การประชุมเชิงปฏิบัติการ

แนวทางการจัดทำร่างหลักเกณฑ์

ภายใต้ร่างพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. .... (ร่าง พ.ร.ฎ.ฯ)

1. ที่มา สถานะ และความจำเป็น ร่าง พ.ร.ฎ.ฯ

ที่มา กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 34/4 ประกอบกับหมวด 3

ในกรณีจำเป็น ให้มีการตราพระราชกฤษฎีกาเพื่อกำหนดให้การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลใด เป็นธุรกิจบริการที่ต้องได้รับใบอนุญาตก่อน

สถานะ ครม. มีมติเมื่อวันที่ 22 กันยายน 2563

เห็นชอบในหลักการร่างพระราชกฤษฎีกาฯ และให้ส่ง สคก. ตรวจพิจารณาโดยรับความเห็นหน่วยงานที่เกี่ยวข้องไปประกอบการพิจารณา

ความจำเป็นที่ต้องกำกับดูแล

1. Digital Identity เป็นปัจจัยที่จะทำให้การขับเคลื่อนธุรกรรมออนไลน์เกิดขึ้นได้
   โดยผู้ใช้บริการสามารถรับบริการจากรัฐหรือเอกชนผ่านทางออนไลน์ได้อีกช่องทางหนึ่ง
   เพิ่มความสะดวก ประหยัดเวลา และลดค่าใช้จ่าย
2. เป็นธุรกิจบริการฯ ที่เกี่ยวข้องกับ Digital Identity ของบุคคล
   เกี่ยวข้องกับตัวตนของผู้ใช้งาน และเกี่ยวโยงไปถึงสิทธิหน้าที่ที่ตามมาของบุคคลดังกล่าว
3. การกำกับดูแลธุรกิจบริการเกี่ยวกับ Digital Identity ที่ได้มาตรฐาน
   จะช่วยลดความเสี่ยง เช่น การปลอมแปลงตัวตน หลอกลวง หรือฉ้อโกง
   และได้ข้อสันนิษฐานตามกฎหมายว่าเป็นบุคคลนั้นจริง
4. เมื่อธุรกิจบริการเกี่ยวกับ Digital Identity ได้มาตรฐาน จะสร้างความเชื่อมั่น
   ในการใช้งานให้กับผู้ที่เกี่ยวข้อง
   - เจ้าของ Digital Identity ที่ไม่ต้องการให้มีคนอื่นปลอมตัวตนมาทำธุรกรรมออนไลน์แทน
   - RP ที่ไม่ได้พิสูจน์และยืนยันตัวตนเจ้าของ Digital Identity ด้วยตนเอง
     แต่ได้อาศัยผลการพิสูจน์และยืนยันตัวตนของ IDP ก่อน RP ให้สิทธิและหน้าที่แก่เจ้าของ ID ในการทำธุรกรรม
   - IDP ต้องพิสูจน์และยืนยันตัวตนเจ้าของ ID เพื่อให้แน่ใจว่าเป็นบุคคลคนนั้นจริง
     ก่อนให้บริการผลการพิสูจน์และยืนยันตัวตนแก่ผู้อื่น (RP)
   - Platform ที่เป็นระบบเชื่อมโยงผู้ที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตน

2. ธุรกิจบริการที่กำกับดูแลตามร่าง พ.ร.ฎ.ฯ

2.1 บริการพิสูจน์และยืนยันตัวตน (Identity Provider Service : IdP)

ที่ให้บริการการพิสูจน์ตัวตน หรือการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน

- ❑ **“การพิสูจน์ตัวตน” (Identity Proofing Service)**
  บริการที่ประกอบด้วยกระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับไอเดนทิตี และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับไอเดนทิตีนั้น
- ❑ **“การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน” (Authenticator Management Service)**
  บริการที่ประกอบด้วยกระบวนการเชื่อมโยงไอเดนทิตีของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น
- ❑ **“บริการยืนยันตัวตน” (Authentication Service)**
  บริการที่ประกอบด้วยกระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันไอเดนทิตีของบุคคลที่ใช้สิ่งที่ใช้ยืนยัน ตัวตนนั้น

2.2 บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)

ที่เป็นเครือข่ายหรือระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

บริการที่ได้รับการยกเว้นไม่กำกับ

1. บริการพิสูจน์และยืนยันตัวตน
   โดยผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์
   ตามกฎหมายว่าด้วยธุรกรรมฯ
   (Certification Authority: CA)

2. บริการพิสูจน์และยืนยันตัวตน
   ที่บุคคลใช้เพื่อประโยชน์ภายในกิจการของบุคคลหรือนิติบุคคลนั้น
   โดยไม่ได้ให้บริการแก่บุคคลภายนอก

3. บริการพิสูจน์และยืนยันตัวตน
   ที่ไม่ได้ทำการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และ
   ไม่ได้ตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัต
   ลักษณ์นั้น
   ตามระดับเงื่อนไขความน่าเชื่อถือที่คณะกรรมการกำหนด
   (เช่น Identity Assurance Level 1)

4. **บริการอื่น ๆ ที่ คธอ. กำหนด**

3. หลักการ ร่าง พ.ร.ฎ.ฯ พร้อมหลักเกณฑ์และมาตรฐานที่ต้องกำหนด

วันใช้บังคับ เมื่อพ้น 180 วัน

รัฐมนตรีรักษาการ รมว. DE

หมวด 1 บททั่วไป

- หลักเกณฑ์และเงื่อนไข ที่ผู้ประกอบธุรกิจต้องปฏิบัติ
- การคำนึงถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคล
- ห้ามผู้ประกอบธุรกิจทำข้อตกลงกีดกัน/ผูกขาด

หมวด 2 การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- กำหนดประเภทบริการที่ต้องขออนุญาต และไม่ต้องขออนุญาต
- กำหนดคุณสมบัติและลักษณะต้องห้ามของผู้ประกอบธุรกิจ
- ขั้นตอนการขออนุญาตและการยื่นเอกสารประกอบที่ผู้ประกอบธุรกิจต้องดำเนินการ
- กำหนดอายุใบอนุญาต (5 ปี)

หมวด 3 การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

- การแจ้งเหตุที่มีความสำคัญของผู้ประกอบธุรกิจต่อสำนักงาน
- รองรับการกำหนดบุคลากรที่จำเป็นต่อการให้บริการของผู้ประกอบธุรกิจ
- หลักเกณฑ์ที่ผู้ประกอบธุรกิจต้องทำในระหว่างการให้บริการ
- การจัดเก็บข้อมูลและการรายงานของผู้ประกอบธุรกิจ
- การเลิกประกอบธุรกิจ หรือการเพิกถอนใบอนุญาตของผู้ประกอบธุรกิจ รวมทั้งการจัดการข้อมูล และการคุ้มครองผู้ใช้บริการ
- การดำเนินการเมื่อผู้ประกอบธุรกิจฝ่าฝืนหลักเกณฑ์ และบทลงโทษ
- การรับรองผลที่ได้กระทำก่อนการเลิกประกอบธุรกิจ

หลักเกณฑ์และมาตรฐานที่ต้องกำหนด
ภายใต้กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ETA) และร่าง พ.ร.ฎ.ฯ

3.1 ETA

มาตรฐานเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดา และนิติบุคคล

- ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level) หรือ IAL
- ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level) หรือ AAL

3.2 ร่าง พ.ร.ฎ.ฯ

(1) ขั้นตอนการขออนุญาต (ลำดับที่ 1-4)

(2) ขั้นตอนระหว่างการให้บริการ (ลำดับที่ 5-10)

Digital ID Management Rule (ลำดับที่ 5-6)

การจัดเก็บและรายงานข้อมูลสำคัญ (ลำดับที่ 7-10)

(3) ขั้นตอนรองรับกรณีเลิกหรือเพิกถอนการให้บริการ (ลำดับที่ 11-13)

ลำดับ	เรื่อง	Control
1	สัดส่วนการถือหุ้น / ทุนจดทะเบียนของผู้ยื่นคำขอ (ม.11 ว.2)	หลักเกณฑ์การขออนุญาตและการพิจารณาอนุญาต
2	คุณสมบัติ / ลักษณะต้องห้าม ของผู้ยื่นคำขอ + กรรมการ กรณีเพิ่มเติม (ม. 12 (13))	หลักเกณฑ์การขออนุญาตและการพิจารณาอนุญาต
3	เอกสารประกอบคำขอ กรณีเพิ่มเติม (ม.13 ว.2)	อิงตามข้อ 5
4	ขั้นตอนการขออนุญาต / การพิจารณาอนุญาต / ค่าธรรมเนียม (ม.14) การขอต่ออายุใบอนุญาต (ม.16) / การขอใบแทนใบอนุญาต (ม.17)	หลักเกณฑ์การขออนุญาตและการพิจารณาอนุญาต
5	หลักเกณฑ์การให้บริการ (ม.21) • สิทธิ หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจ • มาตรการบริหารและจัดการความเสี่ยงของระบบ • มาตรการรักษาความมั่นคงปลอดภัยของระบบและการตรวจสอบ • มาตรการควบคุมและดูแลการทุจริตหรือการฉ้อโกงเกี่ยวกับกระบวนการพิสูจน์และยืนยันตัวตน • มาตรฐานการให้บริการ ซึ่งรวมถึงการจัดการและจัดเก็บข้อมูล • การจัดการกรณีฉุกเฉิน และกรณีมีเหตุการณ์ที่กระทบกับระบบการให้บริการ • การคุ้มครองผู้ใช้บริการ มาตรการบรรเทาความเสียหายและการชดใช้หรือเยียวยาผู้ได้รับความเสียหาย • การใช้บริการจากบุคคลภายนอก • การดูแลฐานะทางการเงินและผลการดำเนินงาน • การบริหารงานตามหลักธรรมาภิบาล • การจัดทำบัญชี การส่งงบแสดงฐานะทางการเงิน และผลการดำเนินงานต่อสำนักงาน • การเปิดเผยข้อมูลเกี่ยวกับการให้บริการ • การกำหนดค่าธรรมเนียมการให้บริการ	• **Fraud Control** • **Security Control** • **Privacy Control** • **Role Requirements for IdP & Digital Platform Service** • **User terms & User Experience Requirements**
6	บุคลากรและคุณสมบัติของบุคลากรที่จำเป็นในการให้บริการ (ม.20)	อิงตามข้อ 5

ลำดับ	เรื่อง	
7	การจัดเก็บข้อมูล (ม. 22)	อิงตามข้อ 5
8	การส่งข้อมูลรายงาน (ม.23)	อิงตามข้อ 5
9	การแจ้งการเปลี่ยนแปลงข้อมูลสำคัญ (ม.18 ว.2) • กรรมการหรือผู้มีอำนาจในการจัดการ • ทุนจดทะเบียนหรือการถือหุ้น • บุคลากร	-
10	การรายงานเรื่องร้องเรียน / การฟ้องร้อง (ม.19)	-
11	หลักเกณฑ์ที่ต้องปฏิบัติ ขณะถูกพักใช้ + เลิกประกอบธุรกิจ (ม.26 ว.5)	• **Role Requirements for IdP & Digital Platform Service**
12	การเลิกประกอบธุรกิจ (ม.26 ว.5)	
13	การป้องกันความเสียหาย และการคุ้มครองประโยชน์หลังเพิกถอนหรือเลิกประกอบธุรกิจ (ม.29)	

Fraud Control

วัตถุประสงค์

เพื่อป้องกันความเสี่ยงด้านการฉ้อโกงหรือทุจริตในกระบวนการพิสูจน์และยืนยันตัวตน
ที่อาจเกิดขึ้น ซึ่งครอบคลุมมาตรการเชิงป้องกัน รับมือ และจัดการผลกระทบของเหตุการณ์ที่เกิดขึ้น

หลักการ

- บทบาทของคณะกรรมการและผู้บริหารในการควบคุม
  และดูแลการทุจริตหรือการฉ้อโกง
- นโยบายการป้องกันและจัดการการฉ้อโกงหรือทุจริต และ
  การบริหารความเสี่ยงด้านการฉ้อโกงหรือทุจริต
- การส่งเสริมมาตรการป้องกันการฉ้อโกงหรือทุจริต
  แก่บุคลากรและผู้ใช้บริการ
- กระบวนการติดตาม เฝ้าระวัง และบริหารจัดการเหตุการณ์
  การฉ้อโกงหรือทุจริตที่เกิดหรือคาดว่าจะเกิดขึ้น
- มาตรการดูแลผู้ใช้บริการที่ได้รับผลกระทบจากเหตุการณ์
  ฉ้อโกงหรือทุจริตที่เกิดขึ้น

Role Requirements

Identity Provider Service

วัตถุประสงค์ในการพิสูจน์ตัวตน

- แยกไอเดนติตี้ของผู้ใช้บริการจากผู้ใช้บริการรายอื่น
- ยืนยันความถูกต้องและแท้จริงของไอเดนติตี้
- ยืนยันความถูกต้องในการเชื่อมโยงของไอเดนติตี้กับผู้ใช้บริการ
- ยืนยันว่าไอเดนติตี้นั้นไม่ถูกปลอมหรือถูกใช้สำหรับฉ้อโกงหรือทุจริต

วัตถุประสงค์ในการยืนยันตัวตน

ตรวจสอบและยืนยันว่า Authenticator ที่ใช้งานถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอนก่อนการยืนยันตัวตนของผู้ใช้บริการ

หลักการ

- ได้พิสูจน์และยืนยันตัวตนตามเงื่อนไขเกี่ยวกับความน่าเชื่อถือตามมาตรฐานที่กำหนด พร้อมจัดทำแนวนโยบายและแนวปฏิบัติเกี่ยวกับการพิสูจน์ตัวตนที่ชัดเจน และครอบคลุมกรณีที่มีเหตุขัดข้องตามมาตรการบริหารความเสี่ยง
- มีกระบวนการเชื่อมโยง ID ด้วย Biometric โดยเทคโนโลยีที่มีประสิทธิภาพ พร้อมการจัดการข้อมูลและจัดเก็บ Biometric ที่เหมาะสม
- มีกระบวนการในการดูแลภาพที่ได้มาให้มีคุณภาพ
- มีกระบวนการป้องกันการปลอมแปลงข้อมูลชีวมิติ (Presentation Attack Detection) ด้วยเทคโนโลยีที่มีประสิทธิภาพ
- มีการตรวจสอบธุรกรรมที่ผิดปกติ (Unusual Transaction) พร้อมมีการตรวจสอบหรือสอบทานความถูกต้องของกระบวนการในการพิสูจน์และยืนยันตัวตน
- มีช่องทางรองรับการให้บริการแก่ผู้ใช้บริการ เช่น การปรับปรุงข้อมูล การแจ้งระงับการใช้งาน ID
- การจัดเก็บข้อมูลที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

Role Requirements

Digital Identity Platform Service

หลักการ

- การเปิดเผยข้อมูลการให้บริการแก่สมาชิกก่อนการใช้บริการ
- การจัดเก็บข้อมูลสำคัญ เช่น ความยินยอม หรือบันทึกกิจกรรมการพิสูจน์และยืนยันตัวตน โดยผู้ให้บริการของ Platform
- ข้อกำหนดด้านความสอดคล้องของระบบ เพื่อประโยชน์ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
- การกำหนดรูปแบบ (format) ของข้อมูลคุณลักษณะหรือชุดข้อมูลคุณลักษณะ (Attribute Profile) ที่ใช้ในการพิสูจน์และยืนยันตัวตน
- ข้อมูลทางเทคนิคที่จำเป็นสำหรับการเชื่อมต่อกับระบบ และมีการทดสอบทางเทคนิคร่วมกัน
- มีช่องทางรองรับการให้บริการแก่ผู้ใช้บริการในการตรวจสอบประวัติการใช้งาน