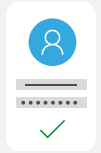
ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ประโยชน์ภายในกิจการของตนเองสามารถนำไปประยุกต์ใช้ได้

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

	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  **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: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐาน

SF ย่อจาก “single-factor”, MF ย่อจาก “multi-factor” และ crypto ย่อจาก “cryptographic”

ศึกษารายละเอียดจาก มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (เลขที่ มธอ. 11 เล่ม 3-2566)