แนวทางการเข้าร่วมระบบ National Digital ID ของสมาคมบริษัทหลักทรัพย์ (ASCO) - 250518

NATIONAL DIGITAL ID



1. โครงสร้าง National Digital ID Platform 2. บทบาทและหน้าที่ของ บริษัท National Digital ID จำกัด (NDID) 3. แนวทางการเข้าร่วมของบริษัทหลักทรัพย์



หลายหน่วยงานมีความต้องการเดียวกัน ที่จะยืนยันตัวตนลูกค้าผ่าน e-channel





ดังนั้นหน่วยงานต่างๆ ตกลงที่จะสร้าง Platform กลางร่วมกัน





Economy

คณะกรรมการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล





Requirement

Digital ID Platform จะเป็นจุดเชื่อมต่อกลางระหว่างภาครัฐ และภาคเอกชน





Basic Authentication Flow









Economy

Authentication Flow : Cross Channel



Channels and (applicable) Authentication Methods (AM) may vary from one IdP's to another, giving the variety and choice of preference to consumers. Technology choice is flexible with possibility for new innovative technology, e.g. biometrics, mobile PKI, etc.

Regulating Body (e.g. EDTA) may specify the standard of each Authentication Method (AM) and specify the "level of assurance" of each AM.



Authentication Flow : Cross Off-line Channel



Please print if page and bring to IdP's service





Basic Authentication (Technical Flow)



Digital ID Platform

Request Bus

6 Identity _Provider (IdP)

The required LoA is specified in the request (req#)

IdP may interact with user using different/many Authentication Method (AM), depending on the required LoA as specified in the request (req#)

153007



Basic Information Request







1. โครงสร้าง National Digital ID Platform 2. บทบาทและหน้าที่ของ บริษัท National Digital ID จำกัด (NDID)

3. แนวทางการเข้าร่วมของบริษัทหลักทรัพย์



หน้าที่ของบริษัท National Digital ID จำกัด







- ออกแนวทางกำกับดูแลสมาชิก ออกใบรับรองให้สมาชิก เพื่อสร้างความมั่นใจ
- ร่วมกำหนด LoA Framework และมาตรฐานต่างๆ สร้างระบบ BCP/ Crisis Management ต่างๆ



แผนพัฒนา National Digital ID Platform

Phase 1 (Q3/2018) - Core Platform Universal ID สำหรับบุคคล ธรรมดา (Mode 2)

- Multiple IdP (RP's Selection)

Phase 2 (Q2/2019)

- **Delegation Flow**
- Multiple IdPs (User's Selection)
- Universal ID สำหรับนิติบุคคล -
 - Depend on DBD's Legal

INDIVIDUAL

No UID Record	Mode 1 No UID Record. Individual/Juristic per Anonymity, no need to expose SpecificID in
<section-header></section-header>	Mode 2 Individual/Juristic person may use one or more Spec SpecificID used successfully to authenticate does not app
	Mode 3 Individual may use SpecificIDs or UID to start the rec authentication. But the restriction combination of the UI complete, otherwise the request is rejected

Phase 3 (Q4/2019)

- Universal ID สำหรับบุคคล ธรรมดา (Mode 3)
- Universal ID สำหรับนิติบุคคล (Mode 4)

JURISTIC

son may use one or more SpecificIDs directly to IdPs. Full Request Bus (with option for RP to put SpecificID too).

ificIDs directly to IdPs and alternatively use UID to request for authentication. If the pear in the UID's IdP Association List, warnings are put forward to all IdPs in the list.

quest for D must be Mode 4

Juristic Person may use SpecificIDs or UID to start the request for authentication. But the restriction combination of the UID must be complete, otherwise the request is rejected. Request may be cascaded to ind-UIDs (directors/representative of the Juristic Person)



วิธีการทำสัญญากลางระหว่างหน่วยงานต่างๆ



สัญญาการใช้บริการ 1.NDID - RP 2.NDID - IdP 3.NDID - AS Extra (NDID - Proxy)

สัญญามาตรฐาน

สัญญาการส่งข้อมูล 4.AS - RP

สัญญามาตรฐาน

สัญญาของ User 5.User - IdP 6.User - RP

สัญญามาตรฐาน

สัญญาอื่นๆ 7.NDID - Insurance 8.NDID - Court 9.Audit Firm - RP 10.Audit Firm - AS 11.Audit Firm - IdP

สัญญามาตรฐาน



มาตรฐานการยื่นยันด้วดน



การยืนยันตัวตน (Identity Proofing) เป็นขั้น ตอนที่ทำกับ IdP ซึ่งมีระดับการพิสูจน์ตัวตนหลาย ระดับที่เรียกว่า Identity Assurance Level (IAL) โดยพิจารณาจาก 3 ปัจจัย คือ

1.การแสดงตน (Presence) ทำได้ทั้ง F2F / Non F2F

2.หลักฐานที่ใช้แสดงตน (Evidence) (เฉพาะ Citizen ID/Passport)

3.การเปรียบเทียบระหว่างหลักฐาน และการ แสดงตน (Identity Proofing) จะใช้ Human หรือระบบก็ได้



Authentication Method (เรียกอะไรก็ได้) คือ สิ่งที่ IdP ออกให้หลังจากทำ KYC แล้ว เพื่อใช้ยืนยันตัวตนได้ทุกช่อง ทาง

ldP ที่ออกให้

Version 200518



Authenticator ที่ออกจากการทำ IAL แบบ Face2Face และ KIOSK สามารถนำไปเป็น ใช้เป็น Authenticator (AAL) บนระบบ NDID เพื่อไปสมัครใช้บริการกับ RP อื่นได้

หมายเหตุ: โปรดอ่านรายละเอียด ฉบับเต็มใน <u>www.digitalid.or.th</u> ประกอบ

Version 140518



หมายเหตุ: ยังเป็น Version ที่อยู่ระหว่างการหารือ ห้ามใช้อ้างอิงโดยเด็ดขาด

Authenticator ที่ออกจากการ Register แบบ Non-Face2Face ในระยะทดลองยังไม่สามารถไปสมัครใช้บริการกับ RP อื่นได้

Version 280418



AAL อ้างอิงตามมาตรฐานของ NIST แต่เนื่องจาก AAL3 ในประเทศไทย ยังไม่มีอุปกรณ์ประเภท Crytographic Device แพร่หลาย จึงเพิ่มความน่าเชื่อถือของ AAL 2 เป็น 2 ระดับย่อย

หมายเหตุ: โปรดอ่านรายละเอียด ฉบับเต็มใน <u>www.digitalid.or.th</u> ประกอบด้วย

ประเภท Authenticator ที่คาดว่าจะใช้งานใน Phase 1

Strongest



Weakest

ขอขอบคุณหน่วยงานดังต่อไปนี้ ที่อนุเคราะห์รวบรวมรูปแบบการยืนยันตัวตนที่มี







สร้าง Ecosystem เพื่อทำ Data Sharing

		-	_	
	Personal Data	Financial Data	Education Data	Working Data
Primary Trusted Source	ข้อมูลพื้นฐาน	ອ້ອມູລສົນກຮັพย์ ເພື່ອມູລສົນກຮັพย์ ເພື່ອມູລສົນກຮັพย์ ເພື່ອມູລສົນກຮັ ເພື່ອມູລສົນກຮັ ເພື່ອມູລສົນກຮັ ເພື່ອມູລສົນກຮັ ເພື່ອມູລສົນກຮັ ເພື່ອມູລສົນ ເພື່ອມູລສາມ ເພື່ອມ ເພື່ອມ ເພື່ອມ ເພື່ອມ ເພື່ອມ ເພິ່ອມ ເພິ່ອມ ເພິ່ອມ ເພິ່ອມ ເພິ່	ອ້ອສູລ Skills ເມື່ອ ເບິດ ເບິດ ເບິດ ເບິດ ເບິດ ເບິດ ເບິດ ເບິດ	ข้อมูล HR Cocoo Cocoo
Secondary Trusted Source	ข้อมูลพื้นฐานและ ที่อยู่ มีมีมีมีมีมี	<section-header></section-header>		ຍ້ອມູລ HR

*หมายเหตุ: เป็นแค่ตัวอย่าง



เกิด Data Sharing ใน Ecosystem







1. โครงสร้าง National Digital ID Platform 2. บทบาทและหน้าที่ของ บริษัท National Digital ID จำกัด (NDID)

3. แนวทางการเข้าร่วมของบริษัทหลักทรัพย์









การได้มาซึ่งข้อมูลมาจาก 3 วิธี ดังนี้

กรณีนี้ RP ต้องนำข้อมูลที่ได้ไป Verify Data เอง

User ให้ Consent และให้ หน่วยงานต้นสังกัดของข้อมูล นั้นๆส่งข้อมูลมาให้ เช่น NCB

User มีเอกสารประกอบ ซึ่งอยู่ในรูป Paper / e-Document ก็ได้

ข้อมูลที่มาจาก AS

ในตัวอย่างนี้ ยังไม่มี AS เลยในระบบ

เอกสาร (Paper Document / e-Documents)

ถ่ายรูปประกอบเอกสาร หรือ สามารถ Upload จาก Gallery ก็ได้

ถ่ายรูป ทะเบียนบ้าน

แนวทางการเข้าร่วม ของ บล. (เป็น RP อย่างเดียว)

วิธีการเชื่อมต่อ

1.ผ่านช่องทาง Streaming และ
Streaming For Fund จะใช้
Facilities ของ SET เอง

2.ผ่านช่องทางของ Selling Agent เอง (ออก Booth, สาขา, Website, Mobile App) 2.1 เชื่อมต่อผ่าน Set Proxy 2.2 ตั้ง Node (Server) เอง

Proc / Cons Proxy

Proc: ต้นทุนต่ำกว่า เนื่องจากไม่ ต้องเสียค่า Maintenance ระบบ และค่าใช้จ่ายลงทุนติดตั้ง Server (Node)

Cons: กรณีที่มี Requirement เฉพาะ ไม่สามารถ Customize ได้

Digital ID Platform

วิธีสื่อสารกันระหว่างแต่ละหน่วยงาน

Timeline

Condition: สำหรับหน่วยงานใด ที่ Test ไม่ผ่านตามจำนวนครั้งที่ระบุ ให้ต่อแถวเพื่อทดสอบระบบใหม่

