

รายการแก้ไข (change history) ของชุดข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล
จากเวอร์ชัน 2.0 (เลขที่ ชมธอ. 18-2564, 19-2564 และ 20-2564) เป็นเวอร์ชัน 3.0 (เลขที่ ชมธอ. 18-2566, 19-2566 และ 20-2566)

1. รายการแก้ไข จาก ชมธอ. 18-2564 เป็น ชมธอ. 18-2566 (กรอบการทำงาน)

ลำดับ	หัวข้อ	รายการแก้ไข
1	2. บทนิยาม	แก้ไขนิยาม 2.2 อັตลัษณ์ ให้สอดคล้องตาม พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
2	2. บทนิยาม	แก้ไขนิยาม 2.4 การพิสูจน์ตัวตน ให้สอดคล้องตาม พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
3	2. บทนิยาม	แก้ไขนิยาม 2.5 สิ่งที่ใช้ยืนยันตัวตน ให้สอดคล้องตาม พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
4	2. บทนิยาม	เพิ่มนิยาม 2.6 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ตาม พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
5	2. บทนิยาม	แก้ไขนิยาม 2.7 การยืนยันตัวตน ให้สอดคล้องตาม พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต
6	2. บทนิยาม	แก้ไขนิยาม 2.8 ผู้พิสูจน์และยืนยันตัวตน โดยปรับคำในความหมาย เป็น “... การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ...”
7	3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล	แก้ไขคำอธิบายใน 3.1 ภาพรวม จาก “ดิจิทัลไอดี (digital identity) คือ อັตลัษณ์ (identity) ที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์” เป็น “อັตลัษณ์ (identity) คือ ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น ในขณะที่ดิจิทัลไอดี (digital identity) จะเป็นอັตลัษณ์ที่บันทึกในรูปแบบอิเล็กทรอนิกส์ ซึ่งบุคคลสามารถนำดิจิทัลไอดีไปใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์” รวมถึงแก้ไขคำอธิบายปลีกย่อยให้เข้าใจได้ง่ายขึ้น
8	3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล	แก้ไขคำอธิบายใน 3.1 ภาพรวม เป็น “การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอັตลัษณ์ของบุคคล และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอັตลัษณ์นั้น” เพื่อให้สอดคล้องกับนิยาม 2.4 การพิสูจน์ตัวตน
9	3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล	แก้ไขคำอธิบายใน 3.1 ภาพรวม เป็น “การยืนยันตัวตน (authentication) เป็นกระบวนการยืนยันอັตลัษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น” เพื่อให้สอดคล้องกับนิยาม 2.7 การยืนยันตัวตน
10	3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล	แก้ไขคำอธิบายใน 3.3 สิ่งที่ใช้ยืนยันตัวตน จาก “สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือ สิ่งที่ใช้บริการครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตนกับ IdP” เป็น “สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือ สิ่งที่ใช้เชื่อมโยงอັตลัษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุม เพื่อใช้ในการยืนยันตัวตนกับ IdP” เพื่อให้สอดคล้องกับนิยาม 2.5 สิ่งที่ใช้ยืนยันตัวตน รวมถึงแก้ไขคำอธิบายปลีกย่อยให้เข้าใจได้ง่ายขึ้น
11	ภาคผนวก ก.	เพิ่มอักษรย่อ FMR (false match rate) และ FNMR (false non-match rate) และแก้ไขลำดับของรายการอักษรย่อ

2. รายการแก้ไข จาก ชมธอ. 19-2564 เป็น ชมธอ. 19-2566 (ข้อกำหนดของการพิสูจน์ตัวตน)

ลำดับ	หัวข้อ	รายการแก้ไข
1	2. การพิสูจน์ตัวตน 3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน	แก้ไขคำอธิบายปลีกย่อย เพื่อให้สอดคล้องกับนิยาม 2.4 การพิสูจน์ตัวตน ของ ชมธอ. 18-2566 (กรอบการทำงาน)
2	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL3 เป็น “ (1) IdP ต้องรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และจากแหล่งข้อมูลที่นำเชื่อถือของหน่วยงานของรัฐเพิ่มเติม (นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง) ...”
3	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL2.1 และ IAL2.2 กรณีใช้บัตรประจำตัวประชาชนแบบเนกประสงค์เป็นหลักฐานแสดงตน เป็น “(1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน”
4	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL2.1 และ IAL2.2 กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน เป็น “(1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (near field communication: NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง”
5	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL2.2 กรณีใช้บัตรประจำตัวประชาชนแบบเนกประสงค์เป็นหลักฐานแสดงตน เป็น “IdP ต้องตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน หรือใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน”
6	4. ข้อกำหนดของการพิสูจน์ตัวตน	ลบคำอธิบายใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL2.2, IAL2.3 และ IAL3 สำหรับ “กรณีใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่นำเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ” เนื่องจากถือว่า การใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่นำเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ เป็นการใช้ข้อมูลจากผลการยืนยันตัวตนของ IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป
7	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ระดับ IAL2.3 กรณีใช้บัตรประจำตัวประชาชนแบบเนกประสงค์เป็นหลักฐานแสดงตน เป็น “(1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ” และเพิ่มคำอธิบาย “(2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบัตรประจำตัวประชาชนและตรวจสอบสถานะของบัตรประจำตัวประชาชน ด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) ทั้งนี้ ในกรณีนี้ IdP ต้องเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้ระบบพิสูจน์และยืนยันตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) เท่านั้น” เพื่อให้รองรับการใช้ระบบ face verification service แทนการใช้เครื่องอ่านบัตรประจำตัวประชาชน
8	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ ระดับ IAL 2.2 เป็น “ข้อกำหนดเช่นเดียวกับ IAL2.1” เนื่องจาก IAL 2.2 จะไม่มีกรณีใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่นำเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ (ใน 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์) แล้ว

ลำดับ	หัวข้อ	รายการแก้ไข
9	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ ระดับ IAL2.3 และ IAL 3 จาก “(2.2) เปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบตรวจสอบของหน่วยงานของรัฐ” เป็น “(2.2) IdP ใช้ระบบพิสูจน์และยืนยันตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติของหน่วยงานของรัฐ”
10	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ จาก “(2) ... อัตราการยอมรับที่ผิดพลาด (false accept rate: FAR) ไม่เกิน 0.1% และอัตราการปฏิเสธที่ผิดพลาด (false reject rate: FRR) ไม่เกิน 3%” เป็น “(2) ... อัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]” เนื่องจากอ้างอิงข้อกำหนดตามเอกสาร [2]
11	4. ข้อกำหนดของการพิสูจน์ตัวตน	แก้ไขคำอธิบายใน 4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL ในส่วนตารางที่ 4 ให้สอดคล้องกับเนื้อหาใน 4.1, 4.2 และ 4.3 ที่ปรับแก้
12	ภาคผนวก ก.	เพิ่มภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)

3. รายการแก้ไข จาก ชมธอ. 20-2564 เป็น ชมธอ. 20-2566 (ข้อกำหนดของการยืนยันตัวตน)

ลำดับ	หัวข้อ	รายการแก้ไข
1	2. ระดับความน่าเชื่อถือของการยืนยันตัวตน	แก้ไขคำอธิบายใน 2.2 ระดับ AAL2 ในส่วนหมายเหตุ: การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัย เพื่อให้เข้าใจได้ง่ายขึ้น
2	3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน	แก้ไขคำอธิบายใน 3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว, 3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว, 3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย และ 3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย จาก “... ผู้ให้บริการลงลายมือชื่อดิจิทัลบนข้อความ (challenge nonce) ...” เป็น “... ผู้ให้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ...”
3	4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน	แก้ไขคำอธิบายใน 4.3 การใช้งานชีวมิติ (ลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์เท่านั้น) จาก “(3) ... อัตราการยอมรับที่ผิดพลาด (false accept rate: FAR) ไม่เกิน 0.1% และอัตราการปฏิเสธที่ผิดพลาด (false reject rate: FRR) ไม่เกิน 3%” เป็น “(2) ... อัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]” เนื่องจากอ้างอิงข้อกำหนดตามเอกสาร [2]
4	4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน	แก้ไขคำอธิบายใน 4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance) เป็น “สิ่งที่ใช้ยืนยันตัวตนที่ใช้ค่า nonce หรือข้อความ (challenge nonce) ในการพิสูจน์ความใหม่ (freshness) ของผลลัพธ์ที่ใช้ยืนยันตัวตนจะมีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ เนื่องจาก IdP สามารถตรวจพบได้ทันทีว่าผลลัพธ์ซึ่งไม่มีค่า nonce หรือข้อความในการพิสูจน์ความใหม่ที่เหมาะสม”
5	ภาคผนวก ก.	เพิ่มภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)