ทำไมต้อง Digital ID

ประชาชนเข้าถึงบริการทั้งภาครัฐและเอกชน
ผ่านระบบออนไลน์

เพิ่มความสะดวกในการทำธุรกรรม

Digital ID
กับการขับเคลื่อนที่ผ่านมา

- ด้านกฎหมาย
- ด้านมาตรฐาน
- ด้านระบบที่รองรับ

ด้านกฎหมาย

การรองรับผลทางกฎหมาย
พร้อมกลไกดูแลความน่าเชื่อถือผู้ให้บริการ

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

- เพิ่มหมวด 3/1 รองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- ให้มีการตรา พ.ร.ฎ. กำหนดธุรกิจบริการที่จำเป็นต้องดูแลเพื่อลดความเสี่ยงของผู้ใช้งาน (ร่าง พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ....) อยู่ระหว่างเสนอ ครม.

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

- หน่วยงานของรัฐมีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ได้มาตรฐาน

ด้านมาตรฐาน

รองรับการใช้งาน Digital ID
เพื่อให้ทำงานร่วมกันบนมาตรฐานเดียวกัน

ETDA Recommendation

มาตรฐานกลางรองรับการใช้งาน
สำหรับ Sector ต่างๆ

- ภาพรวมของ Digital ID Ecosystem
- มาตรฐานการลงทะเบียนและ
  การพิสูจน์ตัวตน ก่อนออก Digital ID
- มาตรฐานการยืนยันตัวตน
  ของผู้ทำธุรกรรมออนไลน์ว่าใครเป็นใคร

ก.ล.ต. ปปง. ธปท. ใช้อ้างอิง
ในการกำหนดหลักเกณฑ์
การใช้ Digital ID ของแต่ละ Sector

อยู่ระหว่างการปรับปรุงมาตรฐาน

DGA Recommendation

มาตรฐานเฉพาะเพื่อบริการของรัฐ

(ร่าง) มาตรฐานการใช้ดิจิทัลไอดี
สำหรับบริการภาครัฐ สำหรับบุคคลธรรมดา
ที่มีสัญชาติไทย

อยู่ระหว่างรับฟังความเห็น

ด้านระบบที่รองรับ

การพัฒนาระบบรองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ให้พร้อมใช้งานใน Sector ต่าง ๆ

Platform

NDID (National Digital ID)

- ผู้ให้บริการ Platform แลกเปลี่ยนข้อมูลการทำ KYC เช่น เปิดบัญชีออนไลน์ (Sandbox BoT)

MNID (Mobile National ID)

- ผู้ให้บริการ Platform แลกเปลี่ยนข้อมูลและเก็บ credential สำหรับพิสูจน์และยืนยันตัวตน (Sandbox NBTC)

ETDA
Digital Service Sandbox

รองรับการทดสอบนวัตกรรมหรือบริการสำหรับ Digital ID Solution ดูแลความเสี่ยง และความสอดคล้องตามกฎหมายและมาตรฐาน

มีผู้ให้บริการทั้งรัฐและเอกชน ให้ความสนใจเข้าร่วม Sandbox เช่น กพร., NDID, DGA, DOPA

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

พ.ร.บ. ธุรกรรมฯ (ฉบับที่ 4)

https://ictlawcenter.etda.or.th/laws

เพิ่มคำนิยาม

- “การพิสูจน์และยืนยันตัวตน”
- “ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล”

รองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เพิ่ม ม.34/3)

- ให้ข้อสันนิษฐานทางกฎหมาย
- กำหนดเงื่อนไขเกี่ยวกับความน่าเชื่อถือ

ให้มีการตรา พ.ร.ฎ. (เพิ่ม ม.34/4)

- กำหนดประเภทธุรกิจบริการที่กำกับดูแล

กำหนดโทษ (เพิ่ม ม.45/1)

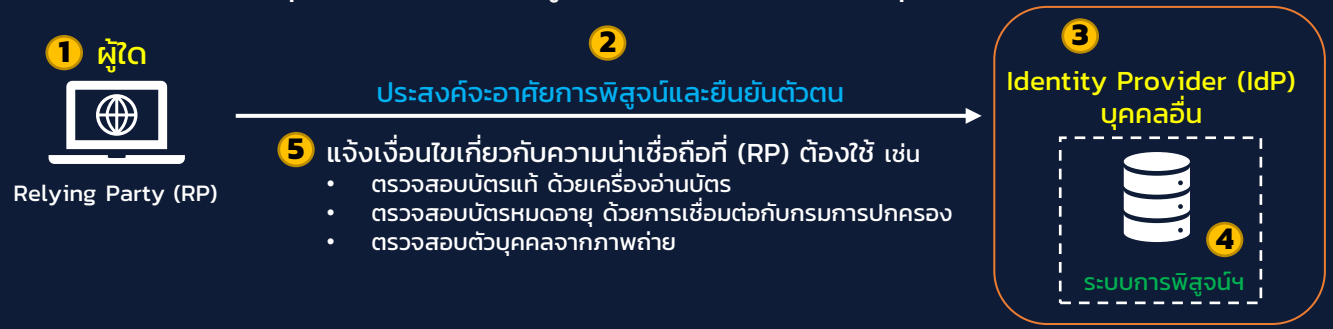
- กรณีไม่ได้รับอนุญาต หรือฝ่าฝืนคำสั่งพักใช้หรือเพิกถอนใบอนุญาต
- จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ

บทเฉพาะกาล (ม.7)

- เมื่อมีพระราชกฤษฎีกาแล้ว ให้ยื่นขออนุญาตภายใน 90 วันนับแต่วันที่ พ.ร.ฎ. มีผลใช้บังคับ

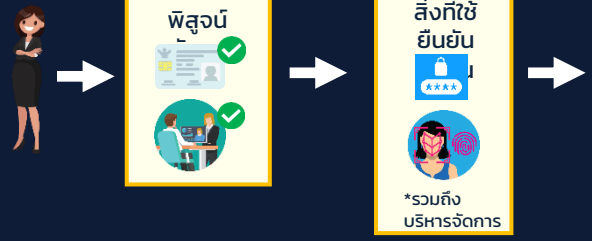
การพิสูจน์และยืนยันตัวตนทางดิจิทัล ตามมาตรา 34/3 วรรค 2

"ผู้ใดประสงค์จะอาศัยการพิสูจน์และยืนยันตัวตนของบุคคลอื่นผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล
อาจแจ้งเงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องใช้
ให้บุคคลอื่นนั้นทราบเป็นการล่วงหน้า และเมื่อได้มีการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามเงื่อนไขดังกล่าวแล้ว
ให้สันนิษฐานว่าบุคคลที่ได้รับการพิสูจน์และยืนยันตัวตนเป็นบุคคลนั้นจริง"

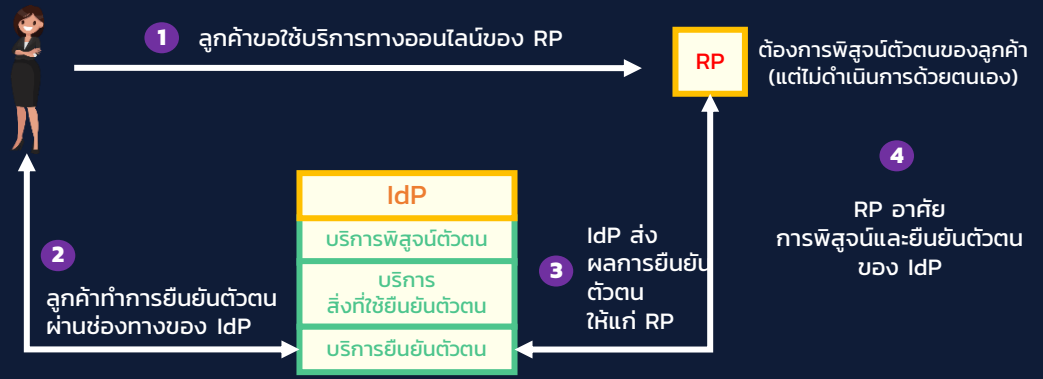


1 สิ่งที่ IdP ต้องทำก่อนให้บริการ

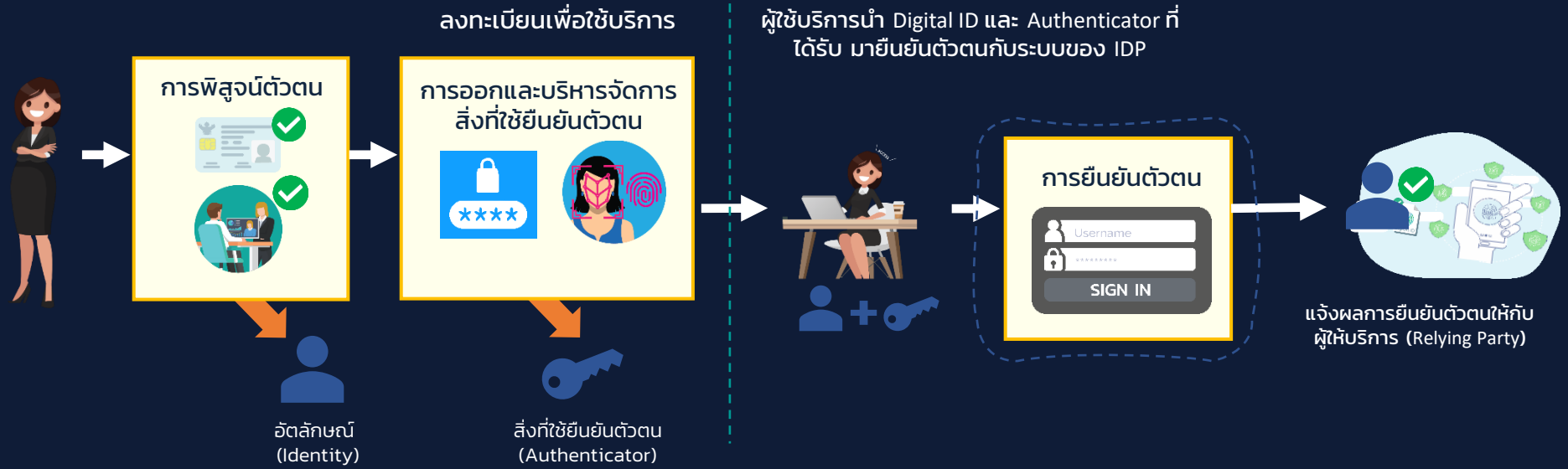
1 ลงทะเบียน และ 2 ออก Authenticator ให้แก่ลูกค้าของ IdP



2 การยืนยันตัวตนของ IdP



กระบวนการที่เกี่ยวข้องกับ “ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล”



- “บริการพิสูจน์ตัวตน” (Identity Proofing Service)
  บริการที่ประกอบด้วย กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น
- “บริการสิ่งที่ใช้ยืนยันตัวตน” (Authenticator Management Service)
  บริการที่ประกอบด้วย กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น
- “บริการยืนยันตัวตน” (Authentication Service)
  บริการที่ประกอบด้วย กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น

อ้างอิงจาก ISO/IEC 29115:2013 [ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework

การพิสูจน์ตัวตนทางดิจิทัล
(Identity proofing)

+

การยืนยันตัวตนทางดิจิทัล
(Authentication)

ระดับความน่าเชื่อถือ
(Assurance Levels)

3

2

1

IAL vs AAL

ระดับความน่าเชื่อถือ (Assurance Levels)

ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level : IAL)

- ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ
- ทำให้มั่นใจว่า ไอเดนทิตีที่ผู้ใช้บริการกล่าวอ้างเป็นไอเดนทิตีของผู้ใช้บริการจริง
  (เช่น ผู้ใช้บริการที่กล่าวอ้างว่าตนเองชื่อ “สมชาย” คือ สมชายตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา)
- IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Levels : AAL)

- ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ
- ทำให้มั่นใจว่า ผู้ใช้บริการคือเจ้าของสิ่งที่ใช้ยืนยันตัวตนจริง
  (เช่น ผู้ที่กำลังเข้าใช้งานระบบ คือ สมชายตัวจริง ไม่ใช่บุคคลอื่นขโมยรหัสผ่านไปใช้)
- AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด

ระดับความน่าเชื่อถือของไอเดนทิตี
Identity Assurance Level (IAL)

ระดับ**ความเข้มงวดในกระบวนการพิสูจน์ตัวตน**ของผู้สมัครใช้บริการ
ซึ่งช่วยจำกัดโอกาสของการพิสูจน์ตัวตนผิดพลาด

IAL	คำอธิบาย
3	มีการแสดงหลักฐานแสดงตน 2 ชิ้น + ตรวจสอบหลักฐานแสดงตน + ตรวจสอบข้อมูลชีวมิติ + พบเห็นเจ้าหน้าที่
2	มีการแสดงหลักฐานแสดงตน + ตรวจสอบหลักฐานแสดงตน
1	ข้อมูลที่ผู้สมัครยืนยันด้วยตนเอง (self-asserted)

Identity Assurance Level (IAL)

IAL 3

หลักฐานแสดงตน คือ

บัตรประจำตัวประชาชน

และ

หนังสือเดินทาง

ตรวจสอบหลักฐานแสดงตนกับผู้ให้ข้อมูลที่น่าเชื่อถือ (AS)

อ่านข้อมูลอิเล็กทรอนิกส์ + ตรวจสอบ online กับ AS

ตรวจสอบตัวบุคคลโดยเปรียบเทียบ

ข้อมูล Biometric

แสดงตนแบบพบเห็นต่อหน้า

(รวมถึงพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์)

IAL 2

บัตรประจำตัวประชาชน

หรือ

หนังสือเดินทาง

2.3

อ่านข้อมูลอิเล็กทรอนิกส์ + ตรวจสอบ online กับ AS

ข้อมูล biometric

2.2

อ่านข้อมูลอิเล็กทรอนิกส์ + ตรวจสอบ online กับ AS

ลักษณะที่ปรากฏ

2.1

อ่านข้อมูลอิเล็กทรอนิกส์

ลักษณะที่ปรากฏ

IAL 1

ไม่มี การตรวจสอบข้อมูลกับผู้ให้ข้อมูลที่น่าเชื่อถือ (AS)

- **1.3** ขอหลักฐานแสดงตน คือ บัตรประจำตัวประชาชน **หรือ** หนังสือเดินทาง
- **1.2** ขอหลักฐานแสดงตน คือ สำเนาบัตรประจำตัวประชาชน **หรือ** สำเนาหนังสือเดินทาง
- **1.1** ไม่ขอหลักฐานแสดงตนใด ๆ

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน Authenticator Assurance Level (AAL)

ระดับ**ความเข้มงวดในกระบวนการยืนยันตัวตน**ของผู้สมัครใช้บริการ
ซึ่งช่วยจำกัดโอกาสของการยืนยันตัวตนผิดพลาด

AAL	คำอธิบาย
3	การยืนยันตัวตนโดยใช้สองปัจจัย (Two-factor authentication) โดยต้องมีปัจจัยประเภทอุปกรณ์ และใช้งานการเข้ารหัสลับ (cryptography)
2	การยืนยันตัวตนโดยใช้สองปัจจัย (Two-factor authentication)
1	การยืนยันตัวตนโดยใช้ปัจจัยเดียว (Single-factor authentication)

Authenticator Assurance Level (AAL)

AAL 3

Multi-Factor crypto device

Crypto Device + Memorized Secret

Crypto Device + Multi-Factor OTP device

OTP Device + Multi-Factor Crypto Software

OTP device + Crypto Software + Memorized Secret

✓ Communication with IdP via protected channel to provide MitM resistance ✓Replay attack resistance ✓ IdP impersonation resistance

AAL 2

2.2

Authenticator in AAL2.1 + Biometric

2.1

Memorized Secret + { Out-of-Band Device (SMS OTP) or OTP Device or Crypto Software }

- Multi-Factor Crypto Software
- Multi-Factor OTP Device

✓ Communication with IdP via protected channel to provide MitM resistance ✓Replay attack resistance

AAL 1

Memorized Secret | Out-of-band Device (SMS OTP) | OTP Device | Crypto Software | Crypto Device

✓ Communication with IdP via protected channel to provide MitM resistance

วิวัฒนาการของระบบพิสูจน์และยืนยันตัวตน

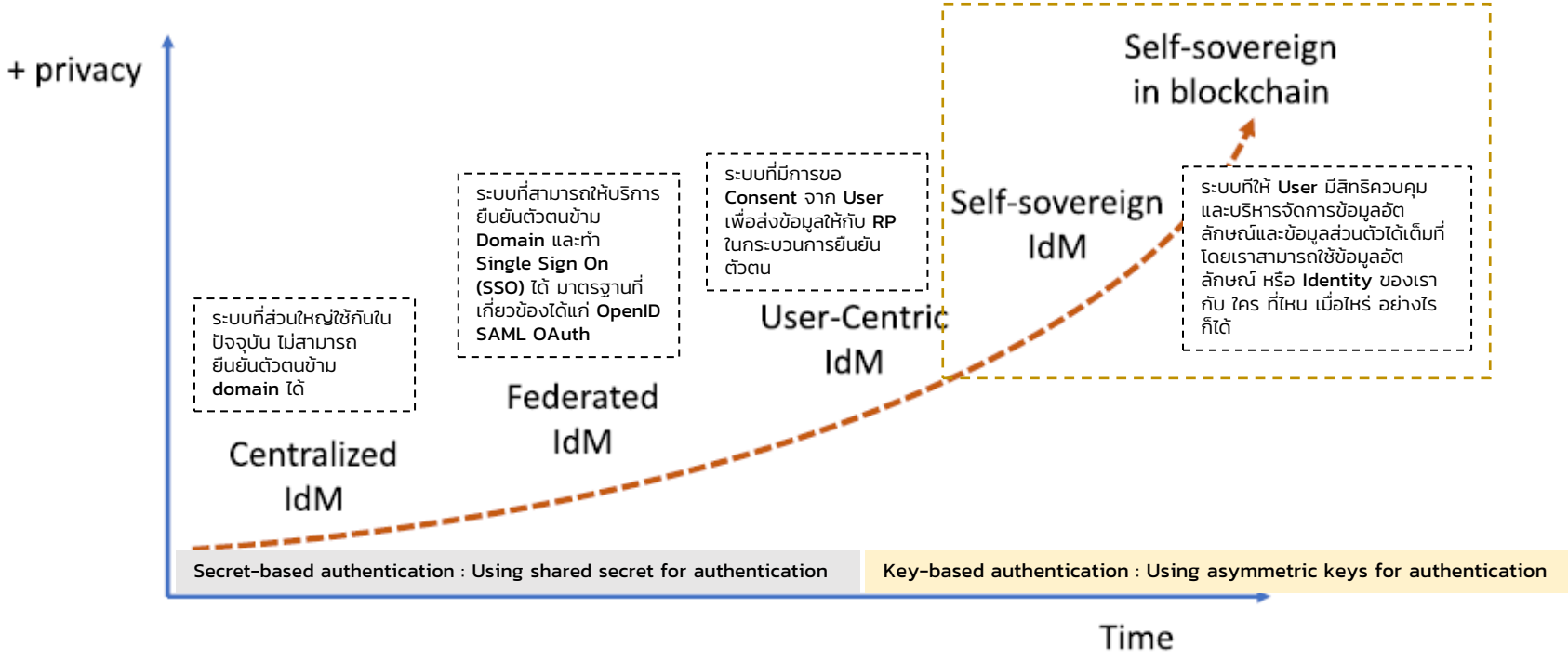


FIGURE 2. Identity management methods evolution over time, according to privacy preservation capabilities.

Reference: J. Bernal Bernabe et al.: Privacy-Preserving Solutions for Blockchain: Review and Challenges