กรอบมาตรฐาน
การพัฒนาองค์กรดิจิทัลภาครัฐ

ดร.ก่อเกียรติ แก้วกิ่ง

ผู้อำนวยการศูนย์สารสนเทศฯ กรมการปกครอง ICAD DOPA

อนุกรรมการมาตรฐานและการกำกับดูแลธุรกรรมทางอิเล็กทรอนิกส์ ETDA

อนุกรรมการเทคโนโลยีสารสนเทศ กองทุนการออมแห่งชาติ NSF

ข้อเสนอแนะมาตรฐานฯ ธุรกรรมอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตน

- การพิสูจน์ยืนยันตัวตนดิจิทัล
- ลายเซ็นอิเล็กทรอนิกส์
- Biometric

เอกสารอิเล็กทรอนิกส์

- การมอบอำนาจทางอิเล็กทรอนิกส์
- ใบรับรองอิเล็กทรอนิกส์
- ใบเสร็จอิเล็กทรอนิกส์

การแลกเปลี่ยนข้อมูล

- บริการนำส่งข้อมูลอิเล็กทรอนิกส์
- ข้อกำหนดทางเทคนิคของชุดข้อมูลร่วมสำหรับการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์

การรักษาความมั่นคงปลอดภัย

- มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ
- ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตน

แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์

ขมธอ. 23-2563

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

ขมธอ. 18 ถึง 20-2566

เทคโนโลยีชีวมิติ

ขมธอ. 29 ถึง 30-2565

ข้อเสนอแนะมาตรฐานฯ (ETDA Recommendation) ว่าด้วย

แนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Guideline)

ขอบข่าย

อธิบายภาพรวมและข้อกำหนดที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ เพื่อให้ผู้ใช้งานที่ต้องการใช้ลายมือชื่ออิเล็กทรอนิกส์มีแนวทางในการลงลายมือชื่ออิเล็กทรอนิกส์และสามารถเลือกใช้วิธีการลงลายมือชื่ออิเล็กทรอนิกส์ที่เหมาะสมกับการทำธุรกรรมทางอิเล็กทรอนิกส์

อย่างไรก็ตาม ข้อเสนอแนะมาตรฐานฉบับนี้เป็นคำแนะนำเกี่ยวกับการปฏิบัติตามข้อกำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งอาจยังมีข้อกำหนดเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายอื่นที่กำหนดไว้เป็นการเฉพาะ ดังนั้น ผู้ใช้งานควรมีการศึกษาข้อกฎหมายอื่น ๆ ที่เกี่ยวข้องประกอบด้วย

ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่แก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2562

หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์ เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

แบ่งได้เป็น 2 ประเภท

ลายมือชื่อตามมาตรา 9

1. ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้
2. แสดงเจตนาของเจ้าของลายมือชื่อกับข้อความที่ลงลายมือชื่อได้
3. ใช้วิธีการที่เชื่อถือได้ * โดยคำนึงถึง
   - ความมั่นคงและรัดกุมของวิธีการที่ใช้
   - ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ ฯลฯ
   - ความรัดกุมของระบบติดต่อสื่อสาร

ลายมือชื่อตามมาตรา 26

กฎหมายให้ถือว่าเป็นลายมือชื่อที่เชื่อถือได้

1. ข้อมูลที่ใช้สร้างลายมือชื่อเชื่อมโยงไปยังเจ้าของลายมือชื่อได้
2. ข้อมูลที่ใช้สร้างลายมือชื่ออยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ
3. สามารถตรวจพบการเปลี่ยนแปลงของลายมือชื่อ / ข้อความ ได้

* นอกจากจะใช้วิธีการที่เชื่อถือได้ในการลงลายมือชื่อแล้ว สามารถเลือกใช้วิธีการอื่นใดหรือพยานหลักฐานอื่นประกอบเพื่อระบุตัวเจ้าของลายมือชื่อ และการแสดงเจตนาของเจ้าของลายมือชื่อได้ด้วย

ประเภทของลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

ประเภทที่ 1
ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

เป็นลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบใด ๆ (เป็นอักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์) ที่มีลักษณะตามที่กำหนดในมาตรา 9 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

ประเภทที่ 2
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดในมาตรา 26 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)

ประเภทที่ 3
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้
ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

เป็นลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดในมาตรา 26 และอาศัยใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามที่กำหนดในมาตรา 28 แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

เช่น ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้เป็นอย่างไร

หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะตามที่กำหนดใน**มาตรา 26** แห่งกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ลายมือชื่อดิจิทัล (Digital Signature)

หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อและตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้

องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์

	การพิสูจน์และยืนยันตัวตน [1]	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
ประเภทที่ 1 **ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป**	มีการพิสูจน์และยืนยันตัวตนที่**น่าเชื่อถือ**และเหมาะสมกับความเสี่ยงของธุรกรรม	มี**กระบวนการหรือหลักฐาน**ที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน	ใช้**หลักฐานหรือบุคคลที่สามที่เชื่อถือได้** เพื่อแสดงว่าไม่มีการเปลี่ยนแปลงความหมายของข้อความที่ลงลายมือชื่อ และรับรองความครบถ้วนของข้อมูล
ประเภทที่ 2 **ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้**	▪ มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือที่**ระดับ IAL2 ขึ้นไป** [2] ▪ มีการยืนยันตัวตนที่**ระดับ AAL2 ขึ้นไป** [3]	ใช้**ลายมือชื่อดิจิทัล**ในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้**ลายมือชื่อดิจิทัล**ในการลงลายมือชื่อต่อข้อความ
ประเภทที่ 3 **ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง**	▪ มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือที่**ระดับ IAL2 ขึ้นไป** ▪ มีการยืนยันตัวตนที่**ระดับ AAL2 ขึ้นไป**	ใช้**ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA**ในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้**ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดย CA**ในการลงลายมือชื่อต่อข้อความ

[1] ข้อเสนอแนะมาตรฐานฯ แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – **ภาพรวมและอภิธานศัพท์ เลขที่ ขมธอ. 18-2561**, เวอร์ชัน 1.0.
[2] ข้อเสนอแนะมาตรฐานฯ แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – **การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2561**, เวอร์ชัน 1.0
[3] ข้อเสนอแนะมาตรฐานฯ แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – **การยืนยันตัวตน เลขที่ ขมธอ. 20-2561**, เวอร์ชัน 1.0

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

01 กรอบการทำงาน -ขมธอ. 18-2566 เวอร์ชัน 3.0

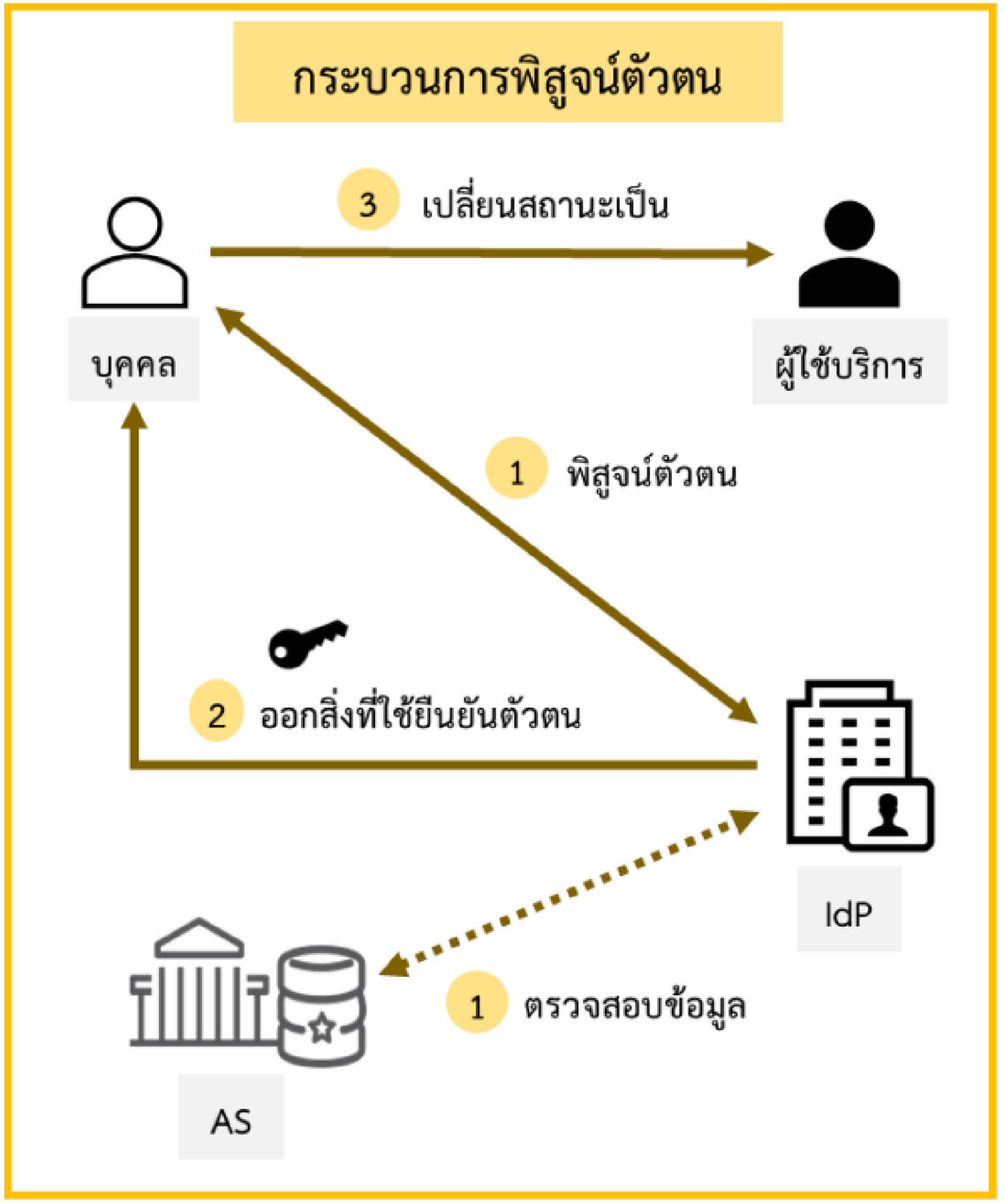
อธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

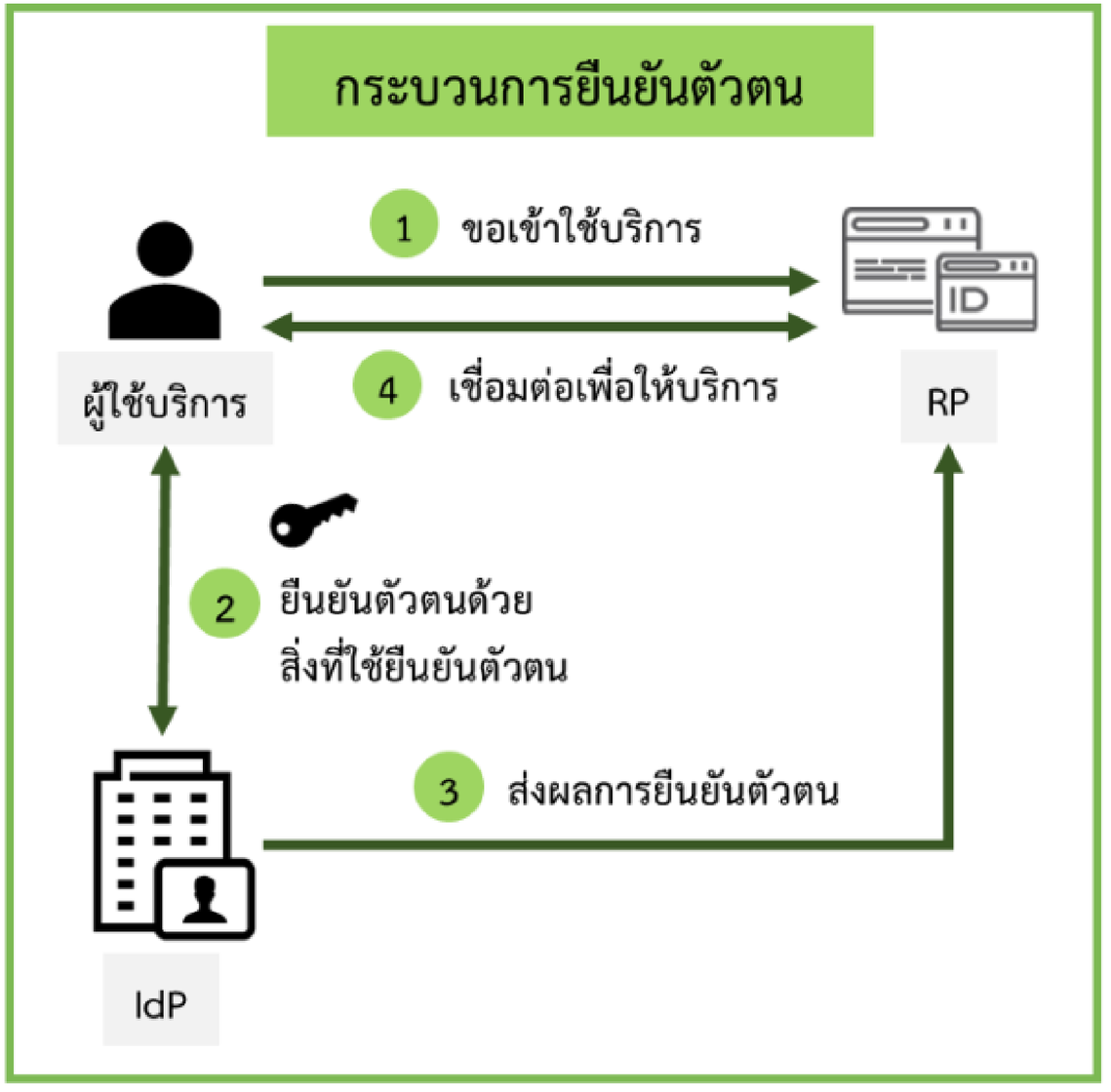
02 ข้อกำหนดของการพิสูจน์ตัวตน -ขมธอ. 19-2566 เวอร์ชัน 3.0

เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

03 ข้อกำหนดของการยืนยันตัวตน -ขมธอ. 20-2566 เวอร์ชัน 3.0

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





IdP คือ ผู้พิสูจน์และยืนยันตัวตน (identity provider)
RP คือ ผู้อาศัยการยืนยันตัวตน (relying party)
AS คือ แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ประโยชน์ภายในกิจการของตนเองสามารถนำไปประยุกต์ใช้ได้

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม | ETDA

	การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์			การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์	
			ตรวจสอบและยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล		
IAL3	ใช้บัตรประชาชน: ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number) และ ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลของหน่วยงานรัฐเพิ่มเติม			พบเห็นต่อหน้า เท่านั้น	Biometric Comparison; หรือ ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติจากชิปของหลักฐานแสดงตน; หรือ ใช้ระบบ Face Verification Service (FVS)
IAL2.3	กรณีใช้บัตรประชาชนโดยมีเครื่องอ่านบัตร: ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	กรณีใช้บัตรประชาชนโดยไม่มีเครื่องอ่านบัตร: ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Laser Code) และ FVS	กรณีใช้หนังสือเดินทาง: ตรวจสอบข้อมูลโดยใช้ NFC และ สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Biometric Comparison; หรือ ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติจากชิปของหลักฐานแสดงตน; หรือ ใช้ระบบ Face Verification Service (FVS)
IAL2.2	ตรวจสอบข้อมูล และ สถานะบัตร (ใช้ Chip Number)	ตรวจสอบข้อมูลจาก IdP ที่เคยทำ IAL2.3 ขึ้นไป และ สถานะบัตร (ใช้ Laser Code)	ตรวจสอบข้อมูลโดยใช้ NFC และ สถานะบัตรประชาชน (ใช้ Laser Code) หรือ เอกสารสำคัญอื่น	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Visual Comparison กับ; หรือ ภาพใบหน้าจากชิปของหลักฐานแสดงตน; หรือ ภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3 ของบุคคลนั้น
IAL2.1	ตรวจสอบข้อมูล	ตรวจสอบข้อมูลจาก IdP ที่เคยทำ IAL2.3 ขึ้นไป	ตรวจสอบข้อมูลโดยใช้ NFC		
IAL1	**อาจ**รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ **โดยไม่จำเป็นต้อง** ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ หรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์				

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากข้อเสนอแนะมาตรฐานฯ
ศึกษารายละเอียดจาก ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (ขมธอ. 19-2566 เวอร์ชัน 3.0)

เผยแพร่: ก.พ. 2566

ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ประโยชน์ภายในกิจการของตนเองสามารถนำไปประยุกต์ใช้ได้

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

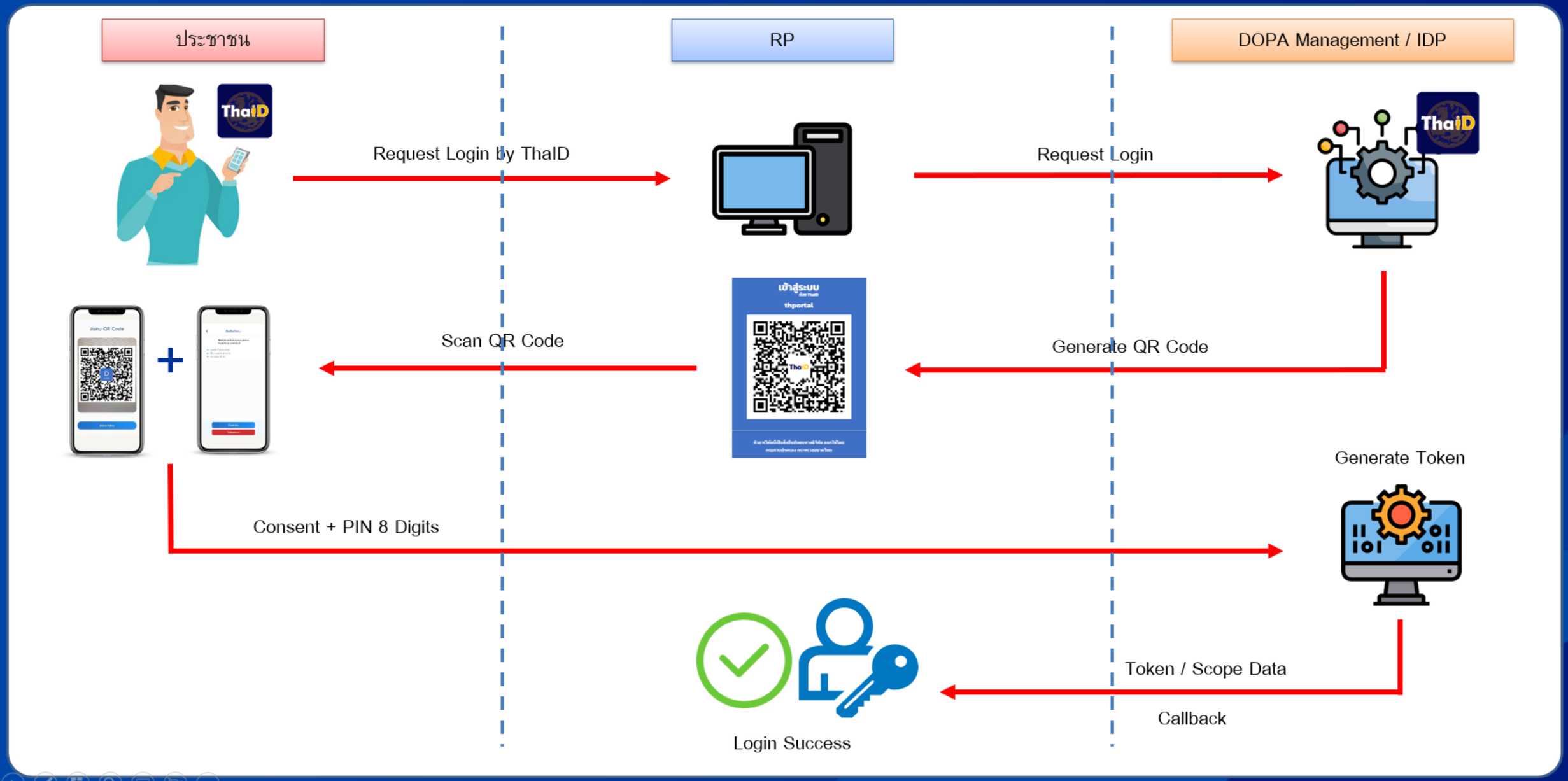
	ข้อกำหนดของการยืนยันตัวตน	ชนิดของสิ่งที่ใช้ยืนยันตัวตน ที่สามารถใช้ได้
AAL3	 ยืนยันตัวตนแบบ Multi-factor authentication และใช้สิ่งที่ใช้ยืนยันตัวตนเป็น Hardware และมี Cryptographic key สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร สามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance) สามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)	**MF** Crypto Device Memorized Secret **และ** **SF** Crypto Device **MF** OTP Device **และ** **SF** Crypto Device **MF** OTP Device **และ** **SF** Crypto Software **SF** OTP Device **และ** **MF** Crypto Software Memorized Secret **และ** **SF** OTP Device **และ** **SF** Crypto Software
AAL2	 ยืนยันตัวตนแบบ Multi-factor authentication สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร สามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)	Memorized Secret **และ** Out-of-band Device **หรือ** **SF** OTP Device **หรือ** **SF** Crypto Software **MF** OTP Device **MF** Crypto Software
AAL1	 ยืนยันตัวตนแบบ Single-factor authentication สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร	Memorized Secret Out-of-band Device **SF** OTP Device **SF** Crypto Software **SF** Crypto Device

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากข้อเสนอแนะมาตรฐานฯ
ศึกษารายละเอียดจาก ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (ขมธอ. 20-2566 เวอร์ชัน 3.0)

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

เผยแพร่: ก.พ. 2566

วิธีการรับ-ส่ง ข้อมูลของแอปพลิเคชัน ThaID



เทคโนโลยีชีวมิติ

การใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์
และยืนยันตัวตน ขมธอ. 29 เล่ม 1-2565

การใช้งานเทคโนโลยีการรู้จำใบหน้า
สำหรับการพิสูจน์และยืนยันตัวตน
ขมธอ. 29 เล่ม 2-2565

การใช้งานเทคโนโลยีการรู้
จำลายนิ้วมือสำหรับการพิสูจน์
และยืนยันตัวตน
ขมธอ. 29 เล่ม 3-2565

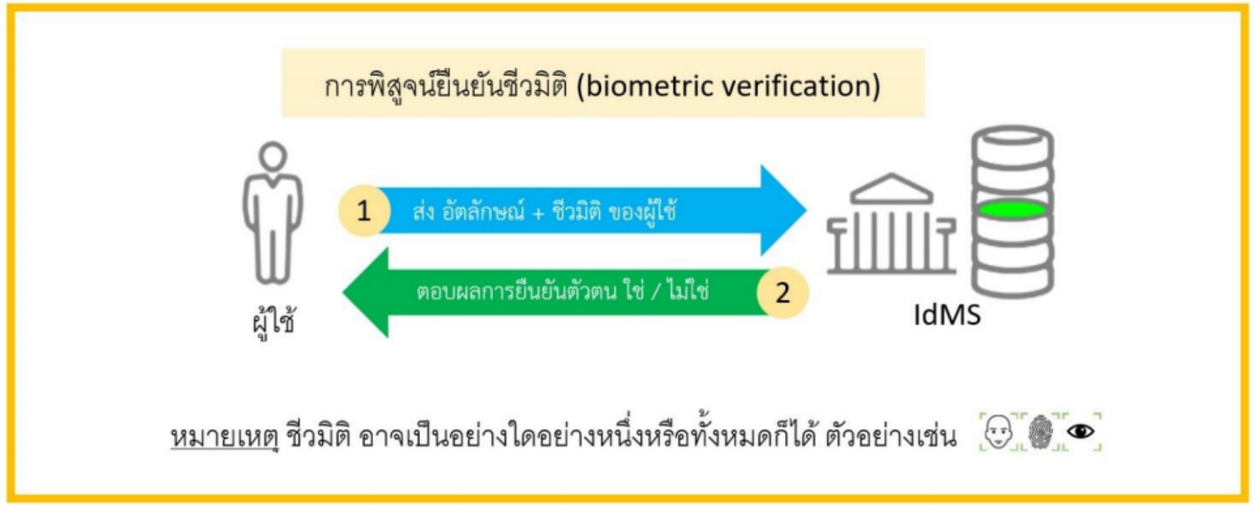
การใช้งานเทคโนโลยีการรู้จำลายม่านตา
สำหรับการพิสูจน์และยืนยันตัวตน
ขมธอ. 29 เล่ม 4-2565

การทดสอบสมรรถนะการทำงาน
เทคโนโลยีชีวมิติ
ขมธอ. 30-2565

ภาพรวมการใช้งานเทคโนโลยีชีวมิติกับระบบบริหารอัตลักษณ์บุคคล (IdMS)

01 การพิสูจน์ยืนยันชีวมิติ (biometric verification)

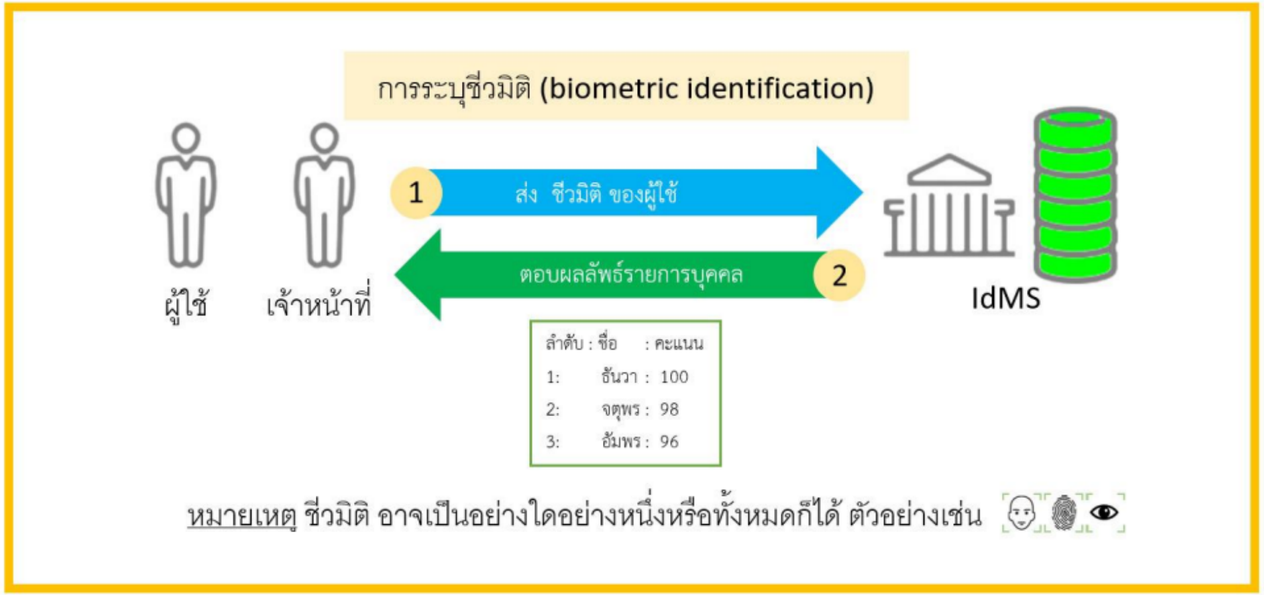
กระบวนการพิสูจน์ยืนยันชีวมิติของผู้ใช้ ซึ่งโดยปกติแล้วจะมีกระบวนการเปรียบเทียบข้อมูลตัวอย่างชีวมิติของผู้เรียกร้องกับข้อมูลอ้างอิงชีวมิติที่เชื่อโยงกับข้อมูลอัตลักษณ์(เช่นเลขประจำตัวประชาชน)



รูปที่ 1 การพิสูจน์ยืนยันชีวมิติ (biometric verification)

02 การระบุชีวมิติ (biometric identification)

กระบวนการค้นหาระบุตัวบุคคลด้วยชีวมิติ กระบวนการจะเปรียบเทียบข้อมูลตัวอย่างชีวมิติของบุคคลเป้าหมายกับข้อมูลอ้างอิงชีวมิติของทุก ๆ บุคคลที่มีอยู่ในฐานข้อมูล

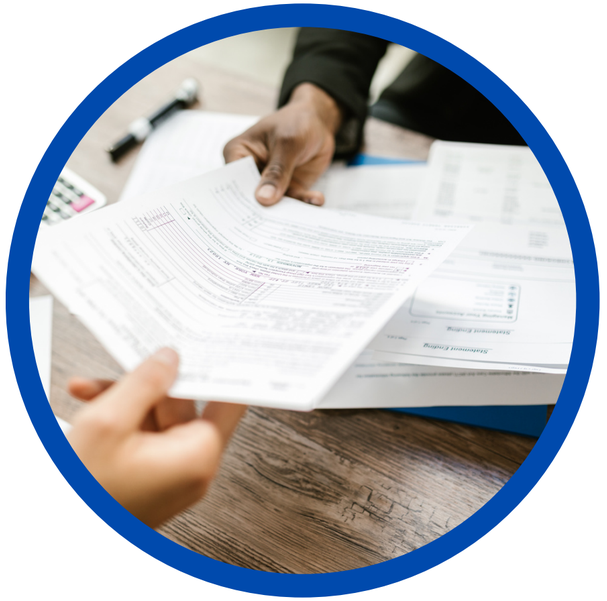


รูปที่ 2 การระบุชีวมิติ (biometric identification)

เอกสารอิเล็กทรอนิกส์

การมอบอำนาจทางอิเล็กทรอนิกส์
ขมธอ. 31-2565

ข้อความอิเล็กทรอนิกส์สำหรับใบเสร็จรับเงินภาครัฐ
ขมธอ. 22-2563



การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์
ขมธอ. 11-2560

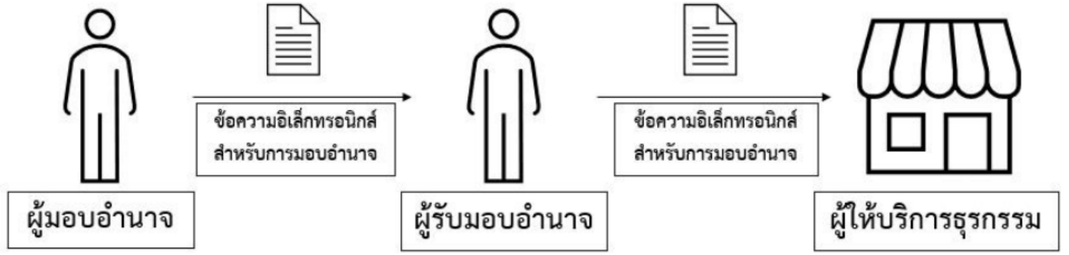
การมอบอำนาจทางอิเล็กทรอนิกส์

01 การมอบอำนาจทางอิเล็กทรอนิกส์

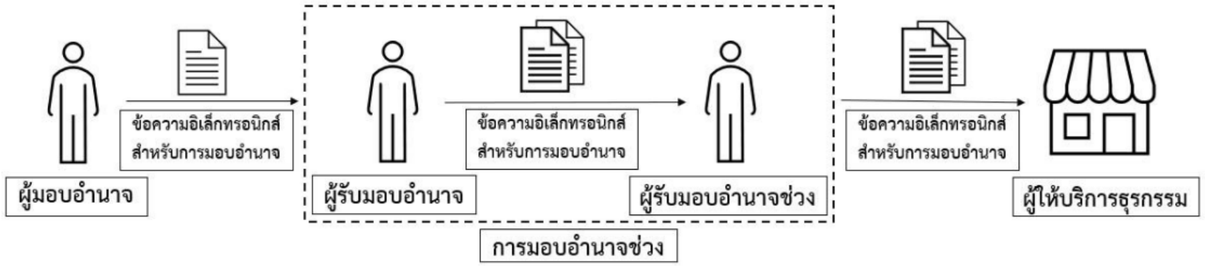
ผู้มอบอำนาจสามารถแสดงเจตนาในการมอบอำนาจด้วยการลงลายมือชื่ออิเล็กทรอนิกส์ประกอบกับข้อความอิเล็กทรอนิกส์สำหรับการมอบอำนาจ ผู้รับมอบอำนาจจะใช้ข้อความอิเล็กทรอนิกส์สำหรับการมอบอำนาจเป็นข้อมูล ประกอบการทำธุรกรรมกับผู้ให้บริการธุรกรรมต่อไป

02 ข้อความอิเล็กทรอนิกส์สำหรับการมอบอำนาจ

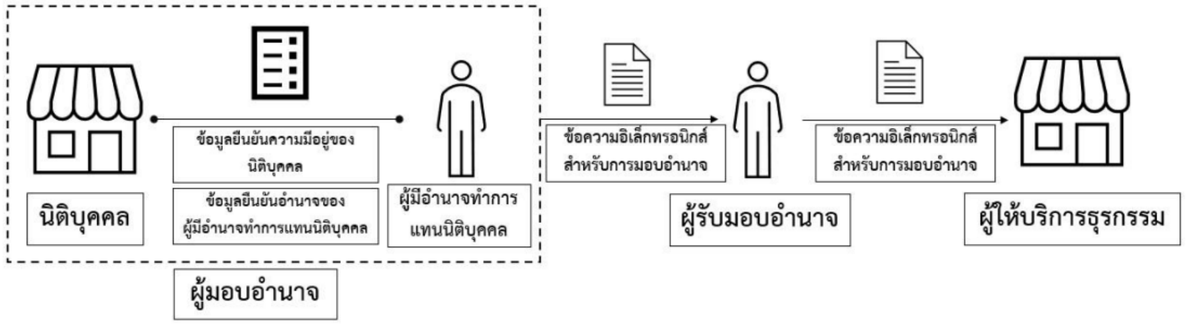
ข้อความอิเล็กทรอนิกส์สำหรับการมอบอำนาจ คือ หนังสือมอบอำนาจที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยข้อความอิเล็กทรอนิกส์สำหรับการมอบอำนาจต้องจัดทำให้อยู่ในสภาพที่สามารถอ่านเข้าใจได้โดยบุคคล (human readable) เพื่อให้บุคคลสามารถเข้าใจความหมายของข้อความที่แสดงผลได้



รูปที่ 1 การมอบอำนาจทั่วไป



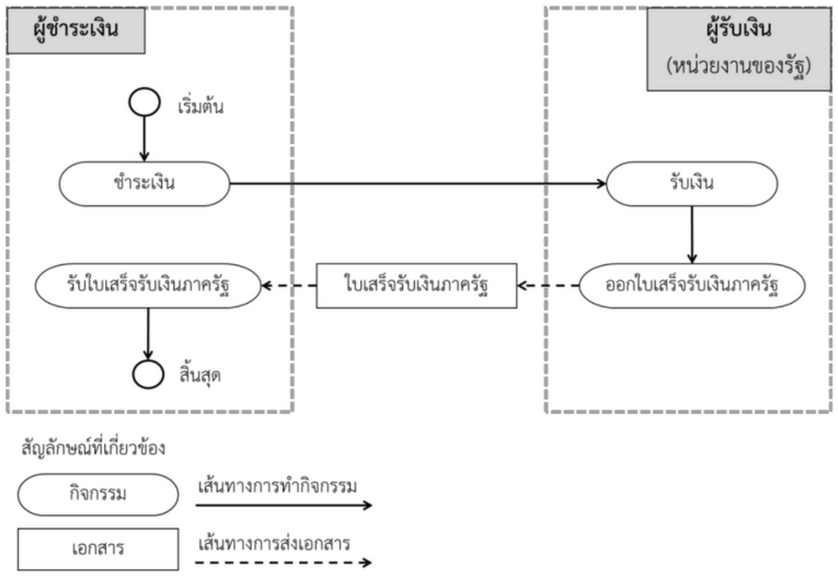
รูปที่ 2 การมอบอำนาจช่วง



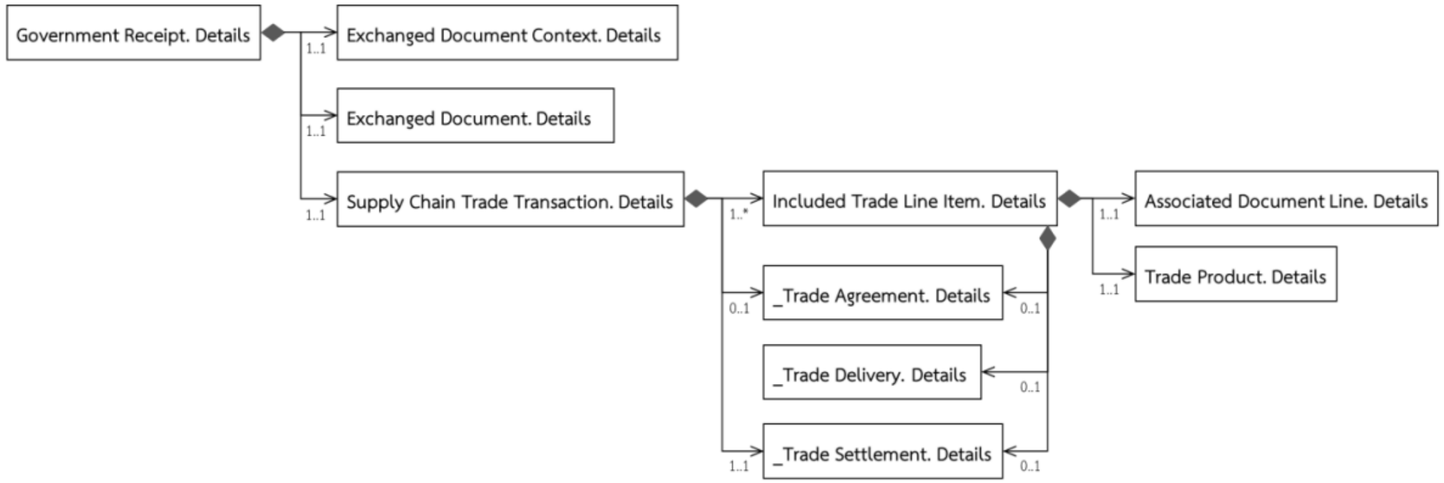
รูปที่ 3 การมอบอำนาจในนามนิติบุคคล

ข้อความอิเล็กทรอนิกส์สำหรับใบเสร็จรับเงินภาครัฐ

กำหนดโครงสร้างข้อมูลของข้อความอิเล็กทรอนิกส์ในรูปแบบ XML ให้สอดคล้องกับมาตรฐานสากล และเพื่อให้หน่วยงานของรัฐนำไปใช้เป็นมาตรฐานประกอบการจัดทำข้อมูลในใบเสร็จรับเงินได้อย่างมีประสิทธิภาพ



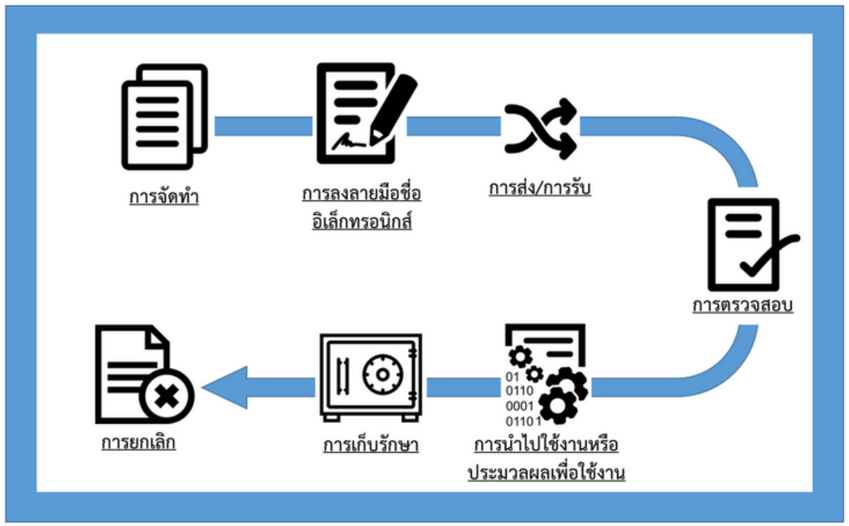
รูปที่ 1 ตัวอย่างการใช้งานใบเสร็จรับเงินภาครัฐ



รูปที่ 2 แบบจำลองโครงสร้างข้อมูลของข้อความอิเล็กทรอนิกส์สำหรับใบเสร็จรับเงินภาครัฐ

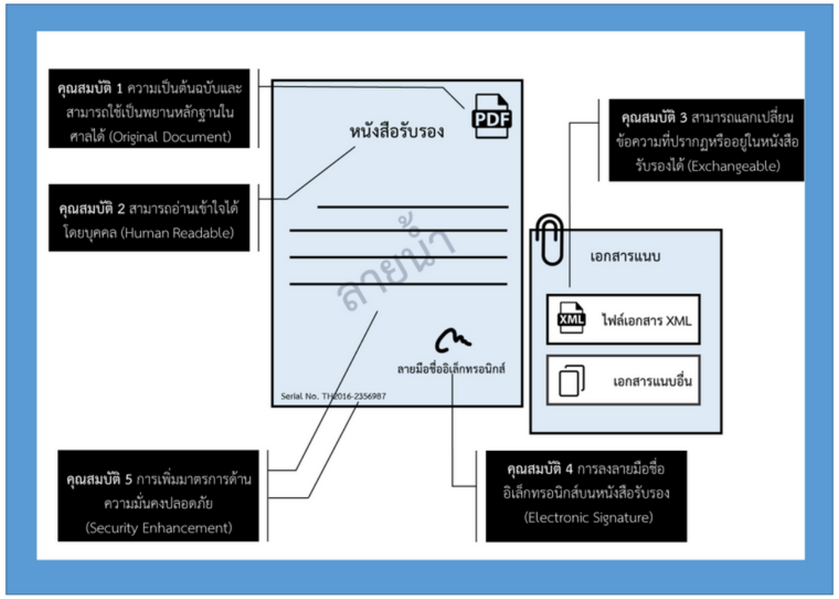
การจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

เพื่อให้หนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ที่จัดทำตามข้อเสนอแนะฯ มีความน่าเชื่อถือ และสามารถใช้งานโดยมีสถานะทางกฎหมายได้เช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิมจึงได้นำเสนอแนวทางการจัดทำหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ให้อยู่ในรูปแบบของไฟล์เอกสาร Portable Document Format (PDF) ซึ่งถูกออกแบบมาเพื่อให้แสดงผลข้อความเสมือนกับการแสดงข้อความบนกระดาษ



รูปที่ 1 วงจรการใช้งานหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์ (Electronic Certificate Life Cycle)

รูปที่ 2 คุณสมบัติของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์



รูปที่ 3 องค์ประกอบต่างๆ ของหนังสือรับรองในรูปแบบอิเล็กทรอนิกส์

การแลกเปลี่ยนข้อมูล

บริการนำส่งข้อมูลอิเล็กทรอนิกส์

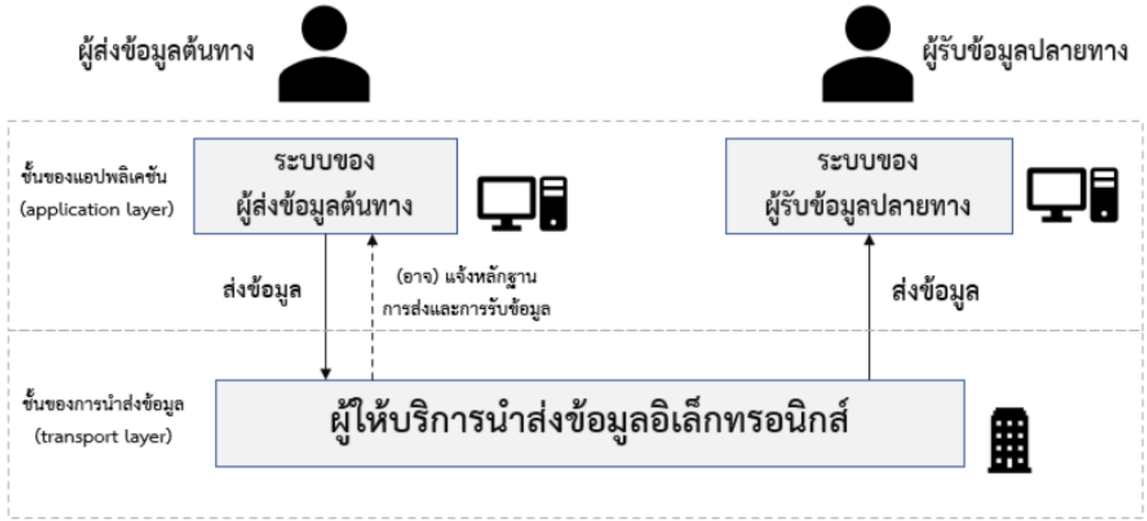
ขมธอ. 35-2566

การใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์

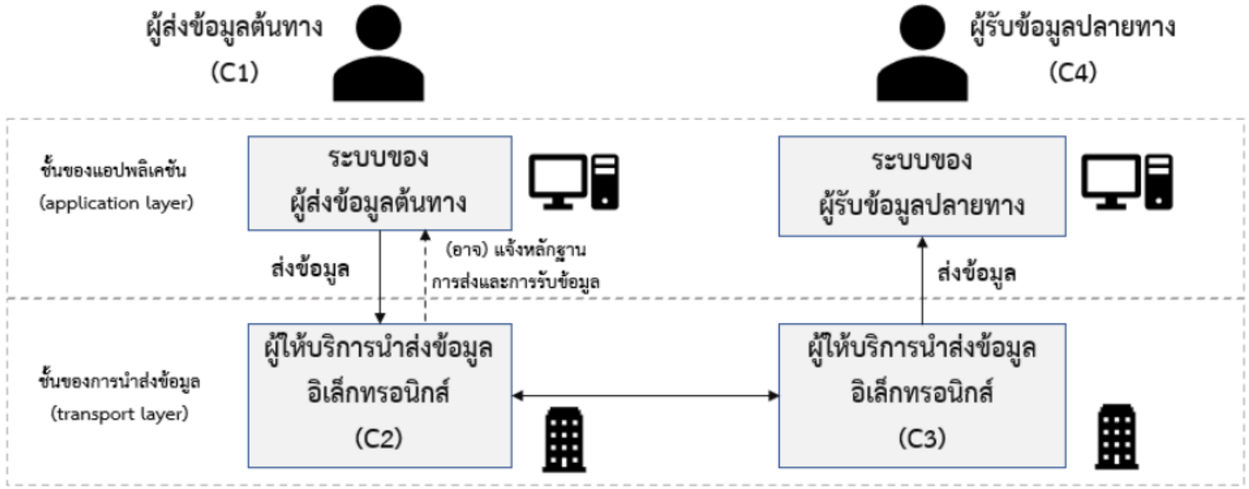
ขมธอ. 14-2560

บริการนำส่งข้อมูลอิเล็กทรอนิกส์

บริการนำส่งข้อมูลอิเล็กทรอนิกส์(electronic delivery service) เป็นการรับส่งข้อมูลระหว่างผู้ส่งข้อมูล ต้นทาง (original sender) กับผู้รับข้อมูลปลายทาง (final recipient) ผ่านผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์โดย ผู้ให้บริการนำส่งข้อมูลอิเล็กทรอนิกส์จะทำหน้าที่จัดทำหลักฐานการส่งและการรับข้อมูลเพื่อยืนยันเหตุการณ์ที่เกิดขึ้น ระหว่างการรับส่งข้อมูล



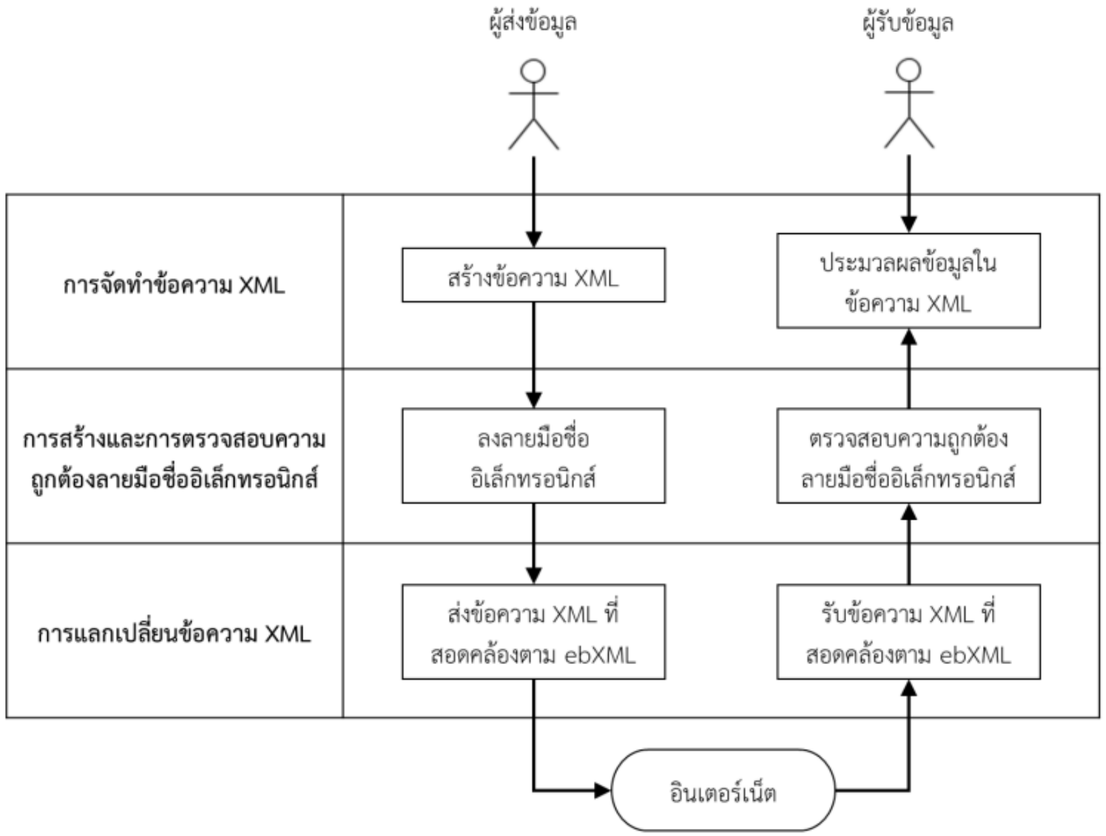
รูปที่ 1 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 3-corner model



รูปที่ 2 การนำส่งข้อมูลอิเล็กทรอนิกส์แบบ 4-corner model

การใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์

จัดทำขึ้นเพื่อสนับสนุนการใช้ข้อความ XML สำหรับการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยและน่าเชื่อถือ รวมทั้งให้ผู้ประกอบการและหน่วยงานต่างๆ มีแนวทางในการสร้างเอกสารอิเล็กทรอนิกส์อยู่ในรูปแบบข้อความ XML ให้เป็นมาตรฐานเดียวกัน



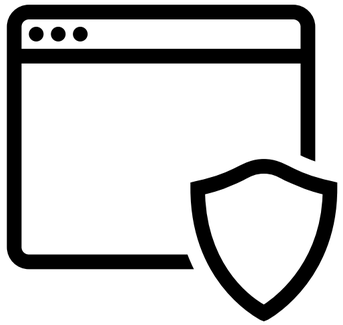
รูปที่ 1 กระบวนการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์โดยใช้ข้อความ XML

การรักษาความมั่นคงปลอดภัย

มาตรฐานการรักษาความมั่นคงปลอดภัย
สำหรับโปรแกรมประยุกต์บนเว็บ
ขมธอ. 4-2559

ความยินยอมสำหรับการประมวลผล
ข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์
ขมธอ. 28-2564

มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บ

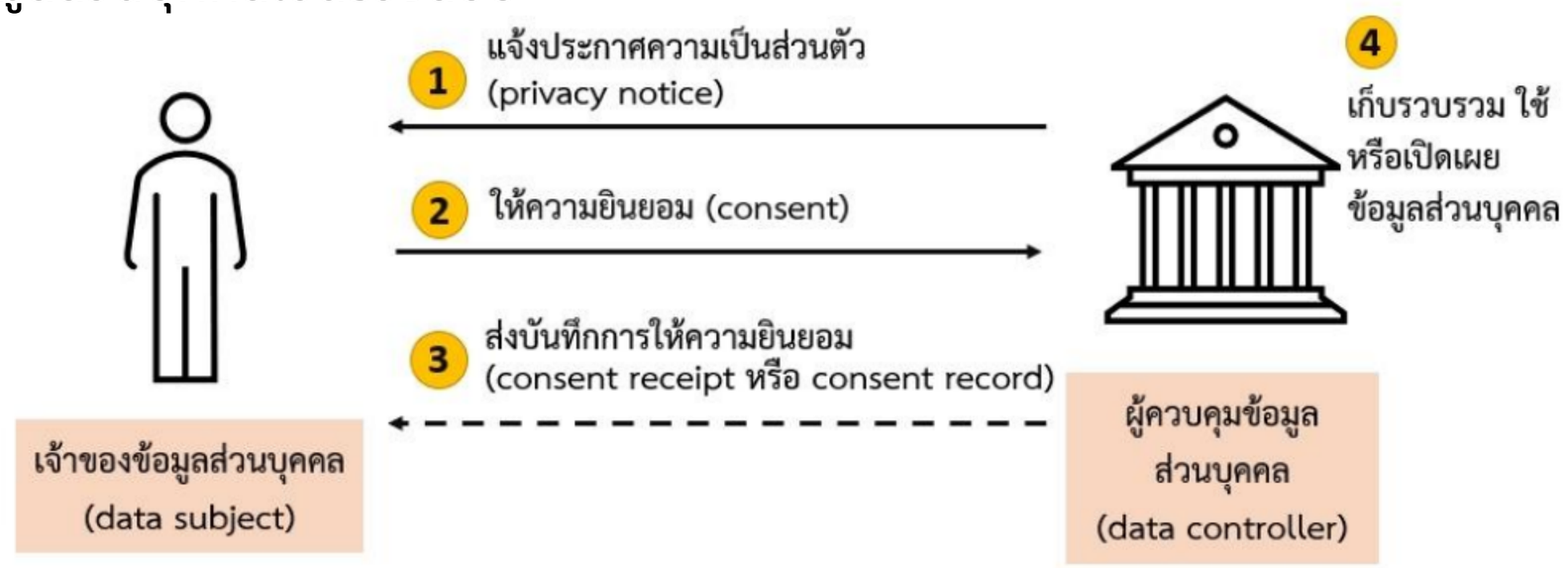


เป็นแนวทางสำหรับการพัฒนาและทดสอบโปรแกรมประยุกต์บนเว็บเพื่อให้มีความมั่นคงปลอดภัย รวมถึงการเสนอแนะแนวทางที่เกี่ยวข้องเพื่อป้องกันการโจมตีและแก้ไขช่องโหว่ที่เกี่ยวข้อง โดยขอบเขตของ ข้อเสนอแนะฉบับนี้มุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บด้วยการพัฒนา และ ทดสอบโปรแกรมประยุกต์บนเว็บให้มีความมั่นคงปลอดภัยจากช่องโหว่ดังต่อไปนี้

(1) SQL Injection
(2) OS Command Injection
(3) Unchecked Path Parameter หรือ Directory Traversal
(4) Improper Session Management
(5) Cross-Site Scripting
(6) Cross-Site Script Request Forgery
(7) HTTP Header Injection
(8) Mail Header Injection
(9) Lack of Authentication and authorization

ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลทางอิเล็กทรอนิกส์

อธิบายภาพรวมและข้อกำหนดที่เกี่ยวข้องกับการแจ้งประกาศความเป็นส่วนตัว (privacy notice) และการขอความยินยอม (consent) จากเจ้าของข้อมูลส่วนบุคคลก่อนหรือในขณะเก็บรวบรวม ข้อมูลส่วนบุคคลผ่านระบบอิเล็กทรอนิกส์รวมถึงแนะนำสาระสำคัญของบันทึกการให้ความยินยอม (consent receipt หรือ consent record) สำหรับส่งให้เจ้าของข้อมูลส่วนบุคคลใช้ตรวจสอบ



รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการขอความยินยอม

Thank You