(ร่าง)

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง หลักเกณฑ์การประกอบธุรกิจบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(Digital Identity Platform Service)

พ.ศ. ....

.....

.....

.....

.....

.....

.....

.....

.....

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์การประกอบธุรกิจบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service) พ.ศ. ....”

ข้อ ๒ ในประกาศนี้

“ระบบ” หมายความว่า ระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล

“ผู้ประกอบธุรกิจ” หมายความว่า ผู้ให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service) ตามพระราชกฤษฎีกา

“สมาชิก” หมายความว่า ผู้ที่เชื่อมต่อกับระบบของผู้ประกอบธุรกิจ

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของสมาชิก

“คำขอ (authentication request)” หมายความถึง คำขอสำหรับการยืนยันตัวตน

"พระราชกฤษฎีกา" หมายความว่า พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ....

หมวด ๑
หน้าที่ทั่วไป

ข้อ ๓ ในการติดต่อหรือให้บริการ ผู้ประกอบธุรกิจต้องเปิดเผยข้อมูลการให้บริการแก่สมาชิกและผู้ที่ประสงค์จะเป็นสมาชิกเพื่อใช้เป็นข้อมูลประกอบการตัดสินใจเลือกใช้บริการและพิจารณาความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการดังกล่าว โดยอย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(๑) ข้อมูลโดยทั่วไปของผู้ประกอบธุรกิจ

(๒) ลักษณะ ขอบเขต และเงื่อนไขการให้บริการ

(๓) ช่องทางการให้บริการ และการติดต่อสื่อสาร

(๔) สิทธิ หน้าที่ ความรับผิดชอบ และเงื่อนไขที่สมาชิกมีหรือต้องปฏิบัติเมื่อใช้บริการ

(๕) ความขัดแย้งทางผลประโยชน์ (ถ้ามี)

(๖) วิธีปฏิบัติระหว่างผู้ประกอบธุรกิจกับสมาชิก ไม่ว่าจะเป็นตามกฎหมาย ประกาศที่เกี่ยวข้อง และวิธีปฏิบัติที่ผู้ประกอบธุรกิจกำหนดขึ้น

ข้อ ๔ ผู้ประกอบธุรกิจต้องจัดเก็บข้อมูลอย่างน้อยในเรื่องดังต่อไปนี้

(๑) ความยินยอมเกี่ยวกับการเปิดเผยข้อมูลของผู้ใช้บริการที่ให้แก่สมาชิก

(๒) ประวัติกิจกรรมการโต้ตอบ (interactions) เกี่ยวกับการพิสูจน์และยืนยันตัวตนที่เกิดขึ้นระหว่างผู้ที่เกี่ยวข้อง เช่น การส่งคำขอ และการตอบกลับ (response) ระหว่าง Platform กับ Identity Provider, Relying Party หรือ Authoritative Source เป็นต้น

ข้อ ๕ การบันทึกความยินยอมของผู้ใช้บริการตามข้อ ๔ (๑) ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

(๑) การประทับเวลา (timestamp)

(๒) สมาชิกที่เกี่ยวข้องกับการขอและส่งข้อมูล

(๓) ชื่อรายการข้อมูลคุณลักษณะ (name of attribute) ที่เกี่ยวข้องกับการเปิดเผยข้อมูล เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ เป็นต้น

(๔) การตัดสินใจของผู้ใช้บริการ เช่น ยินยอม ไม่ยินยอม เป็นต้น

ข้อ ๖ การบันทึกประวัติกิจกรรมการโต้ตอบ (interactions) ตามข้อ ๔ (๒) ต้องประกอบด้วยข้อมูลอย่างน้อยต้องดังต่อไปนี้

(๑) การประทับเวลา (timestamp)

(๒) ประเภทกิจกรรมการโต้ตอบ (interaction type) เช่น การส่งคำขอ การตอบกลับ เป็นต้น

(๓) รหัสเฉพาะของคำขอ (unique request id)

(๔) สมาชิกที่เกี่ยวข้อง

(๕) ชื่อรายการข้อมูลคุณลักษณะ (name of attribute)

(๖) ระดับความน่าเชื่อถือที่ใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๗) สถานะของคำขอ เช่น อนุมัติ อยู่ระหว่างดำเนินการ ปฏิเสธ เป็นต้น

หมวด ๒
ข้อกำหนดด้านความสอดคล้องของระบบ

ข้อ ๗ ผู้ประกอบธุรกิจต้องจัดให้มีระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่สมาชิกสามารถใช้งานร่วมกันได้ โดยต้องมีความสอดคล้องของระบบอย่างน้อยในเรื่องดังต่อไปนี้

(๑) เงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Assurance level)

(๒) การบันทึกประวัติกิจกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนที่เกิดขึ้นระหว่างผู้ที่เกี่ยวข้อง (Auditing & logging)

(๓) โพรโทคอล (Protocol) สำหรับเชื่อมโยงคำขอและการตอบกลับ (response) ระหว่างสมาชิก (Protocol mapping requirements)

ข้อ ๘ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้ประกอบธุรกิจต้องดำเนินการตามเงื่อนไขเกี่ยวกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่คณะกรรมการประกาศกำหนด

ข้อ ๙ ผู้ประกอบธุรกิจต้องจัดให้มีรายชื่อของสมาชิกประกอบการเลือกใช้บริการ โดยมีการจำแนกระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีการให้บริการของสมาชิกแต่ละราย

ข้อ ๑๐ การบันทึกประวัติกิจกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตน ให้ผู้ประกอบธุรกิจกำหนดรหัสเฉพาะของคำขอ (unique request id) สำหรับคำขอทุกรายการที่มาจาก RP หรือ AS และจัดเก็บข้อมูลจราจรทางอิเล็กทรอนิกส์ (log) ของกิจกรรมที่เกิดขึ้นระหว่างสมาชิกซึ่งใช้รหัสเฉพาะของคำขอ (unique request id) เดียวกัน

ข้อ ๑๑ ในการกำหนดโพรโทคอล (Protocol) สำหรับเชื่อมโยงคำขอ และการตอบกลับ (response) ต้องสามารถเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยสมาชิกผู้ส่งคำขอได้ และสามารถเชื่อมโยงการตอบกลับ (response) ไปยังคำขอต้นทางได้ (original Authentication Request) โดยอย่างน้อยต้องสามารถเชื่อมโยงและจับคู่ (mapping) รายการต่อไปนี้เข้าด้วยกันได้อย่างถูกต้องและครบถ้วน

(๑) รายการข้อมูลคุณลักษณะหรือชุดข้อมูลคุณลักษณะ (Attribute Profile) ในคำขอและการตอบกลับ

(๒) ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (assurance levels)

ข้อ ๑๒ ผู้ประกอบธุรกิจต้องจัดให้มีกระบวนการที่สมาชิกผู้ส่งคำขอสามารถคัดแยก IdP ที่มีความสามารถในระดับที่สอดคล้องตามคำขอของสมาชิกได้

ข้อ ๑๓ ผู้ประกอบธุรกิจต้องจัดให้มีการกำหนดรูปแบบ (format) ของข้อมูลคุณลักษณะหรือชุดข้อมูลคุณลักษณะ (Attribute Profile) ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบของผู้ประกอบธุรกิจ

ข้อ ๑๔ ผู้ประกอบธุรกิจต้องจัดทำนโยบายการเปิดเผยข้อมูลคุณลักษณะ (attribute sharing policy) ที่สอดคล้องกับข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Control) และประกาศให้ผู้เกี่ยวข้องได้รับทราบเป็นการทั่วไป

หมวด ๓
ข้อกำหนดด้านเทคนิค

ข้อ ๑๕ ผู้ประกอบธุรกิจต้องจัดเตรียมข้อมูลทางเทคนิคที่จำเป็นสำหรับการเชื่อมต่อกับระบบของผู้ประกอบธุรกิจและแจ้งให้สมาชิกทราบ เพื่อประโยชน์แก่สมาชิกในการเข้าใช้บริการ

ข้อ ๑๖ ผู้ประกอบธุรกิจต้องจัดให้มีแผนการทดสอบ (Testing Plan) ที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Security Policy) และเป็นไปตามที่ประกาศกำหนด

ข้อ ๑๗ ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบทางเทคนิค และรายงานผลการทดสอบต่อสำนักงาน ตามที่ประกาศกำหนด

ข้อ ๑๘ ก่อนเริ่มให้บริการแก่ผู้ที่ประสงค์จะเข้าเป็นสมาชิก ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการใช้งานร่วมกันกับผู้ประสงค์จะเข้าเป็นสมาชิกรายดังกล่าวตามที่ประกาศกำหนด และรายงานผลการทดสอบต่อสำนักงาน

ข้อ ๑๙ หากผู้ที่ประสงค์จะเข้าเป็นสมาชิกรายใด ไม่สามารถทดสอบการใช้งานร่วมกันกับผู้ประกอบธุรกิจได้ หรือผลการทดสอบไม่สามารถดำเนินการได้โดยสมบูรณ์ ให้ผู้ประกอบธุรกิจปฏิเสธการให้บริการ

หมวด ๔
การดูแลผู้ใช้บริการ

ข้อ ๒๐ ผู้ประกอบธุรกิจต้องจัดให้มีวิธีการหรือช่องทางที่ผู้ใช้บริการสามารถตรวจสอบประวัติการใช้งาน (User Dashboard) และสามารถบริหารจัดการความยินยอมของผู้ใช้บริการได้

ประวัติการใช้งานตามวรรคหนึ่งให้ประกอบด้วยรายการอย่างน้อย ดังต่อไปนี้

(๑) ประวัติกิจกรรมที่ดำเนินการกับ IdP กรณีที่ได้ดำเนินการผ่านระบบของผู้ประกอบธุรกิจ

(๒) ประวัติการให้ความยินยอมในการเปิดเผยข้อมูล

ทั้งนี้ ประวัติการใช้งานดังกล่าว ต้องไม่มีการบันทึกข้อมูลส่วนบุคคลของผู้ใช้บริการ

ประกาศ ณ วันที่ .. .. พ.ศ. ๒๕๖๔

(.....)
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์