

Standard Requirements for Token Securities Distributed Ledgers Guideline

Korea Securities Depository
Token Securities Department

This guideline explains in detail the standard requirements that a distributed ledger must satisfy to support the stable issuance and circulation of token securities. It specifies the matters covered by Article 23-2(2)(2) of the amended Electronic Securities Act.

Chapter I explains the main elements of the token securities framework, including its concept and management structure. Chapter II presents the standard requirements for token securities distributed ledgers by subject area. Chapter III describes the suitability assessment procedures and methods used to verify compliance when KSD participates in a distributed ledger as the electronic registration institution.

CONTENTS

- I Overview of the token securities framework
- II Standard requirements for token securities distributed ledgers
- III Suitability assessment of token securities distributed ledgers

CONTENTS

I Overview of the token securities framework

The concept of token securities

Token securities are a new form of securities issuance that uses distributed ledger technology to digitize securities under the Capital Markets Act. They are shares and other securities electronically registered in electronic registration account books consisting of a distributed ledger and linked books under the Electronic Securities Act ("distributed-ledger-registered shares, etc.).

Compared with conventional electronic securities, the nature of the security and the legal effect of electronic registration are the same. The difference is that a distributed ledger and linked books are used as the electronic registration account books.

Electronic registration: recording information about the creation, change or extinguishment of rights in shares and other securities electronically in electronic registration account books (Article 2(2)).

Electronic registration account books: books compiled electronically to record creation, change and extinguishment of rights; comprising customer account books and own-account books of account management institutions, etc. For token securities, these are established and used on distributed ledgers and linked books (Articles 2(3) and 23-2(1)).

Distributed ledger: a book or management system, or an equivalent arrangement, in which multiple participants record and jointly manage electronic registration information under statutory standards, protected against unauthorized deletion and subsequent alteration by technical measures (Article 2(3-2)).

Distributed ledger and linked books: a distributed ledger together with electronically linked books used to manage separately information unsuitable for recording on the distributed ledger (Article 2(4-2)).

Management framework: comparison with electronic securities

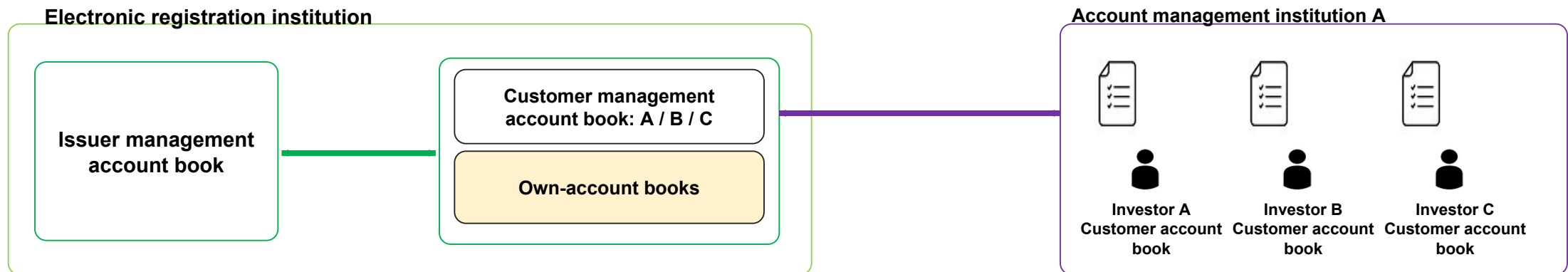
The account operation structure remains the same under the token securities framework.

Electronic registration account books: statutory books in which entries have legal effect; comprising own-account books of account management institutions, etc., and customer account books.

- **Own-account book:** an electronic registration account book opened at the electronic registration institution by an account management institution, etc., as a rights holder (hereafter "own-account book").
- **Customer account book:** an electronic registration account book opened by a rights holder at an account management institution.

Management account books: books in which the electronic registration institution records total quantities; comprising issuer management account books and customer management account books.

- **Issuer management account book:** opened in the issuer's name to manage total issuance by issue.
- **Customer management account book:** opened in the account management institution's name to manage the total quantity of each issue in its customer account books.



Management framework: joint and separate management

Conventional electronic securities use independent institutional systems to manage electronic registration account books separately. Token securities use a distributed ledger network in which multiple participants jointly manage those books.

Responsibility for preparing and managing each type of electronic registration account book remains unchanged.

Management	Conventional electronic securities	Token securities
Joint	None	1. Distributed ledger: network participants (electronic registration or account management institutions) jointly record and manage electronic registration information.
Separate	Each electronic registration or account management institution independently manages electronic registration information.	2. Linked books: each institution separately manages information unsuitable for the distributed ledger, such as personal information.

Management framework: account-book architecture

Conventional electronic account books

Electronic registration institution



Issuer management account book

Customer management account book

Own-account books

Independent institutional systems
Connect via messages (CCF), as needed



Account management institution

Customer account book



Account management institution

Customer account book

Distributed ledger account books

Electronic registration institution



Node



Distributed ledger



Own-account books
Customer account books

Linked book: reasons
for changes

Issuer management
account book

Customer management
account book

Total quantity
management



Issuer account
management institution

Linked books: personal
information, reasons for changes



Account management institution

Linked books: personal
information, reasons for changes

Management framework: distributed ledger and linked books

Definition: electronic registration account books consisting of a distributed ledger and its linked books.

Distributed ledger: a book and management system (blockchain) in which multiple participants record and jointly manage electronic registration information according to defined standards.

Linked books: books managed separately by each participant outside the distributed ledger for electronic registration information unsuitable for the ledger, such as personal information.

Participants: the electronic registration institution (KSD) and account management institutions (such as securities firms).

- Under the Electronic Securities Act, the actors who enter and preserve registration information and the scope of information they enter are already prescribed.
- Roles are allocated by reflecting the rights and responsibilities of each actor in the distributed ledger system design.

Step	Recording and management procedure
1. Request an entry	The institution responsible for the relevant account executes a smart contract to request an entry.
2. Consensus and validation	Participants (nodes) verify the integrity of the requested entry data and reach consensus.
3. Joint management	A block containing electronic registration information is created. Participants record and manage it on their nodes, preserving identical information in distributed form.

Institution responsible for an account: electronic registration institution for own-account books; the relevant account management institution for customer account books.

KSD responsibilities as electronic registration institution

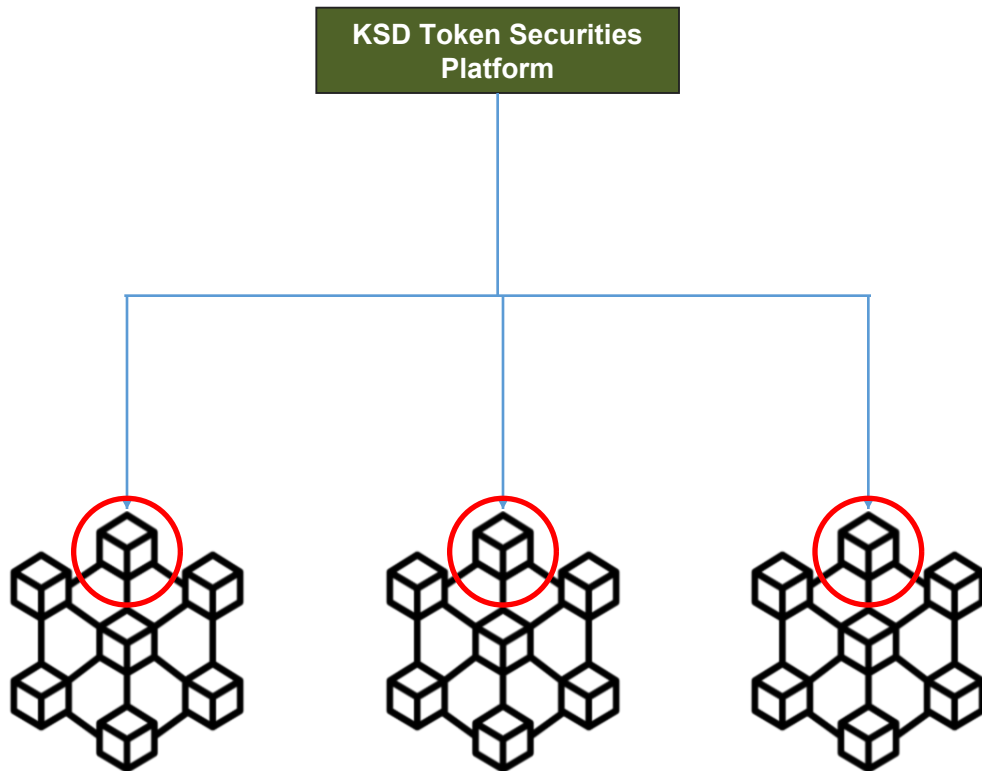
- ✓ **Token securities are recognized as a securities issuance form under the Electronic Securities Act. KSD therefore performs its statutory responsibilities as the electronic registration institution.**

Responsibility	Activities	Change
1. Registration eligibility review	Review external requirements for issuance (preliminary review and issuance registration review). Check distributed ledger requirements and assess suitability for electronic registration operations.*	Existing issuance review; new ledger assessment
2. Total quantity management	Record and manage total issuance and circulation, and verify equality. Collect transaction information from the distributed ledger. Issuance total (issuer management account book) = circulation total (own-account books + customer account books).	Existing role; different method
3. Prepare and manage own-account books	Record and manage own-account books of account management institutions, etc. Execute ledger entries/transactions for issuance, cancellation, account transfer, pledges and related actions.	Existing role; different method
4. Rights administration and certificates	Perform existing statutory responsibilities, including ownership details, exercise of rights on behalf of holders, ownership certificates and electronic registration certificates.	Existing role

* KSD is expected to perform, by delegation, the FSC review of ledger suitability for electronic registration operations among the registration requirements for issuer account management institutions (Article 69).

How KSD participates in distributed ledgers

- ✓ To perform its electronic registration responsibilities effectively and reliably, KSD participates as a node in every distributed ledger.



Total quantity management	Collect information directly through joint management
Own-account ledger entries	Execute transactions directly

CONTENTS

II Standard requirements for token securities distributed ledgers

Structure of the standard requirements

	Major category	Category	Subcategory (number of detailed requirements)
Distributed ledger standard requirements	Technology and infrastructure	A. Ledger participants	1. Scope of participants (2)
			2. Participation methods (2)
		B. Ledger configuration and operation	1. Node configuration (3)
			2. Permission management (2)
			3. Consensus algorithm (3)
	Electronic registration operations		4. Smart contract implementation (4)
			5. Other operations (4)
		C. Ledger infrastructure	1. Security (4)
			2. Wallet/key management (2)
		D. Registration functions	1. Registration institution participation (3)
			2. Registration smart contracts (3)
			3. Account/issue management (3)
			4. Smart contract operation (2)
		E. Data management	1. Information recorded for registration (2)
			2. Preservation of registration information (1)

2 major categories, 5 categories, 15 subcategories and 40 detailed requirements. Parentheses indicate the number of detailed requirements in each subcategory.

Requirement classification	
Identifier	A-1-1
Assessment	Checklist Supporting documents

[1] Consortium membership list:
participation method and node permissions
for each institution.

Requirement
✔ Participants jointly managing electronic registration information are limited to electronic registration institutions and account management institutions.
Details
Because the distributed ledger is an electronic registration account book used to prepare and manage electronic registration information, participation is restricted to institutions authorized by the Electronic Securities Act: electronic registration institutions and account management institutions (Article 19). This is a private distributed ledger. - There is no restriction on the "distributed ledger operator" that provides the network or related systems.* Participants may receive the following three permissions. They must at least have permissions 1 and 3 to prepare and manage (query) information; consensus/validation permission is not mandatory. 1. Request entries for accounts (wallets) they are authorized to maintain (execute transactions): the registration institution for own-account books; the relevant account management institution for customer account books. 2. Create blocks by reaching consensus on and validating requested entries (participate in recording registration information). 3. Jointly manage and query registration information (blocks) on the ledger. * An operator is a platform provider responsible for network configuration and operation that supports participants' registration operations without performing those operations directly. A participant may also be an operator.

Technology / infrastructure - A. Participants / 1. Scope of participants

Requirement classification	
Identifier	A-1-2
Assessment	Checklist

Requirement
 An account management institution may not participate merely as a member without opening customer account books on the ledger.
Details
Under A-1-1, even an institution listed as an account management institution in Article 19 is restricted from participating if its purpose is not to open customer account books and prepare/manage electronic registration information. - The purpose of adopting a distributed ledger is joint management of electronic registration account books. - Example: participation solely to provide a consensus/validation node is restricted.

Requirement classification	
Identifier	A-2-1
Assessment	Checklist Supporting documents

[1] Consortium membership list:
participation method and node permissions
for each institution.

Requirement



Only distributed ledger participants may join the ledger network through nodes.

Details

Node participation is presented as the most common method of joining the network.

- Participants may use nodes they build and operate themselves, or obtain nodes provided by a third party. Participants remain responsible for use of third-party nodes (an area of self-regulation).

Nodes perform the network role of recording and managing electronic registration information. Only eligible ledger participants may therefore participate through nodes.

- Under A-1-1, this covers all nodes with Read or Write permissions for block information (for example, Besu validators and members).

Requirement classification	
Identifier	A-2-2
Assessment	Checklist Supporting documents

[1] Consortium membership list:
participation method and node permissions
for each institution.

Supporting materials for proxy-node use
(e.g. a copy of the delegation agreement).

Requirement



Indirect participation through another participant's node (such as a proxy node) is permitted subject to conditions.

Details

Recording and management of registration information through another participant's node is permitted (proxy nodes).

- Linked books containing real-name information must still be directly managed, as for ordinary participants.

To ensure the user's own account management remains reliable, the following proxy-node requirements must be met:

1. The user must have a process to record/query registration information through the proxy node.
2. The user must separately extract and directly preserve the ledger's registration information.
3. The provider must guarantee the authenticity of the key signatures for customer wallets/accounts managed by the user.

Requirements 1 and 2 ensure timely, reliable registration operations. Requirement 3 prevents arbitrary interference by the provider in the user's registration operations.

User: an account management institution using a provider's node as a proxy for registration operations.

Provider: a party making its own node available as a proxy for a third-party user's registration operations.

Requirement classification	
Identifier	B-1-1
Assessment	Checklist Supporting documents

[2] Consensus/validation node configuration list: number (share) of nodes and participant list.

Requirement
✓ At least three independent institutions must participate through nodes that take part in consensus.
Details
Multiple independent institutions must hold distributed consensus/validation shares to prevent a single institution from undermining joint management through unilateral consensus/validation. - No single institution may hold 50% or more of the node share for consensus/validation. Reference: action when ledger requirements cease to be satisfied after deployment. - From the time a failure to meet the standard requirements occurs, the ledger is a legally non-conforming electronic registration account book. - New electronic registration must stop, and a restoration process must begin immediately. - If restoration is not possible within a certain period and rights holders require protection, conversion to conventional electronic securities is necessary (Article 23-2(6)(3)).

Requirement classification	
Identifier	B-1-2
Assessment	Checklist Supporting documents

[3] Node configuration environment:
explanation of infrastructure types and
distribution.

Supplement incident-response arrangements
if nodes share one IDC or AZ.

Requirement
✓ Nodes must be distributed both logically and physically.
Details
Distributed node configuration is necessary to prevent failure of some nodes from stopping the entire network. * This includes all nodes with functions for input, consensus, validation and storage of generated blocks. Avoid placing nodes in a single Internet Data Center (IDC, on-premises) or in the same Availability Zone (AZ, cloud). This is a recommendation. - If unavoidable, an incident-response arrangement must be presented.

Requirement classification	
Identifier	B-1-3
Assessment	Checklist Supporting documents

[2] Consensus/validation node configuration list: assessment of the adequacy of node numbers (shares) and participants.

Requirement



The number of consensus nodes must reflect incident response and the characteristics of the consensus algorithm.

Details

Sufficient nodes are required to prevent consensus/validation failures or improper consensus caused by node failures or external attacks.

Compliance with the Blockchain Cryptographic Technology Guidelines (December 2020, National Intelligence Service and others) is recommended.

Extract from Guideline 4-2:

If x is the maximum number of nodes that may fail simultaneously in the service environment ($x \geq 2$ recommended), the number of consensus nodes N must satisfy:

- Without considering Byzantine failures: $N \geq 2x + 1$.
- Considering Byzantine failures: $N \geq 3x + 1$.
- If the consensus protocol requires more nodes, such as $N \geq 4x + 1$, that standard must be followed.

Requirement classification	
Identifier	B-2-1
Assessment	Checklist Supporting documents

[4] Ledger role framework: mapping of responsible parties and node permissions by role.

[5] Node/network management and operation policy.

Requirement
✓ The roles of ledger participants and operators must be clearly defined and managed.

Details
Establish a system to allocate and manage ledger roles (network operator, consensus/validation, transaction creation, data query, information storage, etc.). - Define the network operator and establish management of roles and permission scope for each node type. Establish policies for granting permissions to nodes and a technical management system.

Requirement classification	
Identifier	B-2-2
Assessment	Checklist

Requirement
✓ Smart contract execution permissions, including transaction creation, must be controlled for each wallet (account).
Details
Permission to record electronic registration information for a wallet/account must be limited to the ledger participant legally responsible for preparing that information: - Electronic registration institution: own-account books. - Account management institution: customer account books.

Requirement classification	
Identifier	B-3-1
Assessment	Checklist Supporting documents

[6] Consensus algorithm description: algorithm type and detailed settings, suitability assessment or compliance with official guidance, etc.

Requirement
✓ Use a consensus algorithm that guarantees timely and final electronic registration.
Details
A ledger entry (electronic registration) confers legal effect on securities rights. Timeliness and finality are therefore necessary to protect investors. The consensus algorithm must guarantee deterministic finality so that information is not changed or cancelled during electronic registration processing on the ledger.

Requirement classification	
Identifier	B-3-2
Assessment	Checklist Supporting documents

[6] Consensus algorithm description: algorithm type and detailed settings, suitability assessment or compliance with official guidance, etc.

Requirement
✓ Configure consensus so that no single institution or node can create information unilaterally.
Details
Apply a consensus algorithm that prevents control, collusion or operational failure caused by one or a small number of consensus/validation institutions. Provide evidence of suitability assessment/certification by a specialist institution or compliance with official guidelines, such as: - Blockchain Cryptographic Technology Guidelines (National Intelligence Service, TTA and others). - Cryptographic Algorithm Guide (KISA). - Guide to the Use of Cryptographic Technology in the Financial Sector (Financial Security Institute).

Requirement classification	
Identifier	B-3-3
Assessment	Checklist Supporting documents

[6] Consensus algorithm description: algorithm type and detailed settings, suitability assessment or compliance with official guidance, etc.

Requirement
✓ Ensure that electronic registration information can be recorded in chronological order.
Details
Independently establish consistent reference times and ordering criteria based on the principle that entries follow the time of the underlying act giving rise to registration. Because transaction time and the time rights take effect are important for securities, consensus/validation must be implemented in transaction-creation order. - An ordering function within the consensus mechanism that sorts transactions chronologically is recommended.

Requirement classification	
Identifier	B-4-1
Assessment	Checklist Supporting documents

[7] Permission-control measures and incident-response protocols: emergency permission controls and incident-response protocols.

Requirement
✓ Prepare measures to maintain business continuity when smart contracts fail or contain errors.

Details
Verify management measures for security incidents or critical errors. - Example: permission-control measures using master-key functions. Prepare specific handling procedures and scenario-based plans (incident-response protocols) for failures or errors. - Example: restoration of individual consensus nodes within an institution. Applying an upgrade pattern to smart contracts is recommended to address potential code errors and changes to business logic.

Requirement classification	
Identifier	B-4-2
Assessment	Checklist Supporting documents

[8] Smart contract verification confirmation.

Requirement
✓ Consortium participants must verify smart contract code.
Details
Use functional verification and business-logic testing to confirm that implemented smart contracts operate accurately under the business rules. Verify the integrity of contract execution, including: - Input validation. - Execution permissions based on role-based access control (RBAC). - Checks of defenses against replay attacks and overflow.

Requirement classification	
Identifier	B-4-3
Assessment	Checklist Supporting documents

[9] Smart contract vulnerability inspection results.

Requirement
✓ Ensure the security of smart contracts.
Details
Security review and secure coding are necessary. - Review smart contract security during design and implementation. - Follow secure-coding guidelines that identify and block known vulnerabilities. Source-code vulnerability checks are recommended. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	B-4-4
Assessment	Checklist

Requirement
✓ Establish procedures for registering, modifying and retiring smart contracts.
Details
A separate configuration-management system is recommended. - Measures to secure that system, including access controls, are necessary. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	B-5-1
Assessment	Checklist Connection/function tests

Requirement
✓ Ledger entries must be protected against unauthorized deletion and subsequent alteration.
Details
The block header must include the hash of the preceding block, and hashes must be unique. - Hashes must use a secure cryptographic algorithm and be generated from the entire block's data.

Requirement classification	
Identifier	B-5-2
Assessment	Checklist Connection/function tests

Requirement
✓ Creation or trading of virtual assets for fees or seigniorage is entirely prohibited in electronic registration processing.

Details
Use of virtual assets as compensation must be prevented to ensure smooth and stable electronic registration operations. Details are expected to be specified in the Enforcement Decree of the Electronic Securities Act.

Requirement classification	
Identifier	B-5-3
Assessment	Checklist

Requirement



Maintain consistent time across distributed ledger nodes.

Details

The time of ledger entries must remain accurate and consistent to protect investors' rights reliably.

- Independently establish and consistently apply reference times and ordering criteria based on the chronological order of underlying acts giving rise to registration.
- Ensure time synchronization among ledger nodes, using UTC.

Requirement classification	
Identifier	B-5-4
Assessment	Checklist Supporting documents

[10] Ledger performance measurement sheet.

Requirement



Manage ledger performance so that it is appropriate for electronic registration operations.

Details

Regularly analyze usage and trends to prevent ledger failures and optimize performance, thereby supporting stable electronic registration operations.

Requirement classification	
Identifier	C-1-1
Assessment	Checklist Supporting documents

[11] Security inspection results.

Requirement
✓ Ensure security in operating the distributed ledger network.
Details
Perform legally required security inspections for the ledger network (electronic financial infrastructure). - Conduct vulnerability analysis/assessment and internal security review of electronic financial infrastructure. Use encrypted protocols or dedicated lines for communication between nodes and for API communication with external systems. When configuring VPN connections to KSD nodes, follow KSD standards to prevent private-IP conflicts between participants and ensure network availability. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	C-1-2
Assessment	Checklist Supporting documents

[11] Security inspection results.

Requirement
✓ Ensure security in operating distributed ledger nodes.
Details
Consensus protocol integrity and fault tolerance: - Prevent alteration/forgery of protocol messages and signatures and block replay attacks. Ensure BFT-level reliability so that failures or malicious behavior by some nodes do not stop the network.* Monitoring and anomaly detection: real-time monitoring of synchronization between nodes and detection of anomalies, such as total-quantity mismatches and abnormal high-volume transactions, are recommended. Server infrastructure: participants must secure the server operating system through measures such as anti-malware software, controls on externally exposed RPC ports and disabling unnecessary system services. * This is not limited to traditional BFT protocols such as PBFT; other methods providing an equivalent level of fault tolerance are also possible. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	C-1-3
Assessment	Checklist Supporting documents

[11] Security inspection results.

Requirement
✓ Establish and operate security policies suited to the ledger infrastructure environment.
Details
Establish operational permissions and access-control policies, including the scope of access control and management rules. - Include management of system and data access logs. Provide system security functions: operating-system security settings, vulnerability inspections, and security patch management for servers, nodes and software. Establish other security policies and environments reflecting the characteristics of on-premises, cloud and other infrastructure. Prepare a vulnerability inspection plan and conduct inspections periodically. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	C-1-4
Assessment	Checklist Supporting documents

[12] Incident-response policies and procedures.

Requirement
✓ Establish a response framework for failures and security incidents.

Details
Clearly define response procedures and responsibility for failures and other incidents. Establishing and operating a business continuity plan (BCP) and disaster recovery system (DRS) to maintain service continuity during failures is recommended. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	C-2-1
Assessment	Checklist Supporting documents

[13] Key management policy description.

Requirement
✓ Establish and operate wallet/key management policies.
Details
Establish and operate procedures for creating, retiring and replacing wallets and keys. Prepare a response framework for lost or stolen keys. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	C-2-2
Assessment	Checklist

Requirement
 Keys must be stored securely under the responsibility of the entity managing the account or wallet.

Details
Signing keys must be securely stored and used. If another institution is entrusted with key storage, controls must prevent that institution from signing arbitrarily, preserving the authenticity of signatures. Compliance with the separate guide to be provided by the Financial Security Institute is recommended.

Requirement classification	
Identifier	D-1-1
Assessment	Checklist Connection/function tests

Requirement
 The electronic registration institution must participate directly through a node (the "total quantity management node").

Details
Take measures allowing the registration institution to participate directly as a node and perform its responsibilities, including total quantity management and preparing/managing own-account books of account management institutions, etc. KSD will establish and separately provide detailed connection methods and standards in the KSD Standard Development Requirements. - These provide VPN-based connection standards between the KSD Token Securities Platform and the distributed ledger.

Requirement classification	
Identifier	D-1-2
Assessment	Checklist Supporting documents Connection/function tests

[2] Consensus/validation node configuration list.

Requirement
✓ The total quantity management node must have the permissions and functions needed for the registration institution's operations.
Details
Ensure that the node has the required Read permissions/functions for ledger transaction information and Write permissions/functions for entries such as account management institutions' own-account books. Consensus/validation permission for block creation may also be granted to this node (a consortium choice). - If granted, the registration institution counts toward the minimum of three consensus-participating institutions under B-1-1.

Requirement classification	
Identifier	D-1-3
Assessment	Checklist Supporting documents Connection/function tests

[14] Explanatory materials, such as a white paper on the underlying technology.

Requirement



When introducing a ledger technology not previously used in the token securities market, provide technical support for the registration institution to participate.

Details

Based on its assessment of market readiness, KSD is building the KSD Token Securities Platform to connect with Hyperledger Besu, Hyperledger Fabric and Avalanche (as of July 2026).

When introducing a new underlying ledger technology other than these, consult the registration institution in advance and actively provide technical support for connection to the KSD Token Securities Platform and for node participation.

Requirement classification	
Identifier	D-2-1
Assessment	Checklist Supporting documents Connection/function tests

[15] Electronic registration function implementation specification.

Requirement
✓ Provide securities electronic registration functions in the form of smart contracts.
Details
Provide standardized smart contract functions to process electronic registration operations and rights entries reliably, including issuance/cancellation, account transfers, pledges, attachments and disposal restrictions. Development methods remain at the developer's discretion for areas not specified by this guideline or the KSD Standard Development Requirements.

Requirement classification	
Identifier	D-2-2
Assessment	Checklist Connection/function tests

Requirement
 Functions needed for the registration institution's responsibilities must comply with the KSD Standard Development Requirements.

Details
Functions connecting operations with the registration institution must follow KSD standards, including collecting transaction information for quantity management and executing entries in own-account books of account management institutions, etc. - Registration information collection: dedicated standard events within smart contracts. - Own-account book entries: dedicated smart contract functions. - Business status notifications (such as completion/results of issuance review): dedicated smart contract functions. - Other information queries (account/issue information, balance information, etc.): state-information query functions.

Requirement classification	
Identifier	D-2-3
Assessment	Checklist Connection/function tests

Requirement
 Provide functions to resolve erroneous excess entries.
Details
Provide policies and functional systems to detect and resolve excess quantities in customer account books. - If excess quantities require circulation restrictions, implement the necessary policies and functions. Policies and systems to detect and resolve erroneous entries are recommended.

Requirement classification	
Identifier	D-3-1
Assessment	Checklist

Requirement
 Each token securities issue must be deployed as one smart contract.
Details
Deploy a single issue smart contract for each issue identified by ISIN. Issuance through an issue smart contract deployed without the registration institution's issuance review is invalid.

Requirement classification	
Identifier	D-3-2
Assessment	Checklist Supporting documents Connection/function tests

[16] Issue status management specification.

Requirement



Provide functions to manage each issue's status, including whether circulation is permitted.

Details

Manage the current state throughout each issue's lifecycle: issuance, circulation and extinguishment of rights.

- At minimum, a status indicating whether circulation is permitted must be provided.
- In principle, the party deploying each issue's smart contract should manage this status.

Implement a function allowing the registration institution to impose temporary circulation restrictions when necessary for operations (included in the KSD Standard Development Requirements).

Requirement classification	
Identifier	D-3-3
Assessment	Checklist Connection/function tests

Requirement
 Provide smart contract functions to verify the validity of rights holders and account management institutions for each account, under KSD requirements.

Details
Implement an account registry (whitelist) smart contract identifying each account's rights holder and account management institution, following the KSD Standard Development Requirements. For efficient total quantity management, account management institution identifiers must use KSD's 6-4-2 account-number structure, based on own accounts and customer management accounts opened at KSD: - 6: account management institution identifier. - 4: operational serial number. - 2: property classification (01: own-account book; 02: customer account book).

Requirement classification	
Identifier	D-4-1
Assessment	Checklist

Requirement
 A security must be issued and circulated on only one distributed ledger.

Details
Each token securities issue must be issued and circulated on a single ledger. After issuance, transfer of part or all of the issue to another distributed ledger is prohibited (interoperability prohibited). This operating rule is expected to be incorporated into the Enforcement Decree of the Electronic Securities Act.

Requirement classification	
Identifier	D-4-2
Assessment	Checklist Supporting documents Connection/function tests

[17] Smart contract implementation/change policy.

Requirement
✓ Obtain prior approval from the registration institution for smart contract operation and changes.
Details
A new issue smart contract may be deployed only after its validity has been verified through the registration institution's technical assessment. If a contract in use requires a change, notify the registration institution beforehand of the change, its reasons and details. - Include an impact assessment for registration and total quantity management operations. Decide whether to proceed after final consultation with the institution. Deploy the compiled code of the contract that passed suitability assessment and connection testing without changes; bytecode/hash values must match.

Electronic registration - E. Data management / 1. Registration information

Requirement classification	
Identifier	E-1-1
Assessment	Checklist Supporting documents Connection/function tests

[18] Distributed ledger and linked-book management/operation policy.

Requirement
 Electronic registration information recorded on the distributed ledger and in linked books must comply with relevant laws.
Details
Prepare electronic registration account books in accordance with the data designated for recording in on-chain and off-chain areas. Detailed criteria for this requirement are expected to be finalized and reflected in subordinate legislation, including the Enforcement Decree of the Electronic Securities Act.

Electronic registration - E. Data management / 1. Registration information

Requirement classification	
Identifier	E-1-2
Assessment	Checklist Connection/function tests

Requirement
 The main data formats on the ledger must comply with the KSD Standard Development Requirements.

Details
Implement on-chain recording formats according to KSD data standards. - Standards focus on mandatory registration information; other information remains discretionary.

Electronic registration - E. Data management / 2. Information preservation

Requirement classification	
Identifier	E-2-1
Assessment	Checklist Supporting documents

[17] Smart contract implementation/change policy.

Requirement
 Preserve and manage information recorded on the ledger and in linked books as required by relevant laws.
Details
Keep rights holders' real-name information and similar data in off-chain linked books and observe statutory retention periods. For on-chain customer account books whose rights-holder real-name information has been destroyed, provide policies and systems to restrict account queries and preserve/manage query logs. Detailed criteria for this requirement are expected to be finalized and incorporated into subordinate legislation, including the Enforcement Decree of the Electronic Securities Act.

CONTENTS

III Suitability assessment of token securities distributed ledgers

Assessment procedure

1. Apply for ledger connection

Before starting token securities operations, the ledger operator applies to KSD for connection between its ledger and the KSD Token Securities Platform.

2. Document review

KSD reviews the submitted checklist and supporting documents to verify compliance with the standard requirements.

3. Connection/function testing

Connect systems and deploy KSD nodes in a test environment. Verify functional suitability through scenario tests for each operational function.

4. Complete assessment and connect production

KSD formally registers ledgers that have passed stages 2 and 3 on its platform and assigns ledger codes. Systems are connected and KSD nodes formally deployed in the operating environment; token securities operations may then begin.

An account management institution wishing to use the ledger must separately notify the total quantity management system (e-SAFE), under Article 23-2(4) of the Electronic Securities Act.

Assessment methods

KSD verifies compliance with ledger standard requirements through document review and connection/function testing.

Document review: the operator must submit a checklist containing its self-assessment against each requirement (using the KSD form). Separate supporting materials are also required for requirements KSD must verify as a ledger participant.

Connection/function testing: after connecting the ledger to the KSD Token Securities Platform and deploying nodes, scenario tests for individual operations verify the suitability of smart contracts and other functions, and compliance with the KSD Standard Development Requirements.

Reference: supporting document list

No.	Supporting document	Main contents	Related requirement
1	Consortium membership list	Participation methods and node permissions by institution, including total quantity management node permissions	A-1-1, A-2-1, A-2-2
2	Consensus/validation node configuration list	Adequacy of node numbers/shares and member institution list	B-1-1, B-1-3, D-1-2
3	Node configuration environment	Infrastructure types and distribution arrangements	B-1-2
4	Ledger role framework	Map activities and permissions by operator/node participant role	B-2-1
5	Node/network management and operation policy		B-2-1
6	Consensus algorithm description	Algorithm type and detailed settings	B-3-1, B-3-2, B-3-3
7	Permission-control measures and incident-response protocols	Emergency permission controls and incident response	B-4-1
8	Smart contract verification confirmation	Verification results for each participant	B-4-2
9	Smart contract vulnerability inspection results	Security review, secure coding and source-code vulnerability checks	B-4-3
10	Ledger performance measurement sheet	Processing speed, optimization status and trend analysis	B-5-4
11	Security inspection results		C-1-1, C-1-2, C-1-3
12	Incident-response policies and procedures	Internal controls such as BCP and DRS	C-1-4
13	Key management policy description	Wallet/key creation, retirement and replacement procedures; theft prevention	C-2-1
14	Explanatory materials/white paper on underlying technology		D-1-3
15	Registration function implementation specification		D-2-1
16	Issue status management specification	Account transfer restrictions and permission assignments	D-3-2
17	Smart contract implementation/change policy		D-4-2, E-2-1
18	Ledger and linked-book management/operation policy		E-1-1

Reference: proposed scenario-test operations

No.	Operation	Description
1	Issuance registration	Preliminary review and registration for securities issuance.
2	Cancellation ex officio	Cancellation by the registration institution for reasons such as redemption through KSD.
3	Cancellation upon application	Cancellation at the request of rights holders or other eligible parties.
4	Account transfer	Transfer of securities ownership between account management institutions, or between an account management institution and the registration institution.
5	Create/cancel pledge	Pledge creation/cancellation; the registration institution connects only for own-account books.
6	Create/cancel attachment	Attachment creation/cancellation; the registration institution connects only for own-account books.
7	Issue/revoke registration certificate	Electronic registration certificates and related disposal restrictions.
8	Issue/revoke ownership certificate	Ownership certificates and related disposal restrictions.
9	Conversion	Conversion between token securities and conventional electronic securities.
10	Total quantity verification	Real-time reconciliation for each operation; end-of-day total quantity verification for closing balance reconciliation.

1. Tests cover on-chain operations linked to the ledger. Fully off-chain operations such as rights determination will be separately explained and may be tested on request.

2. Detailed processes for each operation are expected to be provided separately in the KSD Standard Development Requirements.

Reference: process before token securities issuance

Step	Process	Notes
1. Customer registration	Register as a KSD customer (omit if already registered).	Same as conventional electronic securities
2. Ledger standard-requirements assessment	1) Operator applies for assessment and account-book registration with the required documents. 2) KSD reviews the checklist and additional materials. 3) KSD assesses suitability for registration operations through document review and connection/function tests in the test environment; a temporary test code is assigned. 4) Assign a formal code and issue a review-approval certificate (for issuer account management institutions only). 5) Formally deploy the KSD quantity management node and begin quantity management.	Connection and testing time varies by ledger technology
3. Notify use of ledger	Account management institution notifies KSD through e-SAFE of the evaluated ledger it intends to use. Available after completion of step 2; simplified function testing is conducted.	Notify four weeks before starting use
4. Registration suitability review	Apply for preliminary review of the token securities to be issued. Available after completion of step 2.	Same as conventional electronic securities