiffrement ?

Bordereau de livraison	5 jours
Paiement sans contact	3 ans
Virements internationaux	10 ans
Données personnelles de santé	20 ans ?
Résultats R&D d'une entreprise	30 ans ?
…	

Harvest Now, Decrypt Later

- Hypothèse :
  - Une organisation « hostile » enregistre aujourd'hui des flux de données en transit, protégés par RSA 2048
- Dans l'état actuel de la technologie, il n'est pas possible de lire ces données
- Dans 5 ans ou 10 ans, la probabilité d'un décodage de ces données via un ordinateur quantique est élevée
- Dans 5 ans ou 10 ans, les données chiffrées aujourd'hui auront-elle encore de la valeur pour cette organisation ?

Captation des données en transit chiffrées

- Les flux concernés sont tous les flux réseau échangés entre les applications, par exemple :
  - http
  - Serveurs d'application (tWAS, Liberty, …)
  - IBM MQ
  - …

Solution : PQC

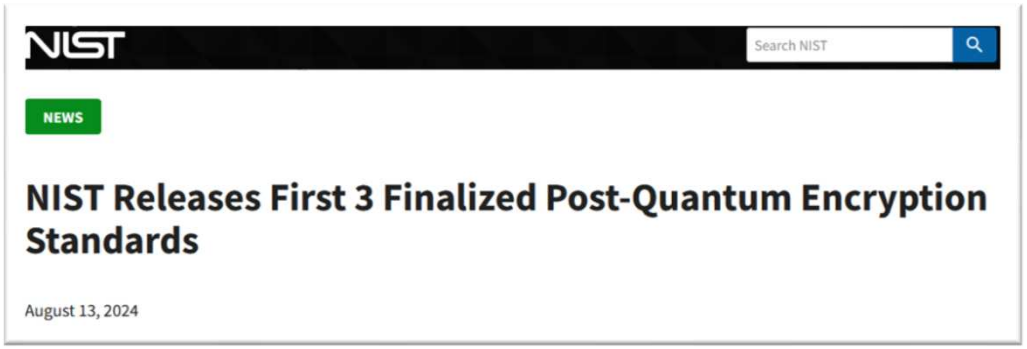
- De nombreuses sociétés (dont IBM) travaillent depuis plusieurs années sur des systèmes de chiffrement résistants aux attaques de type « algorithme de Shor ».

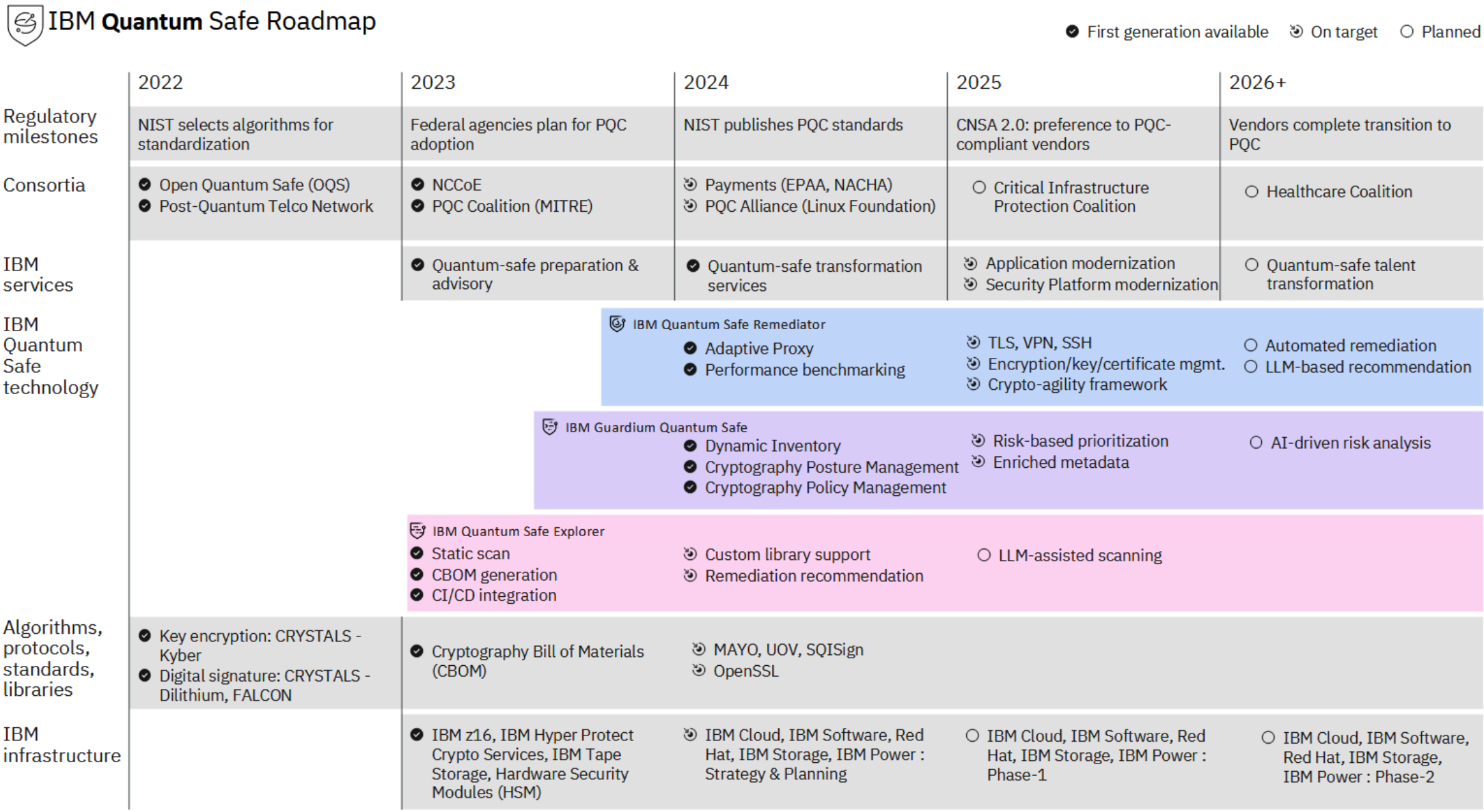
Cryptographie Post Quantique

Post Quantum Cryptography

IBM & PQC

- En 2016, le NIST a lancé un projet pour développer des outils de chiffrement « Quantum Safe »
- En 2024, trois algorithmes résistants ont été annoncés
  - Dont deux développés par IBM




IBM Quantum Safe Roadmap
First generation available
On target
Planned
2022
2023
2024
2025
2026+
Regulatory milestones
NIST selects algorithms for standardization
Federal agencies plan for PQC adoption
NIST publishes PQC standards
CNSA 2.0: preference to PQC-compliant vendors
Vendors complete transition to PQC
Consortia
Open Quantum Safe (OQS)
Post-Quantum Telco Network
NCCoE
PQC Coalition (MITRE)
Payments (EPAA, NACHA)
PQC Alliance (Linux Foundation)
Critical Infrastructure Protection Coalition
Healthcare Coalition
IBM services
Quantum-safe preparation & advisory
Quantum-safe transformation services
Application modernization
Security Platform modernization
Quantum-safe talent transformation
IBM Quantum Safe technology
IBM Quantum Safe Remediator
Adaptive Proxy
Performance benchmarking
TLS, VPN, SSH
Encryption/key/certificate mgmt.
Crypto-agility framework
Automated remediation
LLM-based recommendation
IBM Guardium Quantum Safe
Dynamic Inventory
Cryptography Posture Management
Cryptography Policy Management
Risk-based prioritization
Enriched metadata
AI-driven risk analysis
IBM Quantum Safe Explorer
Static scan
CBOM generation
CI/CD integration
Custom library support
Remediation recommendation
LLM-assisted scanning
Algorithms, protocols, standards, libraries
Key encryption: CRYSTALS - Kyber
Digital signature: CRYSTALS - Dilithium, FALCON
Cryptography Bill of Materials (CBOM)
MAYO, UOV, SQISign
OpenSSL
IBM infrastructure
IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)
IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Strategy & Planning
IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Phase-1
IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power : Phase-2

Impact sur les flux IBM MQ

Avec un chiffrement TLS 2024, les données MQ échangées :

- Via des canaux DQM & cluster MQ
- Via des canaux SVRCONN
- Via des messages chiffrés avec AMS

peuvent être captées pour analyse ultérieure (5 ans +)

→ Nécessite de passer au chiffrement post quantique pour MQ

IBM MQ & PQC

- IBM Hursley : Projet « Quantum Safe communications »
  - https://www.ibm.com/quantum/quantum-safe
  - Concerne également DataPower, …
- Extension du GSKIT pour inclure des algos Quantum Safe
- Algorithmes : CRYSTALS-Kyber et CRYSTALS-Dilithium en version « Round 3 »
- Technical Preview basée sur MQ 9.4.2
  - Permet de tester MQ avec un chiffrement PQC
  - Beta non publique

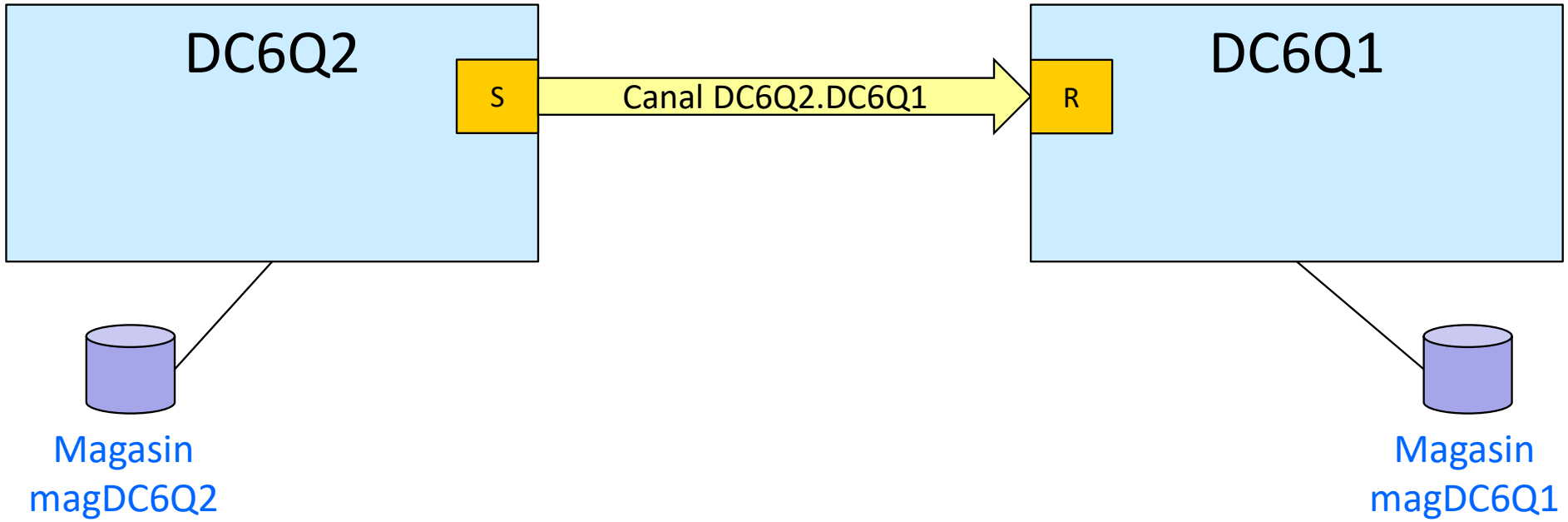
MQ Build 942 QPC Disclaimers

The information in this document has been checked as accurate and current as of February 2025. It is possible that some statements or information in this document may be out of date at the time of reading.

As the following is using technical preview functionality within a third-party library it is subject to change and withdrawal. It also is a work in progress and functionality outside of the scope demonstrated in the example below may be unstable, buggy or non-functional. As such, **this build must not be used within production environments and is supplied as a technical preview for testing only.**

IBM's statements regarding its plans, directions and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

« Démo »



Magasins

- magDC6Q1.p12

```
runmqakm -keydb -create -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd -pqc true
runmqakm -cert -create -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd -dn CN=CA -label ca -ca true
runmqakm -cert -create -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd -dn CN=QMGR -label qmgr -ca_label ca
runmqakm -cert -extract -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd -label ca -file /var/mqm/mags/rsa.cer
```

- magDC6Q2.p12

```
runmqakm -keydb -create -db /var/mqm/mags/magDC6Q2.p12 -pw passw0rd -pqc true
runmqakm -cert -add -db /var/mqm/mags/magDC6Q2.p12 -pw passw0rd -label ca -file /var/mqm/mags/rsa.cer
```

Queue Managers

- DC6Q1

```
runmqsc DC6Q1
ALTER QMGR SSLKEYR('/var/mqm/mags/magDC6Q1.p12') KEYRPWD('passw0rd') CERTLABL('qmgr')
DEFINE CHANNEL(DC6Q2.DC6Q1) CHLTYPE(RCVR) SSLCIPH(ANY_TLS13_OR_HIGHER) SSLCAUTH(OPTIONAL) REPLACE
END
```

- DC6Q2

```
runmqsc DC6Q2
ALTER QMGR SSLKEYR('/var/mqm/mags/magDC6Q2.p12') KEYRPWD('passw0rd')
DEFINE QLOCAL(DC6Q2) USAGE(XMITQ) REPLACE
DEFINE CHANNEL(DC6Q2.DC6Q1) CHLTYPE(SDR) XMITQ(DC6Q2) CONNAME('localhost(14641)') +
   SSLCIPH(TLS_AES_256_GCM_SHA384) REPLACE
END
```

CHSTATUS

```
DISPLAY CHSTATUS(DC6Q2.DC6Q1) SSLCIPH SECPROT
AMQ8417I: Display Channel Status details.
   CHANNEL(DC6Q2.DC6Q1)                    CHLTYPE(SDR)
   CONNAME(127.0.0.1(14641))               CURRENT
   RQMNAME(DC6Q1)                          SECPROT(TLSV13)
   SSLCIPH(TLS_AES_256_GCM_SHA384)         STATUS(RUNNING)
   SUBSTATE(MQGET)                         XMITQ(DC6Q2)
```

Passage en mode « Quantum »

- Mise à jour des certificats

```
runmqakm -cert -create -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd -pqcdemor qmgr
runmqakm -cert -list -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd

Certificates found
* default, - personal, ! trusted, # secret key
-       qmgr-pq-rev
-       ca-pq-rev
-       qmgr
-       ca
```

```
runmqakm -cert -details -label qmgr-pq-rev -db /var/mqm/mags/magDC6Q1.p12 -pw passw0rd
Label : qmgr-pq-rev
Key Size : 256
Version : X509 V3
Serial : ced65b409cdf91e974996a292c41d826b6e7b6659dcf5f3c901aebe8679e91e7
Issuer : CN=CA
Subject : CN=QMGR
Not Before : March 15, 2025 9:44:01 AM GMT+00:00
Not After : March 16, 2026 9:44:01 AM GMT+00:00
Public Key
...
Public Key Type : GSK_Dilithium
(1.3.6.1.4.999999999.999999999.999999999.718375.55524.2.6003), Parameters: GSKASNAny:
GSKASNObject: OBJECT(tag=2, class=0) value: -----BEGIN HEX-----
02 02 01 00                                                ....
Signature Algorithm : GSK_Dilithium_with_SHA256
(1.3.6.1.4.999999999.999999999.999999999.718375.55524.2.6005)
Value
...
```

Activation du PQC

```
DISPLAY CHSTATUS(DC6Q2.DC6Q1) SSLPQC SSLPQCP
AMQ8417I: Display Channel Status details.
   CHANNEL(DC6Q2.DC6Q1)                    CHLTYPE(RCVR)
   CONNAME(127.0.0.1)                      CURRENT
   RQMNAME(DC6Q2)                          STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       SSLPQC(FALSE)
```

```
runmqsc DC6Q1
ALTER QMGR SSLPQC(ENABLED)
END
```

```
runmqsc DC6Q2
ALTER QMGR SSLPQC(ENABLED)
END
```

Vérification du PQC

```
DISPLAY CHSTATUS(DC6Q2.DC6Q1) SSLPQC SSLPQCP
AMQ8417I: Display Channel Status details.
   CHANNEL(DC6Q2.DC6Q1)                    CHLTYPE(SDR)
   CONNAME(127.0.0.1(14641))               CURRENT
   RQMNAME(DC6Q1)                          STATUS(RUNNING)
   SUBSTATE(MQGET)                         XMITQ(DC6Q2)
   SSLPQC(TRUE)                            SSLPQCP(TRUE)
```

Et maintenant ?

Quantum Safe IBM MQ. Actions you can take now.

By Rob Parker posted Mon October 14, 2024 08:23 AM

Quantum computers pose a risk to the protection of data, both at rest and in transit. While today's standards of encryption are sufficient to protect against binary computers, the computational power of Quantum computers break these standards. New quantum resilient encryption algorithms and standards are needed to protect against the Quantum threat.

https://community.ibm.com/community/user/integration/blogs/robert-parker1/2024/10/14/quantum-safe-ibm-mq-actions-you-can-take-now

Liens & Sources

- Cryptographie post-quantique
  - https://fr.wikipedia.org/wiki/Cryptographie_post-quantique
- Qu'est-ce que la cryptographie post-quantique ?
  - https://www.ibm.com/fr-fr/topics/quantum-safe-cryptography
- Algorithme de Shor
  - https://fr.wikipedia.org/wiki/Algorithme_de_Shor
- Make the world quantum safe (roadmap)
  - https://www.ibm.com/quantum/quantum-safe
- NIST Releases First 3 Finalized Post-Quantum Encryption Standards
  - https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- Quantum Safe IBM MQ. Actions you can take now
  - https://community.ibm.com/community/user/integration/blogs/robert-parker1/2024/10/14/quantum-safe-ibm-mq-actions-you-can-take-now
- ChatGPT (pour les graphiques)
- Midjourney (pour les images)

Fin du module

Page blanche intentionnellement