Compliance Brief

THALES

CYBERSECURITY

Complying with The Digital Asset Basic Act of Korea

cpl.thalesgroup.com

THALES

CYBERSECURITY

The Digital Asset Basic Act of Korea (DABA) – the country's first comprehensive law for digital assets was passed on June 10th, 2025. The DABA will complement the Korean Virtual Asset User Protection Act (VAUPA) and create clearer licensing, reserve, and operational obligations for stablecoin issuers and other digital asset businesses.

What is the Digital Asset Basic Act (DABA) of Korea?

The DABA provides a comprehensive framework for Korea's digital asset ecosystem, defining asset types by legal and economic characteristics, setting licensing and conduct standards for Virtual Asset Service Provider (VASPs), and outlining rules on issuance, circulation, disclosure, and unfair trading practices. Its goals are to:

- **Define digital assets** more broadly than VAUPA, including stablecoins, NFTs, and certain tokenized assets.
- **Establish licensing requirements** for issuers, custodians, and trading platforms.
- **Set prudential standards** for reserve management, disclosures, and audits.
- **Create a supervisory authority** for the Financial Services Commission (FSC) to regulate and sanction violations.

There are three Stablecoin Bills built on DABA, each with specific rules for stablecoins, such as issuance, reserves, and payments, and they formed a layered system for digital assets in Korea:

Three Stablecoin Bills built on DABA:

- Act on Payment Innovation Using Value-Pegged Digital Assets
- Act on Value-Stable Digital Asset Issuance Business
- Act on the Issuance and Distribution of Value-Stable Digital Assets

The Korean Virtual Asset User Protection Act (VAUPA), which has been effective since July 2024, focuses primarily on user protection, exchange registration, and unfair trading practices. The Digital Asset Basic Act (DABA) aims to fill gaps by addressing issuance, reserve backing, and systemic risk. It essentially regulates stablecoins in much the same way as other financial instruments.

How Thales Helps with the Provisions in the Digital Asset Basic Act (DABA) Compliance

Thales' solutions can help organizations address the Provisions in Section 3 of the DABA by simplifying compliance and automating security, reducing the burden on security and compliance teams. The solutions deliver crypto-agility, enabling the seamless adoption of post-quantum encryption algorithms through firmware updates rather than hardware replacement, and ensuring organisations can maintain strong cryptographic controls, minimize operational disruption, and stay aligned with evolving standards and threats.

The Provisions	How Thales Helps	Solution Areas
Article 54: Selection, Use, and Management of Access Media 1. "... when conducting transactions ... in an automated manner, select, use, and manage access media and **verify the user's identity, authority, and transaction instructions**..." 2. "... When issuing access media ... shall issue them only upon the user's request and after **verifying their identity**..." 3. **No one shall engage** in the following acts ... managing access media: • "...Transferring or receiving..." • "... Lending or borrowing ... in exchange for compensation..." • "...Lending or borrowing ... for criminal purposes..." • "... collateral for pledge"	• Limit access to systems and data based on **roles and context** with policies. • Apply **contextual security measures** based on risk scoring. • Centralize **access policies and enforcement** to multiple hybrid environments in a single pane of glass. • Enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who accesses what data, when, and what was done to the data. • Provide a **unified strategy** for access control across all user populations. • Enable a consistent and **policy-driven approach** to identification, authentication, and authorization of all users to their IT assets, data, and services. • **Manage all users**, including the workforce, contractors, third-party users such as customers, suppliers, logistics, and B2B or B2C type users.	**Data Security** Data Activity Monitoring Data Risk Analytics Transparent Encryption **Identity & Access Management** Authenticators Identity Verification Multi-Factor Authentication Thales OneWelcome Identity Platform Workforce Access Management

The Provisions	How Thales Helps	Solution Areas
Article 55: Obligation to Ensure Security 1. "... ensure that transactions are **processed securely** when conducting electronic transactions..." 2. "... comply with standards set by the Financial Services Commission regarding **authentication method**s, including the use of certificates under the **"Digital Signature Act", and IT infrastructure...**" 3. "... Digital asset operators designated by Presidential Decree shall **annually establish plans for IT infrastructure** ... and submit them to the Financial Services Commission..."	• Protect private keys associated with the **digital signatures** and secure cryptographic operations in a **FIPS 140-3 Level 3** validated tamper-resistant device. • **Manage encryption keys** centrally, provide granular access control, and configure security policies. • Detect and alert administrators if **abnormal access attempts** are found, and administrators can respond quickly. • Detect and pinpoint **critical threats to data**, prioritizes what matters most, and provides actionable insights. • **Record access** and detect login attempts on the database system. • Flag **access anomalies** for investigation by the security team, and integrate seamlessly with SIEM solutions for a more comprehensive approach to threat and anomaly detection. • Manage and **monitor access controls** to enterprise-wide systems effectively and **log all user access** and authentication activities. • **Produce audit trail and reports** of all access events to all systems, **stream logs** to external SIEM systems. • Manage authentication and access control by supporting **Multi-Factor Authentication** and Single Sign-On (**SSO**) and displaying access log reports. • Offer a **high level of assurance** of the user identity attempting to gain logical access to the network with PKI certificate-based smart cards.	**Data Security** Data Activity Monitoring Data Risk Analytics File Activity Monitoring Hardware Security Modules Key Management Transparent Encryption **Identity & Access Management** Adaptive Access Control Authentication Service – Private Cloud Multi-Factor Authentication PKI certificate-based smart cards Risk-Based Authentication Single Sign-On (SSO) Workforce Access Management
Article 57: Vulnerability Analysis and Assessment of IT Facilities 1. "... analyze and assess the following matters regarding **electronic financial infrastructure** ... and report the results to the Financial Services Commission (FSC): • Organization, facilities, and **internal controls** • Electronic devices and **access media** • **Incident response measures** for digital asset operators • Other matters **prescribed by Presidential Decree** 2. "...establish and **implement remediation** plans based on the vulnerability analysis and assessment results..."	• Offer **advanced API Verification capabilities** to strengthen your defenses against potential vulnerabilities. • Run **assessment tests** on data stores such as MySQL or so to scan for known vulnerabilities. • **Scan your databases** with over 1,500 predefined vulnerability tests based on CIS and PCI-DSS benchmarks to help you keep your databases covered for the latest threats. • Integrate **bot protection, API security**, and machine learning to safeguard against all **OWASP Top 10 threats**. • Protect applications immediately, reducing the urgency of manual code updates with **Virtual Patching**.t	**Application Security** API Security Web Application Firewall **Data Security** Data Activity Monitoring

The Provisions	How Thales Helps	Solution Areas
Article 58: Prohibition of Electronic Infringement Acts 1. **No one** shall engage in the following acts: • "**Unauthorized persons accessing digital asset…** or authorized persons exceeding their authority to manipulate, destroy, conceal, or leak stored data…" • "…Introducing programs such as computer viruses, logic bombs, or mail bombs **to destroy data or disrupt the operation…**" • "…errors or failures in electronic financial infrastructure … to **disrupt stable operation** of IT facilities…" 2. "… be **liable for damages** to users resulting from the following …" • "…. caused by f**orgery or alteration** of access media…" • "… occurring during electronic **transmission** or processing of contracts or transaction **instructions**…" • "…caused by **failure to report** or **false reporting** of security incidents to the FSC or Korea Internet & Security Agency (KISS)…" • "… **malfunction** of electronic devices, information and communication networks, and information and communication equipment … or loss of information…" • "… caused by the use of **access media** obtained intentionally or negligently by a **third party … operators …**"	• Monitor API activity, track usage, **detect anomalies**, and identify potential unauthorized access attempts. • **Safeguard** critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic. • **Detect system threats** with Web Application Firewall, API Security and Database Security and stream logs to SIEM system. • **Encrypt data** to protect against unauthorised disclosure and access, even from the third party providers. • **Pseudonymize sensitive data** once it is created and make sure cleartext data will not be processed or stored by unauthorized and to prevent exposure of real data applications and personnel. • Gain **full sensitive data activity visibility** and enable **continuous monitoring** to capture and analyze all data store activity, providing **detailed audit trails** that show who accesses what data, when, and what was done to the data. • Monitor 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. • Offer FIPS 140-3 Level 3 **root of trust** for credentials and encryption keys. • Secure **data in transit** at Layers 2, 3, and/or 4 without slowing down the network. • Protect data with **real-time alerting or user access blocking** of policy violations. • Pinpoint **risky data access activity** for all users, including privileged users. • Enforce **user rights management** based on data type and user role and produce reports for audit trails. • **Record all changes** to permissions, along with the identity of the perpetrator and session details. • **Apply contextual security** measures based on risk scoring. • **Monitor user behavior** such as admin login from a new location/IP or a wrong system access pattern to alert and prevent attacks.	**Application Security** API Security DDoS Protection Web Application Firewall **Data Security** Data Activity Monitoring Data Risk Analytics File Activity Monitoring Hardware Security Modules High-Speed Encryption Tokenization Ransomware Protection Transparent Encryption **Identity & Access Management** Adaptive Access Control Delegated User Management Fraud & Risk Management Workforce Access Management
Article 78: Long-term Retention and Integrity of Transaction Records	• Gain visibility by monitoring and **auditing all database activity**. • **Produce audit trail and reports** of all access events to all systems, **stream logs** to external SIEM systems. • Provide a **clear audit trail** for demonstrating cryptographic control from centralized key management systems, logging all key lifecycle events such as key creation, rotation, and access. • Offer **encryption logs**, data access attempts, and encryption/decryption events, providing auditable proof of data protection **without application modifications**.	**Data Security** Data Activity Monitoring Key Management Transparent Encryption

The Provisions	How Thales Helps	Solution Areas
Article 94: Compliance Matters for Digital Asset Wallet Management Operators 1. "... shall not engage in the following..." • Storing users' digital assets • Depositing or withdrawing digital assets using users' digital asset wallets without their consent • Other acts prescribed by Presidential Decree that may harm user protection or transaction order	• **Secure users' digital assets** by storing, protecting and managing private keys and seeds of wallets with Hardware Security Modules (HSM) and ensure that cryptographic keys cannot be accessed, modified or used by unauthorized devices or people. • Offer **tamper-evident hardware** protection, which is critical for digital signing solutions. • Protect the **entire lifecycle** of the **cryptographic** keys to sign transactions in a FIPS 140-3 dedicated cryptographic module to secure client digital assets. • **Protect cryptographic keys** against compromise while providing encryption, signing, and authentication services. • Streamline **key management** on-premises and in the cloud environments with key lifecycle management. • Adopt **Post-Quantum Agility** to deal with the threats from quantum computing.	**Data Security** Cloud Key Management Hardware Security Modules Key Management

Three Stablecoin Bills built on DABA:

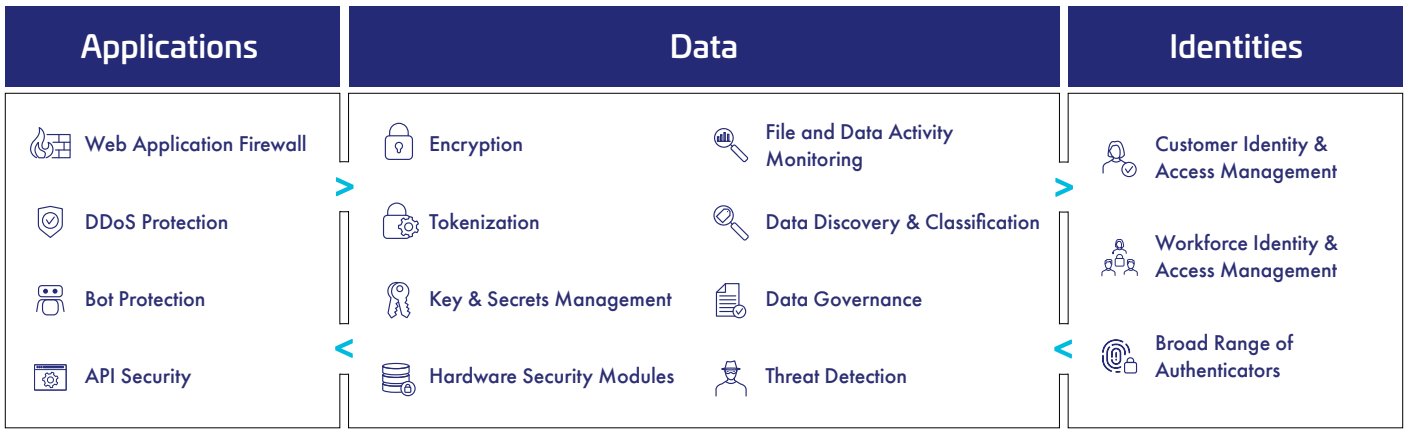
Requirements in Three Stablecoin Bills	How Thales Helps	Solution Areas
Act on the Issuance and Distribution of Value-Stable Digital Assets		
Article 5: Anti-Money Laundering (AML) and Travel Rule Compliance	• Adopt robust **user authorization and authentication** based on the criticality of IT assets by defining the right access policies, step-up authentication, and enforcing phishing-resistant authenticators.	**Identity & Access Management** SafeNet Trusted Access (STA)
Article 16: • Management and Isolation of Reserve Assets • Transparency and Integrity of Disclosures	• Ensure complete **separation of roles** between cloud provider admins and your organization, and restrict access to sensitive data. • **Protect the root-of-trust** of a cryptographic system within FIPS 140-2 Level 3 - a highly secure environment.	**Data Security** Hardware Security Modules Transparent Encryption
Article 18: Obligation of Redemption and Service Continuity	• Offer FIPS 140-2 Level 3 **root of trust** for credentials and keys. • Provide a **single-pane view of access events** across your app estate to ensure that the right user can access the right application at the right level of trust.	**Data Security** Hardware Security Modules **Identity & Access Management** SafeNet Trusted Access (STA)
Article 20: Internal Control and Segregation of Duties (SoD)	• **Simplify key management** across on-premises and multi-cloud deployments by centralizing control on the FIPS 140-2 Level 3 environment. • **Enforce separation of duty** between your data and external party by securely storing encryption keys outside of the corresponding cloud with the Hold-Your-Own-Key (HYOK) approach.	**Data Security** Key Management

Requirements in Three Stablecoin Bills	How Thales Helps	Solution Areas
Article 23: Long-term Retention and Integrity of Transaction Records	• Gain visibility by monitoring and **auditing all database activity**. • **Produce audit trail and reports** of all access events to all systems, **stream logs** to external SIEM systems. • **Prevent unauthorized access** and alteration to its internals, including the audit logs. • Provide a **clear audit trail** for demonstrating cryptographic control from centralized key management systems, logging all key lifecycle events such as key creation, rotation, and access. • Offer **encryption logs**, data access attempts, and encryption/decryption events, providing auditable proof of data protection **without application modifications**.	**Data Security** Data Activity Monitoring Key Management Transparent Encryption
Article 32: Priority Claims and System Stability	• **Monitor API activity,** track usage, detect anomalies, and identify potential unauthorized access attempts. • **Safeguard** critical network assets from **DDoS attacks and Bad Bots** while continuing to allow legitimate traffic.	**Application Security** API Security DDoS Protection Web Application Firewall
Act on Value-Stable Digital Asset Issuance Business		
Article 5: Internal Control and Segregation of Duties (SoD)	• Ensure complete **separation of roles**, and restrict access to sensitive data.	**Data Security** Key Management
Article 19: Anti-Money Laundering (AML) and Travel Rule Compliance	• Adopt robust **user authorization and authentication** based on the criticality of IT assets by defining the right access policies, step-up authentication, and enforcing phishing-resistant authenticators.	**Identity & Access Management** SafeNet Trusted Access (STA)
Article 25: Obligation of Redemption and Service Continuity	• Store, protect, and manage **private keys and seeds of wallets** with FIPS 140-2 Level 3 - a highly secure environment. • **Protect the entire lifecycle** of the keys to sign transactions in a dedicated cryptographic module to secure client digital assets. • Offer **a single-pane view of access** events across your app estate to ensure that the right user can access the right application at the right level of trust.	**Data Security** Hardware Security Modules **Identity & Access Management** SafeNet Trusted Access (STA)
Article 33: Transparency and Integrity of Disclosures	• **Encrypt sensitive data** to minimize the impact of data leakage, ensuring leaked information remains unusable. • Ensure complete **separation of roles**, and restrict access to sensitive data.	**Data Security** Transparent Encryption

Requirements in Three Stablecoin Bills	How Thales Helps	Solution Areas
Act on Payment Innovation Using Value-Pegged Digital Assets		
Article 13: Management and Isolation of Reserve Assets	• Secure sensitive data and critical applications by **storing, protecting, and managing cryptographic keys** – high assurance, tamper-resistant, network-attached appliances offering market-leading performance.	**Data Security** Hardware Security Modules
Article 21: Priority Claims and System Stability	• **Discover and classify** potential risks for all public, private, and shadow APIs. • Safeguard critical network assets from DDoS **attacks and Bad Bots** while continuing to allow legitimate traffic. • Detect and prevent cyber threats with **web application firewall**, ensuring seamless operations and peace of mind.	**Application Security** API Security DDoS Protection Web Application Firewall

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

Security for What Matters Most



Application Security: Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, APIs, and a secure Content Delivery Network (CDN).

Data Security: Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

Identity & Access Management: Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

Organizations can leverage Thales' suite of identity, application and data security solutions available on a single unified platform to become compliant today and stay compliant in the future. Contact us now!

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.