ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 20-2561

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน

DIGITAL IDENTITY GUIDELINE FOR THAILAND – AUTHENTICATION

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน

ขมธอ. 20-2561

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 28 กันยายน พ.ศ. 2561

คณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานคณะทำงานร่วม

นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

รองประธานคณะทำงาน

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงาน

นายอภิวัฒน์ อินขัด	กรมการกงสุล
นายวีนัส สีสุข	กรมการปกครอง
นายสัญชัย เตชนิมิตวัช	
นายสุชาติ ธานีรัตน์	
นายเผด็จ เรือนจันทร์	กรมพัฒนาธุรกิจการค้า
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นางอารีย์พันธ์ เจริญสุข	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวนิชา สาทรกิจ	
นางวณิสรา สุขวัฒน์	
นายสุวิจักขณ์ ธรรมชัยพจน์	สำนักงานป้องกันและปราบปรามการฟอกเงิน
นายสรรเพชญ แสงเนตรสว่าง	
นายบัญชา มนูญกุลชัย	ธนาคารแห่งประเทศไทย
นายสุวิทย์ ตันรุ่งเรือง	
นางสาวสาริกา อภิวรรธกกุล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายศุภกิจ สัตยารัฐ	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายอนุชิต ชื่นชมภู	บริษัท ไปรษณีย์ไทย จำกัด
นายณัฐ เลิศฤทธิ์	
นางสาวนันทวัน วงศ์ขจรกิตติ	กองทุนเงินให้กู้ยืมเพื่อการศึกษา
นางวรวรรณ ธาราภูมิ	สมาคมบริษัทจัดการลงทุน
นางสาวยุภาวรรณ ศิริชัยนฤมิตร	ตลาดหลักทรัพย์แห่งประเทศไทย
นายฐานิสร์ ฟอลเล็ต	สมาคมการค้าผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย
นายฐากร ปิยะพันธ์	สมาคมธนาคารไทย
นางสาวสุญาณี ภูริปัญญวานิช	สมาคมธนาคารไทย
นายสุวิชชา สุดใจ	สมาคมธนาคารไทย
นายศีลวัต สันติวิสัฏฐ์	สมาคมธนาคารไทย
นางอภิพันธ์ เจริญอนุสรณ์	สมาคมธนาคารไทย
นางประราลี รัตน์ประสาทพร	สมาคมธนาคารไทย
นางภัทธีรา ดิลกรุ่งธีระภพ	สมาคมบริษัทหลักทรัพย์ไทย

นายพิเชษฐ สิทธิอำนวย	สมาคมบริษัทหลักทรัพย์ไทย
นายญาณศักดิ์ มโนมัยพิบูลย์	สมาคมบริษัทหลักทรัพย์ไทย
นายสุรศักดิ์ กลิ่นศรีสุข	สมาคมประกันชีวิตไทย
นายจรุง เชื้อจินดา	สมาคมประกันชีวิตไทย
นายพีระพัฒน์ เมฆสิงห์วี	สมาคมประกันวินาศภัยไทย
นายชูชัย วชิรบรรจง	สมาคมประกันวินาศภัยไทย

คณะทำงานและเลขานุการร่วม

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
นายธนฉัตร วิจารณ์ปรีชา	ธนาคารเกียรตินาคิน จำกัด (มหาชน)

ผู้ช่วยเลขานุการ

นายนครินทร์ ลิ้มรังษี	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการกำหนดและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) สำหรับการยืนยันตัวตนผู้ใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) เพื่อให้ IdP มีแนวทางในการยืนยันตัวตนผู้ใช้บริการตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) ที่เป็นมาตรฐานเดียวกัน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management, National Institute of Standards and Technology, US Department of Commerce, June 2017

และได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความครบถ้วนสมบูรณ์ และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน ฉบับนี้ จัดทำขึ้นตามความร่วมมือด้านการมาตรฐานระหว่าง หน่วยงานภาครัฐและเอกชนในคณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ร่วมกับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

การให้บริการของรัฐแก่ประชาชนและภาคธุรกิจหรือการให้บริการของภาคธุรกิจแก่ประชาชนในปัจจุบัน ประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนที่มีความซับซ้อน มีความสิ้นเปลืองทั้งเวลาและทรัพยากร เกิดภาระแก่ทั้งผู้แสดงตนและผู้มีหน้าที่ในการตรวจสอบความถูกต้องและยืนยันตัวตน รัฐบาลจึงได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID Platform) ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ (Ease of Doing Business) และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำมาตรฐานเกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (Digital Identity Guideline for Thailand) ขึ้น ประกอบด้วยมาตรฐานทั้งหมด 3 ฉบับ ดังนี้

(1) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ (Overview and Glossary)

เป็นเอกสารอธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้งานดิจิทัลไอดีสำหรับประเทศไทย การบริหารความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ

(2) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) ตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL)

(3) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (Authentication)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการกำหนดและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL)

สารบัญ

สารบัญตาราง

หน้า

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การยืนยันตัวตน

ตามที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การยืนยันตัวตน ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ นั้น เนื่องจากมีถ้อยคำที่สมควรแก้ไข จึงให้ยกเลิกประกาศดังกล่าว ทั้งนี้ เพื่อให้มีแนวทางในการกำหนดและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) สำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ทางดิจิทัลตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) ให้เป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน เลขที่ ขมธอ. ๒๐-๒๕๖๑ ปรากฏตามท้ายประกาศฉบับนี้ ทั้งนี้ ตั้งแต่วันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กุมภาพันธ์ พ.ศ. ๒๕๖๒

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการยืนยันตัวตนผู้ใช้บริการ (authentication) เพื่อให้ IdP มีแนวทางในการยืนยันตัวตนและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) ที่เป็นมาตรฐานเดียวกัน

ข้อเสนอแนะมาตรฐานฉบับนี้ อ้างอิงข้อกำหนดเกี่ยวกับการยืนยันตัวตนตามมาตรฐาน NIST Special Publication 800- 63B – Digital Identity Guidelines – Authentication and Lifecycle Management ของหน่วยงาน National Institute of Standards and Technology (NIST) เป็นหลัก และนำข้อกำหนดดังกล่าวมาประยุกต์เป็นแนวทางการใช้งานของประเทศไทยที่สอดคล้องกับมาตรฐานสากล

ในข้อเสนอแนะมาตรฐานฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) มีดังต่อไปนี้ [1]

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

[1] อ้างอิงข้อมูลจาก ISO/IEC Directives Part 2: Principles and rules for the structure and drafting of ISO and IEC documents

2. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL) ของผู้ใช้บริการแบ่งออกเป็น 3 ระดับ ดังนี้

2.1 ระดับ AAL1

ระดับ AAL1 มีความน่าเชื่อถือปานกลางว่า ผู้ใช้บริการคือบุคคลที่ได้ลงทะเบียนและพิสูจน์ตัวตนกับ IdP โดยระดับ AAL1 กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย หรือหากต้องการความมั่นคงปลอดภัยที่สูงขึ้น สามารถใช้สิ่งที่ใช้ยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ได้

2.1.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน

การยืนยันตัวตนที่ระดับ AAL1 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) รหัสลับจดจำ (memorized secret)
(2) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band devices)
(3) อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device)
(4) ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device)
(6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่กำหนดให้ใช้งานได้ในระดับ AAL2 และ AAL3

2.1.2 ข้อกำหนดทั่วไป

(1) ช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและ IdP ต้องเป็นช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของข้อมูล (confidentiality) และป้องกันการโจมตีโดยคนกลาง (man-in-the-middle attack)

(2) หลังจากที่ผู้ใช้บริการได้ยืนยันตัวตนจะได้รับ session ในการเข้าใช้บริการ ซึ่งผู้ใช้บริการควรยืนยันตัวตนซ้ำ (reauthentication) เพื่อเข้าใช้บริการอย่างน้อย 1 ครั้งทุกรอบ 30 วัน

2.2 ระดับ AAL2

ระดับ AAL2 มีความน่าเชื่อถือสูงว่า ผู้ใช้บริการคือบุคคลที่ได้ลงทะเบียนและพิสูจน์ตัวตนกับ IdP โดยระดับ AAL 2 กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนด้วยการใช้ปัจจัยของการยืนยันตัวตน (authentication factor) 2 ปัจจัยที่แตกต่างกัน ซึ่งอาจเป็น (1) สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย (multi-factor authenticator) เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านแบบใช้ครั้งเดียวหลังจากตรวจสอบลายนิ้วมือของผู้ใช้บริการ หรือ (2) สิ่งที่ใช้ยืนยันตัวตนปัจจัยเดียว (single-factor authenticator) อย่างน้อย 2 สิ่งที่เป็นปัจจัยต่างกัน เช่น การใช้รหัสผ่านควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์มือถือ

2.2.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน

การยืนยันตัวตนที่ระดับ AAL2 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device)
(2) ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software)
(3) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่กำหนดให้ใช้งานได้ในระดับ AAL3

กรณีที่ใช้สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว 2 สิ่งที่เป็นปัจจัยต่างกัน ต้องใช้รหัสลับจดจำ (memorized secret) ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นปัจจัยประเภทสิ่งที่ผู้ใช้บริการมี (something you have) จากตัวเลือกต่อไปนี้

(1) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(2) อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device)
(3) ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software)
(4) อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device)

ข้อสังเกต: ชีวมิติ (biometric) ไม่ถือเป็นสิ่งที่ใช้ยืนยันตัวตน (authenticator) แต่เป็นเพียงปัจจัยของการยืนยันตัวตน (authentication factor) เท่านั้น จึงไม่สามารถใช้งานชีวมิติเพียงลำพังได้ เมื่อต้องการใช้ชีวมิติในการยืนยันตัวตน ต้องใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย (multi-factor authenticator) เช่น อุปกรณ์ OTP หลายปัจจัยที่สร้างรหัสผ่านแบบใช้ครั้งเดียวเมื่อตรวจสอบพบว่าลายนิ้วมือผู้ใช้บริการถูกต้อง

2.2.2 ข้อกำหนดทั่วไป

(1) ช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและ IdP ต้องเป็นช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของข้อมูล (confidentiality) และป้องกันการโจมตีโดยคนกลาง (man-in-the-middle attack)

(2) หนึ่งในสิ่งที่ใช้ยืนยันตัวตนที่ใช้ต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay attack)

(3) เมื่ออุปกรณ์ส่วนตัวของผู้ใช้บริการ เช่น โทรศัพท์มือถือ ถูกใช้เพื่อการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือ เทคโนโลยีชีวมิติ) ต้องไม่ถูกนับเป็นปัจจัยของการยืนยันตัวตน เนื่องจาก IdP ไม่สามารถควบคุมได้ว่าการล็อคหรือปลดล็อคอุปกรณ์ดังกล่าว เป็นไปตามหลักเกณฑ์ที่ IdP กำหนด

(4) การใช้งานชีวมิติในการยืนยันตัวตน ต้องดำเนินการตามข้อกำหนดในหัวข้อ 3.2.3

(5) หลังจากที่ผู้ใช้บริการยืนยันตัวตนจะได้รับ session ในการเข้าใช้บริการ ซึ่งผู้ใช้บริการต้องยืนยันตัวตนซ้ำ (reauthentication) เพื่อเข้าใช้บริการอย่างน้อย 1 ครั้งทุกรอบ 12 ชั่วโมง และต้องยืนยันตัวตนซ้ำกรณีไม่ทำกิจกรรมใด ๆ (inactivity) เป็นระยะเวลามากกว่า 30 นาที

2.3 ระดับ AAL3

ระดับ AAL 3 มีความน่าเชื่อถือสูงมากว่า ผู้ใช้บริการคือบุคคลที่ได้ลงทะเบียนและพิสูจน์ตัวตนกับ IdP โดยระดับ AAL3 กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนด้วยการพิสูจน์ว่าตนครอบครองกุญแจ (key) ผ่านเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตน (authentication factor) ตั้งแต่ 2 ปัจจัยขึ้นไป

2.3.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน

การยืนยันตัวตนที่ระดับ AAL3 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic device)
(2) อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) ร่วมกับ รหัสลับจดจำ (memorized secret)
(3) อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device) ร่วมกับ อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device)
(4) อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device) ร่วมกับ ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) ร่วมกับ ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software)
(6) อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) ร่วมกับ ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) และรหัสลับจดจำ (memorized secret)

2.3.2 ข้อกำหนดทั่วไป

(1) ช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและ IdP ต้องเป็นช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของข้อมูล (confidentiality) ป้องกันการโจมตีโดยคนกลาง (man-in-the-middle attack)

(2) สิ่งที่ใช้ยืนยันตัวตนต้องสามารถป้องกัน IdP ปลอม (IdP impersonation attack) และป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay attack)

(3) เมื่ออุปกรณ์ส่วนตัวของผู้ใช้บริการ เช่น โทรศัพท์มือถือ ถูกใช้เพื่อการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือ เทคโนโลยีชีวมิติ) ต้องไม่ถูกนับเป็นปัจจัยของการยืนยันตัวตน เนื่องจาก IdP ไม่สามารถควบคุมได้ว่าการล็อค หรือปลดล็อคอุปกรณ์ดังกล่าว เป็นไปตามหลักเกณฑ์ที่ IdP กำหนด

(4) การใช้งานชีวมิติในการยืนยันตัวตน ต้องดำเนินการตามข้อกำหนดในหัวข้อ 3.2.3

(5) หลังจากที่ผู้ใช้บริการได้ยืนยันตัวตนจะได้รับ session ในการเข้าใช้บริการ ซึ่งผู้ใช้บริการต้องยืนยันตัวตนซ้ำ (reauthentication) เพื่อเข้าใช้บริการอย่างน้อย 1 ครั้งทุกรอบ 12 ชั่วโมง และต้องยืนยันตัวตนซ้ำ กรณีไม่ทำกิจกรรมใด ๆ (inactivity) เป็นระยะเวลามากกว่า 15 นาที

3. ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน

3.1 ชนิดของสิ่งที่ใช้ยืนยันตัวตน

3.1.1 รหัสลับจดจำ (memorized secret)

รหัสลับจดจำ (memorized secret) เป็นข้อมูลลับที่ผู้ใช้บริการจดจำและใช้ยืนยันตัวตน โดยทั่วไปมักอยู่ในรูปแบบรหัสผ่าน (password) หรือเลขรหัสส่วนตัว (PIN) ทั้งนี้ รหัสลับจดจำที่ใช้ต้องมีความซับซ้อนในระดับที่ยากแก่การคาดเดาโดยผู้ไม่หวังดี

รหัสลับจดจำจัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการรู้ (something you know)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) รหัสลับจดจำต้องมีความยาว ดังนี้

(1.1) ความยาวอย่างน้อย 8 อักขระ กรณีที่ผู้ใช้บริการเป็นผู้กำหนดรหัสลับจดจำเอง

(1.2) ความยาวอย่างน้อย 6 อักขระ กรณีที่ IdP เป็นผู้สร้างรหัสลับจดจำแบบสุ่มให้กับผู้ใช้บริการ

(2) รหัสลับจดจำต้องไม่อยู่ในรายชื่อรหัสลับที่ไม่ปลอดภัย (blacklist) โดยรายชื่อรหัสลับที่ไม่ปลอดภัยอาจประกอบด้วย รหัสผ่านที่เคยถูกโจมตีในอดีต คำศัพท์ที่บรรจุในพจนานุกรม (dictionary word) และตัวอักษรซ้ำหรือตัวอักษรเรียงกัน (เช่น aaaaaaaa หรือ 1234abcd)

(3) IdP ควรจัดให้มีตัวช่วยตรวจสอบระดับความปลอดภัยของรหัสลับจดจำ เพื่อสนับสนุนให้ผู้ใช้บริการตั้งรหัสลับจดจำที่ปลอดภัย

(4) IdP ต้องจัดให้มีกลไกจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

3.1.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)

อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) เป็นอุปกรณ์ที่สามารถสื่อสารข้อมูลกับ IdP อย่างปลอดภัยผ่านช่องทางสื่อสารที่แยกจากช่องทางหลักซึ่งใช้ยืนยันตัวตน

อุปกรณ์สื่อสารช่องทางอื่นจัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have)

ตัวอย่างการทำงานของอุปกรณ์สื่อสารช่องทางอื่น เช่น

(1) IdP ส่งข้อมูลลับเป็นตัวเลข 6 หลักให้กับผู้ใช้บริการผ่านอุปกรณ์สื่อสารช่องทางอื่น เพื่อให้ผู้ใช้บริการส่งกลับข้อมูลลับดังกล่าวผ่านช่องทางสื่อสารหลักเพื่อยืนยันตัวตน

(2) IdP ส่งข้อมูลลับซึ่งเป็นตัวเลข 6 หลักให้กับผู้ใช้บริการผ่านช่องทางสื่อสารหลัก เพื่อให้ผู้ใช้บริการส่งกลับข้อมูลลับดังกล่าวผ่านอุปกรณ์สื่อสารช่องทางอื่นเพื่อยืนยันตัวตน

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) อุปกรณ์สื่อสารช่องทางอื่นต้องสร้างช่องทางสำหรับรับหรือส่งข้อมูลลับกับ IdP (ช่องทางอื่น) ซึ่งเป็นช่องทางที่แยกจากช่องทางที่ใช้ยืนยันตัวตน (ช่องทางหลัก) โดยข้อมูลต้องไม่สามารถรั่วไหลระหว่างช่องทางหลักกับช่องทางอื่นโดยไม่ได้รับความยินยอมจากผู้ใช้บริการ ทั้งนี้ อุปกรณ์ปลายทางที่สื่อสารกับ IdP ผ่านช่องทางหลักและช่องทางอื่นอาจเป็นอุปกรณ์เดียวกันได้

(2) วิธีการที่ไม่สามารถพิสูจน์ได้ว่าผู้ใช้บริการครอบครองวัตถุหรืออุปกรณ์ที่ใช้ยืนยันตัวตน (เช่น ส่งข้อมูลลับผ่าน voice-over-IP (VoIP) หรืออีเมล) ต้องไม่ถูกใช้เป็นวิธีการยืนยันตัวตนด้วยอุปกรณ์สื่อสารช่องทางอื่น

(3) อุปกรณ์สื่อสารช่องทางอื่นต้องยืนยันตัวตนกับ IdP ด้วยวิธีการใดวิธีการหนึ่ง ดังต่อไปนี้

(3.1) สร้างช่องทางที่มีความปลอดภัย (authenticated protected channel) กับ IdP ด้วยวิธีการเข้ารหัสลับ (cryptography) โดยกุญแจเข้ารหัสลับต้องถูกเก็บไว้ในพื้นที่ปลอดภัย (secure storage) บนอุปกรณ์ (เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element)

(3.2) ยืนยันตัวตนผ่านโครงข่ายโทรศัพท์สาธารณะ (PSTN) โดยใช้ SIM card หรือเทียบเท่า ซึ่งต้องใช้วิธีนี้เมื่อข้อมูลลับถูกส่งจาก IdP ไปยังอุปกรณ์สื่อสารช่องทางอื่นผ่านโครงข่ายโทรศัพท์สาธารณะ (SMS หรือเสียง) เท่านั้น

(4) การยืนยันตัวตนของผู้ใช้บริการต้องใช้วิธีการใดวิธีการหนึ่งดังนี้

(4.1) การส่งข้อมูลลับทางช่องทางหลัก: IdP ต้องส่งข้อมูลลับที่สร้างขึ้นแบบสุ่มไปยังอุปกรณ์สื่อสารช่องทางอื่น จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับดังกล่าวทางช่องทางหลัก

(4.2) การส่งข้อมูลลับทางช่องทางอื่น: IdP ต้องส่งข้อมูลลับที่สร้างขึ้นแบบสุ่มไปยังผู้ใช้บริการทางช่องทางหลัก จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับดังกล่าวจากอุปกรณ์สื่อสารช่องทางอื่น

(4.3) การพิสูจน์ข้อมูลลับโดยผู้ใช้บริการ: IdP ต้องส่งข้อมูลลับที่สร้างขึ้นแบบสุ่มไปยังผู้ใช้บริการทางช่องทางหลัก และส่งข้อมูลเดียวกันไปยังอุปกรณ์สื่อสารช่องทางอื่น จากนั้น IdP ต้องรอให้ผู้บริการยืนยันการเข้าใช้งานทางช่องทางอื่น

(5) ข้อมูลลับที่ใช้ตอบกลับโดยผู้ใช้บริการต้องมีความยาวอย่างน้อย 6 อักขระ และอาจเป็นตัวเลขทั้งหมด

(6) IdP ต้องกำหนดช่วงเวลาตอบกลับข้อมูลลับจากผู้ใช้บริการให้ไม่เกิน 10 นาที ข้อมูลลับที่ได้หลังจากช่วงเวลาดังกล่าวต้องถือว่าเป็นข้อมูลลับที่ไม่ถูกต้อง

(7) IdP ต้องยอมรับข้อมูลลับที่ตอบกลับจากผู้ใช้บริการเพียงครั้งเดียวในช่วงเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay attack)

(8) IdP ต้องจัดให้มีกลไกสำหรับจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

3.1.3 อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device)

อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device) เป็นอุปกรณ์ฮาร์ดแวร์ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) สำหรับสร้างรหัสผ่านแบบใช้ครั้งเดียว (OTP) อุปกรณ์ OTP ปัจจัยเดียวบรรจุข้อมูล 2 ค่าสำหรับสร้างรหัสผ่าน คือค่าของกุญแจสมมาตร (symmetric key) ที่จะไม่เปลี่ยนแปลงตลอดอายุการใช้งาน และค่า nonce จะเปลี่ยนแปลงตามจำนวนครั้งที่อุปกรณ์ OTP ถูกใช้งาน หรือเปลี่ยนแปลงตามเวลาปัจจุบัน ผู้ใช้บริการยืนยันตัวตนโดยนำ OTP ที่ปรากฏบนอุปกรณ์ไปแสดงต่อ IdP เพื่อยืนยันว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตน

อุปกรณ์ OTP ปัจจัยเดียวจัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

ค่าของ OTP ต้องมีความยาวอย่างน้อย 6 อักขระ และอาจเป็นตัวเลขทั้งหมด

(1) กรณีที่ค่า nonce ที่ใช้สร้าง OTP อยู่บนพื้นฐานของเวลา (time-based) ค่า nonce ต้องถูกเปลี่ยนอย่างน้อยทุก 2 นาที และ OTP ที่สร้างขึ้นต้องสามารถใช้งานได้เพียงครั้งเดียว

(2) ช่องทางที่ IdP ใช้รับ OTP จากผู้ใช้บริการต้องเข้ารหัสลับ (encryption) เพื่อป้องกันการดักข้อมูล (eavesdropping) และการโจมตีโดยคนกลาง (man-in-the-middle attack)

(3) IdP ต้องจัดให้มีกลไกสำหรับจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด ตามข้อกำหนดในหัวข้อ 3.2.2

3.1.4 อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device)

อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP devices) เป็นอุปกรณ์ฮาร์ดแวร์ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) ซึ่งจะสร้าง OTP เมื่อผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่ 2 เช่น รหัสผ่าน (password) หรือ ลายนิ้วมือ (fingerprint)

อุปกรณ์ OTP หลายปัจจัย จัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have) โดยจะสร้าง OTP เมื่อผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่ 2 ซึ่งเป็นปัจจัยประเภท สิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) ปัจจัยของการยืนยันตัวตนที่ 2 ต้องเป็นปัจจัยประเภทสิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

(2) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นรหัสลับจดจำ รหัสลับจดจำต้องเป็นตัวเลขสุ่มอย่างน้อย 6 หลัก หรือเป็นไปตามข้อกำหนดในหัวข้อ 3.1.1

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามข้อกำหนดในหัวข้อ 3.2.3

(4) ค่าของ OTP ต้องมีความยาวอย่างน้อย 6 อักขระ และอาจเป็นตัวเลขทั้งหมด

(5) การยืนยันตัวตนแต่ละครั้ง ต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(6) กรณีที่ค่า nonce ที่ใช้สร้าง OTP อยู่บนพื้นฐานของเวลา (time-based) ค่า nonce ต้องถูกเปลี่ยนอย่างน้อยทุก 2 นาที และ OTP ที่สร้างขึ้นต้องสามารถใช้งานได้เพียงครั้งเดียว

(7) ช่องทางที่ IdP ใช้รับ OTP จากผู้ใช้บริการต้องเข้ารหัสลับ (encryption) เพื่อป้องกันการดักข้อมูล (eavesdropping) และการโจมตีโดยคนกลาง (man-in-the-middle attack)

(8) IdP ต้องจัดให้มีกลไกสำหรับจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

3.1.5 ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) คือสิ่งที่ใช้ยืนยันตัวตนที่เป็นกุญแจรหัสลับ (cryptographic key) ซึ่งเก็บบนฮาร์ดดิสก์ หรืออุปกรณ์อิเล็กทรอนิกส์

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับปัจจัยเดียวทำได้ผ่านทางเกณฑ์วิธีรหัสลับ (cryptographic protocol) เช่น ให้ผู้ใช้บริการลงลายมือชื่อบนข้อความที่ถูกส่งมาจาก IdP ด้วยซอฟต์แวร์เข้ารหัสลับ แล้วส่งข้อความที่ลงลายมือชื่อแล้วกลับคืนให้ IdP เพื่อตรวจสอบลายมือชื่อ

ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software) จัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) กุญแจเข้ารหัสลับต้องถูกเก็บไว้ในพื้นที่ปลอดภัย (secure storage) บนอุปกรณ์ (เช่น keychain storage, trusted platform module (TPM) หรือ trusted execution environment (TEE))

(2) กุญแจเข้ารหัสลับต้องถูกป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยควบคุม (access control) ให้สามารถเข้าถึงได้โดยซอฟต์แวร์ที่กำหนดเท่านั้น

(3) กุญแจเข้ารหัสลับและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Revision 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” และค่า challenge nonce ต้องมีความยาวอย่างน้อย 64 บิต

3.1.6 อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device)

อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device) เป็นอุปกรณ์ที่ใช้กุญแจเข้ารหัสลับ (cryptographic key) ที่บรรจุอยู่ในอุปกรณ์เพื่อสร้างผลลัพธ์ที่ใช้ยืนยันตัวตนผ่านการเชื่อมต่อกับอุปกรณ์ปลายทาง (endpoint) อุปกรณ์เข้ารหัสลับปัจจัยเดียวสามารถใช้กุญแจเข้ารหัสลับที่ฝังอยู่ภายในอุปกรณ์ (embedded cryptographic key) โดยไม่ใช้ปัจจัยของการยืนยันตัวตนอื่น ๆ เพิ่มเติม

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับปัจจัยเดียวทำได้ผ่านทางเกณฑ์วิธีรหัสลับ (cryptographic protocol) เช่น ให้ผู้ใช้บริการลงลายมือชื่อบนข้อความที่ถูกส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ แล้วส่งข้อความที่ลงลายมือชื่อแล้วกลับคืนให้ IdP เพื่อตรวจสอบลายมือชื่อ

แม้ว่าอุปกรณ์เข้ารหัสลับจะบรรจุซอฟต์แวร์อยู่ภายใน ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับคือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับ (embedded software) ต้องถูกควบคุมโดย IdP หรือผู้ออกอุปกรณ์ (issuer)

อุปกรณ์เข้ารหัสลับปัจจัยเดียว จัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) กุญแจเข้ารหัสลับต้องไม่สามารถถูกนำออกจากอุปกรณ์เข้ารหัสลับได้

(2) กุญแจเข้ารหัสลับต้องถูกป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาต

(3) ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับ (embedded software) ต้องถูกควบคุมโดย IdP หรือผู้ออกอุปกรณ์ (issuer)

(4) อุปกรณ์เข้ารหัสลับปัจจัยเดียวต้องเป็นไปตามมาตรฐาน FIPS 140-2 ระดับ 1 หรือระดับสูงกว่า

(5) กุญแจเข้ารหัสลับและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Revision 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” และค่า challenge nonce ต้องมีความยาวอย่างน้อย 64 บิต

3.1.7 ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software) คือสิ่งที่ใช้ยืนยันตัวตนที่เป็นกุญแจรหัสลับ (cryptographic key) ซึ่งเก็บบนฮาร์ดดิสก์ หรืออุปกรณ์อิเล็กทรอนิกส์ ซึ่งจะสามารถใช้งานได้เมื่อผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่ 2 เช่น รหัสผ่าน (password) หรือ ลายนิ้วมือ (fingerprint)

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับหลายปัจจัยทำได้ผ่านทางเกณฑ์วิธีรหัสลับ (cryptographic protocol) เช่น ให้ผู้ใช้บริการลงลายมือชื่อบนข้อความที่ถูกส่งมาจาก IdP ด้วยซอฟต์แวร์เข้ารหัสลับ แล้วส่งข้อความที่ลงลายมือชื่อแล้วกลับคืนให้ IdP เพื่อตรวจสอบลายมือชื่อ

ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software) จัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have) โดยจะใช้งานได้เมื่อใช้ปัจจัยของการยืนยันตัวตนที่ 2 ซึ่งเป็นปัจจัยประเภท สิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) ปัจจัยของการยืนยันตัวตนที่ 2 ต้องเป็นปัจจัยประเภทสิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

(2) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นรหัสลับจดจำ รหัสลับจดจำต้องเป็นตัวเลขสุ่มอย่างน้อย 6 หลักหรือเป็นไปตามข้อกำหนดในหัวข้อ 3.1.1 และต้องถูกจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามข้อกำหนดในหัวข้อ 3.2.3

(4) การยืนยันตัวตนแต่ละครั้ง ต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(5) กุญแจเข้ารหัสลับควรถูกเก็บไว้ในพื้นที่ปลอดภัย (secure storage) บนอุปกรณ์ (เช่น keychain storage, trusted platform module (TPM) หรือ trusted execution environment (TEE))

(6) กุญแจเข้ารหัสลับต้องถูกป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาต โดยควบคุม (access control) ให้สามารถเข้าถึงได้โดยซอฟต์แวร์ที่กำหนดเท่านั้น

(7) กุญแจเข้ารหัสลับและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Revision 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” และค่า challenge nonce ต้องมีความยาวอย่างน้อย 64 บิต

3.1.8 อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic devices)

อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic devices) เป็นอุปกรณ์ที่ใช้เข้ารหัสลับด้วยกุญแจเข้ารหัสลับ (cryptographic key) ที่อยู่ในตัวอุปกรณ์ ซึ่งจะสามารถใช้งานได้เมื่อผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่ 2

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับหลายปัจจัยทำได้ผ่านทางเกณฑ์วิธีรหัสลับ (cryptographic protocol) เช่น ให้ผู้ใช้บริการลงลายมือชื่อบนข้อความที่ถูกส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ แล้วส่งข้อความที่ลงลายมือชื่อแล้วกลับคืนให้ IdP เพื่อตรวจสอบลายมือชื่อ

แม้ว่าอุปกรณ์เข้ารหัสลับจะบรรจุซอฟต์แวร์อยู่ภายใน ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับคือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับ (embedded software) ต้องถูกควบคุมโดย IdP

อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic device) จัดเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have) โดยจะใช้งานได้เมื่อใช้ปัจจัยของการยืนยันตัวตนที่ 2 ซึ่งเป็นปัจจัยประเภท สิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

ข้อกำหนดเกี่ยวกับคุณสมบัติ

(1) ปัจจัยของการยืนยันตัวตนที่ 2 ต้องเป็นปัจจัยประเภทสิ่งที่ผู้ใช้บริการรู้ (something you know) หรือ สิ่งที่ผู้ใช้บริการเป็น (something you are)

(2) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นรหัสลับจดจำ รหัสลับจดจำต้องเป็นตัวเลขสุ่มอย่างน้อย 6 หลักหรือเป็นไปตามข้อกำหนดในหัวข้อ 3.1.1 และต้องถูกจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่ 2 เป็นชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามข้อกำหนดในหัวข้อ 3.2.3

(4) การยืนยันตัวตนแต่ละครั้ง ต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(6) กุญแจเข้ารหัสลับต้องไม่สามารถถูกนำออกจากอุปกรณ์เข้ารหัสลับได้

(7) กุญแจเข้ารหัสลับต้องถูกป้องกันจากการเข้าถึงที่ไม่ได้รับอนุญาต

(8) ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับ (embedded software) ต้องถูกควบคุมโดย IdP หรือผู้ออกอุปกรณ์ (issuer)

(9) อุปกรณ์เข้ารหัสลับหลายปัจจัย ต้องเป็นไปตามมาตรฐาน FIPS 140-2 ระดับ 2 หรือระดับสูงกว่า

(10) กุญแจเข้ารหัสลับและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Revision 1 “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths” และค่า challenge nonce ต้องมีความยาวอย่างน้อย 64 บิต

3.2 ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

3.2.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นวัตถุ

IdP ต้องจัดให้มีคู่มืออธิบายวิธีป้องกันสิ่งที่ใช้ยืนยันตัวตนสูญหายหรือถูกขโมย และต้องมีกลไกเพิกถอนหรือระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนเมื่อได้รับแจ้งจากผู้ใช้บริการว่าสิ่งที่ใช้ยืนยันตัวตนสูญหายหรือถูกขโมย

3.2.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

IdP ต้องมีกระบวนการป้องกันการโจมตีแบบเดาสุ่ม (online guessing attack) เช่น การพยายามเข้าสู่ระบบด้วยการสุ่มรหัสผ่าน โดย IdP ต้องจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่องของผู้ใช้บริการแต่ละรายให้ไม่เกิน 100 ครั้ง หากครบจำนวนที่กำหนด IdP ต้องระงับการยืนยันตัวตนของผู้ใช้บริการรายดังกล่าว

ทั้งนี้ เพื่อป้องกันการโจมตีที่ทำให้ผู้ใช้บริการถูกระงับใช้บริการเนื่องจากยืนยันตัวตนผิดพลาดครบจำนวนที่กำหนด IdP อาจเลือกใช้วิธีการป้องกันดังนี้

(1) ให้ผู้ใช้บริการผ่านแบบทดสอบ CAPTCHA ก่อนยืนยันตัวตนแต่ละครั้ง
(2) หน่วงเวลาของการยืนยันตัวตนเพิ่มขึ้นทุกครั้งที่ผู้ใช้บริการยืนยันตัวตนผิดพลาด
(3) ยอมรับการยืนยันตัวตนจาก IP address ที่ผู้ใช้บริการเคยยืนยันตัวตนสำเร็จมาก่อนเท่านั้น

3.2.3 การใช้งานชีวมิติ (biometric)

การใช้งานชีวมิติ (biometric) เช่น ลายนิ้วมือ (fingerprint) ม่านตา (iris) และใบหน้า (facial characteristics) สำหรับการยืนยันตัวตน ถือเป็นปัจจัยของการยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการเป็น (something you are)

ข้อเสนอแนะมาตรฐานฉบับนี้ สนับสนุนการใช้งานชีวมิติในขอบเขตจำกัด เนื่องจากเหตุผลดังนี้

(1) การใช้งานชีวมิติแต่ละประเภทมีโอกาสเกิดการยอมรับที่ผิดพลาด (false matching) ซึ่งทำให้เกิดความไม่มั่นใจว่าผู้ที่กำลังยืนยันตัวตนคือผู้ที่เคยลงทะเบียนและพิสูจน์ตัวตนไว้จริง และอาจถูกโจมตีโดยปลอมแปลงชีวมิติ (spoofing attack)

(2) การเปรียบเทียบชีวมิติ (biometric comparision) อยู่บนพื้นฐานของความน่าจะเป็น (probabilistic) ในขณะที่ปัจจัยของการยืนยันตัวตนชนิดอื่น ใช้การเปรียบเทียบว่าข้อมูลตรงกันหรือไม่ (deterministic)

(3) การระงับหรือยกเลิกการใช้งานชีวมิติสามารถทำได้อย่างมีข้อจำกัด

(4) ชีวมิติไม่ถือว่าเป็นข้อมูลลับ ซึ่งทำให้ผู้ไม่หวังดีที่ต้องการแอบอ้างตัวตนสามารถขโมยชีวมิติ เช่น การขโมยลายนิ้วมือจากการล่อลวงให้สัมผัสวัตถุ การเก็บภาพความละเอียดสูงของม่านตา และการเก็บภาพความละเอียดสูงของลายนิ้วมือ

ด้วยเหตุผลข้างต้น การใช้งานชีวมิติมีข้อกำหนด ดังนี้

(1) ชีวมิติต้องถูกใช้เป็นส่วนหนึ่งของการยืนยันตัวตนแบบหลายปัจจัย โดยใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนประเภท สิ่งที่ผู้ใช้บริการมี (something you have) เท่านั้น

(2) การเก็บตัวอย่างชีวมิติต้องดำเนินการผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) ระหว่าง IdP และอุปกรณ์รับข้อมูล (sensor)

(3) การอ่านชีวมิติจากผู้ใช้บริการควรมีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection: PAD) เช่น การตรวจจับความมีชีวิตอยู่จากภาพของผู้ใช้บริการ (liveness detection)

(4) เทคโนโลยีที่ใช้เปรียบเทียบชีวมิติของผู้ใช้บริการต้องมีอัตราการยอมรับที่ผิดพลาด (false match rate (FMR)) ไม่เกิน 1 ใน 1,000

(5) IdP ต้องจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติให้ผิดพลาดอย่างต่อเนื่องได้ไม่เกิน 5 ครั้ง กรณีทั่วไป หรือไม่เกิน 10 ครั้ง กรณีที่ใช้งานการตรวจจับการปลอมแปลงชีวมิติ (PAD) หากครบกำหนดดังกล่าวแล้ว IdP ต้องดำเนินการอย่างใดอย่างหนึ่ง ดังนี้

   (5.1) หน่วงเวลาอย่างน้อย 30 วินาทีก่อนอนุญาตให้ยืนยันตัวตนครั้งถัดไป และเพิ่มการหน่วงเวลาก่อนอนุญาตให้ยืนยันตัวตนครั้งต่อไปแบบ exponential เช่น หน่วงเวลาอย่างน้อย 30 วินาที 1 นาที 2 นาที 4 นาที 8 นาที และเพิ่มขึ้นตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด

   (5.2) ระงับการยืนยันตัวตนด้วยชีวมิติและให้ผู้ใช้บริการยืนยันตัวตนด้วยวิธีอื่น

4. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

4.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (authenticator binding)

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (authenticator binding) คือการสร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ เพื่อทำให้สิ่งที่ใช้ยืนยันตัวตนสามารถใช้ยืนยันตัวตนผู้ใช้บริการได้

ข้อกำหนดในการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนมีดังนี้

(1) IdP ต้องเก็บรักษาข้อมูลสิ่งที่ใช้ยืนยันตัวตนทุกชิ้นที่ถูกเชื่อมโยงกับไอเดนทิตีของผู้ใช้บริการ โดยอย่างน้อยต้องประกอบด้วยวันและเวลาที่สิ่งที่ใช้ยืนยันตัวตนถูกเชื่อมโยงกับไอเดนทิตี

(2) IdP ต้องเก็บรักษาข้อมูลเกี่ยวกับจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่อง เพื่อจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามข้อกำหนดในหัวข้อ 3.2.2

(3) IdP ต้องตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนว่าเป็นไปตามข้อกำหนดของระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ระดับใด

4.2 การสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกโจรกรรม หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่เสี่ยงต่อการใช้งานโดยผู้ไม่ประสงค์ดี ดังนั้น IdP จึงควรให้ความสำคัญกับแนวปฏิบัติในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม และเสียหาย

ข้อกำหนดเกี่ยวกับการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน มีดังนี้

(1) IdP ต้องจัดให้มีช่องทางสำหรับรายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน

(2) IdP ต้องจัดให้มีวิธีการยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ที่ใช้ตรวจสอบว่ารายงานการสูญหาย ถูกโจรกรรมและเสียหายของสิ่งที่ใช้ยืนยันตัวตนมาจากผู้ใช้บริการที่กล่าวอ้างจริง

(3) IdP ต้องระงับการใช้งาน เพิกถอน หรือทำลายสิ่งที่ใช้ยืนยันตัวตนทันทีหลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม หรือเสียหาย

(4) สำหรับผู้ใช้บริการผ่านการลงทะเบียนที่ระดับ IAL2 หรือ IAL3 หากสิ่งที่ใช้ยืนยันตัวตนทั้งหมดสำหรับการยืนยันตัวตนหลายปัจจัย (multi-factor authentication) สูญหาย ถูกโจรกรรม หรือเสียหาย IdP ต้องดำเนินการพิสูจน์ตัวตนผู้ใช้บริการใหม่อีกครั้ง ทั้งนี้ IdP อาจดำเนินการพิสูจน์ตัวตนแบบไม่เต็มรูปแบบ (abbreviated identity proofing) โดยใช้วิธีการที่เหมาะสมเพื่อตรวจสอบความสัมพันธ์ระหว่างตัวตนผู้ใช้บริการกับข้อมูลและหลักฐานแสดงตนที่ IdP เคยจัดเก็บไว้ในการพิสูจน์ตัวตนครั้งก่อนหน้า

4.3 การหมดอายุ

ข้อกำหนดเกี่ยวกับการหมดอายุของสิ่งที่ใช้ยืนยันตัวตน มีดังนี้

(1) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(2) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ IdP ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนไม่สำเร็จเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

(3) IdP ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนใหม่หรือต่ออายุการใช้งานสิ่งที่ใช้ยืนยันตัวตน ในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการจะหมดอายุ

(4) เมื่อผู้ใช้บริการใช้งานสิ่งที่ใช้ยืนยันตัวตนใหม่ IdP อาจเพิกถอนสิ่งที่ใช้ยืนยันตัวตนเดิมได้ทันที

4.4 การเพิกถอน

การเพิกถอนสิ่งที่ใช้ยืนยันตัวตน คือการยุติความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ โดย IdP ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนทันที เมื่อมีกรณีใดกรณีหนึ่งดังนี้

(1) ไอเดนทิตีถูกยกเลิก เช่น ผู้ใช้บริการเสียชีวิต ผู้สมัครใช้บริการถูกตรวจพบว่าไม่มีตัวตนจริง
(2) ผู้ใช้บริการต้องการเพิกถอนสิ่งที่ใช้ยืนยันตัวตนหรือยกเลิกการใช้บริการกับ IdP
(3) IdP ตรวจพบในภายหลังว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่ IdP กำหนด

5. การบริหารจัดการ session

5.1 ข้อกำหนดทั่วไป

โดยทั่วไปแล้ว เมื่อผู้ใช้บริการยืนยันตัวตนสำเร็จ ผู้ใช้บริการควรจะสามารถเข้าถึงบริการหรือทำกิจกรรมต่าง ๆ หลังจากนั้นได้โดยไม่จำเป็นต้องยืนยันตัวตนซ้ำ (reauthentication) เพื่อให้เกิดความสะดวกในการเข้าใช้บริการ

IdP ควรพิจารณาการบริหารจัดการ session (session management) ให้เหมาะสมเนื่องจากการยืนยันตัวตนผู้ใช้บริการซ้ำบ่อยเกินไปทำให้เกิดความไม่สะดวกต่อผู้ใช้บริการ ในขณะที่การลดจำนวนของการยืนยันตัวตนผู้ใช้บริการซ้ำ (reauthentication) จนเหลือน้อยเกินไปก็จะทำให้ความน่าเชื่อถือของการยืนยันตัวตนลดลง

ข้อกำหนดเกี่ยวกับการบริหารจัดการ session (กรณีที่มีการใช้งาน) มีดังนี้

(1) session อาจเริ่มต้นหลังจากการยืนยันตัวตนและต่อเนื่องจนกระทั่ง session ถูกยกเลิก โดยการยกเลิก session อาจเกิดจากการไม่มีกิจกรรมใดๆ เกิดขึ้น (inactivity) การยกเลิกโดยผู้ใช้บริการ หรือเหตุการณ์อื่น ๆ ทั้งนี้ session อาจดำเนินการต่อจากเดิมได้ด้วยการยืนยันตัวตนซ้ำ (reauthentication)

(2) session ที่สร้างขึ้นระหว่างแอปพลิเคชันของผู้ใช้บริการ เช่น web browser (session subject) และ RP หรือ IdP (session host) ต้องมีความลับ (secret) ที่ใช้งานร่วมกันระหว่าง session subject และ session host เพื่อให้ผู้ใช้บริการสามารถใช้บริการได้อย่างต่อเนื่อง โดย session subject ต้องแสดงความลับที่ตนเองครอบครองโดยตรง หรือพิสูจน์การครอบครองความลับผ่านกลไกการเข้ารหัสลับ (cryptographic mechanism)

(3) ความลับที่ใช้เชื่อมโยง session (session binding) มีข้อกำหนด ดังนี้

(3.1) ต้องถูกสร้างขึ้นโดย session host ระหว่างการปฏิสัมพันธ์ (interaction) ซึ่งมักจะเกิดขึ้นทันทีหลังจากการยืนยันตัวตน

(3.2) ต้องถูกสร้างขึ้นโดยวิธีการสุ่ม

(3.3) ต้องถูกลบหรือทำให้ใช้งานไม่ได้ (invalidate) โดย session subject เมื่อผู้ใช้บริการยกเลิก session

(3.4) ควรถูกลบจาก session subject เมื่อผู้ใช้บริการออกจากระบบ (log out) หรือเมื่อความลับหมดอายุการใช้งาน

(3.5) ไม่ควรเก็บไว้ในสถานที่ที่ไม่ปลอดภัย เช่น HTML5 Local Storage เนื่องจากเสี่ยงต่อการโจมตีแบบ cross-site scripting (XSS)

(3.6) ต้องถูกส่งหรือรับจากอุปกรณ์ของผู้ใช้บริการผ่านช่องทางที่มีความปลอดภัย (protected channel)

(3.7) ต้องหมดอายุและใช้งานไม่ได้หลังจาก

ก. 30 วัน หรือ 60 นาที ที่ไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL1

ข. 12 ชั่วโมง หรือ 30 นาที ที่ไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL2

ค. 12 ชั่วโมง หรือ 15 นาที ที่ไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL3

(3.8) ต้องไม่สามารถใช้งานผ่านช่องทางการสื่อสารระหว่าง session host และ session subject ที่ไม่ปลอดภัย (insecure communication) และ session ที่สร้างขึ้นแล้วต้องไม่ถูกลดระดับไปสู่ช่องทางที่ไม่ปลอดภัยในภายหลัง (เช่น จาก https เป็น http)

5.2 กลไกบริหารจัดการ session (session management mechanism)

5.2.1 cookies

cookies เป็นกลไกที่นิยมใช้สำหรับสร้าง session และติดตาม (track) ผู้ที่เข้าใช้บริการ โดยมีข้อกำหนดการใช้งาน cookies ดังนี้

(1) ต้องแท็ก (tag) ให้สามารถเข้าถึงได้เฉพาะ HTTPS session

(2) ต้องสามารถเข้าถึงได้โดยใช้ชุดของ hostnames และ paths ที่น้อยที่สุดเท่าที่ปฏิบัติได้

(3) ควรแท็ก (tag) ให้ไม่สามารถเข้าถึงได้โดย JavaScript (HttpOnly)

(4) ควรแท็ก (tag) ให้หมดอายุเมื่อครบช่วงเวลาของ session

5.2.2 access token

access token เช่น OAuth ใช้สำหรับอนุญาตให้แอปพลิเคชันเข้าถึงกลุ่มบริการในฐานะของผู้ใช้บริการหลังการยืนยันตัวตนสำเร็จ โดย RP ต้องไม่ถือว่าการแสดง OAuth access token คือการที่ผู้ใช้บริการยังคงสถานะใช้บริการอยู่หากไม่มีสัญญาณ (signal) อื่น ๆ ประกอบ

OAuth access token และ refresh tokens อื่น ๆ ที่เกี่ยวข้อง อาจมีสถานะใช้งานได้ (valid) หลังจากสิ้นสุด session และผู้ใช้บริการออกจากการใช้งานแอปพลิเคชัน

5.2.3 การระบุอุปกรณ์ (device identification)

วิธีการระบุอุปกรณ์ เช่น TLS หรือ token binding อาจนำมาใช้สร้าง session ระหว่างผู้ใช้บริการและ RP ได้

5.3 การยืนยันตัวตนซ้ำ (reauthentication)

การยืนยันตัวตนซ้ำตามช่วงเวลาที่กำหนดของแต่ละระดับ AAL ต้องเกิดขึ้นเพื่อยืนยันว่าผู้ใช้บริการยังคงมีสถานะใช้งานอยู่ (นั่นคือ ผู้ใช้บริการไม่ได้เดินจากไป โดยไม่ได้ออกจากระบบ (log out))

ก่อนที่ session จะสิ้นสุดเนื่องจากหมดเวลาหรือด้วยเหตุผลอื่น ๆ ผู้ใช้บริการต้องยืนยันตัวตนซ้ำเพื่อต่ออายุการใช้งาน session โดยมีวิธีการดังนี้

(1) ระดับ AAL1 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

(2) ระดับ AAL2 : ยืนยันตัวตนโดยใช้รหัสลับจดจำ (memorized secret) หรือชีวมิติ (biometric)

(3) ระดับ AAL3 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด

6. แนวทางการกำหนดระดับ AAL ของประเทศไทย

แนวทางการกำหนดระดับ AAL ของประเทศไทยที่มีการแบ่งระดับ AAL2 ออกเป็น 2 ระดับย่อย ได้แก่ ระดับ AAL2.1 และระดับ AAL2.2 สามารถแสดงได้ตามตารางที่ 1

ตารางที่ 1 แนวทางการกำหนดระดับ AAL ของประเทศไทย

ข้อกำหนด	AAL1	AAL2.1	AAL2.2	AAL3
ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ ● memorized secret ● out-of-band devices ● SF OTP device ● SF cryptographic software ● SF cryptographic device ● สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL2 และ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ ● MF OTP device ● MF cryptographic software ● memorized secret ร่วมกับ - out-of-band device หรือ - SF OTP device หรือ - SF cryptographic software หรือ - SF cryptographic device ● สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL3	ชีวมิติ (biometric) ร่วมกับชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ ● MF OTP device ● MF cryptographic software ● memorized secret ร่วมกับ - out-of-band device หรือ - SF OTP device หรือ - SF cryptographic software หรือ - SF cryptographic device ● สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ ● MF cryptographic device ● SF cryptographic device ร่วมกับ memorized secret ● MF OTP device ร่วมกับ SF cryptographic device ● MF OTP device ร่วมกับ SF cryptographic software ● SF OTP device ร่วมกับ MF cryptographic software ● SF OTP device ร่วมกับ SF cryptographic software และ memorized secret
การยืนยันตัวตนซ้ำ	อย่างน้อยทุก 30 วัน	อย่างน้อยทุก 12 ชั่วโมง หรือ 30 นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้นโดยผู้ใช้บริการ	อย่างน้อยทุก 12 ชั่วโมง หรือ 30 นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้นโดยผู้ใช้บริการ	อย่างน้อยทุก 12 ชั่วโมง หรือ 15 นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้นโดยผู้ใช้บริการ
การป้องกันการโจมตีโดยคนกลาง (man-in-the-middle attack) ของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและ IdP	จำเป็น	จำเป็น	จำเป็น	จำเป็น
การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay attack) ของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น	จำเป็น	จำเป็น	จำเป็น
การป้องกัน IdP ปลอม (IdP impersonation attack) ของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น	ไม่จำเป็น	ไม่จำเป็น	จำเป็น

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