Compliance Brief

Complying with the MAS Advisory On Addressing The Cybersecurity Risks Associated With Quantum

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What is the Advisory?

On 20th February 2024, The Monetary Authority of Singapore (MAS) issued Circular No. MAS/TCRS/2024/01 on Advisory On Addressing The Cybersecurity Risks Associated With Quantum ("Advisory") to CEOs of financial institutions ("FIs"), urging them to address cybersecurity risks arising from developments in quantum computing, and highlights mitigating measures that financial institutions should consider.

The Advisory from MAS sets the scene by highlighting the recognized risks associated with the advent of quantum computers – specifically the threat posed to conventional asymmetric cryptography used widely in today's public key infrastructure with two core recommendations on attaining cryptographic agility and implementing quantum security.

The advisory highlights three initiatives to attain crypto-agility that FIs should consider as part of their quantum transition efforts:

- Keep abreast of the latest developments in quantum computing and raise awareness of the associated cybersecurity risks.
- Maintain an inventory of all cryptographic assets and identify priority assets for migration to a quantum-resistant state.
- Develop strategies and build capabilities to address the cybersecurity risks associated with quantum.

How can Thales help with Advisory on Addressing The Cybersecurity Risks Associated With Quantum?

Thales is committed to delivering solutions that support a Post-Quantum crypto agile strategy and secure FIs against quantum threats requires cybersecurity solutions that support Quantum Resistant Algorithms (QRA), and also offer options for Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG).

Building a Future-Proof Quantum Strategy

- **Quantum-Resistant Algorithms:** QRAs are fundamental to protecting against quantum attacks, whether using Lattice based, Multivariate, Hash based, or Code-based cryptography
- **Quantum Random Number Generation:** QRNG is a high bit rate random number source harnessing the inherent randomness in quantum mechanics to create encryption keys
- **Quantum Key Distribution:** QKD distributes encryption keys between shred parties based on the principles of quantum physics and the properties of quantum mechanics

Thales helps FIs address the three initiatives to attain crypto-agility.

Advisory On Addressing The Cybersecurity Risks Associated With Quantum	Thales Solutions
1.Keeping abreast of the latest developments in quantum computing "...possible mitigation using quantum security solutions such as PQC and QKD..." "...requesting that vendors provide quantum-resistant solutions when they become commercially available ..."	Thales Luna HSMs and High-speed Encryptors provide a crypto-agile approach to ensure PQC-readiness for FIs. • Fortify your encryption keys with Quantum-safe **Thales Luna HSM** which is commercially available with NIST quantum-resistant finalist algorithms added. ◦ Quantum-Resistant Algorithms (QRA) with PQC FM with Hash Based Signing (SP800-208) ◦ Integrated/ Custom-made PQC: Implement your own Post- Quantum Crypto using Luna's Functionality Module (FM) or with various Partner FMs/integrations ◦ QRNG: Inject quantum entropy with QRNG and Luna HSM's secure key storage • Secure Data in Transit with **Thales High Speed Encryption (HSE) network encryption** solutions that support Post-Quantum Cryptography (PQC) with a crypto-agile, FPGA-based architecture. HSE is the first commercially available quantum-resistant network encryption solution, providing FIs with long-term data protection today against future quantum attacks. It offers FIs a single platform to encrypt everywhere – from network traffic between data centers and headquarters to backup and disaster recovery sites, whether on-premises or in the cloud.

Advisory On Addressing The Cybersecurity Risks Associated With Quantum	Thales Solutions
2. Maintaining an inventory of cryptographic assets "...**Identifying and maintaining an inventory of cryptographic solutions** used in the FI, and determining those which are potentially vulnerable and need to be **replaced with quantum-resistant alternatives** when the solutions become commercially ..." "... **Classifying IT and data assets** that are dependent on the **potentially vulnerable cryptographic** solutions..." "...Assessing whether existing system infrastructures can support crypto-agility, and consider upgrading them over time ..."	FIs can achieve crypto-agility and maintain the inventory of cryptographic assets with Thale's key management and quantum-safe solutions. • FIs can rely on **Thales key management** to keep an inventory of cryptographic assets. Leveraging FIPS 140-2-compliant virtual or hardware appliances, **Thales key management** tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. • PQC Ready **Thales Luna HSM** protects encryption keys with centralized key management and helps FIs manage the cryptographic assets inventory effectively. Luna HSM provides FIs visibility to the cryptographic algorithms and key lengths that are in use, the ownership and responsible parties for maintaining cryptographic assets, and the specific system or application where the cryptographic algorithm is embedded or used. • Asymmetric crypto for PIN or password transmission is vulnerable in quantum computing. A hybrid key establishment solution with key material protected by a **Luna HSM** can mitigate the risks, it supports quantum-safe algorithms and contains multiple options for key agreement and key transport based on different mathematical problems that create a strong quantum-safe solution. • **Thales High Speed Encryption (HSE) network encryption** solutions protect data in motion and support all four NIST Quantum Resistant Public Key algorithms (finalists) in all products (plus other non-finalist algorithms) with a crypto-agile, FPGA-based architecture. HSE is quantum-ready and QKD compatible for more than a decade with Quantum Random Number Generation (QRNG) integrated.
3. Developing strategies and building capabilities to address cybersecurity risks associated with quantum "...Uplifting the **technical competencies**..." "...Where resource permits, **consider proof-of-concept trials with quantum security solutions** to sensitize the FI on their potential impact ..."	**PQC starter kit** allows FIs to develop and build capabilities to test quantum-safe solutions safely. Thales **PQC starter kit** that partners with Quantinuum accelerates the process of testing quantum-resilient measures in a safe environment. The kit helps you set up a trusted environment in a trusted Luna HSM to test PQC-ready keys to understand the implications of these changes for your infrastructure without impacting key management processes in production environments.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us