มาตรฐานสำหรับการออกและให้บริการ หลักทรัพย์โทเคน

Standard for Securities Tokenization



ศูนย์พัฒนาโครงสร้างพื้นฐานตลาดทุน
Capital Market Infrastructure Center

November 2026

Digital Securities Ecosystem (DSE) : Landscape

ก.ล.ต. ส่งเสริม **Digital Securities Ecosystem (DSE)** ที่เอื้อต่อการออกเสนอขายและให้บริการหลักทรัพย์อิเล็กทรอนิกส์ เพื่อเพิ่มประสิทธิภาพ ลดต้นทุน และเพิ่มโอกาสในการเข้าถึงผลิตภัณฑ์และบริการทางการเงินของผู้ลงทุน **พร้อมสนับสนุนให้เกิด Interoperability** ระหว่างระบบซึ่งจะช่วยลดข้อจำกัดในการเชื่อมต่อระบบและเพิ่มประสิทธิภาพของกระบวนการในตลาดทุน

PRODUCTS

Tokenized Securities

- Local Issuer: Tokenized Bond, Tokenized Fund
- Foreign Issuer: Tokenized EQ/DR, Tokenized Fund

Tokenized Settlement

- Deposit Token
- e-Money Token
- THBS - Thai Baht Stable Coin

SERVICES

Traditional Services

- Underwriter / Broker / Dealer
- Asset Management Company
- Depository
- Registrar
- Bank
- e-Money Provider

Tokenization-Related Services

- **Tokenizer** (หลักทรัพย์)
- **Trading Platform : Bulletin** — On-Chain / Atomic Swap
- **Tokenizer** (เงินฝาก / e-money / THB Stable Coin)
- **Wallet Provider** (เก็บ securities token)
- Custody
- Tokenized Securities
- Tokenized Settlement
- Shared / Interoperable Ledger
- Custody
- **Wallet Provider** (เก็บ deposit / e-money token / THBS)

STANDARDS

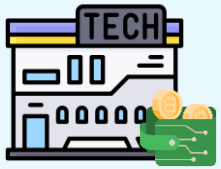
DLT-Architecture | Token Requirements | Interoperable Capability | Cybersecurity

REGULATION

พ.ร.บ. หลักทรัพย์อิเล็กทรอนิกส์ | **กฎลำดับรองที่เกี่ยวข้อง**

Tokenization Related Services

ระบบนิเวศ DSE ประกอบด้วยผู้ให้บริการหลายประเภทที่สนับสนุนการดำเนินกิจกรรมตลอดวงจรชีวิตหลักทรัพย์โทเคน ตั้งแต่การออกเสนอขาย การซื้อขายและโอนเปลี่ยนมือ ตลอดจนการเก็บรักษาทรัพย์สิน การกำกับดูแลจึงแตกต่างกันตามบทบาทและลักษณะบริการ

ประเภทผู้ให้บริการ	บทบาทหน้าที่ / ขอบเขตบริการ	การกำกับดูแล
Tokenizer 	Securities Tokenizer คือ **ผู้ให้บริการที่ใช้เทคโนโลยี DLT/Blockchain ในการสนับสนุนหรือดำเนินการเกี่ยวกับการออกและให้บริการหลักทรัพย์โทเคน** โดยอาจครอบคลุมงานสนับสนุนจัดทำทะเบียนหลักทรัพย์ การให้บริการกระเป๋าหรือการเก็บรักษาทรัพย์สินของลูกค้า ตลอดจนการสนับสนุนการชำระราคาที่เกี่ยวข้องกับหลักทรัพย์โทเคน ทั้งนี้ ผู้ให้บริการสามารถเลือกขอบเขตการให้บริการได้ตามความเหมาะสม	กำหนดมาตรฐาน / แนวปฏิบัติตามขอบเขตการให้บริการ เว้นแต่จะขอประกอบธุรกิจเป็น**นายทะเบียนหลักทรัพย์**
Bulletin Platform 	Bulletin Platform Operator หรือ ผู้ให้บริการแพลตฟอร์มประกาศความประสงค์ซื้อขาย **ทำหน้าที่เผยแพร่และแสดงข้อเสนอซื้อ ขาย แลกเปลี่ยนหลักทรัพย์โทเคน เพื่ออำนวยความสะดวกให้ผู้ซื้อและผู้ขาย** สามารถทำความตกลง / สัญญากันได้	อาจพิจารณาในลักษณะเดียวกับ**นายหน้าซื้อขายหลักทรัพย์**
Wallet Provider 	แบ่งออกเป็น 2 กรณี **(1) ผู้ให้บริการเก็บรักษาหลักทรัพย์โทเคน (Custodial Service)** : ทำหน้าที่รับฝากหลักทรัพย์โทเคนแทนผู้ลงทุน รวมถึงควบคุม Private Key เพื่อทำธุรกรรมที่เกี่ยวข้อง **(2) ผู้ให้บริการกระเป๋าหลักทรัพย์โทเคน (Non-Custodial Service)** : ในลักษณะของการให้บริการ software ในการจัดเก็บหลักทรัพย์โทเคน โดยผู้ลงทุนจะต้องเป็นผู้ควบคุม Private Key ด้วยตนเอง***	พิจารณาตามหลักเกณฑ์การเก็บรักษาทส. ลูกค้าของธุรกิจหลักทรัพย์** กำหนดมาตรฐาน / แนวปฏิบัติฯ

** อยู่ระหว่างพิจารณาปรับปรุงหลักเกณฑ์ให้รองรับระบบงานเก็บรักษาทรัพย์สินเหมือนฝั่ง ผปก. DA
*** wallet address ต้องเป็นไปตาม white-list ของนายทะเบียนเท่านั้น จึงจะสามารถทำธุรกรรมโอนได้

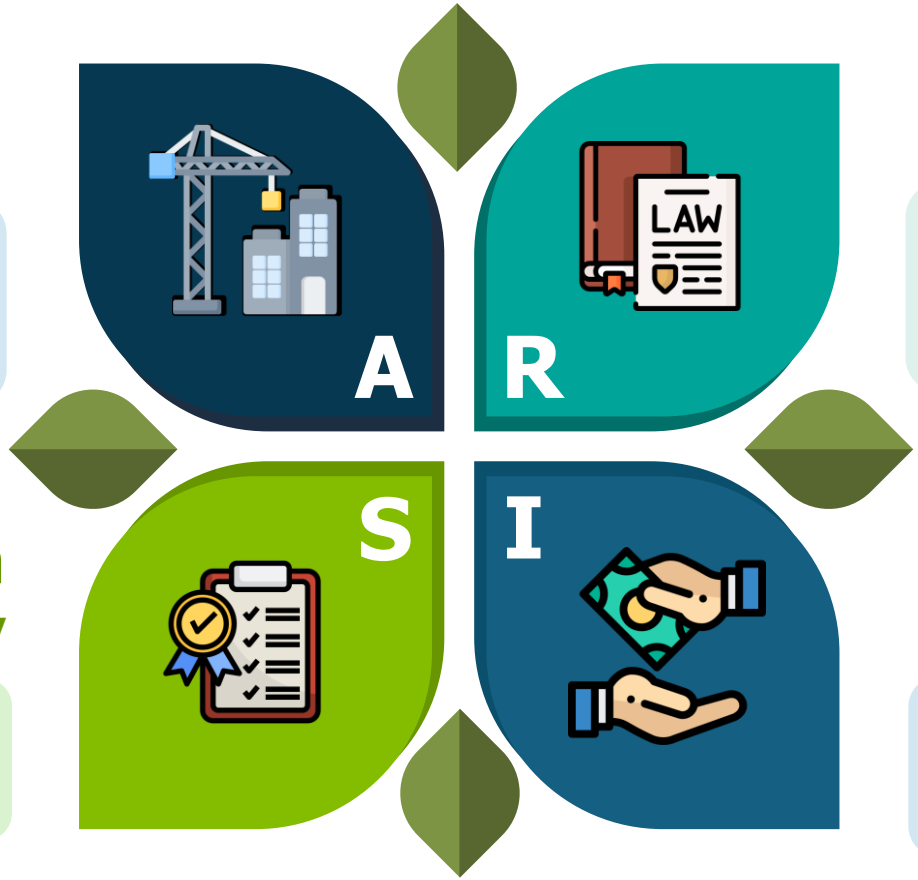
แนวทางส่งเสริม Digital Securities Ecosystem - DSE

สนับสนุนให้เกิด ecosystem ที่เอื้อต่อการเกิด 'หลักทรัพย์อิเล็กทรอนิกส์' รวมถึงเชื่อมโยงระบบที่หลากหลาย (interoperability) ผ่านการกำหนดมาตรฐาน เพื่อเพิ่มประสิทธิภาพให้กับธุรกรรมในตลาดทุน

- **Financial Inclusion and Enhanced Liquidity**
- **Automated Verification**
- **Operational Efficiency And Cost reduction**
- **Real-time Settlement**
- **Transparent / Data-Driven Suspicious**

Project Acceleration

ผลักดัน Use Case ของ Securities Tokenization ในอุตสาหกรรมตลาดทุน รวมถึงเปิดพื้นที่สนับสนุนให้ผู้ประกอบธุรกิจเข้าร่วมทดสอบภายใต้ Sandbox เพื่อประเมินความเสี่ยงก่อนใช้งานจริง



Regulatory Realignment

ทบทวนและปรับปรุงกฎเกณฑ์ที่เป็นอุปสรรคต่อการทำ Tokenization ในหลักทรัพย์ เช่น ตราสารหนี้และหน่วยลงทุน รวมถึงผลักดันการแก้กฎหมายรองรับหลักทรัพย์อิเล็กทรอนิกส์

Standardization for Interoperability

จัดทำมาตรฐานกลาง Securities Tokenization เพื่อให้ผู้ประกอบธุรกิจสามารถเชื่อมต่อและทำงานร่วมกันได้อย่างมีประสิทธิภาพในระดับอุตสาหกรรม

Integration of On-Chain Settlement

ผนวกรวมโทเคนชำระเงินดิจิทัลทุกรูปแบบ ได้แก่ deposit token, e-money และ Thai Baht Stablecoin เพื่อผลักดันการชำระราคาแบบ On-Chain Settlement ช่วยเพิ่มประสิทธิภาพการทำธุรกรรมในตลาดทุนดิจิทัล

Milestones Toward a Securities Tokenization

เดินสายหารือ
กลุ่มผู้ที่สนใจออกเสนอขาย MMF/Bond Token (24 ก.พ. 2569)

ปรับปรุงหลักเกณฑ์
เพื่อรองรับการทำ real time settlement (T+0) ของ Tokenized Fund (1 เม.ย. 2569)

สภาผู้แทนราษฎร
เห็นชอบร่าง พ.ร.บ. หลักทรัพย์อิเล็กทรอนิกส์ (10 มิ.ย. 2569)
ปัจจุบัน อยู่ระหว่างชี้แจงในชั้นคณะกรรมาธิการ

เปิดรับสมัคร
ผู้สนใจเข้าทดสอบการออกเสนอขาย Bond Token ภายใต้ Sandbox ศูนย์รับฝากหลักทรัพย์โทเคน (ต่อเนื่องตลอดปี 2569 - 2570)

จัดทำมาตรฐาน
สำหรับหลักทรัพย์โทเคน และนำมารับฟังความคิดเห็นกับ Stakeholder ในตลาดทุน

2569

เริ่มทดสอบ **Bond Token Sandbox** (ระยะเวลา 1 ปี)

สำนักงานประกาศ **มาตรฐานสำหรับการออกและให้บริการหลักทรัพย์โทเคน**

คาดว่า พ.ร.บ. หลักทรัพย์อิเล็กทรอนิกส์ **มีผลใช้บังคับ**

2570

การปรับปรุงร่าง พ.ร.บ. หลักทรัพย์อิเล็กทรอนิกส์ฯ

ปลดล็อกข้อจำกัดกฎหมายเดิมที่ไม่สอดคล้องกับรูปแบบธุรกรรมดิจิทัล โดยจะรองรับการออก การถือครอง การโอน และการให้บริการหลักทรัพย์ในรูปแบบอิเล็กทรอนิกส์ได้อย่างครบวงจร เอื้อต่อการพัฒนาระบบนิเวศ DSE

ประเด็น พ.ร.บ. หลักทรัพย์ฯ ปัจจุบัน

มาตรา 225 225/1	ต้องฝากหลักทรัพย์ไว้ที่ศูนย์รับฝากฯ จึงถือว่า "ได้จัดทำใบหลักทรัพย์" แล้ว (scripless) (ไม่สามารถออกหลักทรัพย์ดิจิทัลได้)
มาตรา 227	ผู้ลงทุนสามารถขอออกใบหลักทรัพย์ ภายหลังได้ (มีภาระต้นทุนออกใบหลักทรัพย์ และระบบงานรองรับเพิ่ม)
มาตรา 228 228/1	ต้องโอนผ่านศูนย์รับฝากฯ หรือฝากหลักทรัพย์ไว้ที่ศูนย์รับฝากฯ จึงถือว่าหลักประกันมีผลสมบูรณ์ตามกฎหมาย (ไม่สามารถให้บริการโอน หรือรับหลักประกันได้เอง)

ร่าง พ.ร.บ. หลักทรัพย์อิเล็กทรอนิกส์ฯ และกฎลำดับรอง



กำหนดประเภท ลท.
(เริ่มจากหุ้นกู้)



กำหนดลักษณะ ลท. Elec / วิธีการออกและส่งมอบ



Registrar
การจัดทำทะเบียน



Custody
การถือหลักทรัพย์แทนโดยผู้ให้บริการ



Collateral Platform
การวาง-บังคับหลักประกัน



การซื้อขายใน Exchange
(ไม่มีกฎลำดับรอง**)

* รวมถึง มาตราอื่น ๆ ที่จะไม่มีกฎลำดับรอง ได้แก่ การขอออก statement (ไม่ใช่หลักทรัพย์) เป็นใบกระดาษยังสามารถทำได้ และการ migrate จากใบหลักทรัพย์ไปเป็นหลักทรัพย์ elec โดยความยินยอมจากผู้ออกฯ และ ผลท.

** เนื่องจากกำหนดให้ต้องปฏิบัติตามที่ คกก. ของศูนย์ซื้อขายฯ นั้นเป็นผู้กำหนดวิธีการเอง

10 มิ.ย. 68
ค.ร.ม.
เห็นชอบหลักการ

พ.ค. 69
ค.ร.ม. ร้องขอให้รัฐสภาพิจารณา
ร่างกฎหมายต่อไป (มีการตั้ง ค.รม. ใหม่)

10 มิ.ย. 69
ส.ส. ลงมติ
รับร่างหลักการ

ปัจจุบัน
อยู่ระหว่างเข้าชี้แจง กมธ.
/ เตรียมจัดทำหลักการกฎลำดับรอง

การพัฒนามาตรฐาน Securities Tokenization

กำหนดมาตรฐานกลางสำหรับอุตสาหกรรม (Common Industry Standards) เพื่อให้การออกและให้บริการหลักทรัพย์โทเคนเป็นไปในแนวทางเดียวกัน มีความถูกต้อง ปลอดภัย และสามารถเชื่อมโยงและทำงานร่วมกับระบบที่เกี่ยวข้องในตลาดทุนได้ (Interoperability) ครอบคลุมตลอดวงจรชีวิตของหลักทรัพย์โทเคน (Securities Token Lifecycle)

1 Legal Standard



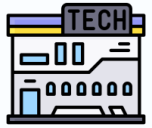
กำหนดความเชื่อมโยงทางกฎหมายระหว่างหลักทรัพย์กับโทเคน (Legal Linkage) ให้ชัดเจนและตรวจสอบได้ เพื่อคงสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ รวมถึงกำหนดเงื่อนไข / กลไกที่เกี่ยวข้องกับการดำเนินการตลอดวงจรชีวิตหลักทรัพย์โทเคน

2 Token Standard



กำหนดมาตรฐานกลางสำหรับการออกแบบและการทำงานของโทเคน (Token Design & Functionality) เพื่อให้โทเคนมีโครงสร้างและคุณสมบัติที่สอดคล้องกัน สามารถตรวจสอบและทำงานร่วมกับระบบที่เกี่ยวข้องได้ (Interoperability)

3 Tokenizer Standard



กำหนดขอบเขตการให้บริการและมาตรฐานสำหรับผู้ให้บริการสนับสนุนการออกหลักทรัพย์โทเคน (Securities Tokenizer) ครอบคลุมการปฏิบัติงานที่เกี่ยวข้องกับการให้บริการหลักทรัพย์โทเคนตลอดวงจรชีวิต การให้บริการกระเป๋าหรือการเก็บรักษาทรัพย์สิน และการสนับสนุนบริการชำระราคา

4 Cybersecurity Standard



กำหนดมาตรฐานด้านความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี (Security & Technology Risk) ครอบคลุมการควบคุมสิทธิและกุญแจ Smart Contract การเฝ้าระวัง การจัดการเหตุการณ์ และความต่อเนื่องในการให้บริการ (Operational Resilience)

ETDA www.etda.or.th | GL1 | Project Guardian | cmta. | ERC Standards

ขอบเขตการใช้งานมาตรฐาน Securities Tokenization

Scope | 3 กลุ่มเป้าหมายหลัก สำหรับการออกและให้บริการหลักทรัพย์โทเคน



01

ISSUER

ผู้ออกหลักทรัพย์โทเคน

ขอบเขตความรับผิดชอบ

- การออกหลักทรัพย์โทเคน
- การเสนอขายหลักทรัพย์โทเคน
- รับผิดชอบงานในฐานะผู้ออกและเสนอขาย



02

SECURITIES TOKENIZER

ผู้ให้บริการสนับสนุนฯ

ขอบเขตการสนับสนุน

- สนับสนุนกระบวนการออก
- สนับสนุนการเสนอขาย
- บริการอื่นตามขอบเขตที่รับผิดชอบ



03

INTERMEDIARIES

ผู้ประกอบธุรกิจตัวกลาง

ขอบเขตการให้บริการ

- กระเป๋าอิเล็กทรอนิกส์ (Wallet)
- การเก็บรักษา (Custody)
- ธุรกรรมหลักทรัพย์โทเคน



กลุ่มใช้อ้างอิงเพิ่มเติม

ผู้ให้บริการเทคโนโลยี · ผู้ให้บริการอื่นที่เกี่ยวข้อง · ผู้สนใจศึกษา

ปรับใช้ตามบทบาท หน้าที่ และขอบเขตงาน

โดยคำนึงถึงกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

Legal Standard - มาตรฐานด้านกฎหมายสำหรับหลักทรัพย์โทเคน

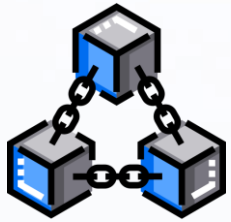


3.1
หลักการสำหรับการออกหลักทรัพย์โทเคน



3.2
การออกเสนอขายหลักทรัพย์โทเคน

Valid issuance and security-token linkage



3.3
การออกแบบเทคโนโลยี

Register integrity and smart contract alignment



3.4
การเปิดเผยข้อมูล

Product, operational, technology, and risk information



3.5
การดำเนินการหลังเสนอขาย

Transfers, corporate actions, and lifecycle controls



3.6
การจัดการกับเหตุการณ์พิเศษ

Access recovery and legally binding authority orders





แหล่งข้อมูลอ้างอิง :
- CMTA - Standard for the tokenization of debt instruments using distributed ledger technology : May 2025
- Monetary Authority of Singapore Guide on the Tokenisation of Capital Markets Products : November 2025

Legal Standard - Principles of Securities Token

3.1



หลักการสำหรับการออกหลักทรัพย์โทเคน

การนำหลักทรัพย์มาออกในรูปแบบโทเคนเป็นการเปลี่ยนแปลงรูปแบบการบันทึกและการบริหารจัดการหลักทรัพย์โดยอาศัยเทคโนโลยีเป็นเครื่องมือ จึงต้องไม่ก่อให้เกิดการเปลี่ยนแปลงสถานะ สิทธิ หน้าที่ หรือผลทางกฎหมายของหลักทรัพย์

หลักทรัพย์ที่ออกในรูปแบบโทเคนได้ (Eligible Securities)

- หลักทรัพย์โทเคน (Tokenized Securities) **ไม่ก่อให้เกิดหลักทรัพย์ประเภทใหม่** โดยสิทธิ หน้าที่ และผลทางกฎหมายของหลักทรัพย์ยังคงเป็นไปตามกฎหมายที่เกี่ยวข้อง
- ต้องเป็นหลักทรัพย์ที่ออกโดยชอบด้วยกฎหมาย



หน่วยลงทุน กองทุนรวม



ตราสารหนี้

การคงไว้ซึ่งสิทธิและผลทางกฎหมาย (Preservation)

- ผู้ถือฯ ยังคงมี **สิทธิและหน้าที่** เช่นเดียวกับผู้ถือฯ รูปแบบอื่นตามประเภทของหลักทรัพย์
- ผู้ถือฯ สามารถใช้สิทธิได้เช่นเดียวกับหลักทรัพย์กระดาษ / scripless เช่น การโอน การรับผลประโยชน์
- เมื่อมีการเปลี่ยนแปลงหรือโอนสิทธิ ต้องสามารถ **ระบุผู้มีสิทธิในหลักทรัพย์โทเคน** ได้อย่างชัดเจน



การถือครองหลักทรัพย์โทเคนผ่านผู้ประกอบธุรกิจตัวกลาง (Intermediated Holding)

- ผู้ถือฯ สามารถจัดเก็บและควบคุมโทเคนผ่านกระเป๋าอิเล็กทรอนิกส์ด้วยตนเอง (Non-custodial wallet) หรือจัดเก็บผ่านผู้ประกอบธุรกิจตัวกลาง (Custodial Service) ก็ได้
- การจัดเก็บผ่านผู้ประกอบธุรกิจตัวกลาง ต้องสามารถ **ระบุและพิสูจน์ตัวตนผู้ถือฯ ได้อย่างชัดเจน** โดยไม่ทำให้สิทธิ หน้าที่ และผลทางกฎหมายของผู้ถือฯ เปลี่ยนไป



กระเป๋าอิเล็กทรอนิกส์ (non-custodial wallet)



ผู้ให้บริการเก็บทรัพย์สิน (Custodial service)

Legal Standard - Technology Design Supporting the Legal Characteristics of Tokenized Securities

3.3

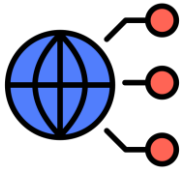


การออกแบบเทคโนโลยีเพื่อรองรับผลทางกฎหมายของหลักทรัพย์โทเคน

ผู้ออกหลักทรัพย์ควรเลือกใช้และออกแบบเทคโนโลยีที่เหมาะสม โดยอาจใช้บล็อกเชน / DLT สัญญาอัจฉริยะ (Smart Contract) หรือกลไกทางเทคโนโลยีอื่น เพื่อรองรับการดำเนินการที่เกี่ยวข้องกับหลักทรัพย์โทเคน

การเลือกใช้เทคโนโลยี
(Technology Selection)

ควรคำนึงถึงความสามารถในการบันทึกข้อมูล การดำเนินการและบริหารจัดการตลอดอายุของหลักทรัพย์



การออกแบบสัญญาอัจฉริยะ
(Smart Contract Design)

ควรออกแบบให้สามารถรองรับสิทธิ หน้าที่ ข้อจำกัด และผลทางกฎหมายของหลักทรัพย์ได้อย่างถูกต้อง ตลอดอายุของหลักทรัพย์

แนวปฏิบัติ : เทคโนโลยีที่เลือกใช้ควรรองรับ

- **ผลทางกฎหมายของหลักทรัพย์**
  - ✓ การควบคุมโดยผู้มีสิทธิ (Control)
  - ✓ ความถูกต้องครบถ้วนของข้อมูล (Integrity)
  - ✓ ความโปร่งใส (Transparency)
  - ✓ ความสามารถในการตรวจสอบ (Verifiability)



- **การจัดทำทะเบียนหลักทรัพย์**
  - ✓ การบันทึกและปรับปรุงข้อมูลทะเบียนหลักทรัพย์
  - ✓ การกำหนดระบบทะเบียนหลักทรัพย์ที่ใช้เป็นหลัก



แนวปฏิบัติ : การออกแบบสัญญาอัจฉริยะ



- **ออกแบบให้สอดคล้องกับ**
  - ✓ สิทธิ หน้าที่ ข้อจำกัด
  - ✓ เงื่อนไขใดที่ต้องรองรับหรือดำเนินการผ่านระบบเทคโนโลยี
  - ✓ การดำเนินการตามข้อกำหนดและเงื่อนไขการให้บริการหลักทรัพย์โทเคน
- **มีมาตรการรองรับกรณีที่สิทธิ หน้าที่ ข้อจำกัด** ไม่สามารถหรือไม่จำเป็นต้องดำเนินการผ่านสัญญาอัจฉริยะ

Legal Standard - Issuance and Offering of Tokenized Securities

3.2



การออกและเสนอขายหลักทรัพย์โทเคน

ผู้ออกหลักทรัพย์ต้องดำเนินการให้เป็นไปตามกฎหมาย และหลักเกณฑ์ที่ใช้บังคับกับหลักทรัพย์แต่ละประเภท และต้องสามารถระบุ/เชื่อมโยงหลักทรัพย์กับโทเคนได้อย่างชัดเจน

ออกหลักทรัพย์โดยชอบด้วยกฎหมาย (Valid Issuance)

จัดให้มีการเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน (Legal Linkage)

ข้อกำหนดการออกหลักทรัพย์โทเคน (Tokenization Terms)

การสร้าง การจัดสรร และการส่งมอบหลักทรัพย์โทเคน

แนวปฏิบัติ :

- **การออกเสนอขายหลักทรัพย์โทเคน** ยังคงต้องปฏิบัติตาม พ.ร.บ. หลักทรัพย์ฯ / หลักเกณฑ์ที่เกี่ยวข้อง
- **การปฏิบัติตามหลักเกณฑ์เฉพาะของหลักทรัพย์**
  - ❑ การเสนอขายตราสารหนี้ PO / HWN
  - ❑ การจัดตั้งกองทุนรวม / การทำ share class

แนวปฏิบัติ :

- **ระบุความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน** โดยมีกลไกเชื่อมโยง เช่น unique identifier / รหัส ISIN
- จัดให้มีช่องทาง**ตรวจสอบความเชื่อมโยงฯ** ผ่านระบบ / เอกสาร / website
- มีกลไก**รองรับการเปลี่ยนแปลง**หรือยกเลิกความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน

แนวปฏิบัติ :

- จัดทำและเปิดเผยข้อกำหนด /เงื่อนไขการออกหลักทรัพย์โทเคน (Tokenization Terms) **เพิ่มเติมจากข้อกำหนดสิทธิ**
- ครอบคลุมสาระสำคัญที่เกี่ยวข้อง เช่น ข้อมูลพื้นฐาน ผู้เกี่ยวข้องกับการให้บริการหลักทรัพย์โทเคน วิธีการตรวจสอบเชื่อมโยงหลักทรัพย์กับโทเคน เงื่อนไขข้อจำกัด (ถ้ามี) และการดำเนินการกรณีสูญเสีย key

แนวปฏิบัติ :

- ควรมีกลไกหรือมาตรการในการ**สร้าง (mint)** และ**จัดสรร (allocate)** หลักทรัพย์โทเคนให้สอดคล้องกับจำนวนและประเภทของหลักทรัพย์
- มีกระบวนการตรวจสอบความถูกต้อง ก่อนส่งมอบให้แก่ผู้ลงทุนที่มีสิทธิได้รับจัดสรรตามผลการเสนอขายอย่างถูกต้อง
- จัดให้ผู้ถือฯ สามารถตรวจสอบความถูกต้องในการส่งมอบได้ด้วยตนเอง

Legal Standard - Disclosure relating to Securities Token

3.4



การเปิดเผยข้อมูลเกี่ยวกับหลักทรัพย์โทเคน

การออกเสนอขายหลักทรัพย์โทเคนอาจมีลักษณะ กลไก หรือเงื่อนไขเพิ่มเติมที่เกิดจากการใช้เทคโนโลยี ซึ่งอาจมีผลต่อสิทธิหรือผลทางกฎหมายของหลักทรัพย์ จึงควรเปิดเผยข้อมูลที่มีลักษณะเฉพาะทั้ง 4 ด้าน

ลักษณะของหลักทรัพย์โทเคน (Product-specific disclosure) +

การดำเนินงานที่เกี่ยวข้อง (Operational-specific disclosures) +

เทคโนโลยีที่ใช้สำหรับหลักทรัพย์โทเคน (Technology-specific disclosures) +

ความเสี่ยงเกี่ยวกับหลักทรัพย์โทเคน (Risk-specific disclosures)



แนวปฏิบัติ :

- **ลักษณะและประเภทของหลักทรัพย์โทเคน** รวมถึง สิทธิ หน้าที่ และผลประโยชน์ของผู้ถืออย่างชัดเจน
- **ความเชื่อมโยงระหว่างหลักทรัพย์กับโทเคน** รวมถึงข้อมูลการถือครอง ทะเบียน และการแสดงสิทธิบนโทเคน
- **เงื่อนไขและข้อจำกัดที่สำคัญ** เช่น การโอน การซื้อขาย และการเข้าถึงข้อมูลที่เกี่ยวข้องตาม Tokenization Terms

แนวปฏิบัติ :

- **กระบวนการออกและส่งมอบ** ครอบคลุม การจัดสรร การส่งมอบ และการชำระราคา รวมถึงกลไกที่เกี่ยวข้อง
- **การถือครองและการให้บริการหลักทรัพย์โทเคน** ครอบคลุมรูปแบบ Wallet หรือการเก็บรักษาทรัพย์สิน รวมถึงวิธีการโอน
- **กระบวนการตลอดวงจรชีวิต** เช่น การใช้สิทธิผลประโยชน์ การทำ Corporate Actions หรือการจัดการเหตุการณ์หรือสถานการณ์พิเศษ

แนวปฏิบัติ :

- **ข้อมูลเทคโนโลยี DLT** ที่ใช้ในออกหลักทรัพย์โทเคน รวมถึงข้อมูลที่จำเป็นต่อความเข้าใจระบบ
- **กลไก Smart Contract** และการทำงานของระบบ หน้าที่สำคัญ เงื่อนไขการทำงาน และอำนาจในการการควบคุมหรือเปลี่ยนแปลง
- **ความสมบูรณ์และข้อจำกัดของธุรกรรม** เช่น กลไก Finality และช่วงเวลาหรือเงื่อนไขที่ทำให้ธุรกรรมสมบูรณ์

แนวปฏิบัติ :

- **ความเสี่ยงSmart Contract** เช่น ทำงานผิดพลาด ไม่เป็นไปตามเงื่อนไข ซึ่งอาจกระทบต่อสิทธิผู้ถือหลักทรัพย์โทเคน
- **ความเสี่ยงจากระบบ DLT** ข้อจำกัดของระบบ ความขัดข้อง การโอนไม่สำเร็จ และผลกระทบต่อการถือครองหรือใช้สิทธิ
- **ความเสี่ยงด้านการเก็บรักษา** เช่น การควบคุม Private Key ความผิดพลาดผู้ให้บริการ และความเสี่ยงเทคโนโลยีหรือโครงสร้างพื้นฐานที่เกี่ยวข้อง

Legal Standard - Post Issuance Operations of Tokenized Securities

3.5



การดำเนินการภายหลังเสนอขายหลักทรัพย์โทเคน

หลักทรัพย์โทเคนอาจมีการโอนระหว่างผู้ถือหลักทรัพย์ และมีการดำเนินการที่เกี่ยวข้องกับสิทธิและผลประโยชน์ตามลักษณะและเงื่อนไขของหลักทรัพย์ ผู้ออกหลักทรัพย์จึงควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับการดำเนินการดังกล่าวให้เป็นไปตามหลักเกณฑ์ที่เกี่ยวข้อง

การโอนหลักทรัพย์โทเคน
(Transfer of Tokenized Securities)

เพื่อรองรับการโอน / รับโอนหลักทรัพย์โทเคนให้มีความถูกต้องตามเจตนาของผู้โอนและผู้รับโอน

แนวปฏิบัติ : ควรมีกลไกรองรับ



- **ตรวจสอบและยืนยันตัวตน** : ของผู้รับโอนว่าตามสิทธิ / เงื่อนไขที่กำหนด / อยู่ในบัญชี whitelist ก่อนแล้วจึงดำเนินการโอน
- **ควบคุมและบังคับใช้เงื่อนไขในการโอน** : กำหนดผ่าน Smart Contract หรือกลไกทางเทคนิคอื่น โดยต้องป้องกันการโอนที่ไม่เป็นตามเงื่อนไขหรือข้อจำกัดได้
- **ตรวจสอบย้อนหลังธุรกรรมการโอน** : transaction hash, block number หรือข้อมูลที่ระบุ wallet address ของผู้โอนและผู้รับโอน

การดำเนินการตามสิทธิของผู้ถือหลักทรัพย์โทเคน (Corporate actions)

เพื่อรองรับการดำเนินการตามสิทธิและผลประโยชน์ รวมถึงการดำเนินการอื่นที่มีผลต่อสิทธิหรือสถานะของหลักทรัพย์โทเคนตามเงื่อนไข

แนวปฏิบัติ : ควรมีกลไกรองรับ



- **การกำหนดและระบุผู้มีสิทธิ** : กำหนดวันเวลา (record date) และใช้ข้อมูลทะเบียนผู้ถือโทเคนประกอบ
- **ดำเนินการตามสิทธิและผลประโยชน์ของผู้ถือหลักทรัพย์** : ใช้ smart contract หรือระบบงานอื่นในการดำเนินการเกี่ยวกับ Corporate actions
- **ตรวจสอบย้อนหลังการดำเนินการตาม Corporate actions** : กำหนดหมายเลขอ้างอิง และเชื่อมโยงข้อมูลกับผู้มีสิทธิ

Legal Standard – Special Circumstances Management

3.6



การจัดการกรณีพิเศษที่เกี่ยวข้องกับหลักทรัพย์โทเคน

ผู้ออกหลักทรัพย์ควรมีกลไกหรือกระบวนการที่เหมาะสมเพื่อรองรับกรณีหรือสถานการณ์ที่นอกเหนือจากการดำเนินงานตามปกติ ซึ่งทำให้ผู้ถือหลักทรัพย์ไม่สามารถใช้หรือเข้าถึงสิทธิของตน หรือทำให้ผู้ออกหลักทรัพย์ต้องดำเนินการกับหลักทรัพย์โทเคนเพื่อให้เป็นไปตามกฎหมาย

การสูญเสียหรือไม่สามารถเข้าถึงหลักทรัพย์โทเคน

เช่น การสูญหายหรือชำรุดของอุปกรณ์ หรือสูญเสีย Private Key ที่ใช้เข้า wallet

แนวปฏิบัติ :

- **การพิสูจน์ตัวตนและสิทธิ** : ของผู้ยื่นคำขอ โดยพิจารณา Re-KYC และตรวจสอบข้อมูลความเชื่อมโยงระหว่างผู้ยื่นคำขอกับ wallet address ที่เคยใช้
- **การดำเนินการเพื่อให้เข้าถึงหลักทรัพย์โทเคนได้** : อาจใช้ฟังก์ชันการกู้คืนหรือโอนย้ายการถือครองโทเคน โดยต้องไม่ทำให้เกิดการถือครองซ้ำซ้อน และรักษาความถูกต้องของทะเบียนผู้ถือและสถานะของหลักทรัพย์โทเคนได้
- **การจัดเก็บหลักฐานและตรวจสอบย้อนหลัง** : จัดเก็บข้อมูลผู้ยื่นคำขอ ข้อมูลการดำเนินการบนบล็อกเชน / DLT

การดำเนินการตามคำสั่งศาลหรือหน่วยงานรัฐที่มีอำนาจสั่งการ

แนวปฏิบัติ

- **กระบวนการรับและตรวจสอบคำสั่ง :** ความถูกต้องของคำสั่ง ขอบเขตคำสั่ง และหลักทรัพ์โทเคนที่ต้องดำเนินการ
- **การดำเนินการตามคำสั่ง :** เช่น สั่งระงับการโอนหรือธุรกรรม / สั่งยกเลิกหรือเพิกถอนธุรกรรม / สั่งให้โอนการถือครองไปยังบุคคลหรือ wallet address ที่กำหนด

Token Standard - มาตรฐานด้านเทคนิคสำหรับหลักทรัพย์โทเคน



4.1

หลักการออกแบบและสถาปัตยกรรมของโทเคน

Token Design Principles and Architecture



4.2

ฟังก์ชันการทำงานของโทเคน

Token Functional Requirements



4.3

ข้อกำหนดด้านข้อมูลของโทเคน

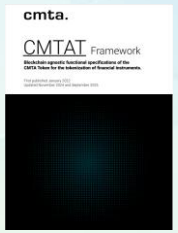
Token Data Requirements



4.4

ข้อกำหนดด้านการทำงานร่วมกันระหว่างระบบ

Interoperability Requirements









แหล่งข้อมูลอ้างอิง :

- CMTAT Framework: Blockchain Agnostic Functional Specifications of the CMTA Token for the Tokenization of Financial Instruments: June 2025
- Tokenization Standards: The Missing Link for Institutional Adoption : February 2025
- Project Guardian : Fixed Income Framework : November 2025
- Project Guardian: Enabling Open and Interoperable Networks : June 2023

Token Standard - Token Design Principles and Architecture

4.1



หลักการออกแบบและสถาปัตยกรรมของโทเคน

กำหนดให้เลือกโครงสร้างพื้นฐานให้เหมาะกับผลิตภัณฑ์ ทำงานได้ถูกต้องตรวจสอบได้ รองรับกิจกรรมตลอดวงจรชีวิต และรองรับการเปลี่ยนแปลงและการเชื่อมต่อในอนาคต โดยรักษาข้อมูลและสิทธิผู้ถือ ทั้งนี้ มาตรฐานไม่ได้กำหนดให้ต้องใช้เทคโนโลยีหรือโครงสร้างใดเป็นการเฉพาะ โดยเปิดกว้างตามหลัก Technology Neutrality

หลักการออกแบบโทเคน (Token Design Principles)

ออกแบบให้โทเคนแทนสิทธิได้ ถูกต้องตรวจสอบได้ และมีคุณลักษณะที่เหมาะสม



แยกองค์ประกอบตามหน้าที่ : เพื่อลดความซับซ้อนของระบบ และรองรับการปรับเปลี่ยนแต่ละส่วนได้โดยกระทบองค์ประกอบอื่นน้อยที่สุด



รองรับการปรับปรุงและพัฒนา : เพื่อรองรับการเปลี่ยนแปลงของหลักทรัพย์ กฎหมาย หรือความต้องการทางธุรกิจในอนาคต



รองรับการตรวจสอบและติดตามย้อนหลัง : เพื่อสนับสนุนการตรวจสอบย้อนหลัง การกำกับดูแล และการพิสูจน์ความถูกต้อง



รองรับการทำงานร่วมกัน : เพื่อสนับสนุนการแลกเปลี่ยนเชื่อมโยงข้อมูล และการทำงานร่วมกันโดยไม่สร้างข้อจำกัดที่ไม่สมเหตุสมผลต่อการเชื่อมต่อ

หลักการเลือกโครงสร้างพื้นฐาน (Infrastructure Selection Principles)

สอดคล้องกับลักษณะและวัตถุประสงค์ของหลักทรัพย์โทเคน และคำนึงถึงหลักการสำคัญ



การเลือกเทคโนโลยีและรูปแบบเครือข่าย : สอดคล้องกับผลิตภัณฑ์ กฎหมาย และความเสี่ยงที่เกี่ยวข้อง



คุณลักษณะเหมาะสม : ข้อมูลถูกต้อง ตรวจสอบได้ และมี finality ชัดเจน และรองรับปริมาณธุรกรรมได้



การรองรับการกำกับดูแล : สามารถบังคับใช้กลไกการกำกับดูแลที่เหมาะสมตลอดวงจรชีวิตของหลักทรัพย์โทเคนได้



รองรับการทำงานร่วมกับระบบอื่น : ความสามารถในการรองรับการเชื่อมต่อและการทำงานร่วมกับโครงสร้างพื้นฐานดิจิทัลอื่นในอนาคต

Token Standard - Token Functional Requirements

4.2



ฟังก์ชันการทำงานของโทเคน

ฟังก์ชันการทำงานของหลักทรัพย์โทเคนควรรองรับการออก การโอน การใช้สิทธิ การกำกับดูแล และการสิ้นผลของโทเคน ให้สอดคล้องกับสิทธิและเงื่อนไขของหลักทรัพย์โดยข้อมูลถูกต้องและตรวจสอบย้อนหลังได้



ฟังก์ชันพื้นฐาน (Core Functions)

จัดการอุปทาน การถือครอง และสถานะให้ถูกต้อง



ฟังก์ชันการบริหารจัดการ (Administrative Functions)

บริหารโทเคนโดยรักษาข้อมูล สิทธิ และเงื่อนไขที่กำหนด



ฟังก์ชันการกำกับดูแล (Compliance Functions)

ตรวจสอบและบังคับใช้ข้อกำหนดก่อนธุรกรรมมีผล



ฟังก์ชันเพิ่มเติม (Additional / Optional Functions)

เลือกใช้ตามผลิตภัณฑ์ และกำหนดเงื่อนไขให้ชัดเจน



ข้อเสนอแนะขั้นต่ำ

- **จัดการอุปทาน** : ออก เพิ่ม ลด หรือทำลายโทเคน ตามเงื่อนไข
- **การโอน :** ตรวจสิทธิ ยอดการโอน และข้อจำกัด ป้องกันรายการซ้ำ ปรับยอดทั้งสองฝ่าย
- **ตรวจยอดและสถานะ :** แสดงยอดรายบัญชี จำนวนรวม สิทธิ และข้อจำกัดล่าสุด



ข้อเสนอแนะขั้นต่ำ

- **จัดการสถานะ :** Freeze / Unfreeze / Suspend พร้อมระบุผลและประวัติ
- **กู้คืนหรือโอนย้าย :** Recovery / Forced Transfer โดยรักษาสิทธิและข้อมูลผู้ถือ
- **เรียกคืนหรือเพิกถอน :** เรียกคืน เพิกถอน หรือยุติโทเคน พร้อมอัปเดตข้อมูลและตรวจสอบย้อนหลังได้
- **ปรับปรุงหรือย้ายสัญญา :** รักษาความต่อเนื่อง ข้อมูล สิทธิ และภาระผูกพัน



ข้อเสนอแนะขั้นต่ำ

- **คุณสมบัติของผู้ถือ :** รองรับ Whitelist / Blacklist หรือเงื่อนไขอื่นเพิ่มเติม เช่น ประเภทผู้ลงทุน ถิ่นที่อยู่ หรือสัญชาติ
- **เงื่อนไขของธุรกรรม :** ตรวจข้อจำกัด ตามกฎหมาย กฎเกณฑ์ หรือเงื่อนไขของหลักทรัพย์ เช่น เพดานถือครอง และจำนวนผู้ถือ



ข้อเสนอแนะขั้นต่ำ

- **Snapshot :** บันทึกสถานะ ณ เวลาที่กำหนด เพื่ออ้างอิงสิทธิหรือผลตอบแทน
- **Partition / Segregation :** แยกสิทธิ สถานะ หรือข้อจำกัด โดยไม่กระทบส่วนอื่น
- **Batch Operation :** ทำธุรกรรมหลายรายการพร้อมกันได้
- **ฟังก์ชันอื่น :** เช่น การออกเสียง การจ่ายผลตอบแทน หรือแปลงสิทธิตามเงื่อนไข

Token Standard - Token Data Requirements

4.3



ข้อกำหนดด้านข้อมูลของโทเคน

รองรับข้อมูลของหลักทรัพย์โทเคนและข้อมูลอ้างอิงที่เกี่ยวข้อง โดยอาจจัดเก็บในลักษณะ on-chain หรือ off-chain ร่วมกัน (Hybrid) ทั้งนี้ ข้อมูลที่จัดเก็บในแต่ละระบบควรสามารถเชื่อมโยงและอ้างอิงถึงโทเคนได้อย่างถูกต้องและน่าเชื่อถือ

ข้อมูลหลักของโทเคน (Core Token Data)

ควรรองรับข้อมูลหลักของโทเคน

ข้อมูลอ้างอิงและเอกสาร (Reference Information)

ควรรองรับการเชื่อมโยงหรือการอ้างอิงข้อมูลและเอกสารที่เกี่ยวข้อง

การกำกับดูแลข้อมูลของโทเคน (Token Data Governance)

ควรมีการกำกับดูแลและบริหารจัดการตลอดวงจรชีวิตของหลักทรัพย์

ข้อเสนอแนะขั้นต่ำ

- **ตัวตนของโทเคน :** มีตัวระบุเป็นเอกลักษณ์ เช่น Token ID
- **ข้อมูลอ้างอิงหลักทรัพย์ :** เชื่อมโยงหลักทรัพย์หรือรุ่น เช่น ISIN / Issue ID
- **ข้อมูลผู้ออก :** ระบุชื่อ LEI หรือเลขทะเบียนนิติบุคคล
- **คุณลักษณะหลักทรัพย์ :** ประเภท สกุลเงิน หน่วย และจำนวนที่ออก
- **สิทธิและเงื่อนไข :** สิทธิ หน้าที่ ดอกเบี้ย ไถ่ถอน หรือแปลงสภาพ

ข้อเสนอแนะขั้นต่ำ

- **ข้อมูลและเอกสารสำคัญ :** ครอบคลุมสิทธิ เงื่อนไข การออกเสนอขายและการเปิดเผยข้อมูลตามข้อกำหนด เช่น ข้อกำหนดสิทธิ หนังสือชี้ชวน แบบแสดงรายการ และ Corporate Action Notice
- **การเชื่อมโยงและอ้างอิง :** มีกลไกในการเชื่อมโยงระหว่างโทเคนและข้อมูลและเอกสารสำคัญ ได้อย่างถูกต้อง น่าเชื่อถือ และตรวจสอบได้ เช่น การใช้ Hash

ข้อเสนอแนะขั้นต่ำ

- **แหล่งข้อมูลหลัก :** กำหนด Authoritative Source รายประเภท ให้ชัดเจนเมื่อข้อมูลอยู่หลายระบบ
- **ความสอดคล้องของข้อมูล** ตรวจพบและแก้ข้อมูลที่ไม่ตรงกัน โดยอ้างอิงแหล่งข้อมูลหลัก
- **การเปลี่ยนแปลงและเวอร์ชัน :** ระบุเวอร์ชันและสถานะการใช้บังคับ ปรับข้อมูลและลิงก์ให้ตรงกับฉบับปัจจุบัน

Token Standard - Interoperability Requirements

4.4



ข้อกำหนดด้านการทำงานร่วมกันระหว่างระบบ

การออกแบบโทเคนควรคำนึงถึงความสามารถในการทำงานร่วมกันระหว่างระบบ (Interoperability) ในลักษณะที่ไม่ปิดกั้นการเพิ่มผู้เกี่ยวข้อง การเชื่อมโยงกับระบบหรือโครงสร้างพื้นฐานอื่นในอนาคต

ขอบเขตการทำงานร่วม (Interoperability Scope)

กำหนดขอบเขตการทำงานร่วมกัน

ข้อกำหนดทางเทคนิคร่วม (Interoperability Technical)

กำหนดรายละเอียดทางเทคนิคร่วมกัน

การปฏิบัติงานร่วม (Operational Interoperability)

กำหนดการปฏิบัติงานหรือการประสานงานร่วมกัน

การกำกับดูแลร่วม (Interoperability Governance)

กำหนดกลไกการกำกับดูแลร่วมกัน

ข้อเสนอแนะขั้นต่ำ

- **กิจกรรมทางธุรกิจ :** ระบุกิจกรรม วัตถุประสงค์ และผลลัพธ์ตลอดวงจรชีวิต
- **ผู้เกี่ยวข้อง :** ระบุแต่ละฝ่าย บทบาท ความรับผิดชอบ และการประสานงาน
- **ระบบและโครงสร้างพื้นฐาน :** ระบุหน้าที่และความสัมพันธ์ ทั้ง DLT/Blockchain และระบบเดิม

ข้อเสนอแนะขั้นต่ำ

- **แบบจำลองและโครงสร้างข้อมูล :** กำหนดชนิด ความหมาย และ mapping
- **การเชื่อมต่อและแลกเปลี่ยน :** กำหนดคำขอ ผลตอบรับ ข้อผิดพลาด และป้องกันการประมวลผลซ้ำ
- **เหตุการณ์และพฤติกรรม :** ระบุเงื่อนไข สถานะ และผลให้ตรงกัน
- **ตัวระบุและข้อมูลอ้างอิงร่วม :** มีเอกลักษณ์และเชื่อมโยงข้ามระบบได้
- **มาตรฐานและความเข้ากันได้ :** ใช้มาตรฐานที่ยอมรับ รองรับ mapping เวอร์ชัน ช่วงเปลี่ยนผ่าน และรายใหม่

ข้อเสนอแนะขั้นต่ำ

- **บทบาทและความรับผิดชอบ :** กำหนดผู้รับผิดชอบแต่ละขั้นตอน และเงื่อนไขส่งต่องาน
- **กระบวนการและลำดับงาน :** ระบุสถานะ เวลา เงื่อนไขเริ่ม–จบ การยืนยันผล และการกระทบยอด
- **การประสานงาน :** ระบุผู้ติดต่อ ข้อมูล ช่องทาง การตอบรับ และการส่งต่อปัญหา
- **เหตุผิดปกติและขัดข้อง :** จำกัดผลกระทบ กู้คืน ป้องกันรายการซ้ำ กระทบยอดก่อนกลับให้บริการ

ข้อเสนอแนะขั้นต่ำ

- **บทบาทในการกำกับดูแล :** กำหนดผู้ดูแลกติกา อำนาจอนุมัติ ความเสี่ยง และการยุติข้อขัดแย้ง
- **บริหารการเปลี่ยนแปลง :** ประเมิน อนุมัติ ทดสอบ แจ้งล่วงหน้า พร้อมช่วงเปลี่ยนผ่านและ Rollback
- **สื่อสารและประสานงาน :** แจ้งกติกา เวอร์ชัน มติ และการเปลี่ยนแปลง พร้อมเก็บหลักฐาน
- **ติดตามและทบทวน :** กำหนดรอบ ผู้รับผิดชอบ และแผนปรับปรุงทบทวนเพิ่มเมื่อมีเหตุสำคัญ

Tokenizer Standard – มาตรฐานผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน



5.1

Scope of Services

บทบาทและขอบเขตการให้บริการ



5.2

Eligibility and Qualifications

คุณสมบัติและความพร้อมของผู้ให้บริการ



5.3

Conduct Standards

แนวทางการปฏิบัติหน้าที่และการให้บริการ

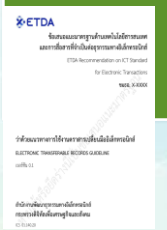


5.4

Operational Guidelines

แนวทางการดำเนินงานตามขอบเขตของผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน





แหล่งข้อมูลอ้างอิง :

- Bank For International Settlement, Principles for financial market infrastructures : April 2012
- United Nations, UNCITRAL Model Law on Electronic Transferable Records: July 2018
- สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์, ร่างข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

Tokenizer Standard - Scope of Services

5.1



บทบาทและขอบเขตการให้บริการ

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน อาจมีรูปแบบการประกอบธุรกิจและขอบเขตการให้บริการที่แตกต่างกัน โดยมีขอบเขตการให้บริการหลัก โดยแบ่งออกเป็น 3 ด้าน ดังนี้

งานด้านการออก การบันทึกการทำรายการ และการดูแลหลักทรัพย์โทเคน

เกี่ยวข้องกับการจัดให้หลักทรัพย์สามารถถูกสร้างและออกในรูปแบบโทเคน จัดทำและบันทึกข้อมูลตลอดจนการดำเนินการที่ทำให้เกิดหรือเปลี่ยนแปลงสถานะ สิทธิหรือความเป็นเจ้าของในหลักทรัพย์โทเคนตลอดวงจรชีวิตหลักทรัพย์

- การออกหลักทรัพย์โทเคน
- การจัดทำและบันทึกข้อมูลหลักทรัพย์โทเคน
- การส่งมอบและรับมอบหลักทรัพย์โทเคน
- การโอนและการรับโอนหลักทรัพย์โทเคน
- การใช้หลักทรัพย์โทเคนเป็นหลักประกัน
- การให้บริการด้านสิทธิประโยชน์และการดำเนินการตามสิทธิของผู้ถือหลักทรัพย์

งานด้านการถือครองและการดูแลรักษาหลักทรัพย์โทเคน

เกี่ยวข้องกับการจัดให้ผู้ลงทุนหรือผู้มีสิทธิสามารถถือครอง เข้าถึง และควบคุมหลักทรัพย์โทเคนผ่านกลไกทางอิเล็กทรอนิกส์ที่เหมาะสม

- การจัดให้มีหรือให้บริการเกี่ยวกับ **Non-Custodial Wallet**
- การรับฝากหรือเก็บรักษาหลักทรัพย์โทเคน หรือ **Custodial Service**

งานด้านการชำระราคาและการส่งมอบหลักทรัพย์โทเคน (Settlement)

การจัดให้มีกระบวนการและกลไกสำหรับการชำระราคาและส่งมอบหลักทรัพย์โทเคนเพื่อเป็นไปตามเงื่อนไขของการทำธุรกรรม

- การจัดกระบวนการชำระราคา (Settlement Processing)
- การเชื่อมโยงการชำระราคาและส่งมอบ (Exchange of Value)
- การเชื่อมต่อกับระบบ (Settlement Infrastructure) หรือสินทรัพย์ที่ใช้ในการชำระราคา (Settlement Asset)
- การติดตามและจัดการสถานะการชำระราคา

Tokenizer Standard - Eligibility and Qualifications

5.2



คุณสมบัติและความพร้อมของผู้ให้บริการ

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน ควรแสดงถึงความพร้อม และให้บริการตามบทบาท/ขอบเขตการให้บริการที่ตนรับผิดชอบ เพียงพอและเหมาะสมกับลักษณะ ขนาด ความซับซ้อน และระดับความเสี่ยงของการให้บริการ โดยคุณสมบัติแบ่งออกเป็น 4 ปัจจัยดังต่อไปนี้

ฐานะทางการเงินและเงินทุน



แนวปฏิบัติ :

- ควรจัดให้มีเงินทุนหรือแหล่งเงินทุนที่มีคุณภาพและสภาพคล่องเพียงพอ เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง
- **ควรมีมูลค่าไม่น้อยกว่า 6M - Operational Expenses** อ้างอิงจากงบการเงินล่าสุด

โครงสร้างองค์กรและการกำกับดูแล



แนวปฏิบัติ :

- **การจัดโครงสร้างองค์กรและแบ่งหน้าที่รับผิดชอบ** : ให้สอดคล้องกับลักษณะ ขนาด ความซับซ้อน และขอบเขตการให้บริการ
- **การแบ่งแยกหน้าที่และสอบทาน** : เพื่อให้การปฏิบัติงาน อนุมัติ ตรวจสอบ มีการควบคุม ถ่วงดุลที่เหมาะสม
- **การกำกับดูแลและการตัดสินใจ** : กำหนดเรื่องที่ผ่านพิจารณา BoD และจัดให้มีการรายงานที่จำเป็น
- **การป้องกันและจัดการ COI** : เช่น จำกัดการเข้าถึงข้อมูล กำหนดผู้มีอำนาจอนุมัติ หรือการเปิดเผย COI

บุคลากรและความเหมาะสมในการปฏิบัติหน้าที่



แนวปฏิบัติ :

- มีบุคลากร **เพียงพอและเหมาะสม** กับการดำเนินธุรกิจ
- บุคลากรมี **คุณสมบัติ ความรู้ และประสบการณ์** ที่สอดคล้องกับหน้าที่
- มีการ **พัฒนาศักยภาพบุคลากร** อย่างต่อเนื่องให้เท่าทันต่อการเปลี่ยนแปลง

ระบบงานและความพร้อมในการให้บริการ



แนวปฏิบัติ :

- ระบบ **บริหารความเสี่ยงและระบบการควบคุมภายใน** ที่มีประสิทธิภาพ
- ระบบ **จัดเก็บข้อมูลและหลักฐานการประกอบธุรกิจ** ที่เพียงพอ ถูกต้องครบถ้วนและสามารถตรวจสอบย้อนหลังได้
- ระบบ **บริหารจัดการเหตุการณ์ผิดปกติและ BCM** เพื่อรองรับการดำเนินงานในภาวะฉุกเฉิน
- การกำกับดูแล **ผู้ให้บริการภายนอก (outsourcing)** อย่างมีประสิทธิภาพและเหมาะสมกับความเสี่ยง (ถ้ามี)
- จัดให้มี **แผนการฟื้นฟูกิจการ การกอบกู้ระบบงาน และการยุติ** การประกอบธุรกิจอย่างเป็นระเบียบ

Tokenizer Standard – Conduct Standards

5.3



แนวทางการปฏิบัติหน้าที่และการให้บริการ

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน ควรปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต เป็นธรรม และคำนึงถึงประโยชน์ของผู้ใช้บริการและผู้ถือหลักทรัพย์ โดยให้บริการตามบทบาทและหน้าที่ที่ตนรับผิดชอบอย่างเหมาะสม โปร่งใส และไม่กระทำการที่อาจก่อให้เกิดความเสียหายแก่ผู้ใช้บริการหรือผู้ถือหลักทรัพย์โดยไม่เหมาะสม

การปฏิบัติหน้าที่ซื่อสัตย์ สุจริต เป็นธรรม

แนวปฏิบัติ :

- **ซื่อสัตย์ สุจริต และเป็นธรรม :** ควรปฏิบัติหน้าที่โดยไม่แสวงหาผลประโยชน์โดยมิชอบ
- **ความรู้ ความสามารถ และความระมัดระวัง :** ควรปฏิบัติหน้าที่ด้วยความระมัดระวังที่เหมาะสมกับความเสี่ยงของการให้บริการ
- **คำนึงถึงประโยชน์และสิทธิ :** ควรดำเนินการโดยคำนึงถึงสิทธิและประโยชน์ของผู้ใช้บริการ พร้อมให้บริการอย่างมีประสิทธิภาพ
- **ไม่ใช้ข้อมูล/อำนาจหน้าที่โดยมิชอบ :** ไม่ใช้อำนาจหรือโอกาสที่ได้รับเพื่อแสวงหาประโยชน์โดยมิชอบหรือก่อให้เกิดความเสียหายแก่ผู้ใช้บริการ

การจัดการความขัดแย้งทางผลประโยชน์

แนวปฏิบัติ :

- **ระบุและประเมินความขัดแย้งทางผลประโยชน์** ที่อาจเกิดขึ้นจากบทบาทที่หรือการให้บริการที่ทับซ้อนกันอย่างเหมาะสม
- **ป้องกันและจัดการความขัดแย้งทางผลประโยชน์** เพื่อให้การปฏิบัติหน้าที่และการตัดสินใจเป็นไปอย่างเป็นธรรม
- **เปิดเผยความขัดแย้งทางผลประโยชน์** ที่ไม่สามารถจัดการได้อย่างเพียงพอ เพื่อให้ผู้ใช้บริการรับทราบและประเมินความเสี่ยงที่เกี่ยวข้องได้

การเปิดเผยข้อมูลและความโปร่งใส

แนวปฏิบัติ :

- เปิดเผยข้อมูลลักษณะ **ขอบเขตการให้บริการ บทบาท หน้าที่และความรับผิดชอบ** ผู้ให้บริการ
- **กระบวนการและเงื่อนไขบริการ** ค่าธรรมเนียม ค่าใช้จ่าย การใช้บริการ outsourcing ที่อาจกระทบต่อบริการ
- **ความเสี่ยงและข้อจำกัดบริการ** ที่อาจส่งผลต่อสิทธิของผู้ใช้บริการ
- จัดให้ผู้ใช้บริการ **เข้าถึงข้อมูลที่จำเป็น** และควรปรับปรุงข้อมูลดังกล่าวให้ถูกต้องเป็นปัจจุบัน
- จัดให้มี **ช่องทางอิเล็กทรอนิกส์** สำหรับข้อมูลที่เกี่ยวข้องกับหลักทรัพย์โทเคน ที่โปร่งใสและสามารถตรวจสอบได้

การรักษาความลับและข้อมูล

แนวปฏิบัติ :

- **การใช้และเปิดเผยข้อมูล :** ควรใช้และเปิดเผยข้อมูลเท่าที่จำเป็น พร้อมคุ้มครองข้อมูลและไม่ใช้เพื่อประโยชน์โดยมิชอบ
- **การจำกัดการเข้าถึงข้อมูล :** ควรกำหนดสิทธิการเข้าถึงข้อมูลตามความจำเป็นและมีมาตรการป้องกันการใช้ข้อมูลโดยมิชอบ
- **การรักษาความลับ** ของข้อมูลและควบคุมการใช้หรือเปิดเผยข้อมูลอย่างเหมาะสมตลอดระยะเวลาที่มีหน้าที่เก็บรักษาข้อมูล

การจัดการข้อร้องเรียนและข้อพิพาท

แนวปฏิบัติ :

- ควรจัดให้มี **ช่องทางรับข้อร้องเรียน** พร้อมสื่อสารให้ผู้ใช้บริการรับทราบ
- ควรกำหนด **ขั้นตอนการรับ พิจารณาและจัดการข้อร้องเรียน** โดยคำนึงถึงสิทธิผู้ใช้บริการ/ผู้ถือหลักทรัพย์โทเคน
- ควรกำหนดหลักเกณฑ์การ **ยกระดับข้อร้องเรียน/ข้อพิพาท** ที่กระทบผู้ให้บริการไปยังผู้ที่มีอำนาจอย่างเหมาะสม
- ควร **บันทึกและจัดเก็บ** ข้อร้องเรียนอย่างเหมาะสม **เพื่อติดตาม ตรวจสอบและปรับปรุง** การใช้บริการอย่างต่อเนื่อง

Tokenizer Standard – Operational Guidelines

5.4



แนวทางการดำเนินการตามขอบเขตของผู้การให้บริการ

ผู้ให้บริการสนับสนุนการออกและเสนอขายหลักทรัพย์โทเคน ควรมีระบบและกระบวนการที่เหมาะสม เพื่อให้ดำเนินงานได้อย่างมีประสิทธิภาพและสามารถบริหารความเสี่ยงที่เกี่ยวข้องได้อย่างเหมาะสมตามรูปแบบธุรกิจและขอบเขตการให้บริการ

งานด้านการออก การบันทึกการทำรายการ และการดูแลหลักทรัพย์โทเคน

- **การออกหลักทรัพย์โทเคน (Issuance) :** ข้อมูลมีความถูกต้อง ครบถ้วน และเชื่อมโยงกันได้ มีความเป็นหนึ่งเดียว (Singularity) และสามารถระบุผู้มีสิทธิควบคุม (Exclusive Control)
- **การจัดทำบันทึกข้อมูล (Registration /Record) :** มีระบบบันทึก เชื่อมโยงหลักทรัพย์โทเคนที่ถูกต้องสอดคล้องกับทะเบียนหลักทรัพย์
- **การส่งมอบ-รับมอบ (Delivery) :** ระบุผู้รับมอบได้พร้อมส่งมอบสิทธิควบคุม (Exclusive Control) ป้องกันการส่งมอบซ้ำซ้อน รวมทั้งจัดเก็บหลักฐานที่ถูกต้อง ตรวจสอบย้อนหลังได้
- **การโอน-รับโอน (Transfer) :** มีกลไกตรวจสอบสิทธิและข้อจำกัดก่อนการโอน เมื่อโอนสำเร็จ สิทธิและการควบคุมต้องเปลี่ยนไปยังผู้รับโอน
- **การใช้เป็นหลักประกัน (Pledge) :** รองรับการสร้าง /บันทึกสถานะหลักประกัน กำหนด lock การโอนสิทธิและรองรับการปลด และการบังคับหลักประกัน
- **การให้บริการ Corporate Actions :** มีกลไกรองรับการใช้สิทธิและจัดสรรสิทธิประโยชน์ได้อย่างถูกต้อง ครบถ้วน ตรวจสอบได้

งานด้านการถือครองและการดูแลรักษาหลักทรัพย์โทเคน

กรณี Non-Custodial Wallet : ควรจัดให้มี

- ✓ **การออกแบบและควบคุม Wallet** : ให้เหมาะสมกับหลักทรัพย์โทเคน พร้อมกำหนดกลไกจัดการ Credential ที่ทำให้ผู้มีสิทธิควบคุมสินทรัพย์ได้
- ✓ **การเชื่อมโยงและตรวจสอบสิทธิ** : เชื่อมโยง Wallet กับลูกค้าและหลักทรัพย์โทเคน พร้อมตรวจสอบสิทธิและข้อจำกัดก่อนทำรายการ
- ✓ **การทำรายการและบริหารวงจรชีวิต**: รองรับการรับ ส่งมอบ และโอนหลักทรัพย์ แสดงผลและสถานะอย่างถูกต้อง ตรวจสอบย้อนหลังได้ รวมถึงรองรับการเปลี่ยนแปลง กู้คืน และยุติการใช้งาน

กรณี Custodial Service : ควรจัดให้มี

- ✓ **การดูแลและคุ้มครองทรัพย์สิน** : กระบวนการรับฝาก ส่งคืน และโอนหลักทรัพย์ พร้อมจัดทำบัญชีและแยกทรัพย์สินลูกค้า (Segregation) ให้ระบุเจ้าของและจำนวนได้ชัดเจน
- ✓ **การควบคุมการดำเนินงาน** : บริหารจัดการ Wallet & Key ตรวจสอบคำสั่งและอนุมัติรายการตลอดจนแบ่งแยกหน้าที่เพื่อป้องกันการทุจริตหรือการใช้ทรัพย์สินโดยไม่ได้รับอนุญาต

งานด้านการชำระราคาและการส่งมอบหลักทรัพย์โทเคน

- **การประมวลผลรายการ (Settlement Processing) :** มีกลไกรับและตรวจสอบคำสั่ง ข้อมูลที่เกี่ยวข้อง ความพร้อมหลักทรัพย์โทเคน/สินทรัพย์ที่ใช้ชำระราคา ประมวลผลติดตามสถานะรายการตั้งแต่รับคำสั่งจนเสร็จสมบูรณ์
- **การเชื่อมโยงการชำระราคาและการส่งมอบ (Exchange-of-Value Settlement) :** จัดให้มีกลไก เช่น DvP, DvD และ PvP โดยกำหนดเงื่อนไขให้ภาระผูกพันทั้งสองด้านดำเนินการสำเร็จตามที่กำหนด เพื่อลด Principal Risk พร้อมรองรับ Atomic Settlement และมีกระบวนการจัดการกรณีรายการไม่สำเร็จ
- **การจัดการ Settlement Asset and Infrastructure :** เชื่อมโยงกับระบบหรือผู้ให้บริการที่เกี่ยวข้องเพื่อรับและตรวจสอบผลการชำระราคา พร้อมประเมิน Credit Risk / Liquidity Risk / Operational Risk รวมถึงมีกระบวนการรองรับกรณีระบบขัดข้อง
- **การกำหนด Point of Finality :** พร้อมระบุผลและเงื่อนไขการเพิกถอนรายการ กำหนด Settlement Timing โดยอาจรองรับการชำระราคาระหว่างวันหรือทันที และบันทึกวันเวลาสถานะ และผลของรายการ (Final Settlement)
- **การจัดทำบันทึกและการกระทบยอดผล :** ควรจัดให้มีระบบบันทึก ตรวจสอบ และกระทบยอดการชำระราคาและการส่งมอบหลักทรัพย์โทเคน เพื่อให้ข้อมูลถูกต้องและตรวจสอบได้

Cybersecurity Standard - มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

6.1
การกำกับดูแลและความเสี่ยงด้านเทคโนโลยี
Security and Technology Risk Governance

6.2
ระบบ แอปพลิเคชัน และโครงสร้างพื้นฐาน DLT
System, Application and DLT Infrastructure Security

6.3
การพิสูจน์ตัวตนและควบคุมสิทธิการเข้าถึง
Identity and Access Control

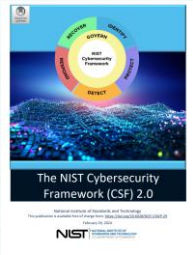
6.4
กุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษ
Cryptographic Key and Privileged Operations Management

6.5
ความปลอดภัยและความน่าเชื่อถือของข้อมูล
Data Protection, Integrity and Cryptographic Assurance

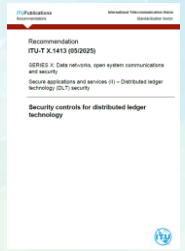
6.6
การติดตามเหตุการณ์ การบันทึกข้อมูล และการตรวจสอบย้อนหลัง
Monitoring, Logging and Auditability

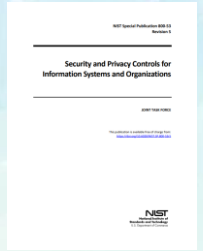
6.7
การบริหารจัดการช่องโหว่และการทดสอบด้านความมั่นคงปลอดภัย
Vulnerability Management and Security Testing

6.8
การตอบสนองต่อเหตุการณ์และความพร้อมด้านการดำเนินงาน
Incident Response and Operational Resilience









แหล่งข้อมูลอ้างอิง :
- NIST — The NIST Cybersecurity Framework (CSF) 2.0 : February 2024
- ITU-T X.1413 — Security Controls for Distributed Ledger Technology : May 2025
- ITU-T X.1402 — Security Framework for Distributed Ledger Technology
- NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations : September 2020 (Updated 2025)

Cybersecurity - Security and Technology Risk Governance

6.1



การกำกับดูแลความมั่นคงปลอดภัยและความเสี่ยงด้านเทคโนโลยี

ควรมีกรอบกำกับดูแล ผู้รับผิดชอบ และมาตรการควบคุมตามระดับความเสี่ยง ครอบคลุมระบบบน DLT ระบบภายนอก และผู้ให้บริการที่เกี่ยวข้อง



การกำกับดูแลและบริหารความมั่นคงปลอดภัย (Security Governance and Management)

กำหนดทิศทางและติดตามมาตรการให้เหมาะกับความเสี่ยงอย่างต่อเนื่อง



การบริหารจัดการการเปลี่ยนแปลงระบบ (Change Management)

ควบคุมการเปลี่ยนแปลงที่กระทบระบบ ข้อมูล ธุรกรรม และสิทธิผู้ถือ



การบริหารจัดการผู้ให้บริการภายนอก (Third-Party Risk Management)

บริหารความเสี่ยงตลอดการใช้บริการตั้งแต่คัดเลือกจนถึงยุติบริการ



ข้อเสนอแนะขั้นต่ำ

- **กรอบกำกับดูแล :** มีนโยบายเป็นลายลักษณ์อักษร **ทบทวนอย่างน้อยปีละครั้ง** หรือเมื่อเปลี่ยนแปลงสำคัญ
- **บทบาทและความรับผิดชอบ :** กำหนดผู้รับผิดชอบชัดเจน และแบ่งแยกหน้าที่สำหรับงานเสี่ยงสูง
- **บริหารความเสี่ยง :** ระบุ ประเมิน จัดการ และติดตามความเสี่ยง การยอมรับความเสี่ยงต้องได้รับอนุมัติ
- **สร้างความตระหนักรู้ :** ฝึกอบรมผู้เกี่ยวข้องให้เหมาะกับบทบาท หน้าที่ และระดับความรับผิดชอบ



ข้อเสนอแนะขั้นต่ำ

- **กระบวนการเปลี่ยนแปลง :** มีขั้นตอน ผู้รับผิดชอบ และผู้อนุมัติ แยกกรณีทั่วไป สำคัญ และฉุกเฉิน
- **ประเมินและอนุมัติ :** ประเมินผลกระทบก่อนเปลี่ยนแปลง พร้อมอนุมัติและแบ่งแยกหน้าที่ตามความเสี่ยง
- **ทดสอบและนำขึ้นใช้งาน :** ทดสอบก่อนใช้จริง ตรวจผล และมีทางย้อนกลับหรือจำกัดผลกระทบ
- **กรณีฉุกเฉินและหลักฐาน :** บันทึกเหตุผลและการอนุมัติ ติดตามผล และทบทวนการเปลี่ยนแปลงย้อนหลัง



ข้อเสนอแนะขั้นต่ำ

- **กระบวนการบริหารผู้ให้บริการ :** กำหนดขั้นตอนเป็นลายลักษณ์อักษร ควบคุมตามความสำคัญและความเสี่ยง
- **ประเมินและคัดเลือก :** ประเมินความพร้อมและความเสี่ยงก่อนใช้บริการ รวมผู้ให้บริการช่วงต่อ
- **ข้อตกลงและการติดตาม :** กำหนดระดับบริการ การแจ้งเหตุ สิทธิเข้าถึงข้อมูล และติดตามตามสัญญา
- **ความต่อเนื่องและการยุติบริการ :** ลดการพึ่งพาหรือกระจุกตัว มีแผนสำรอง ย้าย หรือยุติบริการ

Cybersecurity - System, Application and DLT Infrastructure Security

6.2



ความมั่นคงปลอดภัยของระบบ แอปพลิเคชัน และโครงสร้างพื้นฐาน DLT

ต้องออกแบบ พัฒนา ทดสอบ และดูแลระบบโดยคำนึงถึงความมั่นคงปลอดภัย ครอบคลุมทั้ง On-chain และ Off-chain โดยเลือกมาตรการตามความเสี่ยงและเป็นกลางทางเทคโนโลยี



การออกแบบและพัฒนาระบบอย่างมั่นคงปลอดภัย
(Secure System Development)

คำนึงถึงความปลอดภัยตั้งแต่เริ่มต้น จนถึงการยุติใช้งานระบบ



ความมั่นคงปลอดภัยและการเปลี่ยนแปลง Smart Contract
(Smart Contract Security and Change Management)

Logic ควรสอดคล้องกับสิทธิและเงื่อนไข รวมถึง Logic อัตโนมัติที่ให้ผลเช่นเดียวกัน



ความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน DLT
(DLT Infrastructure Security)

รักษาความถูกต้องของธุรกรรม ความพร้อมใช้งาน และความต่อเนื่อง



ข้อเสนอแนะขั้นต่ำ

- **วงจรการพัฒนาที่ปลอดภัย :** กำหนด Secure Development Lifecycle และข้อกำหนดความปลอดภัยตั้งแต่ต้น
- **สภาพแวดล้อมและสิทธิ :** จำกัด Source Code และเครื่องมือ แยก Dev/Test/Production ป้องกัน Key รั่วไหล
- **ส่วนประกอบและระบบเชื่อมต่อ :** ประเมินความเสี่ยง ติดตามช่องโหว่ และปรับปรุงเวอร์ชันของส่วนประกอบ
- **การทดสอบและเอกสาร :** ทดสอบก่อนใช้จริงหรือเปลี่ยนสำคัญ เก็บเอกสารพัฒนา ตั้งค่า และทดสอบ



ข้อเสนอแนะขั้นต่ำ

- **การออกแบบและข้อกำหนด :** Logic ตรงตามสิทธิ ควบคุมข้อมูลซ้ำ/ไม่ครบ และธุรกรรมระหว่างเครือข่ายทำงานประสานกันอย่างถูกต้อง
- **สิทธิและการตั้งค่า :** จำกัดผู้ดำเนินการและค่าที่สำคัญ รวมความถูกต้องของข้อมูล Oracle
- **ตรวจสอบและนำขึ้นใช้งาน :** ตรวจและทดสอบก่อนใช้หรืออัปเกรด เก็บ Version, Source และ Address
- **ติดตามและรับมือเหตุผิดปกติ :** มีแนวทางระงับ กู้คืน หรือย้าย พร้อมหลักฐานสำหรับตรวจสอบย้อนหลัง



ข้อเสนอแนะขั้นต่ำ

- **องค์ประกอบ การตั้งค่า และสิทธิ :** ระบุ Node/API ตั้งค่าให้ปลอดภัย ประเมิน Validator, Consensus และการกระจุกตัว
- **เครือข่ายและความพร้อมใช้งาน :** ควบคุมการเชื่อมต่อ รองรับปริมาณงานและเหตุขัดข้อง มีระบบหรือบริการสำรอง
- **ติดตามและจัดการเหตุ DLT :** ติดตาม Node, Finality, Oracle/Bridge และ Cross-chain รองรับ Hard Fork และเก็บหลักฐาน

Cybersecurity - Identity and Access Control

6.3



การพิสูจน์ตัวตนและการควบคุมสิทธิการเข้าถึง

ควรระบุตัวตน พิสูจน์ตัวตน และกำหนดสิทธิตามหน้าที่และความจำเป็น โดยครอบคลุมผู้ใช้งาน ผู้ดูแล ผู้ให้บริการภายนอก และบัญชีระบบ ทั้ง On-chain และ Off-chain



การบริหารจัดการตัวตนและสิทธิการเข้าถึง

(Identity and Access Management)

บริหารสิทธิตลอดวงจรชีวิต ตั้งแต่การให้สิทธิ การเปลี่ยนแปลงสิทธิ การทบทวนจนถึงยกเลิกสิทธิ



ข้อเสนอแนะขั้นต่ำ

- **ตัวตนและการพิสูจน์ตัวตน :** ระบุผู้รับผิดชอบของแต่ละบัญชี ใช้ MFA หรือเทียบเท่าสำหรับระบบสำคัญ และหลีกเลี่ยงบัญชีร่วมที่ระบุผู้ใช้ไม่ได้
- **กำหนดและควบคุมสิทธิ :** ให้สิทธิเท่าที่จำเป็นตามหน้าที่ มีการอนุมัติและแบ่งแยกหน้าที่ ปรับหรือยกเลิกสิทธิทันท่วงที
- **ทบทวนสิทธิและบัญชีระบบ :** ทบทวนเป็นระยะ ดูแล System Account, API Key และ Credential ให้ปลอดภัย หมุนเวียนหรือยกเลิกตามเหมาะสม
- **ติดตามและตรวจสอบ :** บันทึกการเข้าถึงและการเปลี่ยนสิทธิ ตรวจจับความผิดปกติ และป้องกัน Log จากการแก้ไขหรือลบโดยมิชอบ



การบริหารจัดการสิทธิพิเศษ

(Privileged Access Management)

บัญชีที่มีสิทธิพิเศษ/เข้าถึงระบบสำคัญสูง เช่น การตั้งค่าระบบ การบริหารจัดการโครงสร้างพื้นฐาน ควรควบคุมให้เข้มงวดกว่าบัญชีทั่วไป



ข้อเสนอแนะขั้นต่ำ

- **ระบุ อนุมัติ และจำกัดสิทธิ :** แยกบัญชีสิทธิพิเศษจากบัญชีทั่วไป จำกัดขอบเขต ระยะเวลา และภารกิจตามความจำเป็น
- **พิสูจน์ตัวตนและควบคุมการใช้ :** ใช้ MFA หรือเทียบเท่า ป้องกัน Credential งานเสี่ยงสูงควรแบ่งหน้าที่หรือมีผู้ควบคุมหลายคน
- **ติดตาม ทบทวน และสิทธิฉุกเฉิน :** บันทึกการใช้ **ทบทวนบัญชีระบบสำคัญอย่างน้อยปีละครั้ง** และเมื่อเปลี่ยนแปลง กำหนดเงื่อนไขฉุกเฉินและยกเลิกเมื่อไม่มีความจำเป็นต้องใช้งาน

Cybersecurity- Cryptographic Key and Privileged Operations Management

6.4



การบริหารจัดการกุญแจเข้ารหัสและการดำเนินการที่มีสิทธิพิเศษ

ควรควบคุมกุญแจและอำนาจที่มีผลต่อระบบ สถานะโทเคน และสิทธิผู้ถือ ครอบคลุมกุญแจในความรับผิดชอบของผู้ให้บริการ ไม่รวม Private Key ที่ผู้ลงทุนถือและควบคุมเอง



การบริหารจัดการวงจรชีวิตของกุญแจเข้ารหัส (Cryptographic Key Lifecycle Management)

ดูแลตั้งแต่สร้าง จัดเก็บ ใช้งาน หมุนเวียน กู้คืน จนถึงยุติการใช้งาน



การบริหารจัดการกุญแจที่มีสิทธิพิเศษ (Privileged Key Management)

ควบคุมเพิ่มเติมสำหรับกุญแจ ที่มีอำนาจหรือผลกระทบสูง



การกำกับดูแลการดำเนินการบนระบบที่มีสิทธิพิเศษ (Governance of Privileged Operations)

การดำเนินการควรอยู่ในอำนาจและเงื่อนไขที่ได้รับอนุมัติ



ข้อเสนอแนะขั้นต่ำ

- **รายการกุญแจและผู้รับผิดชอบ :** มี Key Inventory ระบุวัตถุประสงค์ ผู้ถือครองหรือระบบ ขอบเขต ความสำคัญ และสถานะ
- **สร้าง จัดเก็บ และใช้กุญแจ :** ใช้ความสุ่มปลอดภัย จำกัดสิทธิ ใช้ HSM หรือเทียบเท่า ไม่เปิดเผยกุญแจใน Source/Config
- **หมุนเวียน ยกเลิก และรับมือเหตุ :** กำหนดรอบและแผนเมื่อกุญแจหาย รั่วไหล หรือใช้ไม่ได้ พร้อมกู้คืนโดยรักษาความต่อเนื่อง
- **หลักฐานตลอดวงจรชีวิต :** บันทึกการสร้าง เข้าถึง ใช้ เปลี่ยนแปลง และยกเลิก ป้องกันหลักฐานถูกแก้ไขหรือลบ



ข้อเสนอแนะขั้นต่ำ

- **ระบุและจำแนกกุญแจ :** ระบุ Mint/Burn/Upgrade Key และกุญแจสำคัญ กำหนดผู้ควบคุม วัตถุประสงค์ และขอบเขต
- **ควบคุมการถือครองและใช้งาน :** ไม่ควบคุมโดยคนเดียว เว้นแต่มีมาตรการเทียบเท่าและอธิบายได้ เช่น Multisig, MPC หรือ Threshold
- **ทบทวนกุญแจสิทธิพิเศษ :** ทบทวนผู้ควบคุม ผู้เข้าถึง และมาตรการที่เกี่ยวข้อง **อย่างน้อยปีละครั้ง** หรือเมื่อมีการเปลี่ยนแปลงผู้รับผิดชอบ โครงสร้างการควบคุม หรือเหตุการณ์สำคัญที่เกี่ยวข้อง



ข้อเสนอแนะขั้นต่ำ

- **บทบาทและอำนาจดำเนินการ :** ระบุงานผลกระทบสูง แบ่งผู้เสนอ อนุมัติ ดำเนินการ และตรวจสอบ
- **อนุมัติและควบคุมการดำเนินการ :** อนุมัติก่อนดำเนินการ งานผลกระทบสูงควรใช้ผู้มีอำนาจหลายคนหรือมีกลไกที่เหมาะสมกับระดับความเสี่ยง พร้อมแนวทางฉุกเฉิน
- **หลักฐานและการทบทวน :** เก็บข้อมูลผู้ขอทำรายการ ผู้อนุมัติ ผู้ดำเนินการ เวลา เหตุผล และผลลัพธ์ ติดตามความผิดปกติและทบทวนกระบวนการ

Cybersecurity - Data Protection, Integrity and Cryptographic Assurance

6.5



ความปลอดภัย ความถูกต้องครบถ้วน และการรับรองข้อมูล

ต้องคุ้มครองข้อมูลจากการเปิดเผย สูญหาย หรือแก้ไขโดยไม่ได้รับอนุญาต และพิสูจน์ความถูกต้อง แหล่งที่มา และความสอดคล้องของข้อมูล ทั้งบนระบบ DLT และระบบอื่นที่เกี่ยวข้อง

การรักษาความปลอดภัยของข้อมูล (Data Protection)

คุ้มครองตามความสำคัญ และความอ่อนไหวของข้อมูล

ข้อเสนอแนะขั้นต่ำ

- **จำแนกข้อมูล :** ระบุความสำคัญและความอ่อนไหว เพื่อเลือกมาตรการคุ้มครอง
- **สิทธิและมาตรการคุ้มครอง :** จำกัดการเข้าถึง คุ้มครองขณะจัดเก็บ ประมวลผล และรับส่ง
- **ส่งต่อ เก็บ และทำลาย :** กำหนดการส่งต่อ ระยะเก็บ และลบเมื่อหมดจำเป็นตามข้อกำหนด
- **ตรวจสอบการเข้าถึง :** บันทึกและตรวจการเข้าถึงข้อมูลสำคัญ

การรักษาความถูกต้องครบถ้วนของข้อมูล (Data Integrity)

ข้อมูลควรถูกต้อง ครบถ้วน และสอดคล้องระหว่างระบบ

ข้อเสนอแนะขั้นต่ำ

- **แหล่งข้อมูลและการควบคุม :** ระบุแหล่งและความสัมพันธ์ ป้องกันการแก้ไขโดยมิชอบ
- **ตรวจและกระทบยอด :** ตรวจตามรอบและความเสี่ยง ตรวจจับข้อมูลไม่สอดคล้องกัน
- **จัดการความคลาดเคลื่อน :** วิเคราะห์ อนุมัติการแก้ไข เก็บข้อมูลเดิมและหลักฐานผลแก้ไข

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Protection)

จำกัดการใช้เท่าที่จำเป็น และคำนึงถึงการระบุตัวบุคคล

ข้อเสนอแนะขั้นต่ำ

- **ระบุและประเมินความเสี่ยง :** รวมข้อมูล Wallet ที่เชื่อมโยงถึงบุคคลได้
- **ใช้และเข้าถึงเท่าที่จำเป็น :** จำกัดการเก็บ ใช้ เปิดเผย และสิทธิตามวัตถุประสงค์
- **ลดความเสี่ยงการเชื่อมโยง :** ประเมินการระบุตัวบุคคลจากข้อมูลหลายแหล่ง แม้ DLT ไม่มีชื่อ
- **กรณีที่ต้องเปิดเผยต่อภายนอก :** ดำเนินการให้สอดคล้องตามกฎหมายและเก็บหลักฐานการเปิดเผย

การรับรองด้วยกลไกการเข้ารหัสลับ (Cryptographic Assurance)

พิสูจน์ความถูกต้อง แหล่งที่มา และผู้ดำเนินการ

ข้อเสนอแนะขั้นต่ำ

- **เลือกกลไกเข้ารหัส :** เหมาะกับวัตถุประสงค์และความเสี่ยง หลีกเลี่ยงวิธีล้าสมัย
- **ตรวจความถูกต้องและที่มา :** เช่น Hash, Digital Signature และ Certificate
- **เก็บหลักฐานและทบทวน :** พิสูจน์ย้อนหลังได้ และปรับกลไกตามภัยคุกคามหรือเทคโนโลยีที่เปลี่ยนแปลง

Cybersecurity - Monitoring, Logging and Auditability

6.6



การติดตามเหตุการณ์ การบันทึกข้อมูล และการตรวจสอบย้อนหลัง

ควรติดตามและบันทึกเหตุการณ์สำคัญ เพื่อระบุผู้ดำเนินการ ตรวจพบความผิดปกติ เชื่อมโยงเหตุการณ์ และใช้หลักฐานสนับสนุนการตรวจสอบหรือการตอบสนองได้ทันเวลา



การบันทึกข้อมูลและบริหารจัดการหลักฐาน (Logging, Audit Trail and Evidence Management)

ควรตอบคำถามได้ว่าใครทำอะไร เมื่อใด ผ่านระบบใด และเกิดผลอย่างไร



ข้อเสนอแนะขั้นต่ำ

- **ขอบเขตและรายละเอียด Log :**
  บันทึกการเข้าถึง เปลี่ยนสิทธิ ตั้งค่า ใช้สิทธิพิเศษ และกิจกรรม Smart Contract/DLT ให้ระบุผู้ดำเนินการ เวลาเข้าใช้งาน ระบบที่ใช้งาน และผลลัพธ์ที่ได้
- **คุ้มครองและเก็บหลักฐาน :**
  เวลาแต่ละระบบต้องสอดคล้องกัน ป้องกันแก้ไขหรือลบ แบ่งสิทธิ และกำหนดระยะเก็บตามความเสี่ยงและข้อกำหนด
- **สืบค้น เรียกใช้ และทบทวน :**
  เชื่อมโยงและเรียกหลักฐานได้ในเวลาที่เหมาะสม ทบทวนความครบถ้วนและเพียงพอของ Log เป็นระยะ



การติดตามและตรวจจับเหตุการณ์ผิดปกติ (Monitoring and Detection)

ควรแจ้งเตือน ประเมินผลกระทบ และยกระดับเหตุการณ์ให้ผู้รับผิดชอบตอบสนองได้ทันท่วงที



ข้อเสนอแนะขั้นต่ำ

- **ขอบเขตและเกณฑ์ตรวจจับ :**
  ติดตามตามความเสี่ยง ทั้งสถานะระบบ ธุรกรรม สิทธิพิเศษ และการเชื่อมต่อ API/Oracle/Bridge
- **แจ้งเตือน วิเคราะห์ และยกระดับ :**
  กำหนดระดับความรุนแรง ผู้รับผิดชอบ และการส่งต่อเหตุ ใช้ Log วิเคราะห์ลักษณะและผลกระทบ
- **บันทึกและทบทวนประสิทธิผล :**
  เก็บผลแจ้งเตือนและการจัดการ ปรับเกณฑ์ให้ตรวจพบเหตุสำคัญ และลดการแจ้งเตือนที่ไม่จำเป็น

Cybersecurity - Vulnerability Management and Security Testing

6.7



การบริหารจัดการช่องโหว่และการทดสอบด้านความมั่นคงปลอดภัย

ควรค้นหาจุดอ่อน ประเมินความเสี่ยง ทดสอบมาตรการควบคุม และติดตามการแก้ไข ครอบคลุมทั้งบนระบบ DLT ระบบอื่นที่เกี่ยวข้อง และระบบภายนอกที่เชื่อมต่อหรือพึ่งพากัน



การบริหารจัดการช่องโหว่ (Vulnerability Management)

จัดลำดับการแก้ไขจากความรุนแรง โอกาสถูกโจมตี และผลกระทบต่อระบบ ธุรกรรม และสิทธิผู้ถือ



การทดสอบด้านความมั่นคงปลอดภัย (Security Testing)

ทดสอบประสิทธิผลของมาตรการควบคุม ด้วยขอบเขตและวิธีที่เหมาะกับความเสี่ยง



ข้อเสนอแนะขั้นต่ำ

- **กระบวนการและขอบเขต :**
  มีขั้นตอนเป็นลายลักษณ์อักษร **ประเมินระบบสำคัญอย่างน้อยปีละครั้ง** และจัดทำเพิ่มเมื่อเปลี่ยนแปลงสำคัญหรือพบภัยใหม่
- **ประเมินและแก้ไขตามความเสี่ยง :**
  พิจารณาความรุนแรง โอกาสถูกโจมตี และผลกระทบ หากยังแก้ไม่ได้ให้มีมาตรการทดแทนและอนุมัติการยอมรับความเสี่ยง
- **ติดตามและตรวจสอบย้อนหลัง :**
  ระบุผู้รับผิดชอบ ติดตามจนแก้ไข ลด หรือยอมรับความเสี่ยง เก็บผลประเมิน หลักฐานแก้ไข และการอนุมัติ



ข้อเสนอแนะขั้นต่ำ

- **ขอบเขตและวิธีทดสอบ :**
  ครอบคลุมระบบสำคัญและจุดเชื่อมต่อ **ทำ Penetration Test อย่างน้อยปีละครั้ง** และจัดทำเพิ่มเมื่อเปลี่ยนแปลงหรือมีความเสี่ยงที่มีนัยสำคัญ
- **ผู้ทดสอบและการควบคุมผลกระทบ :**
  ผู้ทดสอบมีความสามารถและเป็นอิสระจากระบบ ใช้บุคลากรภายในหรือภายนอกได้ กำหนดกติกาและคุมผลกระทบต่อระบบจริง
- **รายงาน แก้ไข และติดตาม :**
  รายงานข้อค้นพบและความเสี่ยง ระบุผู้แก้ไข ติดตามจนแล้วเสร็จ และตรวจยืนยันผลสำหรับข้อค้นพบสำคัญ

Cybersecurity - Incident Response and Operational Resilience

6.8



การตอบสนองต่อเหตุการณ์และความพร้อมด้านการดำเนินงาน

ควรควบคุมเหตุและลดผลกระทบ รักษาบริการสำคัญ และกู้คืนระบบกับข้อมูล ภายในระดับที่ยอมรับได้ โดยคำนึงถึงสิทธิผู้ถือและระบบหรือผู้ให้บริการที่พึ่งพากัน



การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Response)

ประเมิน ควบคุม และลดผลกระทบ พร้อมสื่อสารและตรวจสอบย้อนหลัง



ความต่อเนื่องในการดำเนินงาน (Business Continuity)

ให้บริการสำคัญดำเนินต่อได้ หรือกลับมาในระดับที่ยอมรับได้



การสำรองข้อมูลและการกู้คืนระบบ (Backup and Recovery)

กู้คืนได้ตามเป้าหมาย และข้อมูลบนระบบ DLT และระบบอื่นต้องสอดคล้องกัน



ข้อเสนอแนะขั้นต่ำ

- **แผน บทบาท และการยกระดับ :** จัดให้มีแผน กำหนดระดับความรุนแรงและผู้รับผิดชอบ มีเกณฑ์ยกระดับเหตุการณ์ และกำหนดอำนาจตัดสินใจ
- **ควบคุมเหตุและการสื่อสาร :** จำกัดผลกระทบ แจ้งผู้เกี่ยวข้องและหน่วยงานกำกับตามความเหมาะสมและข้อกำหนด
- **หลักฐาน ทบทวน และทดสอบ :** เก็บหลักฐาน วิเคราะห์สาเหตุ **ทดสอบแผนอย่างน้อยปีละครั้ง** และเมื่อเปลี่ยนแปลงสำคัญ



ข้อเสนอแนะขั้นต่ำ

- **บริการสำคัญและผลกระทบ :** ระบุบริการและทรัพยากรสำคัญ จัดลำดับและเป้าหมาย รวมถึงระบบภายนอกและผู้ให้บริการที่ต้องพึ่งพา
- **แผนและการดำเนินงานทดแทน :** มี BCP ระบบสำรอง งาน Manual หรือผู้ให้บริการทดแทน พร้อมแนวทางสื่อสาร
- **ทดสอบและปรับปรุงแผน :** **อย่างน้อยปีละครั้ง** และเมื่อเปลี่ยนแปลงสำคัญ โดยใช้ผลทดสอบและเหตุการณ์จริงประกอบการปรับปรุง



ข้อเสนอแนะขั้นต่ำ

- **ขอบเขตและมาตรการสำรอง :** ระบุข้อมูลและระบบ วิธี ความถี่ ที่เก็บ และระยะเก็บ คุ้มครองและแยกจากระบบจริงตามเหมาะสม
- **เป้าหมายและแผนกู้คืน :** กำหนด RTO/RPO ตามความเสี่ยง ลำดับ ผู้รับผิดชอบ และวิธีตรวจข้อมูลหลังกู้คืน
- **ทดสอบและปรับปรุงการกู้คืน :** **อย่างน้อยปีละครั้ง** และเมื่อเปลี่ยนแปลงสำคัญ โดยพิจารณาความพร้อมใช้งาน เวลาในการกู้คืน และความสอดคล้องของข้อมูลบนระบบ DLT และระบบอื่นที่เกี่ยวข้อง

รับฟังความคิดเห็น : ร่างมาตรฐานสำหรับการออกและให้บริการหลักทรัพย์โทเคน



สำนักงาน ก.ล.ต. ขอเชิญผู้ประกอบธุรกิจและผู้ที่เกี่ยวข้องร่วมแสดงความคิดเห็นและข้อเสนอแนะต่อร่างมาตรฐานฯ เพื่อให้การกำหนดมาตรฐานสอดคล้องกับการดำเนินงานจริงและสนับสนุนการพัฒนาตลาดทุนดิจิทัลของไทย

ร่างมาตรฐาน	ช่องทางนำส่งความเห็น
ดาวน์โหลดเอกสารร่างมาตรฐานฯ และ presentation ได้ที่ Thai Digital Capital Market Innovation Sandbox หรือสแกน QR code ตามด้านล่าง	สามารถนำส่งความคิดเห็น อีเมล : CMIC@sec.or.th --- ตั้งแต่วันนี้ - 30 พฤศจิกายน 2569

สอบถามข้อมูลเพิ่มเติมทางอีเมล CMIC@sec.or.th หรือโทรศัพท์
- Legal Standard โทรศัพท์ : 0-2263-6529 (พีร์นิธิ)
- Token/Cybersecurity Standard โทรศัพท์ : 0-2033-9954 (โสภณ)
- Tokenizer Standard โทรศัพท์ : 0-2263-6153 (คีริศวร์)

Thank You

ช่องทางติดต่อ

พีร์นิธิ / โสภณ / คีริศวร์
ศูนย์พัฒนาโครงสร้างพื้นฐานตลาดทุน
(Capital Market Infrastructure Center)
CMIC@sec.or.th