



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



ทำไมต้อง Digital ID

ประชาชนเข้าถึงบริการทั้งภาครัฐและเอกชนผ่านระบบออนไลน์
เพิ่มความสะดวกในการทำธุรกรรม





กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA

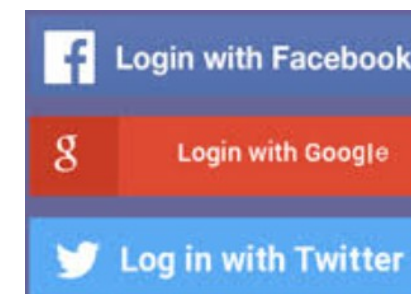
Digital ID คืออะไร



ข้อมูลสำหรับยืนยันตัวตน ในการทำธุรกรรมแบบ physical



ข้อมูลสำหรับยืนยันตัวตน ในการทำธุรกรรมออนไลน์





กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

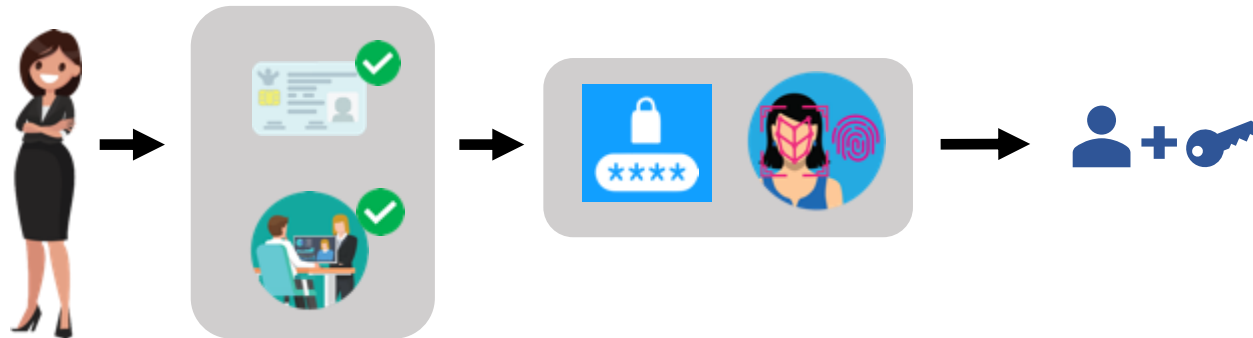
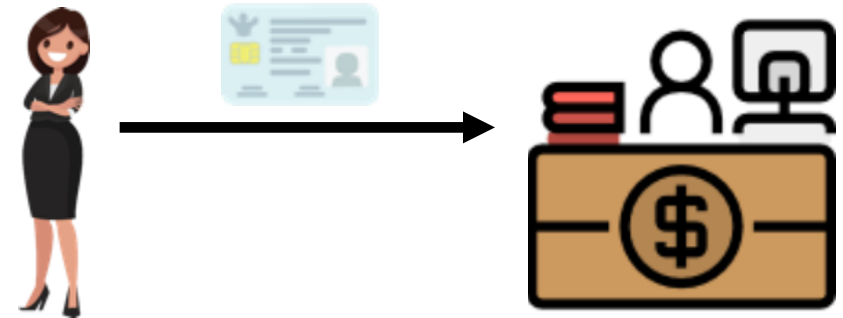


การพิสูจน์ และยืนยันตัวตน คืออะไร

การพิสูจน์ตัวตน



การยืนยันตัวตน





กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



Digital ID

กับการขับเคลื่อนที่ผ่านมา



ด้านกฎหมาย



ด้านมาตรฐาน



ด้านระบบโครงสร้างพื้นฐานที่รองรับ



ด้านกฎหมาย

การรองรับผลทางกฎหมาย
พร้อมกลไกดูแลความน่าเชื่อถือผู้ให้บริการ

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

- เพิ่มหมวด 3/1 รองรับบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล
- ให้มีการตรา พ.ร.ก. กำหนดธุรกิจบริการที่จำเป็นต้องดูแลเพื่อลดความเสี่ยงของผู้ใช้งาน (ร่าง พ.ร.ก. ว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ.)

สถานะ : อยู่ระหว่างพิจารณาของ
สำนักงานคณะกรรมการกฤษฎีกา

พ.ร.บ. การบริหารงานและการให้บริการภาครัฐ ผ่านระบบดิจิทัล พ.ศ. 2562

- หน่วยงานของรัฐมีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ได้มาตรฐาน



ด้านมาตรฐาน

รองรับการใช้งาน Digital ID
เพื่อให้ทำงานร่วมกันบนมาตรฐานเดียวกัน

ETDA Recommendation

มาตรฐานกลางรองรับการใช้งาน
สำหรับ Sector ต่างๆ

- กรอบการทำงาน (Framework)
(ขมรอ. 18-2564)
- ข้อกำหนดของการพิสูจน์ตัวตน
(Identity Proofing Requirements)
(ขมรอ. 19-2564)
- ข้อกำหนดของการยืนยันตัวตน
(Authentication Requirements)
(ขมรอ. 20-2564)

หมายเหตุ: ปรับปรุงจากมาตรฐานเดิม เวอร์ชัน 1.0 ปี 2561

DGA Recommendation

มาตรฐานเฉพาะเพื่อบริการของรัฐ

มาตรฐานและหลักเกณฑ์การจัดทำ
กระบวนการและการดำเนินงานทางดิจิทัล
ว่าด้วยเรื่องการใช้ดิจิทัลไอดี สำหรับ
บริการภาครัฐ สำหรับบุคคลธรรมดา
ที่มีสัญชาติไทย

สถานะ : ประกาศในราชกิจจานุเบกษาแล้ว



ด้านระบบโครงสร้าง พื้นฐานที่รองรับ

การพัฒนาระบบรองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล
ให้พร้อมใช้งานใน Sector ต่าง ๆ

System Infrastructure



D.DOPA



MNID (Mobile National ID)

- ผู้ให้บริการการแลกเปลี่ยนข้อมูล
และเก็บ credential สำหรับพิสูจน์และยืนยัน
ตัวตน (Sandbox NBTC)



NDID (National Digital ID)

- ผู้ให้บริการการแลกเปลี่ยนข้อมูลการทำ KYC
เช่น เปิดบัญชีออนไลน์ (Sandbox BoT)

ETDA Digital Service Sandbox

รองรับการทดสอบนวัตกรรมหรือบริการ
สำหรับ Digital ID Solution
ดูแลความเสี่ยง และความสอดคล้อง
ตามกฎหมายและมาตรฐาน

มีผู้ให้บริการทั้งรัฐและเอกชน ให้ความสนใจ
เข้าร่วม Sandbox เช่น NDID, DOPA

1. นาย ก มาพิสูจน์ตัวตน กับ บริษัท ประกันภัย

การพิสูจน์ตัวตน Identity Proofing

รวบรวมข้อมูล/ตรวจสอบข้อมูล/ตรวจสอบความเชื่อมโยง

- 1 ติดตั้ง / เข้า
Application
DD Insurance

DD



- 2 กรอกข้อมูลเบื้องต้น
(เลขประจำตัวประชาชน)

DD



- 3 เดินทางไปที่
สำนักงาน
สาขา



- 3.1 แสดงบัตรประจำตัวประชาชน
กับเจ้าหน้าที่รวบรวมข้อมูลหลักฐาน)



- 3.2 เสิร์บบัตรประจำตัวประชาชน
(ตรวจสอบหลักฐาน)



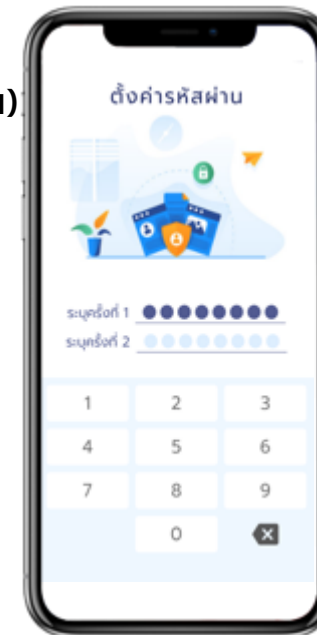
- 3.3 สแกนใบหน้า
(ตรวจสอบ
ความเชื่อมโยง)



การออกและบริหารจัดการ สิ่งที่ใช้ยืนยันตัวตน Authenticator Management

- 4 ตั้งรหัสผ่าน 8 หลัก
(สิ่งที่ใช้ยืนยันตัวตน)

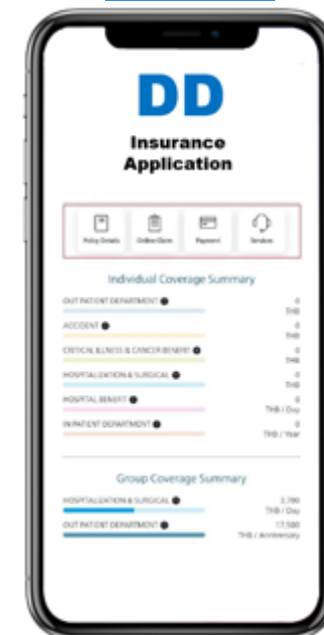
DD



- 5 ลงทะเบียนสำเร็จ

ID : เลขบัตรประชาชน
สิ่งที่ใช้ยืนยันตัวตน : รหัสผ่าน

DD



รูปภาพบางส่วนจาก Application D.DOPA / Application My Allianz

นาย ก ต้องการเคลมประกันออนไลน์ด้วย DD Insurance

(ใช้ App DD Insurance กับบริการของบริษัท ประกันภัย DD เอง)

การยืนยันตัวตน Authentication

1 เข้า Application
DD Insurance

DD



2 ยืนยันตัวตน

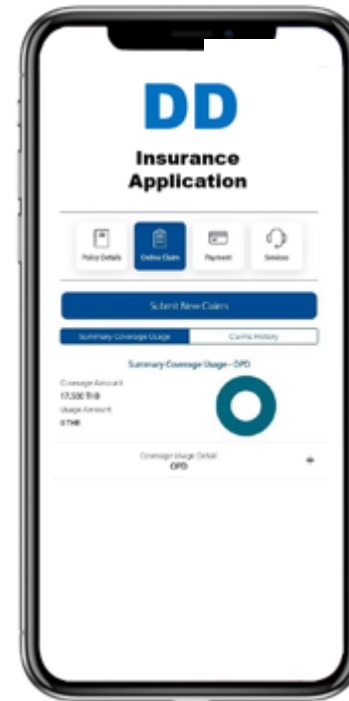
DD



ด้วยการกรอกรหัสผ่าน
(สิ่งที่ใช้ยืนยันตัวตน)

3 เข้าสู่ระบบ

DD



Online Claim

รูปภาพบางส่วนจาก
Application D.DOPA / Application My Allianz

2. นาย ก ต้องการสมัครใช้บริการ AB Hospital (RP) เพื่อพบแพทย์ทาง Online

(กรณียังไม่เคยพิสูจน์และยืนยันตัวตนกับ RP มาก่อน)

นาย ก เข้า Application **AB Hospital**  **AB Hospital**



นาย ก สมัครใช้งาน Application AB Hospital
ได้ 2 ทางเลือก

สมัครใช้บริการใหม่กับ AB Hospital

→ [2.1] ลงทะเบียนใหม่กับ AB Hospital

อาศัย IDP ในการพิสูจน์และยืนยันตัวตน

→ [2.2] ด้วย Application
DD Insurance

รูปภาพบางส่วนจาก Application ทางรัฐ



สมัครใช้บริการใหม่กับ AB Hospital

AB Hospital พิสูจน์และยืนยันตัวตนนาย ก ด้วยตนเอง

-----> [2.1] สมัครใช้บริการใหม่กับ AB Hospital

Identity Proofing

1 รวบรวมข้อมูล/ตรวจสอบข้อมูล/ตรวจสอบความเชื่อมโยง



AB Hospital



AB Hospital



AB Hospital



AB Hospital



Authenticator Management

2 ตั้งรหัสผ่าน
(สิ่งที่ใช้ยืนยันตัวตน)

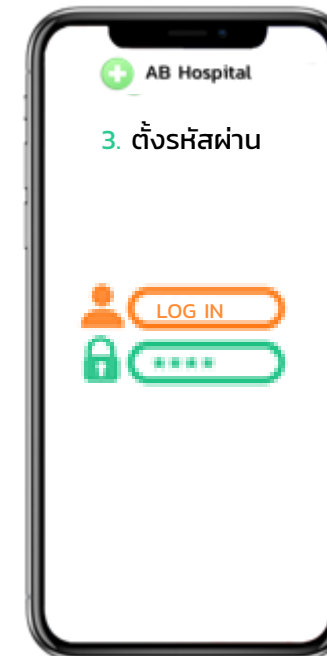
3 ลงทะเบียนสำเร็จ



AB Hospital



AB Hospital





อาศัย IDP ในการพิสูจน์และยืนยันตัวตน User

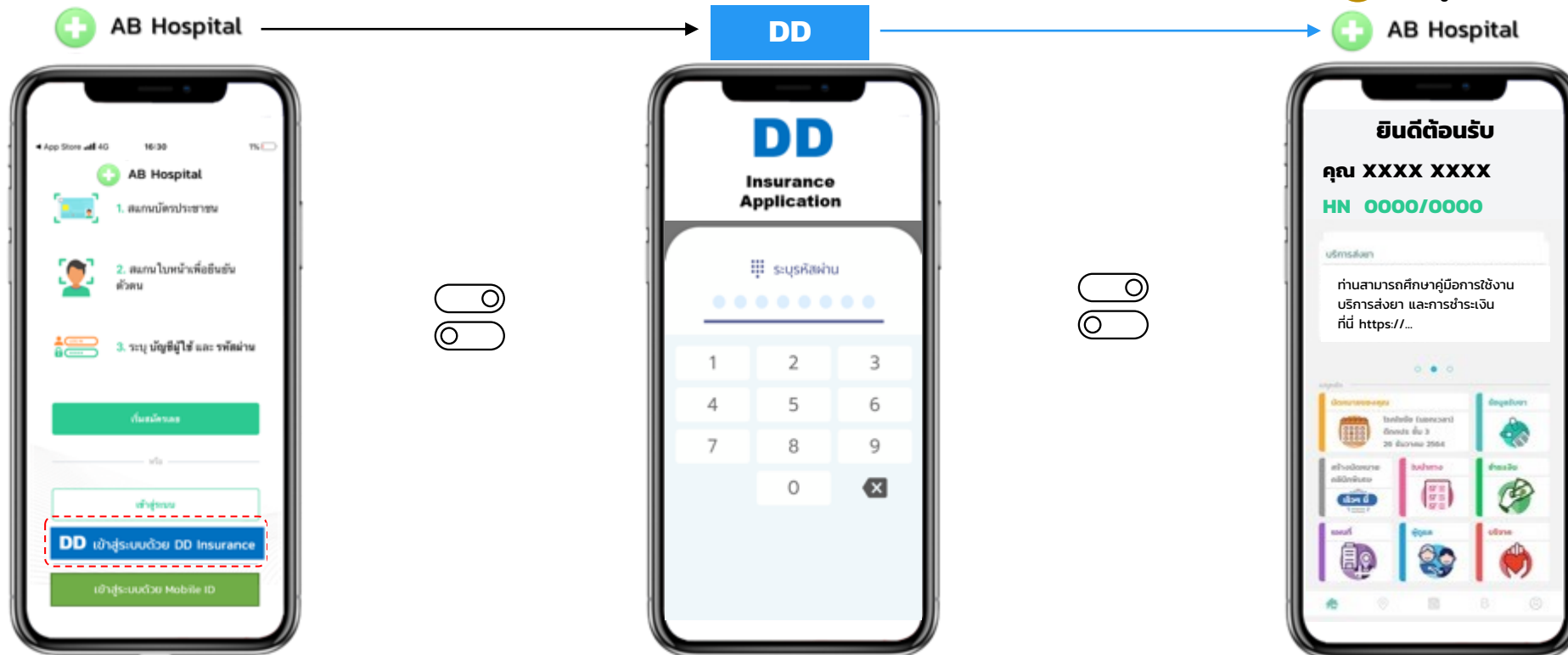
[2.2] ด้วย Application DD Insurance

Authentication

1 ยืนยันตัวตน

DD

2 เข้าสู่ระบบ



ด้วยการกรอกรหัสผ่าน
(สิ่งที่ใช้ยืนยันตัวตน)

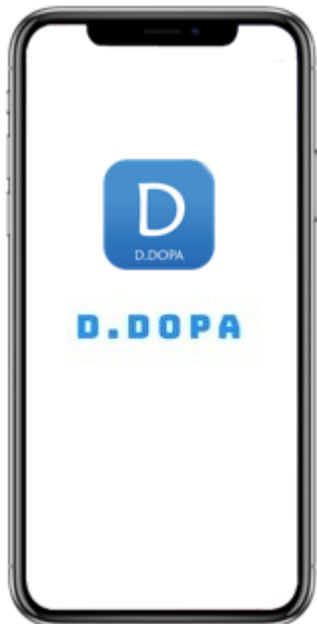
ตัวอย่าง การพิสูจน์และยืนยันตัวตนกับ Application D.DOPA

Identity Proofing

รวบรวมข้อมูล/ตรวจสอบข้อมูล/ตรวจสอบความเชื่อมโยง

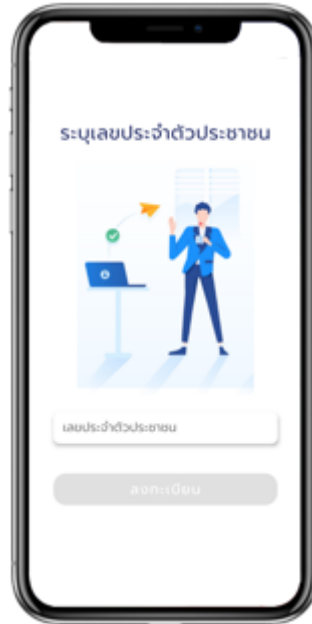
1 ติดตั้ง / เข้า
Application D.DOPA

D.DOPA



2 กรอกข้อมูลเบื้องต้น
(เลขประจำตัวประชาชน)

D.DOPA



3 เดินทางไปที่
สำนักงาน
เขต



3.1 แสดงบัตรประจำตัวประชาชน
กับเจ้าหน้าที่รวบรวมข้อมูล
หลักฐาน)



3.2 เลียนบัตรประจำตัวประชาชน
(ตรวจสอบหลักฐาน)



3.3 สแกนลายพิมพ์นิ้วมือ
(ตรวจสอบความเชื่อมโยง)



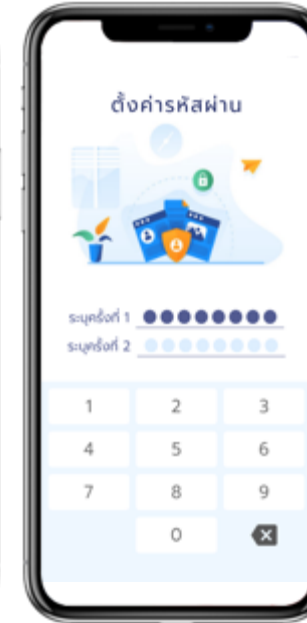
Authenticator Management

4 สแกน QR-Code
เพื่อเชื่อมโยง
Private Key
(สิ่งที่ใช้ยืนยันตัวตน)
กับ ID ของตน



5 ตั้งรหัสผ่าน 8 หลัก
(สิ่งที่ใช้ยืนยันตัวตน)

D.DOPA



6 ลงทะเบียนสำเร็จ

D.DOPA

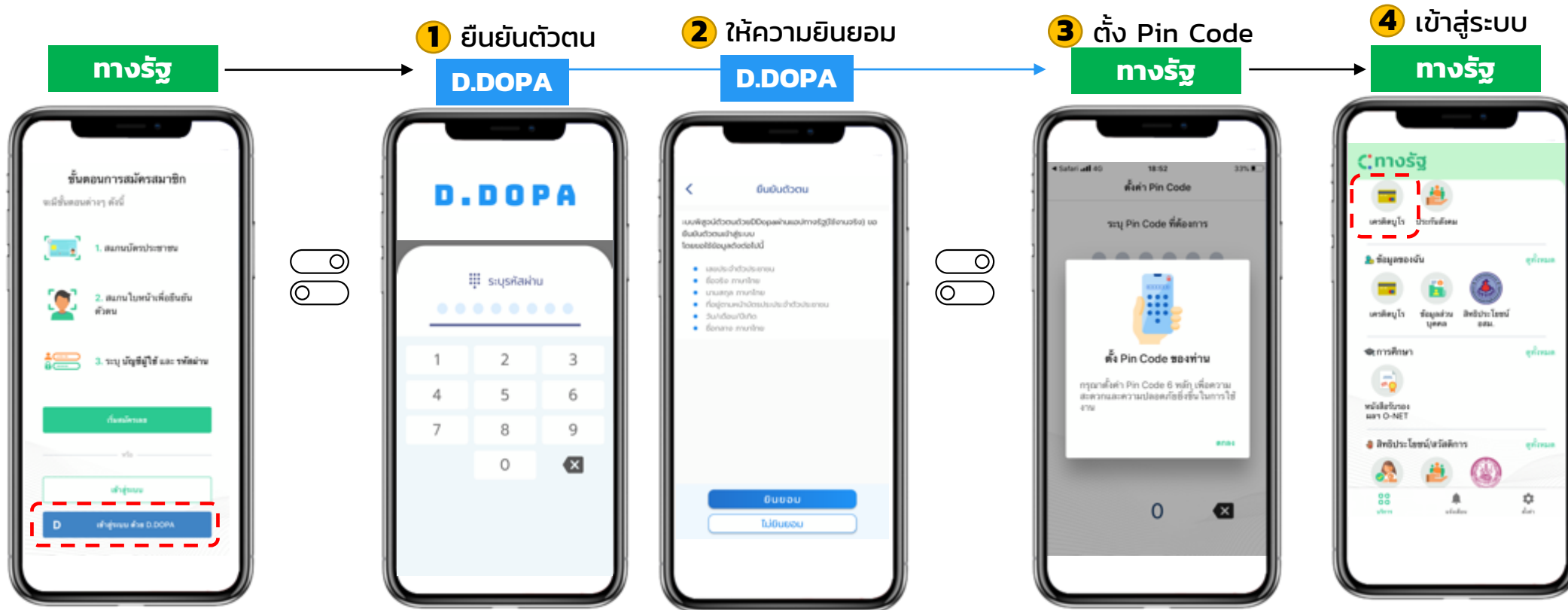


ID : เลขบัตรประชาชน

สิ่งที่ใช้ยืนยันตัวตน : รหัสผ่าน และ Private Key

อาศัย D.DOPA ในการพิสูจน์และ ยืนยันตัวตน กับ App ทางรัฐ

Authentication



ขอข้อมูลเครดิต
จากเครดิตบูโร

ด้วยการกรอกรหัสผ่าน
(สิ่งที่ใช้ยืนยันตัวตน)



กฎหมาย ด้าน Digital ID



พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

เพิ่มคำนิยาม

- “การพิสูจน์และยืนยันตัวตน”
- “ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล”

รองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เพิ่ม ม.34/3)

- ให้ข้อสันนิษฐานทางกฎหมาย
- กำหนดเงื่อนไขเกี่ยวกับความน่าเชื่อถือ

ให้มีการตรา พ.ร.ฎ. (เพิ่ม ม.34/4)

- กำหนดประเภทธุรกิจบริการที่กำกับดูแล

กำหนดโทษ (เพิ่ม ม.45/1)

- กรณีไม่ได้รับอนุญาต หรือฝ่าฝืนคำสั่ง พักใช้หรือเพิกถอนใบอนุญาต
- จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ

บทเฉพาะกาล (ม.7)

- เมื่อมีพระราชกฤษฎีกาแล้ว ให้ยื่นขอ อนุญาตภายใน 90 วันนับแต่วันที่ พ.ร.ฎ. มีผลใช้บังคับ

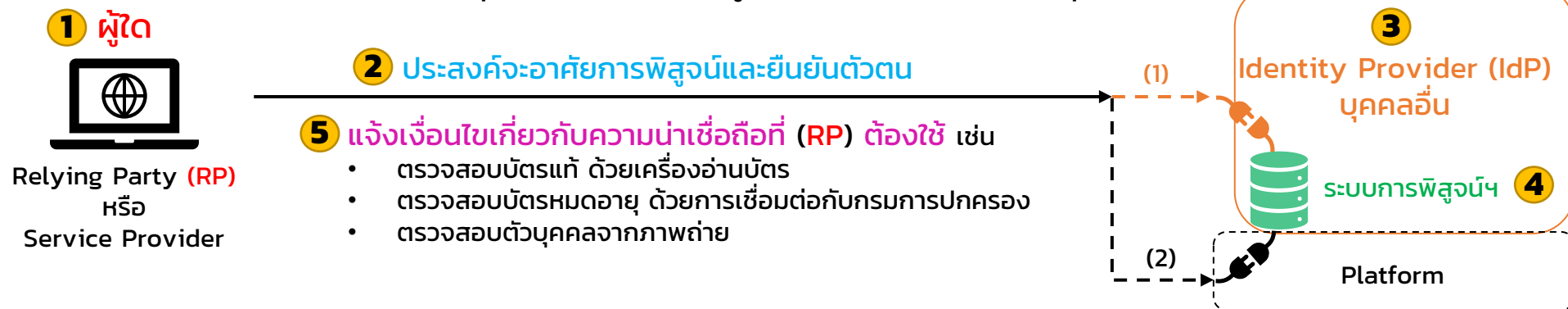
พ.ร.บ. ธุรกรรมฯ (ฉบับที่ 4)



<https://ictlawcenter.etda.or.th/laws>

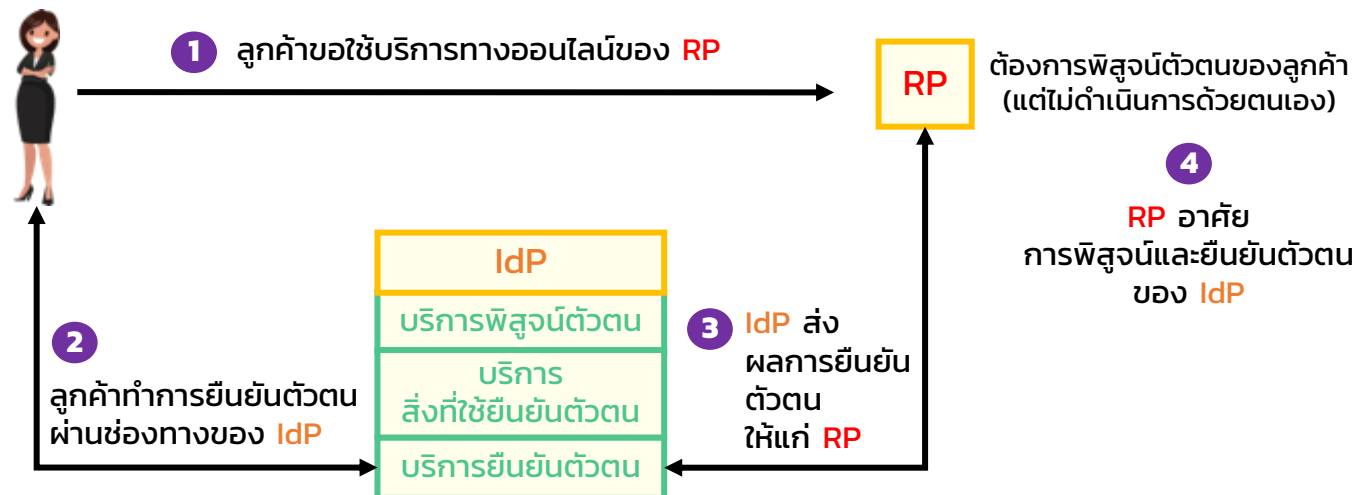
การพิสูจน์และยืนยันตัวตนทางดิจิทัล ตามมาตรา 34/3 วรรค 2

“ผู้ใดประสงค์จะอาศัยการพิสูจน์และยืนยันตัวตนของบุคคลอื่นผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล อาจแจ้งเงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องใช้ ให้บุคคลอื่นนั้นทราบเป็นการล่วงหน้า และเมื่อได้มีการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามเงื่อนไขดังกล่าวแล้ว ให้สันนิษฐานว่าบุคคลที่ได้รับการพิสูจน์และยืนยันตัวตนเป็นบุคคลนั้นจริง”



การพิสูจน์และยืนยันตัวตนโดยอาศัย IdP

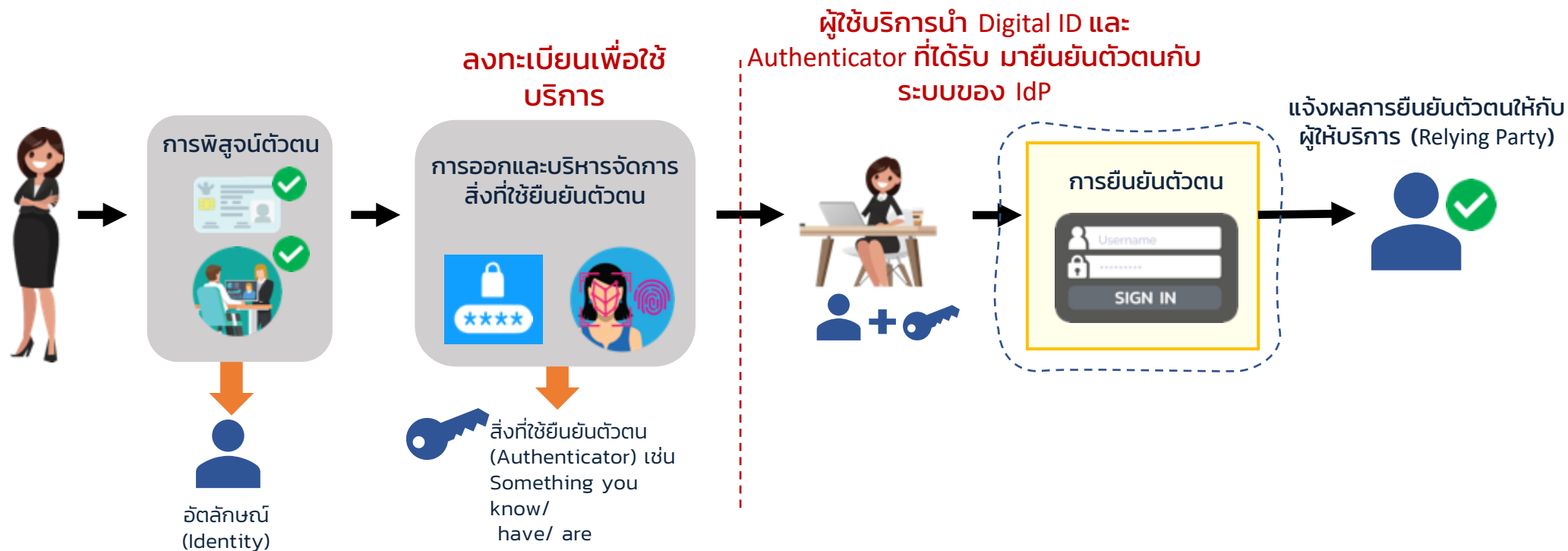
IdP จะต้องเคยพิสูจน์และยืนยันตัวลูกค้ามาก่อน



กระบวนการที่เกี่ยวข้องกับ “ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล”



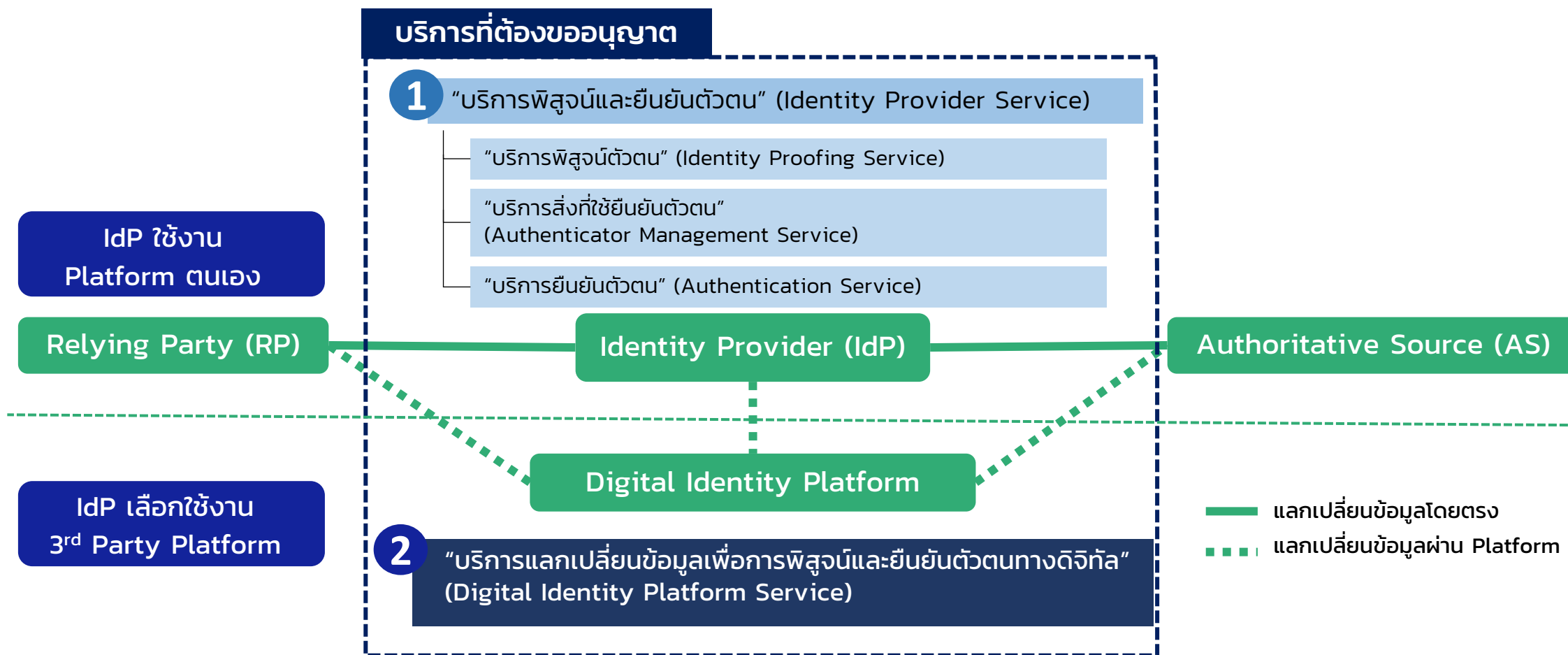
กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



- ❑ “การพิสูจน์ตัวตน” (Identity Proofing Service)
บริการที่ประกอบด้วยกระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น
- ❑ “การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน” (Authenticator Management Service)
บริการที่ประกอบด้วยกระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น
- ❑ “การยืนยันตัวตน” (Authentication Service)
บริการที่ประกอบด้วยกระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น

อ้างอิงจาก ISO/IEC 29115:2013 [ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework]

ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล



❑ “บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล” (Digital Identity Platform Service)

บริการที่เป็นเครือข่ายหรือระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลาง

ที่มาและความจำเป็น ของร่างพระราชกฤษฎีกา



กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม



ความเป็นมา

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562

มาตรา 34/4 ในกรณีจำเป็น ให้มีการตราพระราชกฤษฎีกาเพื่อกำหนดให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใด เป็นธุรกิจบริการที่ต้องได้รับใบอนุญาตก่อน

เหตุผลจำเป็นที่ต้องกำกับดูแล

1. การพิสูจน์และยืนยันตัวตนทางดิจิทัลของบุคคล เป็นกระบวนการสำคัญก่อนทำธุรกรรมออนไลน์ โดยเฉพาะธุรกรรมที่มีความสำคัญ
2. เพื่อให้ธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีมาตรฐาน การให้บริการที่สอดคล้องกัน ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการปลอมแปลงตัวตน การหลอกลวงหรือฉ้อโกง
3. เพื่อดูแลให้ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีธรรมาภิบาลและมาตรฐานในการประกอบธุรกิจที่ดีตลอดทั้งกระบวนการ

หลักการ ร่าง พ.ร.ฎ. ว่าด้วยการควบคุม ดูแลธุรกิจบริการเกี่ยวกับ ระบบการพิสูจน์และยืนยันตัวตน ทางดิจิทัล พ.ศ.

วันใช้บังคับ เมื่อพ้น 180 วัน

รัฐมนตรีรักษาการ สมว. DE

อาศัยอำนาจ ม. 34/3 และ ม. 34/4
ประกอบหมวด 3
กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

หมวด 1 บททั่วไป

- หลักเกณฑ์และเงื่อนไข ที่ผู้ประกอบการต้องปฏิบัติ
- การคำนึงถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคล
- ห้ามผู้ประกอบการทำข้อตกลงกีดกัน/ผูกขาด

หมวด 2 การประกอบธุรกิจบริการเกี่ยวกับ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- กำหนดประเภทบริการที่ต้องขออนุญาต และไม่ต้องขออนุญาต
- กำหนดคุณสมบัติและลักษณะต้องห้ามของผู้ประกอบธุรกิจ
- ขั้นตอนการขออนุญาตและการยื่นเอกสารประกอบ
ที่ผู้ประกอบการต้องดำเนินการ
- กำหนดอายุใบอนุญาต (5 ปี)

หมวด 3 การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- การแจ้งเหตุที่มีความสำคัญของผู้ประกอบธุรกิจต่อสำนักงาน
- รองรับการกำหนดบุคลากรที่จำเป็นต่อการให้บริการของผู้ประกอบธุรกิจ
- หลักเกณฑ์ที่ผู้ประกอบการต้องทำในระหว่างการให้บริการ
- การจัดเก็บข้อมูลและการรายงานของผู้ประกอบธุรกิจ
- การเลิกประกอบธุรกิจ หรือการเพิกถอนใบอนุญาตของผู้ประกอบธุรกิจ
รวมทั้งการจัดการข้อมูล และการคุ้มครองผู้ใช้บริการ
- การดำเนินการเมื่อผู้ประกอบการฝ่าฝืนหลักเกณฑ์ และบทลงโทษ
- การรับรองผลที่ได้กระทำก่อนการเลิกประกอบธุรกิจ

ธุรกิจบริการเกี่ยวกับระบบการพิสูจน์ และยืนยันตัวตนทางดิจิทัลที่กำลังบูม

1. บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service)

ที่ให้บริการการพิสูจน์ตัวตน หรือการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน

☐ “การพิสูจน์ตัวตน” (Identity Proofing Service)

บริการที่ประกอบด้วยกระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น

☐ “การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน” (Authenticator Management Service)

บริการที่ประกอบด้วยกระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น

☐ “บริการยืนยันตัวตน” (Authentication Service)

บริการที่ประกอบด้วยกระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น

2. บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)

ที่เป็นเครือข่ายหรือระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ธุรกิจบริการเกี่ยวกับระบบการพิสูจน์ และยืนยันตัวตนทางดิจิทัลที่กำลังบูม

1. บริการพิสูจน์และยืนยันตัวตน โดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมฯ **(Certification Authority: CA)**
2. บริการพิสูจน์และยืนยันตัวตน ที่บุคคลใช้เพื่อประโยชน์ภายในกิจการของบุคคลหรือนิติบุคคลนั้น **โดยไม่ได้ให้บริการแก่บุคคลภายนอก**
3. บริการพิสูจน์และยืนยันตัวตน ที่ไม่ได้ทำการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลและตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น ตามระดับเงื่อนไขความน่าเชื่อถือที่คณะกรรมการกำหนด **(เช่น Identity Assurance Level 1)**
4. **บริการอื่น ๆ ที่ ครอ. กำหนด**

มาตรฐาน ด้าน Digital ID





ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และ ยืนยันตัวตนทางดิจิทัล

กรอบการทำงาน เลขที่ ขมธอ. 18-2564
ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ ขมธอ. 19-2564
ข้อกำหนดของการยืนยันตัวตน เลขที่ ขมธอ. 20-2564
เวอร์ชัน 2.0

ETDA
สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ขมธอ. 18-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล -
กรอบการทำงาน

DIGITAL IDENTITY -
FRAMEWORK

เวอร์ชัน 2.0

ETDA
สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ขมธอ. 19-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล -
ข้อกำหนดของการพิสูจน์ตัวตน

DIGITAL IDENTITY -
IDENTITY PROOFING REQUIREMENTS

เวอร์ชัน 2.0

ETDA
สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ
และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard
for Electronic Transactions

ขมธอ. 20-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล -
ข้อกำหนดของการยืนยันตัวตน

DIGITAL IDENTITY -
AUTHENTICATION REQUIREMENTS

เวอร์ชัน 2.0

ข้อเสนอแนะมาตรฐาน (ETDA Recommendation) การพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity) เวอร์ชัน 2.0 จำนวน 3 ฉบับ

ขมรอ. 18-2564 กรอบการทำงาน (Framework)

อธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ขมรอ. 19-2564 ข้อกำหนดของการพิสูจน์ตัวตน (Identity Proofing Requirements)

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

ขมรอ. 20-2564 ข้อกำหนดของการยืนยันตัวตน (Authentication Requirements)

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

IAL vs AAL ระดับความน่าเชื่อถือ (Assurance Levels)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level : IAL)

- IAL คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล
- เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง (เช่น บุคคลที่กล่าวอ้างว่าตนเองชื่อ "สมชาย" คือ "สมชาย" ตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา)
- IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด



ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Levels : AAL)

- AAL คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน
- เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง (เช่น บุคคลที่กำลังเข้าใช้บริการ คือ "สมชาย" ตัวจริง ที่กรอกรหัสผ่านถูกต้อง)
- AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด



การพิสูจน์ตัวตน (identity proofing)

การพิสูจน์ตัวตนประกอบด้วยกระบวนการพื้นฐาน 3 กระบวนการ ดังนี้

1. การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

- กระบวนการที่ IdP รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตน
- เพื่อใช้แยกแยะว่าอัตลักษณ์ที่กล่าวอ้างมีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม

2. การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

- กระบวนการที่ IdP ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์
- เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง

3. การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

- กระบวนการที่ IdP ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์ที่กล่าวอ้าง
- เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์จริงของบุคคลที่กำลังพิสูจน์ตัวตน

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน

Identity Assurance Level (IAL)

ระดับ IAL1

- อาจรวบรวมข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted)
- อาจตรวจสอบข้อมูลด้วยวิธีการอื่น ๆ นอกเหนือจากวิธีการในระดับ IAL2 และ IAL3

ระดับ IAL2

- ขอลหลักฐานแสดงตน ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าเป็นข้อมูลของบุคคลที่มีอยู่จริง
- ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์
- สามารถทำได้ทั้ง แบบพบเห็นต่อหน้า (F2F) หรือแบบไม่พบเห็นต่อหน้า (non-F2F) เช่น Kiosk หรือ App
- ในทางปฏิบัติ แบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1, IAL2.2 และ IAL2.3

ระดับ IAL3

- เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้
 - ตรวจสอบกับแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม
 - เปรียบเทียบข้อมูลชีวมิติ (biometric comparison)
- สามารถทำได้แบบพบเห็นต่อหน้า (F2F) เท่านั้น

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่หน่วยงานอื่น
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานสามารถนำไปประยุกต์ใช้ได้

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์						การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์		
IAL3	กรณีใช้บัตรประชาชน			กรณีใช้บัตรประชาชนอิเล็กทรอนิกส์		ตรวจสอบและยืนยัน ช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล	พบเห็นต่อหน้า เท่านั้น	Biometric Comparison กับ ข้อมูลชีวมิติจากชิปหรือข้อมูล ที่น่าเชื่อถือของหลักฐานแสดงตน หรือ ระบบตรวจสอบข้อมูลชีวมิติ ของหน่วยงานรัฐ
	ใช้เครื่อง อ่านบัตร และ สถานะ บัตรประชาชน	ตรวจสอบกับ แหล่งข้อมูลของ หน่วยงานรัฐเพิ่มเติม	ใช้ระบบตรวจสอบ ของกระทรวงมหาดไทย และ ตรวจสอบกับ แหล่งข้อมูลของ หน่วยงานรัฐเพิ่มเติม					
IAL2	IAL2.3	กรณีใช้บัตรประชาชน		กรณีใช้หนังสือเดินทาง		ใช้ระบบตรวจสอบของหน่วยงานรัฐ	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Biometric Comparison กับ ข้อมูลชีวมิติจากชิปหรือข้อมูล ที่น่าเชื่อถือของหลักฐานแสดงตน หรือ ระบบตรวจสอบข้อมูลชีวมิติ ของหน่วยงานรัฐ
		ใช้เครื่อง อ่านบัตร และ สถานะบัตร ประชาชน	ใช้ NFC และ หรือ เอกสารสำคัญอื่น	ใช้ระบบตรวจสอบของหน่วยงานรัฐ				
	IAL2.2	ใช้เครื่อง อ่านบัตร หรือ ผลการยืนยัน ตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC และ หรือ เอกสารสำคัญอื่น		ใช้ระบบตรวจสอบของหน่วยงานรัฐ	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Visual Comparison กับ ภาพใบหน้าจากชิป ของหลักฐานแสดงตน หรือ ภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3
		ใช้เครื่อง อ่านบัตร หรือ ผลการยืนยัน ตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC				
IAL2.1	ใช้เครื่อง อ่านบัตร หรือ ผลการยืนยัน ตัวตนจาก IdP ที่เคยทำ IAL2.3		ใช้ NFC		ใช้ระบบตรวจสอบของหน่วยงานรัฐ	พบเห็นต่อหน้า หรือ ไม่พบเห็นต่อหน้า	Visual Comparison กับ ภาพใบหน้าจากชิป ของหลักฐานแสดงตน หรือ ภาพใบหน้าจาก IdP ที่เคยทำ IAL2.3	
IAL1	อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ โดยไม่จำเป็นต้อง ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ หรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์							
หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญจากข้อเสนอแนะมาตรฐานฯ และแสดงเฉพาะระบบตรวจสอบของหน่วยงานรัฐที่มีอยู่ในปัจจุบัน								

หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญจากข้อเสนอแนะมาตรฐานฯ และแสดงเฉพาะระบบตรวจสอบของหน่วยงานรัฐที่มีอยู่ในปัจจุบัน

สิ่งที่ใช้ยืนยันตัวตน (Authenticator)

- ✓ Authenticator คือ สิ่งที่ใช้บริการครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตนกับ IdP
- ✓ Authenticator มีข้อมูลลับ (secret) ที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นสามารถนำมาใช้ยืนยันตัวตนได้
- ✓ Authenticator อาจประกอบด้วย ปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัย (Single-Factor) หรือประกอบด้วยปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย (Multi-Factor) ก็ได้

ทั้งนี้ **ปัจจัยของการยืนยันตัวตน (Authentication Factor)** แบ่งเป็น 3 ประเภท

1) สิ่งที่คุณรู้ (something you know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ

- เช่น รหัสผ่าน (password) และเลขรหัสส่วนตัว (PIN)

2) สิ่งที่คุณมี (something you have) คือ สิ่งของที่ผู้ใช้บริการเท่านั้นครอบครอง

- เช่น กุญแจเข้ารหัส (cryptographic key) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) และ อุปกรณ์ OTP (OTP device)

3) สิ่งที่คุณเป็น (something you are) คือ ข้อมูลชีวมิติ (biometric data) ของผู้ใช้บริการ

- เช่น ใบหน้า ลายนิ้วมือ หรือม่านตา



ระดับความน่าเชื่อถือของการยืนยันตัวตน

Authentication Assurance Level (AAL)

ระดับ AAL1

- การยืนยันตัวตนแบบปัจจัยเดียว (Single-Factor Authentication)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย

ระดับ AAL2

- การยืนยันตัวตนด้วยปัจจัยที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย (Multi-Factor Authentication)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย

ระดับ AAL3

- การยืนยันตัวตนด้วยปัจจัยที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย (Multi-Factor Authentication)
- ใช้สิ่งที่ใช้ยืนยันตัวตนที่เป็นฮาร์ดแวร์ (hardware based) และบสสุญญาแจะเข้ารหัส (cryptographic key)
- ใช้ authentication protocol ที่มั่นคงปลอดภัย และใช้เกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol)

อนึ่ง ชีวมิต (biometrics) ต้องใช้เป็น "ปัจจัยร่วม" ของการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี) เท่านั้น

เนื่องจากหากตรวจพบว่าผู้ใช้บริการเป็นตัวปลอมหรือสงสัยว่ามีการใช้งานในทางที่ผิด IdP สามารถเพิกถอนอุปกรณ์นั้น ทดแทนการเพิกถอนข้อมูลชีวมิติ

ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่หน่วยงานอื่น
อย่างไรก็ตาม หน่วยงานที่พิสูจน์และยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานสามารถนำไปประยุกต์ใช้ได้

ข้อกำหนดของการยืนยันตัวตน			ชนิดของสิ่งที่ใช้ยืนยันตัวตน ที่สามารถใช้ได้					
AAL3	 ยืนยันตัวตนแบบ Multi-factor authentication และใช้สิ่งที่ใช้ยืนยันตัวตนเป็น Hardware และมี Cryptographic key	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร  สามารถป้องกันการโจมตีแบบส่ง ข้อมูลซ้ำ (replay resistance)  สามารถป้องกันการ IdP ตัวปลอม (IdP impersonation resistance)	 MF Crypto Device	 Memorized Secret และ  SF Crypto Device	 MF OTP Device และ  SF Crypto Device	 MF OTP Device และ  SF Crypto Software	 SF OTP Device และ  MF Crypto Software	 Memorized Secret และ  SF OTP Device  SF Crypto Software
	 ยืนยันตัวตนแบบ Multi-factor authentication	 สามารถป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) จากช่องทางการสื่อสาร  สามารถป้องกันการโจมตีแบบส่ง ข้อมูลซ้ำ (replay resistance)	 Memorized Secret และ  SMS OTP 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	