มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. 11 เล่ม 3-2566

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

DIGITAL IDENTITY –
PART 3: AUTHENTICATION REQUIREMENTS

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

มธอ. 11 เล่ม 3-2566

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประธานกรรมการ

นางอรรชกา สีบุญเรือง

รองประธานกรรมการ

นายวิศิษฏ์ วิศิษฏ์สรอรรถ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

นางสาวสิริธิดา พนมวัน ณ อยุธยา
นายศีลวัต สันติวิสัฏฐ์
นายปณิธิ ชุณหสวัสดิกุล
นายอนุชิต อนุชิตานุกูล
นายกนิษฐ์ สารสิน
นางสาวช่อผกา วิริยานนท์
นายเฉลิมรัฐ นาควิเชียร
นายยรรยง เต็งอำนวย

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอนันต์ กนกศิลป์	สำนักงานปลัดกระทรวงสาธารณสุข
นางรุ่งนิภา อมาตยคง	
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายอภิวัฒน์ อินขัด	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นางสาวรัญศิกานต์ งามบุษบงโสภา	
นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นางสาววิจิตรเลขา มารมย์	
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวจิตสถา ศรีประเสริฐสุข	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และ
นางสาวอรวรี เจริญพร	กิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายณัฐวุฒิ ทิพย์กนก	
นายณรงค์เดช วัชระภาสร	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายกิตตินันท์ ศรีมงคล	
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายอภิสิทธิ์ สุขสาคร	
นายพีรธร วิมลโลหการ	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวอุรัชฎา เกตุพรหม	
นายจำรัส สว่างสมุทร	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายณัฐวุฒิ อมรวิวัฒน์	

เลขานุการ

นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการมาตรฐานและการกำกับดูแล

ประธานอนุกรรมการ

นายยรรยง เต็งอำนวย

อนุกรรมการ

รองศาสตราจารย์ปริทรรศน์ พันธุบรรยงก์	
นายปริญญา หอมเอนก	
นางสาวภรณี หรูวรรธนะ	
นายรอม หิรัญพฤกษ์	
นางสาวสุธีรา ศรีไพบูลย์	
นายอนุชิต อนุชิตานุกูล	
นางสาวสุดจิตร ลาภเลิศสุข	กรมบัญชีกลาง
นางสาวภิญญู กำเนิดหล่ม	กรมสรรพากร
นางสาวรัญศิกานต์ งามบุษบงโสภา	กรมพัฒนาธุรกิจการค้า
นายก่อเกียรติ แก้วกิ่ง	กรมการปกครอง
นางศิริพร ช่างการ	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายกำพล ศรธนะรัตน์	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสินชัย ต่อวัฒนกิจกุล	สำนักงานหลักประกันสุขภาพแห่งชาติ
นางบุษกร ธีระปัญญาชัย	ธนาคารแห่งประเทศไทย
นายภิญโญ ตรีเพชราภรณ์	
นายเอธ แย้มประทุม	
นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายวิบูลย์ ภัทรพิบูล	
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นางสาวธิดารัช ธนภรรคภวิน	

อนุกรรมการและเลขานุการ

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายสิริณัฐ ตั้งธรรมจิต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

ด้วยการเข้าทำธุรกรรมต่าง ๆ จำเป็นต้องมีกระบวนการพิสูจน์และยืนยันตัวตนผู้ที่ประสงค์จะเข้าทำธุรกรรมก่อนเพื่อให้มั่นใจได้ว่าผู้ที่ประสงค์จะเข้าทำธุรกรรมเป็นบุคคลนั้นจริง ประกอบกับในปัจจุบันมีการทำธุรกรรมและการให้บริการในรูปแบบดิจิทัลเพิ่มมากขึ้น ผู้ให้บริการจึงเริ่มมีการพัฒนากระบวนการ พิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่ออำนวยความสะดวกในการเข้าใช้บริการต่าง ๆ ในขณะเดียวกันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้มีการแก้ไขปรับปรุงเพื่อรองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ ซึ่งกลไกดังกล่าวสามารถลดภาระต่อผู้ใช้บริการในการแสดงตน การส่งเอกสารหรือหลักฐานประกอบการพิสูจน์และยืนยันตัวตน รวมถึงช่วยลดขั้นตอนที่ต้องทำกระบวนการเดิมซ้ำ ๆ เพื่อพิสูจน์ตัวตนก่อนเข้าทำธุรกรรม

อย่างไรก็ตาม กระบวนการพิสูจน์และยืนยันตัวตนในปัจจุบันยังมีความหลากหลายและมีข้อกำหนดแตกต่างกันไปตามเงื่อนไขและความจำเป็นของผู้ให้บริการหรือหน่วยงานแต่ละแห่งซึ่งในบางกรณีอาจเกิดความไม่สอดคล้องหรือไม่สามารถนำมาใช้งานร่วมกันได้ ดังนั้น จึงได้มีการพัฒนามาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการดำเนินการที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ได้แก่ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) ซึ่งมีการพัฒนาและปรับปรุงมาอย่างต่อเนื่อง ดังนี้

- เวอร์ชัน 1.0: เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561
- เวอร์ชัน 2.0: เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564
- เวอร์ชัน 3.0: เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566

ในการนี้ เพื่อให้เกิดความสอดคล้องและเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และเพื่อให้ผู้ให้บริการและหน่วยงานต่าง ๆ สามารถใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดีร่วมกันได้บนมาตรฐานและระดับความน่าเชื่อถือที่มีความสอดคล้องกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงเห็นควรให้มีการยกระดับมาตรฐานดังกล่าว โดยนำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566 มาปรับปรุงเป็นชุดมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เลขที่ มธอ. 11) ซึ่งประกอบด้วย

- เล่ม 1 กรอบการทำงาน (Part 1: Framework)
- เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)
- เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน ฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

สารบัญ

สารบัญตาราง

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

1. ขอบข่าย

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก ข้อกำหนดในมาตรฐานฉบับนี้สามารถประยุกต์ใช้ได้กับบริการพิสูจน์และยืนยันตัวตนที่ใช้เพื่อประโยชน์ภายในกิจการของตนเอง ทั้งนี้ ไม่มีเจตนาปิดกั้นหรือห้ามใช้วิธีการอื่นเพื่อเพิ่มประสิทธิภาพของการพิสูจน์และยืนยันตัวตน

ระดับ AAL ในมาตรฐานฉบับนี้กำหนดชนิดของสิ่งที่ใช้ยืนยันตัวตนและเกณฑ์วิธีการยืนยันตัวตน โดยพิจารณาจากคุณสมบัติในการป้องกันการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นผ่านช่องทางออนไลน์เป็นหลัก เช่น การโจมตีโดยคนกลาง (man-in-the-middle attack) และการโจมตีแบบส่งข้อมูลซ้ำ (replay attack) ด้วยเหตุนี้ การยืนยันตัวตนแบบพบเห็นต่อหน้าซึ่งไม่สามารถนำคุณสมบัติและเกณฑ์การกำหนดระดับ AAL ของการยืนยันตัวตนผ่านช่องทางออนไลน์มาพิจารณาใช้ได้จึงไม่อยู่ในขอบข่ายของมาตรฐานฉบับนี้ ในกรณีที่ IdP มีความประสงค์จะให้บริการยืนยันตัวตนแบบพบเห็นต่อหน้า ให้ใช้วิธีการยืนยันตัวตนที่เหมาะสมตามความต้องการที่ผู้อาศัยการยืนยันตัวตน (relying party: RP) กำหนด

มาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL แบ่งออกเป็น 3 ระดับ ดังนี้

2.1 ระดับ AAL1

ระดับ AAL1 ให้ความมั่นใจระดับหนึ่งว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL1 กำหนดให้ใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตน (authentication protocol) ที่มั่นคงปลอดภัย

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL1 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) รหัสลับจดจำ (memorized secret)
(2) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(3) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(4) ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL2 และ AAL3

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

2.2 ระดับ AAL2

ระดับ AAL2 ให้ความมั่นใจระดับสูงว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL2 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตน (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

หมายเหตุ: การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัย สามารถทำได้ 2 วิธี ดังนี้
(1) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว (single-factor authenticator) ซึ่งเป็นปัจจัยที่แตกต่างกัน จำนวน 2 อัน เช่น การกรอกรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตน
(2) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบหลายปัจจัย (multi-factor authenticator) จำนวน 1 อัน เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านใช้ครั้งเดียว (OTP) หลังจากผู้ใช้บริการกรอกเลขรหัสส่วนตัวหรือสแกนลายนิ้วมือสำเร็จ จากนั้น ผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกเพื่อยืนยันตัวตน

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL2 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)
(2) ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(3) รหัสลับจดจำ (memorized secret) ร่วมกับ อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(4) รหัสลับจดจำ (memorized secret) ร่วมกับ อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(5) รหัสลับจดจำ (memorized secret) ร่วมกับ ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)

(6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL3

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(2) สิ่งที่ใช้ยืนยันตัวตนอย่างน้อย 1 อันต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) เมื่อมีการใช้อุปกรณ์ เช่น โทรศัพท์เคลื่อนที่ ในการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือชีวมิติ) ต้องไม่ถือเป็นหนึ่งในปัจจัยของการยืนยันตัวตน เนื่องจาก IdP จะไม่สามารถทราบได้ว่าอุปกรณ์ถูกล็อคอยู่ หรือกระบวนการปลดล็อคเป็นไปตามข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตนชนิดนั้นหรือไม่

2.3 ระดับ AAL3

ระดับ AAL3 ให้ความมั่นใจระดับสูงมากว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL3 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย และใช้สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติเป็นฮาร์ดแวร์ (hardware-based) บรรจุกุญแจเข้ารหัส (cryptographic key) และสามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย รวมถึงการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสต้องดำเนินการด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol)

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL3 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)
(2) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device) ร่วมกับ รหัสลับจดจำ (memorized secret)
(3) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ร่วมกับ อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(4) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(6) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) และรหัสลับจดจำ (memorized secret)

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(2) สิ่งที่ใช้ยืนยันตัวตนต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) สิ่งที่ใช้ยืนยันตัวตนต้องสามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

(4) เมื่อมีการใช้อุปกรณ์ เช่น โทรศัพท์เคลื่อนที่ ในการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือชีวมิติ) ต้องไม่ถือเป็นหนึ่งในปัจจัยของการยืนยันตัวตน เนื่องจาก IdP จะไม่สามารถทราบได้ว่าอุปกรณ์ถูกล็อคอยู่ หรือกระบวนการปลดล็อคเป็นไปตามข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตนชนิดนั้นหรือไม่

2.4 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL

ข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL แต่ละระดับสามารถสรุปได้ตามตารางที่ 1

ตารางที่ 1 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL

ข้อกำหนดของการยืนยันตัวตน	ระดับ AAL		
	AAL1	AAL2	AAL3
ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) memorized secret (2) out-of-band device (3) SF OTP device (4) SF crypto software (5) SF crypto device (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL2 และ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF OTP device (2) MF crypto software (3) memorized secret + out-of-band device (4) memorized secret + SF OTP device (5) memorized secret + SF crypto software (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF crypto device (2) SF crypto device + memorized secret (3) MF OTP device + SF crypto device (4) MF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software (5) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + MF crypto software (6) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software + memorized secret

ข้อกำหนดของการยืนยันตัวตน	ระดับ AAL		
	AAL1	AAL2	AAL3
การป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)	✓	✓	✓
การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)		✓	✓
การป้องกัน IdP ตัวปลอม (IdP impersonation resistance)			✓

หมายเหตุ: SF ย่อมาจาก “single-factor”, MF ย่อมาจาก “multi-factor” และ crypto ย่อมาจาก “cryptographic”

3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่ IdP สามารถออกหรือลงทะเบียนให้กับผู้ใช้บริการเพื่อใช้ในการยืนยันตัวตนตามระดับ AAL มีดังนี้

(1) รหัสลับจดจำ (memorized secret)
(2) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(3) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(4) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)
(5) ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(6) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(7) ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(8) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)

3.1 รหัสลับจดจำ (memorized secret)

รหัสลับจดจำ (memorized secret) หรือที่รู้จักกันโดยทั่วไปว่ารหัสผ่าน (password) หรือเลขรหัสส่วนตัว (personal identification number: PIN) เป็นข้อมูลลับที่ให้ผู้ใช้บริการจดจำ ทั้งนี้ รหัสลับจดจำต้องมีความซับซ้อนในระดับที่ยากแก่การคาดเดาโดยผู้ไม่ประสงค์ดี

รหัสลับจดจำเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณรู้ (something you know)

ข้อกำหนดทางเทคนิค

(1) เลขรหัสส่วนตัว (PIN) ที่ลงทะเบียนใช้กับอุปกรณ์ที่เฉพาะเจาะจงต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก ขณะที่รหัสผ่าน (password) ต้องมีความยาวอย่างน้อย 8 อักขระ

(2) IdP ควรกำหนดรายการรหัสลับจดจำที่ไม่ปลอดภัย (blacklist) เพื่อไม่ให้ผู้ใช้บริการเลือกรหัสลับจดจำจากรายการดังกล่าว เช่น รหัสผ่านที่เคยถูกโจมตีในอดีต คำที่พบในพจนานุกรม ตัวอักษรซ้ำหรือตัวอักษรเรียงลำดับ และคำที่คาดเดาได้โดยง่าย

(3) IdP ควรมีคำแนะนำสำหรับผู้ใช้บริการในการเลือกรหัสลับจดจำที่คาดเดาได้ยาก เช่น ตัวช่วยวัดระดับความปลอดภัยของรหัสผ่าน

(4) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)

อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) เป็นอุปกรณ์ที่สามารถสื่อสารกับ IdP อย่างปลอดภัยผ่านช่องทางสื่อสารรอง (secondary channel) ซึ่งแยกจากช่องทางสื่อสารหลัก (primary channel) ที่ใช้ในการยืนยันตัวตน

อุปกรณ์สื่อสารช่องทางอื่นเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

อุปกรณ์สื่อสารช่องทางอื่นสามารถทำงานด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

(1) ผู้ใช้บริการได้รับข้อมูลลับจากอุปกรณ์สื่อสารช่องทางอื่นผ่านช่องทางสื่อสารรอง และส่งข้อมูลลับนั้นไปยัง IdP โดยใช้ช่องทางสื่อสารหลัก ตัวอย่างเช่น ผู้ใช้บริการได้รับข้อมูลลับเป็นตัวเลข 6 หลักที่ส่งมายังโทรศัพท์เคลื่อนที่ทาง SMS และกรอกข้อมูลลับนั้นบนหน้าต่างยืนยันตัวตน

(2) ผู้ใช้บริการได้รับข้อมูลลับผ่านช่องทางสื่อสารหลัก และใช้อุปกรณ์สื่อสารช่องทางอื่นเพื่อส่งข้อมูลลับนั้นไปยัง IdP โดยใช้ช่องทางสื่อสารรอง ตัวอย่างเช่น ผู้ใช้บริการเห็นข้อมูลลับที่แสดงเป็น QR code บนหน้าต่างยืนยันตัวตน และใช้โทรศัพท์เคลื่อนที่สแกน QR code นั้นเพื่อให้เกิดการส่งข้อมูลลับไปยัง IdP

ข้อกำหนดทางเทคนิค

(1) อุปกรณ์สื่อสารช่องทางอื่นต้องสร้างช่องทางสื่อสารรองที่แยกจากช่องทางสื่อสารหลักเพื่อใช้รับหรือส่งข้อมูลลับกับ IdP ทั้งนี้ อุปกรณ์ปลายทางที่ใช้สื่อสารกับ IdP ผ่านช่องทางสื่อสารหลักและช่องทางสื่อสารรองอาจเป็นอุปกรณ์เดียวกัน โดยอุปกรณ์ดังกล่าวต้องไม่ทำให้ข้อมูลรั่วไหลจากช่องทางหนึ่งไปยังอีกช่องทางหนึ่งได้โดยไม่ได้รับอนุญาตจากผู้ใช้บริการ

(2) วิธีการที่ไม่สามารถแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์ที่เฉพาะเจาะจง เช่น วิธีการที่ใช้ voice-over-IP (VoIP) หรืออีเมล ต้องไม่ถือเป็นวิธีการยืนยันตัวตนด้วยอุปกรณ์สื่อสารช่องทางอื่น

(3) อุปกรณ์สื่อสารช่องทางอื่นต้องมีการยืนยันตัวตนของอุปกรณ์กับ IdP ด้วยวิธีการใดวิธีการหนึ่งดังนี้

(3.1) สร้างช่องทางที่มีความปลอดภัย (authenticated protected channel) กับ IdP โดยใช้กระบวนการเข้ารหัสลับ (cryptography) โดยกุญแจเข้ารหัสต้องถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(3.2) ยืนยันตัวตนของอุปกรณ์ผ่านโครงข่ายโทรศัพท์สาธารณะ โดยใช้ SIM card หรือวิธีการอื่นที่สามารถระบุอุปกรณ์ได้ วิธีการนี้ต้องถูกใช้เฉพาะกรณีที่ IdP ส่งข้อมูลลับมายังอุปกรณ์สื่อสารช่องทางอื่นผ่านโครงข่ายโทรศัพท์สาธารณะเท่านั้น

(4) การยืนยันตัวตนของผู้ใช้บริการต้องใช้วิธีการใดวิธีการหนึ่ง ดังนี้

(4.1) การส่งข้อมูลลับให้ IdP ทางช่องทางสื่อสารหลัก: IdP ต้องส่งข้อมูลลับที่สร้างขึ้นแบบสุ่มไปยังอุปกรณ์สื่อสารช่องทางอื่น จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับนั้นทางช่องทางสื่อสารหลัก

(4.2) การส่งข้อมูลลับให้ IdP ทางช่องทางสื่อสารรอง: IdP ต้องแสดงข้อมูลลับที่สร้างขึ้นแบบสุ่มให้กับผู้ใช้บริการทางช่องทางสื่อสารหลัก จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับนั้นจากอุปกรณ์สื่อสารช่องทางอื่นของผู้ใช้บริการทางช่องทางสื่อสารรอง

(5) ข้อมูลลับที่สร้างขึ้นแบบสุ่มต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(6) IdP ต้องกำหนดระยะเวลาของการตอบกลับข้อมูลลับจากผู้ใช้บริการให้ไม่เกิน 10 นาที หากเกินระยะเวลาที่กำหนด การยืนยันตัวตนดังกล่าวจะถือว่าเป็นการยืนยันตัวตนที่ไม่ถูกต้อง

(7) IdP ต้องยอมรับการตอบกลับข้อมูลลับจากผู้ใช้บริการเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(8) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.3 อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)

อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เป็นฮาร์ดแวร์เฉพาะ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) สำหรับใช้สร้าง OTP โดยผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกบนหน้าต่างยืนยันตัวตนของ IdP เพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์นั้นจริง

อุปกรณ์ OTP แบบปัจจัยเดียวบรรจุข้อมูล 2 ค่าสำหรับใช้สร้าง OTP คือ (1) กุญแจสมมาตร (symmetric key) ซึ่งจะมีค่าคงที่ตลอดอายุการใช้งานของอุปกรณ์ และ (2) nonce ซึ่งจะเปลี่ยนแปลงค่าทุกครั้งที่อุปกรณ์มีการใช้งานหรือเปลี่ยนแปลงค่าตามเวลาปัจจุบัน

อุปกรณ์ OTP แบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) OTP ต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(2) กรณีที่ค่า nonce ที่ใช้สร้าง OTP เปลี่ยนแปลงค่าตามเวลาปัจจุบัน ค่า nonce ต้องมีการเปลี่ยนแปลงอย่างน้อยทุก 2 นาที และ IdP ต้องยอมรับ OTP ที่สร้างจากค่า nonce ดังกล่าวเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.4 อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)

อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) เป็นฮาร์ดแวร์เฉพาะ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) ซึ่งจะสร้าง OTP หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ โดยผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกบนหน้าต่างยืนยันตัวตนของ IdP เพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์นั้นจริง

ในทำนองเดียวกันกับอุปกรณ์ OTP แบบปัจจัยเดียว อุปกรณ์ OTP แบบหลายปัจจัยบรรจุข้อมูล 2 ค่า สำหรับใช้สร้าง OTP คือ (1) กุญแจสมมาตร (symmetric key) ซึ่งจะมีค่าคงที่ตลอดอายุการใช้งานของอุปกรณ์ และ (2) nonce ซึ่งจะเปลี่ยนแปลงค่าทุกครั้งที่อุปกรณ์มีการใช้งานหรือเปลี่ยนแปลงค่าตามเวลาปัจจุบัน

อุปกรณ์ OTP แบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะสร้าง OTP หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยอุปกรณ์ OTP แบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) OTP ต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(6) กรณีที่ค่า nonce ที่ใช้สร้าง OTP เปลี่ยนแปลงค่าตามเวลาปัจจุบัน ค่า nonce ต้องมีการเปลี่ยนแปลงอย่างน้อยทุก 2 นาที และ IdP ต้องยอมรับ OTP ที่สร้างจากค่า nonce ดังกล่าวเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(7) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) เป็นกุญแจเข้ารหัส (cryptographic key) ที่เก็บไว้ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลรูปแบบอื่น

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียวทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น

ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยกุญแจเข้ารหัส และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมกุญแจเข้ารหัสนั้นจริง

ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) กุญแจเข้ารหัสต้องถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(2) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต โดยใช้การควบคุมการเข้าถึง (access control) ซึ่งอนุญาตให้เฉพาะซอฟต์แวร์ที่กำหนดเท่านั้นสามารถเข้าถึงกุญแจเข้ารหัสได้

(3) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)

อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device) เป็นอุปกรณ์ที่ใช้กุญแจเข้ารหัส (cryptographic key) ที่ฝังอยู่ภายในอุปกรณ์ เพื่อสร้างผลลัพธ์ที่ใช้ยืนยันตัวตนและส่งผลลัพธ์นั้นไปยังอุปกรณ์ปลายทาง (endpoint) ผ่านการเชื่อมต่อโดยตรง (เช่น ช่องทาง USB port ของคอมพิวเตอร์)

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์เข้ารหัสลับด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์เข้ารหัสลับนั้นจริง

ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับ คือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับทั้งหมดจะอยู่ภายใต้การควบคุมดูแลของ IdP หรือผู้ผลิตอุปกรณ์

อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) กุญแจเข้ารหัสต้องไม่สามารถนำออกจากอุปกรณ์เข้ารหัสลับได้

(2) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต

(3) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวต้องเป็นไปตามมาตรฐาน FIPS 140-2 Security Requirements for Cryptographic Modules ที่ระดับ 1 เป็นอย่างน้อย

(4) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software) เป็นกุญแจเข้ารหัส (cryptographic key) ที่เก็บไว้ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลรูปแบบอื่น ซึ่งจะสามารถใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยกุญแจเข้ารหัส และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมกุญแจเข้ารหัสนั้นจริง

ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1 และต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) กุญแจเข้ารหัสควรถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(6) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต โดยใช้การควบคุมการเข้าถึง (access control) ซึ่งอนุญาตให้เฉพาะซอฟต์แวร์ที่กำหนดเท่านั้นสามารถเข้าถึงกุญแจเข้ารหัสได้

(7) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)

อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device) เป็นอุปกรณ์ที่ใช้กุญแจเข้ารหัส (cryptographic key) ที่ฝังอยู่ภายในอุปกรณ์ เพื่อสร้างผลลัพธ์ที่ใช้ยืนยันตัวตนและส่งผลลัพธ์นั้นไปยังอุปกรณ์ปลายทาง (endpoint) ผ่านการเชื่อมต่อโดยตรง (เช่น ช่องทาง USB port ของคอมพิวเตอร์)

ทั้งนี้ กุญแจเข้ารหัสจะสามารถใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบหลายปัจจัยทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์เข้ารหัสลับด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์เข้ารหัสลับนั้นจริง

ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับ คือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับทั้งหมดจะอยู่ภายใต้การควบคุมดูแลของ IdP หรือผู้ผลิตอุปกรณ์

อุปกรณ์เข้ารหัสลับแบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1 และต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) กุญแจเข้ารหัสต้องไม่สามารถนำออกจากอุปกรณ์เข้ารหัสลับได้

(6) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต

(7) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัยต้องเป็นไปตามมาตรฐาน FIPS 140-2 Security Requirements for Cryptographic Modules ที่ระดับ 2 เป็นอย่างน้อย

(8) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

4.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี)

IdP ต้องให้คำแนะนำสำหรับผู้ใช้บริการเกี่ยวกับวิธีการป้องกันสิ่งที่ใช้ยืนยันตัวตนจากการสูญหายหรือถูกขโมย และต้องมีกลไกในการเพิกถอนหรือระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนในทันทีหลังจากได้รับแจ้งจากผู้ใช้บริการว่าสิ่งที่ใช้ยืนยันตัวตนสูญหายหรือถูกขโมย

4.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

กรณีที่สิ่งที่ใช้ยืนยันตัวตนชนิดนั้นกำหนดให้ IdP มีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด IdP ต้องมีกระบวนการป้องกันการโจมตีแบบเดาสุ่ม (online guessing attack) เช่น การเดาสุ่มรหัสลับจดจำ โดย IdP ต้องจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่องของผู้ใช้บริการแต่ละราย (เช่น ไม่เกิน 100 ครั้ง) หากเกินจำนวนที่กำหนด IdP ควรระงับการยืนยันตัวตนของผู้ใช้บริการดังกล่าว

เพื่อลดโอกาสจากการโจมตีที่จะทำให้ผู้ใช้บริการถูกระงับใช้งานเนื่องจากการยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด IdP อาจเลือกใช้วิธีการ ดังนี้

(1) กำหนดให้ผู้ใช้บริการต้องผ่านการทดสอบ CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) ก่อนจะยืนยันตัวตน

(2) กำหนดให้ผู้ใช้บริการรอหลังจากยืนยันตัวตนผิดพลาดเป็นระยะเวลาหนึ่ง และจะหน่วงเวลาเพิ่มขึ้นทุกครั้งที่ผู้ใช้บริการยืนยันตัวตนผิดพลาดต่อเนื่องกัน (เช่น เพิ่มขึ้นจาก 30 วินาทีไปจนถึง 1 ชั่วโมงตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด)

(3) ยอมรับเฉพาะการยืนยันตัวตนที่มาจาก IP address ซึ่งผู้ใช้บริการเคยยืนยันตัวตนสำเร็จมาก่อนเท่านั้น

เมื่อผู้ใช้บริการยืนยันตัวตนสำเร็จ IdP ควรมองข้ามการยืนยันตัวตนผิดพลาดครั้งก่อนหน้าของผู้ใช้บริการดังกล่าวที่มาจาก IP address เดียวกัน

4.3 การใช้งานชีวมิติ (ลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์เท่านั้น)

การใช้งานชีวมิติ (biometrics) เช่น ภาพใบหน้า ลายนิ้วมือ และลายม่านตา ในการยืนยันตัวตน ถือเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณเป็น (something you are) ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตนที่สามารถรองรับการใช้งานชีวมิติสำหรับการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ประกอบด้วย อุปกรณ์ OTP แบบหลายปัจจัย ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย และอุปกรณ์เข้ารหัสลับแบบหลายปัจจัย

การใช้งานชีวมิติในการยืนยันตัวตนยังมีข้อจำกัดเนื่องจากเหตุผล ดังนี้ [1]

(1) การใช้งานชีวมิติมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ซึ่งทำให้เกิดความไม่มั่นใจว่าผู้ที่กำลังยืนยันตัวตนคือผู้ใช้บริการตัวจริง และอาจถูกโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack)

(2) การเปรียบเทียบข้อมูลชีวมิติ (biometric comparision) เป็นการเปรียบเทียบบนพื้นฐานของความน่าจะเป็น (probabilistic) ขณะที่ปัจจัยของการยืนยันตัวตนประเภทอื่น ๆ เป็นการเปรียบเทียบอย่างชัดเจนว่าข้อมูลตรงกันหรือไม่ (deterministic)

(3) วิธีการเพิกถอนข้อมูลชีวมิติ ยังมีข้อจำกัดเกี่ยวกับความพร้อมใช้งานและมาตรฐานการทดสอบ

(4) ชีวมิติไม่ถือเป็นข้อมูลลับ เนื่องจากผู้ไม่ประสงค์ดีสามารถขโมยชีวมิติของบุคคลจากการค้นหาข้อมูลทางออนไลน์หรือการถ่ายภาพบุคคลด้วยกล้องโทรศัพท์ (กรณีที่เป็นใบหน้า) การล่อลวงให้บุคคลใช้มือสัมผัสวัตถุ (กรณีที่เป็นลายนิ้วมือ) หรือการถ่ายภาพความละเอียดสูง

(กรณีที่เป็นม่านตา)

ด้วยเหตุนี้ การใช้งานชีวมิติในการยืนยันตัวตนมีข้อกำหนด ดังนี้

(1) ชีวมิติต้องใช้เป็นปัจจัยร่วมของการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี) เท่านั้น เนื่องจากหากตรวจพบว่าผู้ใช้บริการเป็นตัวปลอมหรือสงสัยว่ามีการใช้งานในทางที่ผิด IdP สามารถเพิกถอนสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์นั้น ทดแทนการเพิกถอนข้อมูลชีวมิติ ซึ่งมีข้อจำกัด

(2) การเปรียบเทียบข้อมูลชีวมิติสามารถดำเนินการที่อุปกรณ์ของผู้ใช้บริการหรือที่ระบบงานของ IdP ทั้งนี้ หากการเปรียบเทียบข้อมูลชีวมิติดำเนินการที่ระบบงานของ IdP การรับส่งข้อมูลชีวมิติระหว่างอุปกรณ์รับข้อมูล (sensor) กับ IdP ต้องดำเนินการผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel)

(3) ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]

(4) IdP ต้องมีเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การตรวจจับการมีชีวิตของบุคคล (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

(5) IdP อาจจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติที่ผิดพลาดต่อเนื่อง (เช่น ไม่เกิน 10 ครั้ง) หากเกินจำนวนที่กำหนด IdP อาจเลือกใช้วิธีการ ดังนี้

(5.1) หน่วงเวลาเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และจะหน่วงเวลาเพิ่มขึ้นทุกครั้งที่ผู้ใช้บริการยืนยันตัวตนผิดพลาดต่อเนื่องกัน (เช่น เพิ่มขึ้นจาก 30 วินาทีไปจนถึง 1 ชั่วโมงตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด)

(5.2) ระงับการยืนยันตัวตนด้วยชีวมิติของผู้ใช้บริการ และเสนอให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนชนิดอื่น (ถ้ามี)

4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

กระบวนการยืนยันตัวตนสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำได้ หากการบันทึกและนำผลลัพธ์ที่ใช้ยืนยันตัวตนครั้งก่อนหน้ามาส่งซ้ำไม่สามารถทำให้การยืนยันตัวตนสำเร็จ ทั้งนี้ การป้องกันการโจมตีแบบส่งข้อมูลซ้ำเป็นการดำเนินการเพิ่มเติมจากการสื่อสารผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เนื่องจากผลลัพธ์ที่ใช้ยืนยันตัวตนอาจถูกขโมยโดยผู้ไม่ประสงค์ดีก่อนที่จะส่งเข้าสู่ช่องทางที่มีความปลอดภัย

สิ่งที่ใช้ยืนยันตัวตนที่ใช้ค่า nonce เพื่อพิสูจน์ความใหม่ (freshness) ของผลลัพธ์ที่ใช้ยืนยันตัวตน จะมีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ เนื่องจาก IdP สามารถตรวจพบได้ทันทีว่าผลลัพธ์ซึ่งไม่มีค่า nonce ที่เหมาะสม คือ ผลลัพธ์ที่ใช้ยืนยันตัวตนครั้งก่อนหน้าซึ่งถูกนำมาส่งซ้ำ

สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ ประกอบด้วย อุปกรณ์สื่อสารช่องทางอื่น อุปกรณ์ OTP ซอฟต์แวร์เข้ารหัสลับ และอุปกรณ์เข้ารหัสลับ ขณะที่รหัสลับจดจำไม่มีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ เนื่องจากรหัสลับจดจำถูกนำมาใช้ซ้ำสำหรับการยืนยันตัวตนแต่ละครั้ง

4.5 การป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

การโจมตีด้วยการปลอมตัวเป็น IdP หรือที่รู้จักกันว่า การโจมตีแบบฟิชชิง (phishing attack) เป็นการหลอกลวงให้ผู้ใช้บริการหลงเชื่อเข้ามายืนยันตัวตนบนเว็บไซต์ของ IdP ตัวปลอม

กระบวนการยืนยันตัวตนที่ป้องกัน IdP ตัวปลอม<u>ต้อง</u>สร้างช่องทางที่มีความปลอดภัย (authenticated protected channel) กับ IdP และ<u>ต้อง</u>เชื่อมโยงตัวระบุช่องทาง (channel identifier) ของช่องทางที่มีความปลอดภัยนั้นกับผลลัพธ์ที่ใช้ยืนยันตัวตน ด้วยการใช้กุญแจส่วนตัว (private key) ของผู้ใช้บริการลงลายมือชื่อดิจิทัลกับข้อมูลทั้งสองค่า จากนั้น IdP <u>ต้อง</u>ตรวจสอบลายมือชื่อดิจิทัลด้วยกุญแจสาธารณะ (public key) ที่สัมพันธ์กันเพื่อยืนยันตัวตนของผู้ใช้บริการ ดังนั้น IdP ตัวปลอมจะไม่สามารถนำลายมือชื่อดิจิทัลไปส่งต่อเพื่อยืนยันตัวตนกับ IdP ตัวจริงได้ เนื่องจากช่องทางดังกล่าวมีตัวระบุช่องทางที่แตกต่างกัน

สิ่งที่ใช้ยืนยันตัวตนที่ไม่มีคุณสมบัติในการป้องกัน IdP ตัวปลอม ประกอบด้วย รหัสลับจดจำ อุปกรณ์สื่อสารช่องทางอื่น และอุปกรณ์ OTP เนื่องจากเป็นสิ่งที่ใช้ยืนยันตัวตนที่ให้ผู้ใช้บริการกรอกผลลัพธ์ที่ใช้ยืนยันตัวตนกับ IdP ด้วยตนเอง ซึ่งการกรอกผลลัพธ์ที่ใช้ยืนยันตัวตนด้วยผู้ใช้บริการจะไม่มีการเชื่อมโยงผลลัพธ์นั้นกับเซสชัน (session) ที่กำลังยืนยันตัวตนอยู่ ทำให้ IdP ตัวปลอมสามารถนำผลลัพธ์ที่ได้มานั้นไปส่งต่อให้กับ IdP ตัวจริงและยืนยันตัวตนเป็นผู้ใช้บริการได้สำเร็จ

5. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

IdP ทำหน้าที่เชื่อมโยงอัตลักษณ์ของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตนและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนประกอบด้วยกระบวนการต่าง ๆ ซึ่งขึ้นอยู่กับชนิดของสิ่งที่ใช้ยืนยันตัวตน ดังนี้

(1) การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน
(2) การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน
(3) การหมดอายุและการออกใหม่
(4) การเพิกถอน

5.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (authenticator binding) คือ การสร้างความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับบัญชีของผู้ใช้บริการ เพื่อให้สิ่งที่ใช้ยืนยันตัวตนสามารถใช้ยืนยันบัญชีของผู้ใช้บริการนั้นได้ ทั้งนี้ IdP สามารถเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเข้ากับบัญชีของผู้ใช้บริการโดยการออกสิ่งที่ใช้ยืนยันตัวตนอันใหม่ให้กับผู้ใช้บริการหรือการลงทะเบียนสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว

ข้อกำหนดของการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

(1) IdP ต้องเก็บรักษาข้อมูลของสิ่งที่ใช้ยืนยันตัวตนทั้งหมดที่เกี่ยวข้องกับอัตลักษณ์ของผู้ใช้บริการตลอดอายุการใช้งานของดิจิทัลไอดี

(2) ข้อมูลที่เก็บรักษาต้องประกอบด้วยวันที่และเวลาที่เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเข้ากับบัญชีของผู้ใช้บริการ และควรประกอบด้วยข้อมูลเกี่ยวกับอุปกรณ์ที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น IP address หรือหมายเลขประจำอุปกรณ์

(3) IdP ต้องเก็บรักษาข้อมูลที่จำเป็นสำหรับการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) IdP ต้องตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนว่าเป็นไปตามข้อกำหนดที่ระดับ AAL แต่ละระดับ

(5) กรณีที่ IdP อนุญาตให้มีการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเพิ่มเติมหรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้วเข้ากับบัญชีของผู้ใช้บริการ IdP ต้องให้ผู้ใช้บริการยืนยันตัวตนที่ระดับ AAL ปัจจุบัน (หรือระดับ AAL ที่สูงกว่า) ก่อนที่จะเพิ่มสิ่งที่ใช้ยืนยันตัวตนอันใหม่

(6) เมื่อเพิ่มสิ่งที่ใช้ยืนยันตัวตนอันใหม่แล้ว IdP ควรส่งการแจ้งเตือนให้ผู้ใช้บริการผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนดังกล่าว (เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ)

5.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกขโมย หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่อาจถูกสวมรอยโดยผู้ไม่ประสงค์ดี ดังนั้น IdP ควรมีแนวปฏิบัติที่เหมาะสมในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย และเสียหาย รวมถึงการออกสิ่งที่ใช้ยืนยันตัวตนทดแทนอันเดิม (replacement)

ข้อกำหนดของการสูญหาย ถูกขโมย และเสียหาย

(1) IdP ควรระงับการใช้งาน เพิกถอน หรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน ในทันทีหลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย หรือเสียหาย

(2) IdP ควรให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ก่อนจะอนุญาตให้แจ้งการสูญหาย ถูกขโมย และเสียหายของสิ่งที่ใช้ยืนยันตัวตน เพื่อให้มั่นใจว่าการแจ้งเรื่องดังกล่าวมาจากผู้ใช้บริการตัวจริง

(3) สิ่งที่ใช้ยืนยันตัวตนสำรองต้องเป็นรหัสลับจดจำหรือสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์

ข้อกำหนดของการออกทดแทน

(1) หากสิ่งที่ใช้ยืนยันตัวตนทั้งหมดสูญหาย ถูกขโมย หรือเสียหาย IdP ต้องดำเนินการพิสูจน์ตัวตนของผู้ใช้บริการใหม่ด้วยวิธีการทั้งหมด อย่างไรก็ตาม IdP อาจเลือกใช้การพิสูจน์ตัวตนใหม่ด้วยวิธีการเพียงบางส่วน โดยใช้การตรวจสอบความเชื่อมโยงระหว่างผู้ใช้บริการกับหลักฐานแสดงตนที่ผู้ใช้บริการเคยให้ไว้กับ IdP ในการพิสูจน์ตัวตนครั้งก่อนหน้า

(2) เมื่อออกสิ่งที่ใช้ยืนยันตัวตนทดแทนอันเดิมแล้ว IdP ควรส่งการแจ้งเตือนให้ผู้ใช้บริการทราบ

5.3 การหมดอายุและการออกใหม่

IdP อาจออกสิ่งที่ใช้ยืนยันตัวตนที่กำหนดอายุการใช้งานให้กับผู้ใช้บริการ โดยสิ่งที่ใช้ยืนยันตัวตนที่หมดอายุจะไม่สามารถใช้ในการยืนยันตัวตนได้ ดังนั้น IdP ควรมีแนวปฏิบัติที่เหมาะสมในกรณีสิ่งที่ใช้ยืนยันตัวตนหมดอายุ รวมถึงการออกสิ่งที่ใช้ยืนยันตัวตนอันใหม่ (renewal)

ข้อกำหนดของการหมดอายุ

(1) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(2) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ IdP ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนผิดพลาดเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

ข้อกำหนดของการออกใหม่

(1) IdP ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอันใหม่ ในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนอันเดิมจะหมดอายุ

(2) เมื่อผู้ใช้บริการใช้สิ่งที่ใช้ยืนยันตัวตนอันใหม่ได้แล้ว IdP อาจเพิกถอนสิ่งที่ใช้ยืนยันตัวตนอันเดิมในทันที

5.4 การเพิกถอน

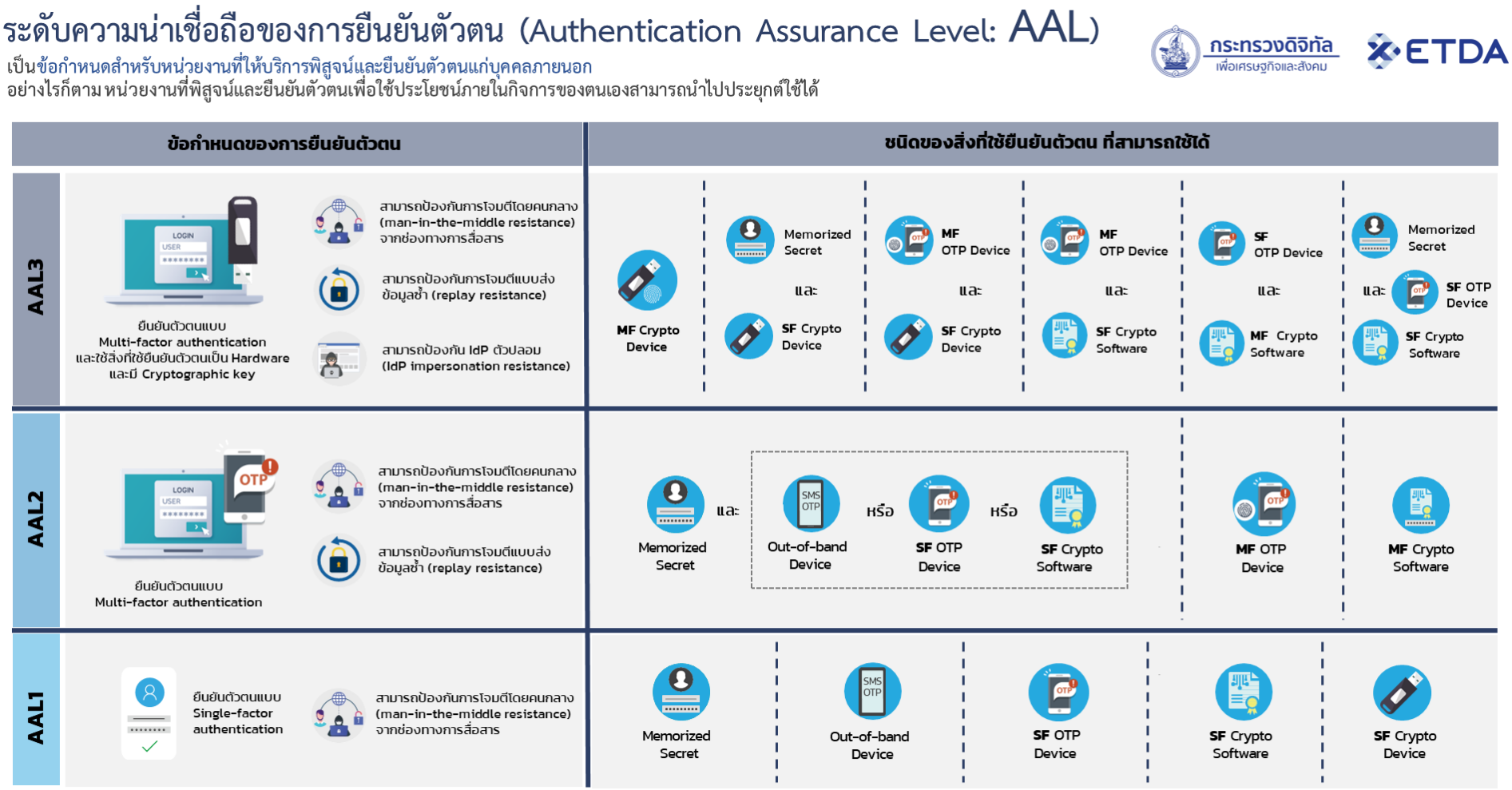
การเพิกถอน (revocation) หรือการยุติการใช้งาน (termination) ของสิ่งที่ใช้ยืนยันตัวตน คือ การลบความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับบัญชีของผู้ใช้บริการ

ข้อกำหนดของการเพิกถอน

(1) IdP ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนในทันที เมื่อทราบกรณี ดังนี้
   (1.1) เมื่อดิจิทัลไอดีหรือบัญชีของผู้ใช้บริการสิ้นสุดลง เช่น การเสียชีวิตของผู้ใช้บริการ หรือการตรวจพบว่าผู้ใช้บริการเป็นตัวปลอม
   (1.2) เมื่อผู้ใช้บริการร้องขอให้เพิกถอนสิ่งที่ใช้ยืนยันตัวตน
   (1.3) เมื่อ IdP พิจารณาว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่กำหนด

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)

อินโฟกราฟิกส์ (infographics) ของระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ซึ่งเป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐานเพื่อนำเสนอข้อมูลเป็นภาพที่สามารถเข้าใจได้ง่าย แสดงตามนี้



หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐาน

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

บรรณานุกรม

[1] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management", June 2017.

[2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4.7, June 2022.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019.

[4] National Institute of Standards and Technology, U.S. Department of Commerce, "FIPS 140-2, Security Requirements for Cryptographic Modules", May 2001.

[5] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.