

การปรับปรุงแนวปฏิบัติ

การนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า (e-KYC)

1. มาตรฐานการพิสูจน์ตัวตนในปัจจุบัน & การเปลี่ยนแปลงของ Digital ID

การปรับปรุงมาตรฐานกลาง จัดทำโดย ETDA*



Overview



Identity proofing



Authentication

- ปี 2561 จัดทำมาตรฐานกลางที่กำหนดวิธีการพิสูจน์และยืนยันตัวตน
- ปี 2564 และ 2566 ปรับปรุงมาตรฐานรองรับการใช้ mobile ID และ D.DOPA

ผู้ให้บริการพิสูจน์และยืนยันตัวตนซึ่งเพิ่มขึ้น

NDID



2563



Mobile ID



2565



ThaiID



2566

2. แนวดำเนินการ

- เนื่องจากผู้ประกอบการได้สอบถามมายังสำนักงาน
- การปรับปรุงมาตรฐานของ ETDA และการเพิ่มขึ้นของผู้ให้บริการพิสูจน์และยืนยันตัวตน



เพื่อความชัดเจนในทางปฏิบัติ สำนักงานจึงได้ปรับปรุงและออกแนวปฏิบัติ นป. 4/2566 เรื่อง การนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้าโดยปรับหลักเกณฑ์ให้เป็นปัจจุบัน



นป. 4/2566

3. สำคัญของการปรับปรุงแนวปฏิบัติ

เพิ่มช่องทางการทำ KYC เพื่อความชัดเจนในการปฏิบัติ



ปรับปรุงมาตรฐานให้เป็นปัจจุบัน

- ยกเลิกระดับ IAL/AAL ในแนวปฏิบัติ แต่กำหนดแค่วิธีการ (ไม่ได้ปรับวิธีการ)
- หากปฏิบัติตามวิธีการที่กำหนด ตามแนวปฏิบัติจะมีระดับ IAL/AAL ดังนี้
 - ระดับ IAL เดิม 2.1+ เป็น IAL 2.2
 - ระดับ AAL เดิม 2.1 เป็น AAL 2

ปรับนิยามและถ้อยคำให้เป็นปัจจุบัน

เช่น ปรับเพิ่มวิธีการบริหารความเสี่ยงกรณีระบบตรวจสอบสถานะการปกครองล้ม / ปรับเพิ่มวิธีการทำ KYC กรณีใช้ passport ให้ชัดเจน (เดิมอยู่ในอีเมลเวียน)

4. วิธีการพิสูจน์ตัวตน (Identity proofing)

1. รวบรวมและตรวจสอบหลักฐาน

1.1 เลียบบัตรประชาชน (dip chip)

- กรณี offline เจ้าหน้าที่ของบริษัทเลียบบัตรประชาชนของลูกค้ากับเครื่องอ่านบัตร
- กรณี online ลูกค้าไปเลียบบัตรประชาชนกับตู้ kiosk หรือ messenger

1.2 ตรวจสอบสถานะบัตร ทาง Web service ของ DOPA

- ตรวจสอบว่าบัตรประชาชนยังใช้งานได้
ไม่เป็นบัตรที่ถูกแจ้งหาย



ขั้นตอน พิสูจน์ตัวตน



2. ตรวจสอบตัวบุคคล

- กรณี offline เจ้าหน้าที่ของบริษัท นำรูปจากการ dip chip มาเทียบกับใบหน้าของลูกค้า
 - กรณี online เจ้าหน้าที่ของบริษัท นำรูปจากการ dip chip มาเทียบกับรูปถ่ายของลูกค้า
- * ต้องเก็บภาพถ่ายเพื่อป้องกันการปฏิเสธการทำธุรกรรม

3. ตรวจสอบช่องทางติดต่อ

- ส่ง link ให้คลิก หรือ OTP ให้ลูกค้ากรอกเข้าระบบของบริษัทเพื่อพิสูจน์ว่าช่องทางติดต่อที่ลูกค้าให้ สามารถใช้ได้ติดต่อได้จริง



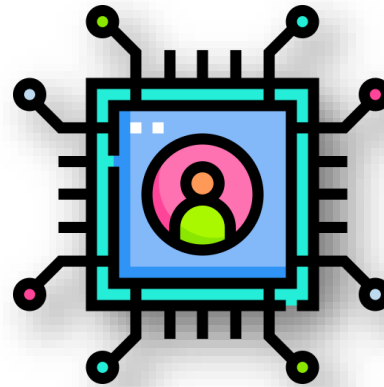
วิธีการยังคงเดิม (ไม่ได้ปรับวิธีการ) แต่ปรับเพิ่มความชัดเจนในทางปฏิบัติ ผู้ประกอบธุรกิจสามารถดำเนินการพิสูจน์ตัวตนด้วยตนเองหรือใช้ Services providers เช่น ThaID, NDID, Mobile ID หรือวิธีการอื่นใดซึ่งสามารถบรรลุวัตถุประสงค์และวิธีการที่สำนักงานกำหนด

5. วิธีการยืนยันตัวตน Authentication

ลูกค้าใช้ authenticators เพื่อยืนยันตัวตนเมื่อต้องการเข้าระบบด้วย 2 factors หรือที่เรียกว่า **2FA** เพื่อดำเนินการดังนี้



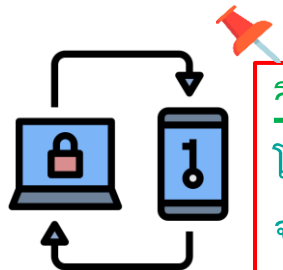
- 1 ยืนยันตัวตนในระหว่างเปิดบัญชี
เช่น กรอกข้อมูล หรือ upload หลักฐานเพิ่ม
(ผ่านการพิสูจน์ตัวตนแล้ว)



- 2 ยืนยันตัวตนในระบบ Digital ID
เพื่อการเปิดบัญชีหลักทรัพย์



- 3 เพื่อเข้าระบบ online เพื่อทำธุรกรรมสำคัญ
(ซื้อ ขาย ฝาก ถอน เปลี่ยนแปลงข้อมูลสำคัญ ลงนาม
สัญญาที่มีผลต่อการให้บริการ การขอ consent)

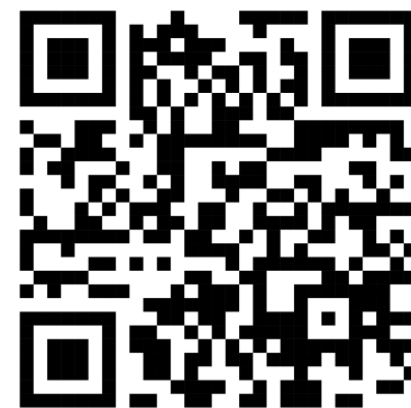


วิธีการยังคงเดิม (ไม่ได้ปรับวิธีการ)

โดยแนวปฏิบัติไม่ได้ระดับ AAL หากดำเนินการตามแนวปฏิบัติ
จะได้ระดับ AAL 2 ตามมาตรฐานที่ ETDA ปรับปรุง



[FAQ บนหน้า website สำนักงาน](#)



ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก
 อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ประโยชน์ภายในกิจการของตนเองสามารถนำไปประยุกต์ใช้ได้

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์					การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์		
IAL3	ใช้บัตรประชาชน				ตรวจสอบและยืนยัน ช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล	พบเห็นต่อหน้า เท่านั้น	Biometric Comparison ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติ จากชิปของหลักฐานแสดงตน หรือ ใช้ระบบ Face Verification Service (FVS)
	[ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)] และ ตรวจสอบความมียุ่จริงของอัตลักษณ์ จากแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม						
IAL2	IAL2.3	กรณีใช้บัตรประชาชน โดยมีเครื่องอ่านบัตร	กรณีใช้บัตรประชาชน โดยไม่มีเครื่องอ่านบัตร	กรณีใช้หนังสือเดินทาง	[สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]	[พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า]	Biometric Comparison ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติ จากชิปของหลักฐานแสดงตน หรือ ใช้ระบบ Face Verification Service (FVS)
		ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code) และ FVS	ตรวจสอบข้อมูล โดยใช้ NFC			
		ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูล โดยใช้ NFC และ [สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]			
		ตรวจสอบข้อมูล	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูล โดยใช้ NFC			
IAL1	IAL2.2	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูล โดยใช้ NFC และ [สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]	[พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า]	Visual Comparison กับ ภาพใบหน้าจากชิป ของหลักฐานแสดงตน หรือ ภาพใบหน้าจาก IdP ที่เคย ทำ IAL2.3 ของบุคคลนั้น	
		ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูล โดยใช้ NFC และ [สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]			
		ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูล โดยใช้ NFC และ [สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]			
		ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูล โดยใช้ NFC และ [สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น]			
IAL1	IAL2.1	ตรวจสอบข้อมูล	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูล โดยใช้ NFC	[พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า]	Visual Comparison กับ ภาพใบหน้าจากชิป ของหลักฐานแสดงตน หรือ ภาพใบหน้าจาก IdP ที่เคย ทำ IAL2.3 ของบุคคลนั้น	
		ตรวจสอบข้อมูล	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูล โดยใช้ NFC			
		ตรวจสอบข้อมูล	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูล โดยใช้ NFC			
		ตรวจสอบข้อมูล	ตรวจสอบข้อมูล จาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูล โดยใช้ NFC			
อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ โดยไม่จำเป็นต้อง ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ หรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์							

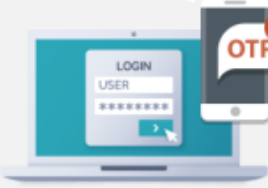
ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ประโยชน์ภายในกิจการของตนเองสามารถนำไปประยุกต์ใช้ได้

ข้อกำหนดของการยืนยันตัวตน			ชนิดของสิ่งที่ใช้ยืนยันตัวตน ที่สามารถใช้ได้							
AAL3	 ยืนยันตัวตนแบบ Multi-factor authentication และใช้สิ่งที่ใช้ยืนยันตัวตนเป็น Hardware และมี Cryptographic key	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร	 สามารถป้องกันการโจมตีแบบส่ง ข้อมูลซ้ำ (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 และ  SF Crypto Software
	 ยืนยันตัวตนแบบ Multi-factor authentication	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร	 สามารถป้องกันการโจมตีแบบส่ง ข้อมูลซ้ำ (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	

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากข้อเสนอแนะมาตรฐานฯ

ศึกษารายละเอียดจาก ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ชมธอ. 20-2566 เวอร์ชัน 3.0)

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