



การกำกับดูแล มาตรฐาน และกฎหมาย ที่เกี่ยวข้องกับบริการ Digital ID

DIGITAL ID คือ

ID เป็นคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ภายในบริบทที่กำหนด

Digital ID จึงเป็น ID ที่อยู่ในรูปแบบ Digital นั้นเอง



**ใช้ระบุตัวบุคคล
ผู้ทำธุรกรรม**



**ไม่ต้องสร้าง Digital ID
ใหม่ทุกครั้ง**

สามารถใช้เข้าถึงบริการต่าง ๆ ได้
จาก Digital ID เดิมที่ผ่านการพิสูจน์
ตัวตนที่น่าเชื่อถือ



**ลดกระบวนการ
ระยะเวลา
และค่าใช้จ่าย ในการ
พิสูจน์ตัวตน**



**ผู้ใช้บริการสามารถ
เข้าถึงบริการดิจิทัล
ของทั้งภาครัฐ
และภาคเอกชนได้ง่ายขึ้น**



1

บุคคลมาแสดงตน
กับ IdP



2

IdP พิสูจน์ตัวตน
ของบุคคล



3

IdP ออกหรือลงทะเบียน
สิ่งที่ใช้ยืนยันตัวตน
(Authenticator)



4

บุคคลเปลี่ยนสถานะ
เป็นผู้ใช้บริการ

การพิสูจน์ตัวตน (Identity proofing)

การยืนยันตัวตน (Authentication)



1

ผู้ใช้บริการขอทำ
ธุรกรรมกับ RP



2

RP ให้ผู้บริการ
ไปยืนยันตัวตนกับ IdP



3

IdP ตรวจสอบสิ่งที่ใช้
ยืนยันตัวตน
และส่งผลให้กับ RP



4

ผู้บริการ
เข้าใช้งานที่ RP



มาตรฐาน ด้าน Digital ID



ข้อเสนอแนะมาตรฐาน ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ETDA
นพช.
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ชมธอ. 18-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล –
กรอบการทำงาน

DIGITAL IDENTITY –
FRAMEWORK

เวอร์ชัน 2.0

ETDA
นพช.
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ชมธอ. 19-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล –
ข้อกำหนดของการพิสูจน์ตัวตน

DIGITAL IDENTITY –
IDENTITY PROOFING REQUIREMENTS

เวอร์ชัน 2.0

ETDA
นพช.
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ชมธอ. 20-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล –
ข้อกำหนดของการยืนยันตัวตน

DIGITAL IDENTITY –
AUTHENTICATION REQUIREMENTS

เวอร์ชัน 2.0

IAL vs AAL

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level : IAL)

- IAL คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล
- เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง (เช่น บุคคลที่กล่าวอ้างว่าตนเองชื่อ "สมชาย" คือ "สมชาย" ตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา)
- IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด



ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Levels : AAL)

- AAL คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน
- เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง (เช่น บุคคลที่กำลังเข้าใช้บริการ คือ "สมชาย" ตัวจริง ที่กรอกรหัสผ่านถูกต้อง)
- AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด



ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน

Identity Assurance Level (IAL)

ระดับ IAL1

- อาจรวบรวมข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted)
- อาจตรวจสอบข้อมูลด้วยวิธีการอื่น ๆ นอกเหนือจากวิธีการในระดับ IAL2 และ IAL3

ระดับ IAL2

- ขอลักษณ์ฐานแสดงตน ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าเป็นข้อมูลของบุคคลที่มีอยู่จริง
- ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์
- สามารถทำได้ทั้ง แบบพบเห็นต่อหน้า (F2F) หรือแบบไม่พบเห็นต่อหน้า (non-F2F) เช่น Kiosk หรือ App
- ในทางปฏิบัติ แบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1, IAL2.2 และ IAL2.3

ระดับ IAL3

- เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้
 - ตรวจสอบกับแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม
 - เปรียบเทียบข้อมูลชีวมิติ (biometric comparison)
- สามารถทำได้แบบพบเห็นต่อหน้า (F2F) เท่านั้น

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์						การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์	
IAL3	กรณีใช้บัตรประชาชน			กรณีใช้บัตรประชาชนอิเล็กทรอนิกส์		ตรวจสอบและยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล	
	ใช้เครื่องอ่านบัตร และ สถานะบัตรประชาชน ตรวจสอบกับแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม			ใช้ระบบตรวจสอบของกระทรวงมหาดไทย และ ตรวจสอบกับแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม		พบเห็นต่อหน้าเท่านั้น	
IAL2	IAL2.3	กรณีใช้บัตรประชาชน		กรณีใช้หนังสือเดินทาง		กรณีใช้หลักฐานแสดงตนอิเล็กทรอนิกส์ที่ออกโดยหน่วยงานรัฐ	
	IAL2.2	ใช้เครื่องอ่านบัตร หรือ ผลการยืนยันตัวตนจาก IdP ที่เคยทำ IAL2.3 และ สถานะบัตรประชาชน		ใช้ NFC และ สถานะบัตรประชาชน หรือ เอกสารสำคัญอื่น		ใช้ระบบตรวจสอบของหน่วยงานรัฐ	
	IAL2.1	ใช้เครื่องอ่านบัตร หรือ ผลการยืนยันตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC		พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	
						พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า Biometric Comparison กับ ข้อมูลชีวมิติจากชิปหรือข้อมูลที่น่าเชื่อถือของหลักฐานแสดงตน ระบบตรวจสอบข้อมูลชีวมิติของหน่วยงานรัฐ	
						พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า Biometric Comparison กับ ข้อมูลชีวมิติจากชิปหรือข้อมูลที่น่าเชื่อถือของหลักฐานแสดงตน ระบบตรวจสอบข้อมูลชีวมิติของหน่วยงานรัฐ	
						พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า Visual Comparison กับ ภาพใบหน้าจากชิปของหลักฐานแสดงตน ภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3	
						พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า Visual Comparison กับ ภาพใบหน้าจากชิปของหลักฐานแสดงตน ภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3	

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญจากข้อเสนอแนะมาตรฐานฯ และแสดงเฉพาะระบบตรวจสอบของหน่วยงานรัฐที่มีอยู่ในปัจจุบัน

ระดับความน่าเชื่อถือของการยืนยันตัวตน

Authentication Assurance Level (AAL)



ระดับ AAL1

- การยืนยันตัวตนแบบปัจจัยเดียว (Single-Factor Authentication)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย

ระดับ AAL2

- การยืนยันตัวตนด้วยปัจจัยที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย (Multi-Factor Authentication)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย

ระดับ AAL3

- การยืนยันตัวตนด้วยปัจจัยที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย (Multi-Factor Authentication)
- ใช้สิ่งที่ใช้ยืนยันตัวตนที่เป็นฮาร์ดแวร์ (hardware based) และบสรุจุญแจเข้ารหัส (cryptographic key)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย และใช้เกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol)

สิ่งที่ใช้ยืนยันตัวตน (Authenticator)

- ✓ Authenticator คือ สิ่งที่ใช้บริการครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตนกับ IdP
- ✓ Authenticator มีข้อมูลลับ (secret) ที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นสามารถนำมาใช้ยืนยันตัวตนได้
- ✓ Authenticator อาจประกอบด้วย ปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัย (Single-Factor) หรือประกอบด้วยปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย (Multi-Factor) ก็ได้

ทั้งนี้ **ปัจจัยของการยืนยันตัวตน (Authentication Factor)** แบ่งเป็น 3 ประเภท

1) สิ่งที่คุณรู้ (something you know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ

- เช่น รหัสผ่าน (password) และเลขรหัสส่วนตัว (PIN)

2) สิ่งที่คุณมี (something you have) คือ สิ่งของที่ผู้ใช้บริการเท่านั้นครอบครอง

- เช่น กุญแจเข้ารหัส (cryptographic key) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) และ อุปกรณ์ OTP (OTP device)

3) สิ่งที่คุณเป็น (something you are) คือ ข้อมูลชีวมิติ (biometric data) ของผู้ใช้บริการ

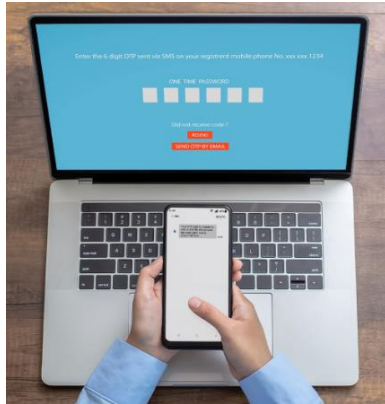
- เช่น ใบหน้า ลายนิ้วมือ หรือม่านตา

ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: **AAL**)

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	 Memorized Secret และ  SF Crypto Device	 MF OTP Device และ  SF Crypto Device	 MF OTP Device และ  SF Crypto Software	 SF OTP Device และ  MF Crypto Software	 Memorized Secret และ  SF OTP Device  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
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

ตัวอย่างอุปกรณ์ authenticator ที่นิยมใช้

อุปกรณ์สื่อสารช่องทางอื่น (Out-of-Band Device)



LINE

QR code login



Generate new QR code

Open the QR code reader on the Android or iOS version of LINE and scan this QR code.

อุปกรณ์ OTP (OTP device)



อุปกรณ์เข้ารหัสลับ (cryptographic device)



FIPS 140-2
VALIDATED



การควบคุมดูแลธุรกิจบริการ Digital ID มุ่งเน้นให้การให้บริการมี
การรักษาความมั่นคงปลอดภัยของระบบให้บริการและ
ข้อมูลของผู้ใช้บริการ และสามารถ ให้บริการได้อย่างต่อเนื่อง
มีประสิทธิภาพ โดยกำหนดหลักเกณฑ์ในการควบคุมดูแล
เพื่อให้เกิดความโปร่งใสและสอดคล้องตามมาตรฐานสากล

พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับ ใบอนุญาต พ.ศ. 2565

เล่ม ๑๓๙ ตอนที่ ๗๘ ก ราชกิจจานุเบกษา ๒๓ ธันวาคม ๒๕๖๕



พระราชกฤษฎีกา
ว่าด้วยการควบคุมดูแลธุรกิจบริการ
เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน
ทางดิจิทัลที่ต้องได้รับใบอนุญาต
พ.ศ. ๒๕๖๕

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๒ ธันวาคม พ.ศ. ๒๕๖๕
เป็นปีที่ ๗ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว
มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตน
ทางดิจิทัลที่ต้องได้รับใบอนุญาต

อาศัยอำนาจตามความในมาตรา ๑๗๕ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย
และมาตรา ๓๔/๔ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒
จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจ
บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕”

● 23 ร.ศ. 65

ประกาศในราชกิจจานุเบกษา

● ให้ใช้บังคับเมื่อพ้นกำหนด 180 วัน

นับแต่ประกาศในราชกิจจานุเบกษา (21 มิ.ย. 66)

● ผู้รักษาการ : สมว.DE

ธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และ ยืนยันตัวตนทางดิจิทัลที่กำลังบูม



บริการพิสูจน์ตัวตน (Identity Proofing Service)

บริการที่ประกอบด้วยกระบวนการรวบรวมและ
ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และ
การตรวจสอบความเชื่อมโยงระหว่างบุคคล
กับข้อมูลเกี่ยวกับอัตลักษณ์นั้น



บริการออกและบริหารจัดการ สิ่งที่ใช้ยืนยันตัวตน (Authenticator Management Service)

บริการที่ประกอบด้วยกระบวนการเชื่อมโยงอัตลักษณ์
ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้
ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น



บริการยืนยันตัวตน (Authentication Service)

บริการที่ประกอบด้วยกระบวนการตรวจสอบสิ่ง
ที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของ
บุคคลที่ใช้ สิ่งที่ใช้ยืนยันตัวตนนั้น



บริการแลกเปลี่ยนข้อมูลเพื่อ การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)

ที่เป็นเครือข่ายหรือระบบเพื่อการเชื่อมโยงและ
แลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และ
ยืนยันตัวตนทางดิจิทัล

ธุรกิจบริการที่ได้รับการยกเว้น

1

บริการพิสูจน์และยืนยันตัวตน
โดยผู้ให้บริการออกใบรับรองเพื่อ
สนับสนุนลายมือชื่ออิเล็กทรอนิกส์
ตามกฎหมายว่าด้วยธุรกรรมฯ
(Certification Authority: CA)

2

บริการพิสูจน์และยืนยันตัวตน
ที่บุคคลใช้เพื่อประโยชน์ภายใน
กิจการของบุคคลนั้น
โดยไม่ได้ให้บริการแก่
บุคคลภายนอก

3

บริการเกี่ยวกับระบบการพิสูจน์
และยืนยันตัวตนทางดิจิทัล
ในกิจการที่คณะกรรมการ
ประกาศกำหนด

หมวด 1 การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- กำหนดประเภทบริการที่ต้องขออนุญาต และไม่
ต้องขออนุญาต
- กำหนดคุณสมบัติของผู้ขอรับใบอนุญาต

หมวด 2 การขออนุญาตและการอนุญาต

- กำหนดรายละเอียดและขั้นตอนการขอรับ
ใบอนุญาต
- กำหนดขั้นตอนการตรวจประเมินความพร้อมของ
ผู้ขอรับใบอนุญาตก่อนเริ่มประกอบธุรกิจ

หมวด 3 หน้าที่ของผู้รับใบอนุญาต

- ลักษณะต้องห้ามของผู้ทำหน้าที่กรรมการ/
ผู้จัดการ/ผู้รับผิดชอบ ในการดำเนินงาน
- เงื่อนไขการใช้บริการจากบุคคลภายนอกเพื่อ
เก็บรวบรวมหรือเก็บรักษาข้อมูล
- การแจ้งการเปลี่ยนแปลงในเรื่องสำคัญ /
เรื่องร้องเรียน
- การจัดเก็บข้อมูลเพื่อประโยชน์ในการ
ตรวจสอบ
- การตรวจประเมินระบบอย่างสม่ำเสมอ

หมวด 4 การควบคุมดูแลการประกอบธุรกิจบริการ

- กำหนดหลักเกณฑ์ตามลักษณะของการ
ให้บริการ
 - 1) มาตรการการบริหารและการจัดการความ
เสี่ยง
 - 2) มาตรการการรักษาความมั่นคงปลอดภัย
 - 3) มาตรการการควบคุมดูแลและป้องกันการ
ทุจริตหรือการฉ้อโกง
 - 4) มาตรฐานการให้บริการ
 - 5) การคุ้มครองผู้ใช้บริการและมาตรการการ
บรรเทาความเสียหายและการชดใช้หรือ
เยียวยา
 - 6) การใช้บริการจากบุคคลภายนอก
 - 7) การเปิดเผยข้อมูลที่สำคัญเกี่ยวกับการ
ให้บริการ
- การนำส่งงบการเงินและสรุปผลการ
ดำเนินงานเกี่ยวกับการให้บริการ อย่างน้อยปี
ละ 1 ครั้ง
- อำนาจพนักงานเจ้าหน้าที่ในการเรียกให้ส่ง
รายงานหรือข้อมูลเพิ่มเติม

หมวด 5 การเลิกประกอบธุรกิจ

- ขั้นตอนการขอเลิกประกอบธุรกิจและ
การยื่นเอกสารประกอบ
- หลักเกณฑ์ วิธีการ เงื่อนไข และระยะเวลา
ในการเลิกประกอบธุรกิจ

หมวด 6 การพักใช้และเพิกถอนใบอนุญาต

- กำหนดเหตุแห่งการเพิกถอน
- ผลของการเพิกถอน

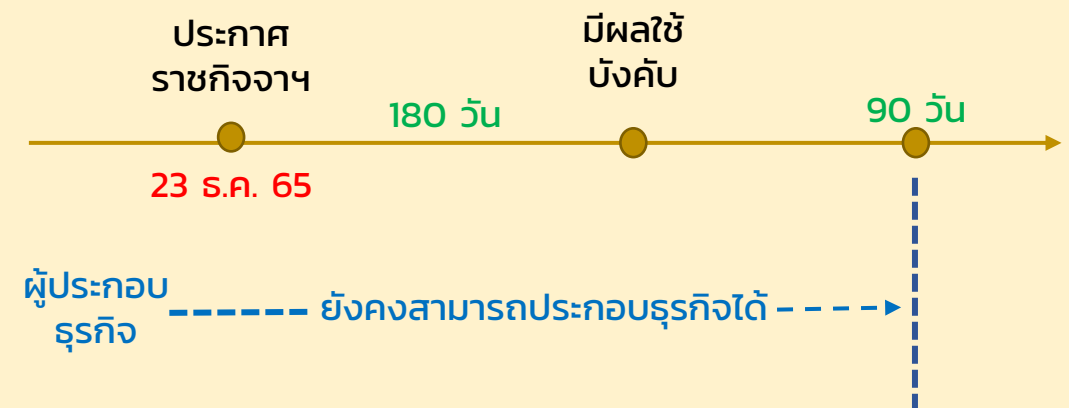
บทเฉพาะกาล

- ผู้ที่ประกอบธุรกิจอยู่แล้วก่อนกฎหมายใช้
บังคับ ให้ยื่นคำขอรับอนุญาตภายใน 90
วัน นับแต่กฎหมายมีผลใช้บังคับ

กลไกทางกฎหมายเพื่อรองรับ ผู้ประกอบการที่ดำเนินการอยู่ในปัจจุบัน

บทเฉพาะกาล

มาตรา 37 ให้ผู้ประกอบการบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตตามพระราชกฤษฎีกานี้ซึ่งได้ประกอบธุรกิจอยู่ในวันก่อนวันที่พระราชกฤษฎีกานี้ใช้บังคับ ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลต่อไปได้ โดยให้ยื่นคำขอรับใบอนุญาตพร้อมด้วยรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจภายในเก้าสิบวันนับแต่วันที่พระราชกฤษฎีกานี้มีผลใช้บังคับ และเมื่อได้ยื่นคำขอรับใบอนุญาตแล้วให้ดำเนินการกิจการต่อไปได้จนกว่าคณะกรรมการจะมีคำสั่งไม่อนุญาต



หากไม่ยื่นคำขอภายใน 90 วัน และยังไม่ประกอบธุรกิจต่อไป
ถือว่า ประกอบธุรกิจโดยไม่ได้รับอนุญาต
ตาม พ.ร.บ.ธุรกรรมฯ มาตรา 45/1

- **Risk Management**
- **Capability Management**
: Key requirements



กลไกการตรวจสอบ

- **การขอรับใบอนุญาต (Licensing)** : มีการตรวจสอบใน 2 ขั้นตอน
(1) การตรวจคุณสมบัติและรูปแบบการ ประกอบธุรกิจในการขอรับใบอนุญาต
(2) ขั้นตอนการขอเริ่มประกอบธุรกิจ (Activate license) เพื่อประเมินความพร้อมก่อนที่จะเริ่มประกอบธุรกิจ
- **การควบคุมติดตามแบบ Ongoing** ในรูปแบบของการตรวจสอบประจำปี และการติดตามความคืบหน้าในการประกอบธุรกิจ เช่น การแจ้งการเปลี่ยนแปลง

The background is a dark blue collage. On the left, a woman's face is partially visible with a white wireframe mesh overlaid on it. In the center, there is a large, detailed close-up of a human eye. On the right, a fingerprint is shown with white lines indicating the ridges. The text "THANK YOU" is centered in a bold, yellow, sans-serif font.

THANK YOU