

สวสอ.

ขับเคลื่อน
แผนยุทธศาสตร์

บนพื้นฐานของข้อมูล
ที่เชื่อถือได้

กำกับดูแล

Digital services

ส่งเสริม Digital
Transformation

ภาครัฐและเอกชน

สนับสนุนการ
เติบโตของ
e-Commerce

โดยการสร้างความเชื่อมั่น

สร้างภูมิคุ้มกัน
ด้าน digital

ให้ชุมชน และประชาชน

เศรษฐกิจ Digital Services + สังคม Digital citizens



www.eta.or.th



ETDA Thailand

ภารกิจ สพรอ. กับ

ธุรกรรมทางอิเล็กทรอนิกส์ Digital ID

1

จัดทำกฎหมายและหลักเกณฑ์
รองรับการดูแล Digital Service ที่มีความสำคัญ เช่น Digital ID

2

จัดทำมาตรฐานและ Guideline การใช้งาน Digital ID
เป็นมาตรฐานกลาง สอดคล้องสากล เช่น ขมรอ.18-20/2564 : การพิสูจน์และยืนยันตัวตนทางดิจิทัล เวอร์ชัน 2.0

3

ให้คำปรึกษาและคำแนะนำการใช้งาน Digital ID
ให้กับหน่วยงานของรัฐและเอกชน

4

มี Testbed และ Sandbox เพื่อทดสอบการใช้งาน Digital ID
เพื่อให้เป็นไปตามกฎหมายและมาตรฐาน



รู้จักกับ DIGITAL ID

Digital ID

คืออะไร

Digital

+

ID (Identity)

อัตลักษณ์



ลักษณะเฉพาะของบุคคล ซึ่งสามารถบ่งบอกหรือจำแนกได้
โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล

คุณลักษณะหรือชุดของคุณลักษณะ คือ อะไร

“Attribute” means an item of information or data associated with a person

(UNCITRAL : Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (A/CN.9/1112))

หมายเหตุ 1: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับบุคคลธรรมดา เช่น เลขประจำตัว ชื่อบุคคล ที่อยู่ วันเดือนปีเกิด อีเมล หมายเลขโทรศัพท์เคลื่อนที่ ภาพใบหน้า หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน

หมายเหตุ 2: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับนิติบุคคล เช่น เลขทะเบียนนิติบุคคล ชื่อนิติบุคคล ที่ตั้งสำนักงานใหญ่ หรือชื่อกรรมการของนิติบุคคล

(ขมรอ.18/2564 – กรอบการทำงาน)

ดิจิทัลไอดี (Digital Identity)

ดิจิทัลไอดี (Digital Identity)

คือ **อัตลักษณ์** (identity)

ที่ถูกรวบรวมและบันทึกใน**รูปแบบดิจิทัล**

ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์

Digital ID สำคัญอย่างไร

Figure 3: The digital identity empowers end-users and relying parties in the 'next evolution' of the digital economy

End-user



I want to get access to public & private digital services in order to participate in the digital economy



I need to trust the system, my digital life and associated risks are organised in an acknowledged ecosystem with clear allocation of responsibilities and liabilities



I want to control my assets and choose to interact with service providers of choice in order to make my life easy

Relying party



I need to trust the system with providing high quality digital identities that makes it more efficient to verify end-users

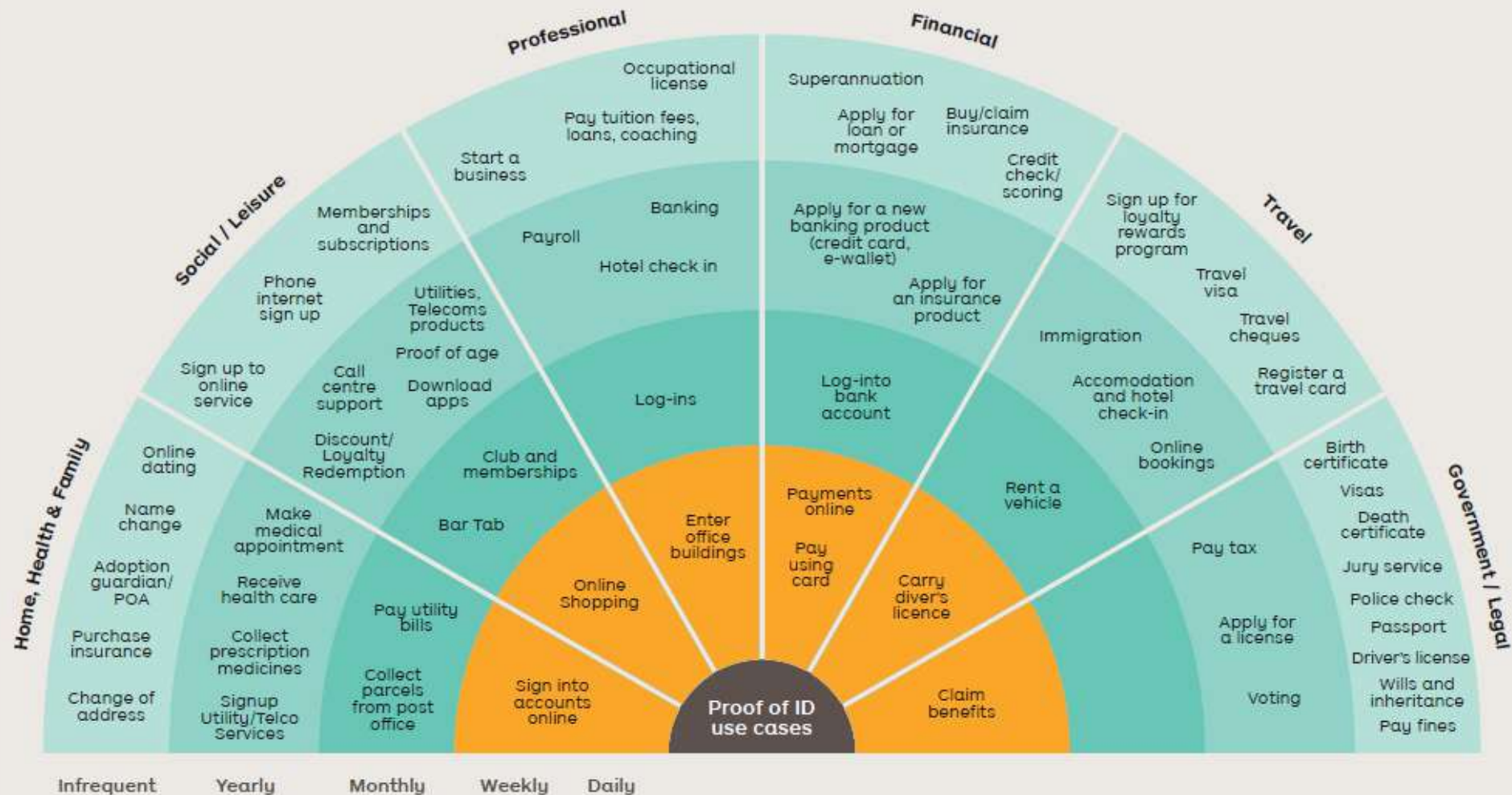


I want to comply with regulation and reduce identity fraud and losses by providing a level of confidence that verifies the end-user's identity



I want to improve the customer experience by reducing frictions in the digital experiences

Identity is used in many moments throughout the year





The Development of **DIGITAL ID**

DIGITAL IDENTITY COMMITTEE

Cooperate between public and private sectors

2017



2018



2019



2020



2021



2022



Thailand Digital ID Framework Phase 1 (2022 – 2024)

Roadmap for public and private sectors to drive Digital ID development



ELECTRONIC TRANSACTIONS ACT (No. 4), B.E. 2562

Provide legal recognition of electronic authentication



IDENTITY PROVIDER & DIGITAL IDENTITY PLATFORM SERVICE from Mobile Operator



DIGITAL IDENTITY STANDARD

- REVISION Version 2018



DIGITAL IDENTITY STANDARD

BIOMETRIC TECHNOLOGY

- Part 1: Biometric Technology Usage for Personal Verification
- Part 2: Facial Recognition Technology Usage for Personal Identity Verification
- Biometric Technology Performance Testing



DIGITAL IDENTITY STANDARDS

- Framework
- Identity Proofing Requirements
- Authentication Requirements



(Draft) Royal Decree on Regulating Digital Identity Services

Supervise Digital ID to ensure trustworthiness



DIGITAL IDENTITY PROVIDER from Department Of Provincial Administration



IDENTITY PROVIDER & DIGITAL IDENTITY PLATFORM SERVICE from Bank



LAW



STANDARD



SERVICE



POLICY

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.)

สถานะ : อยู่ระหว่างกระบวนการเสนอกฎเกล้า

● **พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562**

- หน่วยงานของรัฐมีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ได้มาตรฐาน

● **พ.ร.บ. การปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565**

- สามารถกำหนดให้ใช้การยืนยันตัวตนด้วยวิธีอื่นถ้าเป็นการสะดวกขึ้น

● **แนวทางการปรับปรุงกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ตามมติ ครม. เมื่อวันที่ 5 ต.ค. 2565**

ด้านการพิสูจน์และยืนยันตัวตน

- ☐ **เปิดกว้างระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล** ทั้งโดยหน่วยงานรัฐและเอกชนเป็นบริการสาธารณะ
- ☐ **ระบบที่ได้รับรอง ไม่มีภาระในการพิสูจน์** ถือเป็นระบบที่มีความน่าเชื่อถือ
- ☐ **การรับรองระบบสามารถทำได้โดย** หน่วยงานกำกับดูแลอื่น (regulator) ที่เป็นหน่วยงานของรัฐตามประเภทของธุรกรรม

สถานะ : อยู่ระหว่างรับฟังความคิดเห็น

ด้านมาตรฐาน

รองรับการใช้งาน Digital ID เพื่อให้ทำงานร่วมกันบนมาตรฐานเดียวกัน

● ETDA Recommendation

มาตรฐานกลางรองรับการใช้งานสำหรับ Sector ต่าง ๆ

• ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- กรอบการทำงาน (Framework)
(ขมรอ. 18-2564)
- ข้อกำหนดของการพิสูจน์ตัวตน
(Identity Proofing Requirements)
(ขมรอ. 19-2564)
- ข้อกำหนดของการยืนยันตัวตน
(Authentication Requirements)
(ขมรอ. 20-2564)

หมายเหตุ: ปรับปรุงจากมาตรฐานเดิม เวอร์ชัน 1.0 ปี 2561

• ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการมอบอำนาจอิเล็กทรอนิกส์

- ภาพรวมการมอบอำนาจทางอิเล็กทรอนิกส์
(ขมรอ. 31-2565)

• ข้อเสนอแนะมาตรฐานฯ เกี่ยวกับการใช้ Biometrics จำนวน 3 ฉบับ

1. การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน
(ขมรอ. 29 เล่ม 1-2565)
2. การใช้งานเทคโนโลยีการรู้จำใบหน้า
สำหรับการพิสูจน์และยืนยันตัวตน
(ขมรอ. 29 เล่ม 2-2565)
3. การทดสอบสมรรถนะการทำงานของ
เทคโนโลยีชีวมิติ (ขมรอ. 30-2565)

ด้านมาตรฐาน

รองรับการใช้งาน Digital ID เพื่อให้ทำงานร่วมกันบนมาตรฐานเดียวกัน

● DGA Recommendation

มาตรฐานสำหรับบริการของรัฐ

- มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

สถานะ : ประกาศในราชกิจจานุเบกษาแล้ว

- (ร่าง) มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วยการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับนิติบุคคล

สถานะ : ผ่านความเห็นชอบของคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

อยู่ระหว่างการเสนอหน่วยงานที่เกี่ยวข้องพิจารณารับร่างมาตรฐานฯ เพื่อนำไปพัฒนาและประยุกต์ใช้ต่อไป

Digital ID Framework

กลยุทธ์หลัก 8 หลักการ
เพื่อขับเคลื่อนบริการพิสูจน์และยืนยัน
ตัวตนทางดิจิทัลประเทศไทย

ความครอบคลุม	1	ดิจิทัลไอดีครอบคลุม บุคคล นิติบุคคล และบุคคลต่างชาติ พร้อมรองรับการยืนยันตัวตน การลงลายมือชื่ออิเล็กทรอนิกส์ การมอบอำนาจและการให้ความยินยอมทางอิเล็กทรอนิกส์
	2	ประชาชนสามารถเลือกใช้ดิจิทัลไอดีในระดับความเชื่อมั่นที่เหมาะสมในการเข้าถึง บริการออนไลน์ของภาครัฐ และเอกชน
การออกแบบ	3	กระทรวงมหาดไทยเป็นหน่วยงานหลักในการให้ข้อมูลและบริการ สนับสนุนการพิสูจน์ตัวตน ให้กับ IdP ทั้งภาครัฐและเอกชนในการออกดิจิทัลไอดี สำหรับบุคคลธรรมดาทั้งคนไทย และคนต่างชาติที่มีถิ่นที่อยู่ในประเทศไทย โดยมีกระบวนการกำกับดูแลให้มีมาตรฐานที่น่าเชื่อถือ
	4	การใช้ดิจิทัลไอดีในการทำธุรกรรมของนิติบุคคลเป็นการใช้ดิจิทัลไอดีบุคคลธรรมดาของผู้มีอำนาจของนิติบุคคลนั้น ร่วมกับการมอบอำนาจ หากจำเป็น
	5	กรมพัฒนาธุรกิจการค้า เป็นหน่วยงานหลักในการให้ข้อมูลที่เชื่อถือของนิติบุคคล เพื่อสนับสนุนการทำธุรกรรมของนิติบุคคลผ่านดิจิทัลไอดี
	6	ประชาชนสามารถเข้าถึงบริการภาครัฐผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ น่าเชื่อถือและประชาชนใช้งานอย่างกว้างขวาง โดยไม่ต้องลงทะเบียนพิสูจน์ตัวตนซ้ำซ้อน ด้วยมาตรฐานสากลแบบเปิด (Open Standards)
ธรรมาภิบาล	7	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์กำหนดนโยบายดิจิทัลไอดีในภาพรวม ซึ่งรวมถึง การพัฒนามาตรฐานกลางที่เกี่ยวข้อง เพื่อให้บริการที่เกี่ยวข้องกับดิจิทัลไอดีของรัฐและเอกชน มีมาตรฐานสอดคล้องกัน และเชื่อมโยงแลกเปลี่ยนข้อมูลกันได้ โดยหน่วยงานกำกับในแต่ละ ภาคส่วน (Sector) นำไปประยุกต์ใช้ รวมถึงกำหนดนโยบายเพิ่มเติมให้เหมาะสมกับบริการหรือ ธุรกรรมที่กำกับหรือดูแล
	8	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พัฒนามาตรฐานที่เกี่ยวข้องกับภาครัฐ เพื่อให้บริการที่เกี่ยวข้องกับดิจิทัลไอดีของรัฐและเอกชนได้มาตรฐานสอดคล้องกัน และเชื่อมโยง แลกเปลี่ยนข้อมูลสำหรับบริการดิจิทัลไอดีระหว่างรัฐและเอกชนได้

มติคณะรัฐมนตรี

ที่เกี่ยวข้องกับการดำเนินงานด้าน Digital ID ของประเทศ

1. **มติคณะรัฐมนตรีเมื่อวันที่ 27 กรกฎาคม 2564** เรื่อง แนวทางการพัฒนาระบบรองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือ Digital ID ด้วยการพัฒนา ระบบพิสูจน์และยืนยันตัวตนด้วยใบหน้าทางดิจิทัล (Face Verification Service – FVS)
2. **มติคณะรัฐมนตรีเมื่อวันที่ 3 สิงหาคม 2564** เรื่อง การขับเคลื่อนการให้บริการประชาชนผ่านระบบอิเล็กทรอนิกส์ (e-Service) ในปีงบประมาณ 2565

มติ คณะรัฐมนตรี (1)

เมื่อวันที่ 27 กรกฎาคม 2564

แนวทางการพัฒนาระบบรองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือ Digital ID ด้วยการพัฒนาาระบบพิสูจน์และยืนยันตัวตนด้วย ใบหน้าทางดิจิทัล (Face Verification Service - FVS)

1

คณะรัฐมนตรีรับทราบและอนุมัติให้กระทรวงมหาดไทย (มท.) พัฒนา จัดให้มีระบบ FVS และให้บริการกับหน่วยงานของรัฐและเอกชน โดยมี MDES เป็นที่ปรึกษา พร้อมให้ มท. และ MDES เร่งจัดทำโครงการให้เป็นรูปธรรมโดยเร็วและสอดคล้อง แผนพัฒนารัฐบาลดิจิทัล

2

ให้สำนักงบประมาณ ให้การสนับสนุนค่าใช้จ่ายในการพัฒนาและจัดทำระบบ FVS รวมทั้งค่าใช้จ่ายอื่นใดเพื่อการบริหารงานและการให้บริการ

3

ให้กระทรวงมหาดไทย หรือ MDES แล้วแต่กรณี รายงานการดำเนินงานเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล (Digital Infrastructure) ในส่วนของการพัฒนาระบบ Digital ID ให้คณะรัฐมนตรีทราบเป็นระยะ

มติ คณะรัฐมนตรี (1)

เมื่อวันที่ 27 กรกฎาคม 2564

แนวทางการพัฒนาระบบรองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล หรือ Digital ID ด้วยการพัฒนาาระบบพิสูจน์และยืนยันตัวตนด้วยใบหน้าทางดิจิทัล (Face Verification Service - FVS)

4

ให้ **MDES** และ **DGA** เป็นหน่วยงานหลัก ร่วมกับกระทรวงมหาดไทย กระทรวงการคลัง สปท. สำนักงานคณะกรรมการกฤษฎีกา สำนักงาน ก.พ.ร. และหน่วยงานที่เกี่ยวข้อง ดำเนินการดังนี้

- พิจารณาความเหมาะสมและความเป็นไปได้ในการบูรณาการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของหน่วยงานต่างๆ ให้สามารถเชื่อมโยงกันได้ และเป็นไปในทิศทางเดียวกัน และนำผลไปประกอบการพัฒนาระบบ FVS
- จัดทำมาตรฐานและแนวทางของระบบ FVS ที่สอดคล้องสากล และสอดคล้องกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายที่เกี่ยวข้อง

มติ คณะรัฐมนตรี (2)

เมื่อวันที่ 3 สิงหาคม 2564

การขับเคลื่อนการให้บริการประชาชนผ่านระบบอิเล็กทรอนิกส์ (e-Service) ปีงบประมาณ 2565

- เห็นชอบงานบริการ 12 Agenda เพื่อเร่งขับเคลื่อน ในปีงบประมาณ 2565
- ให้ ก.พ.ร. พิจารณากำหนดประเภทและจัดลำดับความเร่งด่วนงานบริการอื่นเพิ่มเติม (50 งานบริการ)
- ให้ ก.พ.ร. กำหนดบริการเพื่อทำ Digitalize และเป็นตัวชี้วัดให้หน่วยงานดำเนินการ

ให้กระทรวงมหาดไทย และ ก.พ.ร.
ยึดแนวทางระบบ FVS เป็นหลักแทน Digital ID
ในการพัฒนาระบบการพิสูจน์และยืนยันตัวตนฯ

12 Agenda

- ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID)
- ระบบการชำระภาษีที่ดินและสิ่งปลูกสร้าง
- ระบบการแจ้งเตือนสิทธิและช่วยเหลือในการรับสวัสดิการของประชาชน ตลอดช่วงชีวิต
- ศูนย์การร้องเรียนแบบเบ็ดเสร็จ
- ระบบการอำนวยความสะดวกให้แก่ผู้เดินทาง (Ease of Traveling)
- ระบบการออกบัตรสุขภาพอิเล็กทรอนิกส์
- ระบบช่วยเหลือผู้ว่างงานให้กลับเข้าสู่ตลาดแรงงาน
- หนึ่งรหัส หนึ่งผู้ประกอบการ (One Identification: ID one SMEs)
- ระบบขออนุญาตวัตถุอันตรายแบบครบวงจร (Hazardous Substance Single Submission : HSSS)
- ระบบรับรองมาตรฐานสินค้าเกษตร (GAP) พืช ประมง ปศุสัตว์
- ระบบการขึ้นทะเบียนเกษตรกรและระบบการให้ความช่วยเหลือด้านการเกษตร
- ระบบเชื่อมโยงสินค้าข้ามแดนทางบกของกลุ่มประเทศ ACMECS ผ่านระบบ National Single Window

แนวทางการพัฒนาโครงสร้างพื้นฐาน รองรับการใช้งาน Digital ID

หน่วยงานรัฐ พร้อมสนับสนุนข้อมูลสำคัญ
สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

1

ระบบเปรียบเทียบภาพใบหน้า
(Face Verification System)

2

การให้ข้อมูลและบริการเพื่อสนับสนุน
การพิสูจน์ตัวตนบุคคลธรรมดา
ให้กับ IdP ในการออกดิจิทัลไอดี

3

ให้ข้อมูลที่น่าเชื่อถือของนิติบุคคล
เพื่อสนับสนุนการทำธุรกรรมของ
นิติบุคคลผ่านดิจิทัลไอดี



กระทรวงมหาดไทย
โดยกรมการปกครอง (DOPA)



กรมพัฒนาธุรกิจการค้า



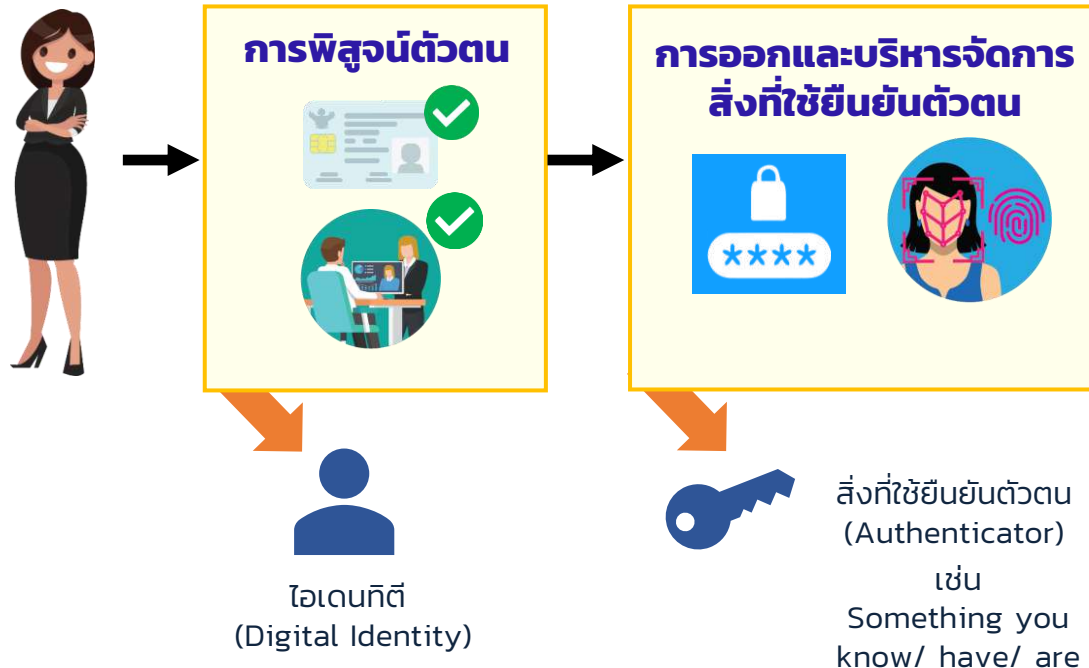
Overview

DIGITAL ID

Ecosystem

ภาพรวมขั้นตอนสำคัญ ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ลงทะเบียนเพื่อใช้บริการ



ผู้ใช้บริการนำ Digital ID และ Authenticator
ที่ได้รับมายืนยันตัวตนกับระบบของผู้ให้บริการ



สิ่งที่ใช้ยืนยันตัวตน (Authenticator)

ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตน
มี**ปัจจัยของการยืนยันตัวตน**
(authentication factor)
อย่างน้อย 1/3 ปัจจัย

(1) สิ่งที่คุณรู้ (something you know)

คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่รู้ เช่น รหัสผ่าน (password) และเลขรหัสส่วนตัว (PIN)

(2) สิ่งที่คุณมี (something you have)

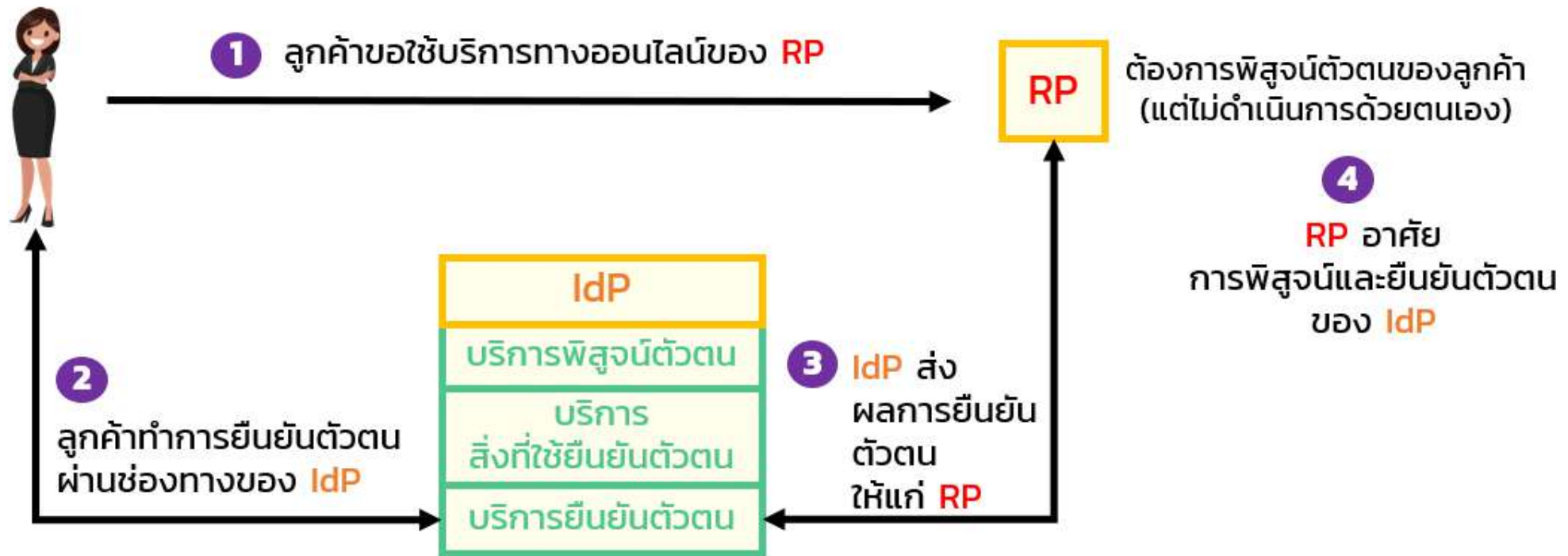
คือ สิ่งของที่ผู้ใช้บริการเท่านั้นมี เช่น กุญแจเข้ารหัส (cryptographic key)
อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) และอุปกรณ์ OTP (OTP device)

(3) สิ่งที่คุณเป็น (something you are)

คือ ข้อมูลชีวมิติ (biometric data) ของผู้ใช้บริการ เช่น ใบหน้าและลายนิ้วมือ

ภาพรวมขั้นตอนสำคัญ ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยอาศัย IdP

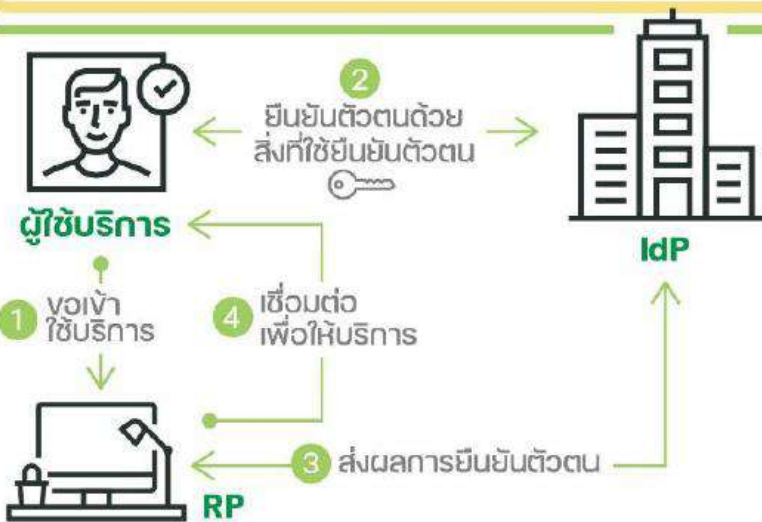
IdP จะต้องเคยพิสูจน์และยืนยันตัวลูกค้ามาก่อน



บุคคลสำคัญ

ที่เกี่ยวข้องกับ Digital ID

กระบวนการพิสูจน์ตัวตน



กระบวนการยืนยันตัวตน

IdP
ผู้พิสูจน์และยืนยันตัวตน
(Identity Provider)

RP
ผู้อาศัยการยืนยันตัวตน
(Relying Party)

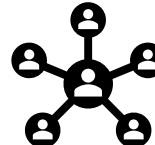
AS
แหล่งข้อมูลที่น่าเชื่อถือ
(Authoritative Source)


ผู้ใช้บริการ
(Subscriber)


ผู้อาศัยการยืนยันตัวตน
(Relying Party : RP)


แหล่งข้อมูลที่น่าเชื่อถือ
(Authoritative source:
AS)


ผู้พิสูจน์และยืนยันตัวตน
(Identity provider:
IdP)


บริการแลกเปลี่ยนข้อมูลเพื่อ
การพิสูจน์และยืนยันตัวตนทางดิจิทัล
(Digital Identity Platform Service)

กระบวนการสำคัญ ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

“การพิสูจน์ตัวตน” (Identity Proofing Service)

ประกอบด้วยกระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับไอดีนิติ และ การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับไอดีนิติ

“การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน” (Authenticator Management Service)

ประกอบด้วยกระบวนการเชื่อมโยงไอดีนิติของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้ว เข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น

“การยืนยันตัวตน” (Authentication Service)

ประกอบด้วยกระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันไอดีนิติของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น

คำศัพท์สำคัญ

ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

การพิสูจน์ตัวตน

(Identity Proofing) เพื่อพิสูจน์ว่าเป็นนาย ก จริง

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
(Identity assurance level: IAL)

การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

(Authenticator Management) เพื่อเชื่อมโยงนาย ก กับ สิ่งที่ใช้ยืนยันตัวตน

การยืนยันตัวตน

(Authentication) เพื่อให้มั่นใจว่าเป็นนาย ก
(ที่พิสูจน์ตัวตนแล้ว) เป็นผู้ที่เข้ามาทำธุรกรรม

ระดับความน่าเชื่อถือของการยืนยันตัวตน
(Authentication assurance level: AAL)

IAL vs AAL

ระดับความน่าเชื่อถือ (Assurance Levels) ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level : IAL)

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

ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authenticator Assurance Levels : AAL)

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

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่หน่วยงานอื่น

อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานสามารถนำไปประยุกต์ใช้ได้

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์						การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์		
IAL3	กรณีใช้บัตรประชาชน			กรณีใช้บัตรประชาชนอิเล็กทรอนิกส์		ตรวจสอบและยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล	พบเห็นต่อหน้าเท่านั้น	Biometric Comparison กับข้อมูลชีวมิติจากฮับหรือข้อมูลที่น่าเชื่อถือของหลักฐานแสดงตน หรือระบบตรวจสอบข้อมูลชีวมิติของหน่วยงานรัฐ
	ใช้เครื่องอ่านบัตร และ สถานะบัตรประชาชน และ ตรวจสอบกับแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม			ใช้ระบบตรวจสอบของกระทรวงมหาดไทย และ ตรวจสอบกับแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม				
IAL2	IAL2.3	กรณีใช้บัตรประชาชน		กรณีใช้หนังสือเดินทาง		กรณีใช้หลักฐานแสดงตนอิเล็กทรอนิกส์ที่ออกโดยหน่วยงานรัฐ	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Biometric Comparison กับข้อมูลชีวมิติจากฮับหรือข้อมูลที่น่าเชื่อถือของหลักฐานแสดงตน หรือระบบตรวจสอบข้อมูลชีวมิติของหน่วยงานรัฐ
		ใช้เครื่องอ่านบัตร และ สถานะบัตรประชาชน		ใช้ NFC และ สถานะบัตรประชาชน หรือ เอกสารสำคัญอื่น				
	IAL2.2	ใช้เครื่องอ่านบัตร หรือ ผลการยืนยันตัวตนจาก IdP ที่เคยทำ IAL2.3 และ สถานะบัตรประชาชน		ใช้ NFC และ สถานะบัตรประชาชน หรือ เอกสารสำคัญอื่น		ใช้ระบบตรวจสอบของหน่วยงานรัฐ	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Visual Comparison กับภาพใบหน้าจากฮับของหลักฐานแสดงตน หรือภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3
		ใช้เครื่องอ่านบัตร หรือ ผลการยืนยันตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC				
IAL2.1	ใช้เครื่องอ่านบัตร หรือ ผลการยืนยันตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC			พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Visual Comparison กับภาพใบหน้าจากฮับของหลักฐานแสดงตน หรือภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3	
IAL1	อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ โดยไม่จำเป็นต้อง ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ หรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์							

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญจากข้อเสนอแนะมาตรฐานฯ และแสดงเฉพาะระบบตรวจสอบของหน่วยงานรัฐที่มีอยู่ในปัจจุบัน
ศึกษารายละเอียดจาก ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล - ข้อกำหนดของการพิสูจน์ตัวตน (ขมรอ. 19-2564 เวอร์ชัน 2.0)

ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่หน่วยงานอื่น

อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานสามารถนำไปประยุกต์ใช้ได้

ข้อกำหนดของการยืนยันตัวตน			ชนิดของสิ่งที่ใช้ยืนยันตัวตน ที่สามารถใช้ได้					
AAL3	 ยืนยันตัวตนแบบ Multi-factor authentication และใช้สิ่งที่ใช้ยืนยันตัวตนเป็น Hardware และมี Cryptographic key	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร  สามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)  สามารถป้องกัน IDP ตัวปลอม (IDP impersonation resistance)	 MF Crypto Device และ  SF Crypto Device และ  MF OTP Device และ  SF Crypto Software และ  SF OTP Device และ  MF Crypto Software และ  Memorized Secret และ  SF OTP Device และ  SF Crypto Software					
AAL2	 ยืนยันตัวตนแบบ Multi-factor authentication	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร  สามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)	 Memorized Secret และ  Out-of-band Device หรือ  SF OTP Device หรือ  SF Crypto Software  MF OTP Device  MF Crypto Software					
AAL1	 ยืนยันตัวตนแบบ Single-factor authentication	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร	 Memorized Secret  Out-of-band Device  SF OTP Device  SF Crypto Software  SF Crypto Device					

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญจากข้อเสนอแนะมาตรฐานฯ

ศึกษารายละเอียดจาก ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ชมร. 20-2564 เวอร์ชัน 2.0)

SF ย่อจาก "single-factor", MF ย่อจาก "multi-factor" และ crypto ย่อจาก "cryptographic"

Thank you