cpl.thalesgroup.com

THALES
Building a future we can all trust

Complying with the Guidelines for Virtual Asset Trading Platforms (VATPs) Operators in Hong Kong

What are the Guidelines for Virtual Asset Trading Platforms (VATPs) Operators?

The Hong Kong Securities and Futures Commission (SFC) has issued regulatory guidance for operators of Virtual Asset Trading Platforms (VATPs) in the form of guidelines, FAQs and handbooks on 1st June 2023. The SFC is one of the first and few regulatory authorities in a major jurisdiction to introduce a comprehensive regime regulating a wide range of virtual asset-related activities. The fact that SFC is providing clear regulatory expectations is critical to fostering responsible development, especially within Hong Kong's virtual assets ("VA") landscape. Adopting the principle of 'same business, same risks, same rules', the SFC aims to support and develop the VA industry by ensuring robust investor protection and critical risk management.

All centralized VATP exchanges which operate in Hong Kong or actively market to Hong Kong investors must be licensed by the SFC. VATP license applicants must submit a robust license application that proves it can meet all of the conditions, or it risks being ineligible for the arrangement by 31st May 2024. Guidelines for Virtual Asset Trading Platforms (VATPs) Operators set out, among others, safe custody of assets, segregation of client assets, avoidance of conflicts of interest and cybersecurity standards and requirements expected of licensed trading platforms.

Virtual Asset Trading Platform Operators

Under the Securities and Futures Ordinance (Cap. 571) (SFO) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO), centralized virtual asset trading platforms carrying on their businesses in Hong Kong, or actively marketing their services to Hong Kong inverstors, are required to be licensed and regulated by the SFC.

How can Thales help VATPs Operators?

Thales helps organizations comply with Guidelines for VATPs Operators by addressing cybersecurity requirements for the Custody of Client Assets and Security of the Platform. VATPs Operators can leverage Thales' suite of identity and data security solutions to become compliant today and stay compliant in the future.

Guidelines for VATPs Operators	Thales Solution
X. Custody of Client Assets – Client virtual assets	
10.6 (c) "The Platform Operator and its Associated Entity should store 98% of client virtual assets in cold storage (such as Hardware Security Module (HSM) - based cold storage)..."	**Secure cold storage with Thales Hardware Security Modules (HSM) with Native Blockchain Algorithm Support BIP32, Milenage and Tuak algorithms and SECP256k1 elliptic curve** • **Luna Network HSMs** are designed to store the private keys used by blockchain members to sign all transactions in a FIPS 140-2 Level 3 dedicated cryptographic processor. Keys are stored throughout their lifecycle; ensuring cryptographic keys cannot be accessed, modified or used by unauthorized devices or people. • **ProtectServer HSMs**, like the Luna Network HSMs, are designed to protect cryptographic keys against compromise while providing encryption, signing, and authentication services. Both Luna and Protect Server HSMs extend native HSM functionality by enabling the development and deployment of custom code within the secure confines of the FIPS 140-2 Level 3 validated Thales HSM as a part of the firmware. Functionality Modules (FMs) allow you to customize your Thales HSM's functionality to suit the needs of your organization, including the implementation of Quantum algorithms.
10.8 (a) "...seeds and private keys should be generated offline and kept in a secure environment, such as a HSM, with appropriate certification for the lifetime of the seeds or private keys."	
10.8 (b) "...authenticate authorised personnel for access to applications governing the use of private keys."	**Seamless integration of authentication and HSMs to achieve trusted identity and access management** • **SafeNet Trusted Access (STA)** delivers fully-automated, highly secure authentication-as-a service with flexible token options. STA with on-premise and SaaS authentication server solution options is tailored to the unique needs of your organization, substantially reducing the total cost of operation.

10.8(d)
"The backups should be stored in a protected form on external media (preferably HSM with appropriate certification)."
	Store backups on external HSMs with the options below:
	• Backup easily and duplicate keys securely to the **Luna Backup HSM** for compliance as well as safekeeping in case of emergency, failure or disaster. Luna Backup HSM provides the highest security & compliance.
	  ◦ Keys always remain in FIPS 140-2 Level 3 certified, intrusion-resistant, tamper-evident hardware
	  ◦ Remote management, backup and restoration for quick disaster recovery
	  ◦ LCD touch screen enables quick review of status including firmware, memory capacity, and more
	  ◦ Standalone support of Quorum (MofN) multi-factor authentication for increased security
	• **Thales ProtectServer HSM** uses Smart Cards which provide the highest security and administrative convenience for secure backup, recovery, and transfer of cryptographic keys.

10.8(e)
"Seeds and private keys are securely stored in Hong Kong"
	Store cryptographic keys securely with on-premises options
	• **Luna Network HSMs** & **ProtectServer HSMs** with on-premise options secure and store seeds and private keys, both the HSMs support BIP32 and use Functionality Module (FM) to securely perform custom cryptography, or add custom blockchain algorithms.
	  ◦ **Luna Network HSMs** secure sensitive data and critical applications by storing, protecting, and managing cryptographic keys – high assurance, tamper-resistant, network-attached appliances offering market-leading performance.
	  ◦ **ProtectServer HSMs** are designed to protect cryptographic keys while providing encryption, signing, and authentication services.

Guidelines for VATPs Operators	Thales Solution
XII. Cybersecurity – Security of platform	

12.12 (a) i
"...robust authentication and authorisation methods and technology to ensure that access to the platform is restricted to authorised persons only on a need to-have basis..."
 	
12.12 (a) ii
"...adopt appropriate user authentication method to enable the relevant user to be uniquely identified..."
 	
12.12 (a) iv
"maintain an adequate access log which records the identity and role of the staff members who have access to its platform, the information accessed, the time of access,..."
 	
12.12 (b)
"two-factor authentication..."
	Security control with robust authentication, role-based access control and audit logging
	• **Thales OneWelcome identity & access management** solutions limit the access of internal and external users based on their roles and context. Backed by strong multi-factor authentication (MFA) and broadest range of authentication methods and form factors (such as Passwordless Devices) , granular access policies and fine-grained authorization policies help ensure that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. A full audit trail of access events as well as automated log are available for export and seamless integrations with SIEM systems.
	  ◦ **SafeNet Trusted Access (STA)** delivers fully-automated, highly secure authentication-as-a service with flexible token options. STA is tailored to the unique needs of your organization, substantially reducing the total cost of operation.
	  ◦ **Certificate-based USB tokens** offers strong multi-factor authentication in a traditional token form factor, enabling organizations to address their PKI security needs. Thales eToken offers strong authentication and applications access control, including remote access, network access, password management, network logon, as well as advanced applications including digital signature, data and email encryption.
	• Both **Luna Network HSMs** & **ProtectServer HSMs** offer Role-Based Access Control for strong separation of duties, Multi-person MofN with multi-factor authentication for increased security & Secure audit logging.
	• **CipherTrust Manager** offers enterprise key management solutions enabling organizations to centrally manage encryption keys, provide granular access control, configure security policies and role-based access control to keys and policies.

Guidelines for VATPs Operators	Thales Solution
12.12 (g) "up-to-date data encryption and secure transfer technology... In particular, the Platform Operator should use a strong encryption algorithm"	DATA ENCRYPTION **Secure files and backup on OS with data encryption** • **CipherTrust Transparent Encryption (CTE)** provides transparent and continuous file-level encryption that protects against unauthorized access by users and processes in physical, virtual, and cloud environments. It is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. CTE secures structured databases and unstructured files across data centers, cloud, containers and big data environments on Linux, Windows, Unix and AIX with a single infrastructure and management environment. **Protect database with Transparent Database Encryption (TDE) for MS SQL and Oracle** • Whether you're running Oracle, Microsoft SQL Server environments, or any combination thereof, **CipherTrust Transparent Encryption** secures sensitive data in databases across your enterprise and offers the capabilities you need to employ strong database encryption, privileged user access controls and detailed data access audit logging, with no changes to applications and minimal performance implications. **Robust key lifecycle management for database solutions and KMIP clients in hybrid environments** • **CipherTrust Manager** is an Enterprise Key Management (EKM) solution that enables a single, centralized platform for managing cryptographic keys and applications. ◦ centralizes encryption key management for Oracle Database and Microsoft SQL Server TDE as well as a variety of additional Thales and third-party encryption solutions ◦ support Key Management Interoperability Protocol (KMIP) for key life-cycle management between encryption systems and enterprise applications, such as MySQL, MongoDB, SAN storage VMWare Infrastructure, Tape Libraries, and more ◦ allow administrators to simultaneously manage multiple, disparate encryption appliances and associated keys through a single, centralized key management platform • **CipherTrust Cloud Key Management (CCKM)** offers keys lifecycle control, centralized management within and among clouds, and visibility of cloud encryption keys. It protects your time as well as your data with a single pane of glass view across regions for cloud native, BYOK and HYOK keys and one straightforward UI to manage all cloud Key Management Services. • **CipherTrust Secrets Management (CSM)** protects and automates access to secrets across DevOps tools and cloud workloads including secrets, credentials, certificates, API keys, and tokens. The solution is powered by Akeyless Vault easily integrates with other third-party applications such as GitHub, Kubernetes, OpenShift and more. SECURE TRANSFER **Tokenization solution to tokenize and mask sensitive & PII data to comply with regulatory requirements** • **CipherTrust Tokenization** makes it simple to secure sensitive data with masking capability protecting data in use including personally identifiable information (PII). It secures and anonymizes sensitive assets—whether they reside in the data center, big data environments or the cloud. **Protect data and encrypt data-in-transit between applications among Bare Metal, Virtual Machine and Container Kubernetes environments with Application Data Encryption and Data Protection Solutions** • **CipherTrust Application Data Protection** offers developer-friendly software tools for application-level encryption of sensitive data and provides the highest level of security, as it can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy. • **CipherTrust Data Protection Gateway (DPG)** protects the data at the earliest possible point, allowing the data to travel securely through the solution to its destination. DPG offers transparent data protection to any RESTful web service or microservice leveraging REST APIs, it is deployed as a container and is fully compatible with Kubernetes orchestration systems such as Helm, Ansible and Terraform, and, of course, Kubernetes horizontal scaling.

Guidelines for VATPs Operators	Thales Solution
12.12 (g) "up-to-date data encryption and secure transfer technology... In particular, the Platform Operator should use a strong encryption algorithm"	**Secure data-in-transit in different geographical locations** • Thales **High Speed Encryptor (HSE)** provides network-independent, data-in motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site to site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception – without performance compromise.
12.12 (h) "...up-to-date security tools to detect, prevent and block any potential unauthorised intrusion, security breach and cyberattack attempts..."	**Security tools to detect and block unauthorized access** • **Luna Network HSMs** & **ProtectServer HSMs** provide the highest level of security by always storing cryptographic keys in hardware. HSMs ensure absolute trust by securing cryptographic keys and identities in a hardware root of trust, which are intrusion-resistant, tamper-evident and FIPS-validated appliance. • **CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)** continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers. It monitors active processes to detect ransomware – identifying activities such as excessive data access, exfiltration, unauthorized encryption, or malicious impersonation of a user, and alerts/blocks when such an activity is detected.
12.15 (a) "The usage capacity of the platform is regularly monitored..."	**Monitor the platform with centralized HSM management solution for compliance and visibility** • Centralize your crypto management HSM resources and reduce IT security infrastructure costs with **Crypto Command Center**, which provides visibility across device pools through easy monitoring and reporting, export logs for monitoring and analysis systems including Splunk and increased security and sharing of hardware through multi-tenancy with role separation.

About Thales

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.

Decisive technology for decisive moments.