ข้อกำหนดแนบท้ายประกาศ สพธอ. ที่ ธพส. ๑/๒๕๖๖
ฉบับที่ ๖
หลักเกณฑ์ตามลักษณะของการให้บริการ

หมวด ๑
บริการพิสูจน์ตัวตน บริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และบริการยืนยันตัวตน

ส่วนที่ ๑ การพิสูจน์ตัวตน

ข้อ ๑ ผู้รับใบอนุญาตต้องบริหารจัดการกระบวนการพิสูจน์ตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ

ข้อ ๒ ในการให้บริการพิสูจน์ตัวตนผู้รับใบอนุญาตต้องมีกระบวนการที่ครอบคลุมการทำงานอย่างน้อยในเรื่องดังต่อไปนี้

๒.๑ ต้องจัดให้ผู้ใช้บริการสามารถปรับปรุงข้อมูลเกี่ยวกับอัตลักษณ์ของตนซึ่งถูกจัดเก็บในกระบวนการพิสูจน์ตัวตนได้ โดยต้องจัดให้มีกระบวนการตรวจสอบที่เกี่ยวข้องอย่างน้อยดังนี้

๒.๑.๑ ตรวจสอบข้อมูลที่ขอปรับปรุงก่อนที่จะบันทึกการเปลี่ยนแปลงข้อมูลในระบบการให้บริการ รวมถึงกรณีที่มีการเปลี่ยนแปลงสถานะของอัตลักษณ์ดิจิทัลนั้น เช่น การระงับชั่วคราว การใช้งานใหม่

๒.๑.๒ ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติต้องมีการตรวจสอบว่าอัตลักษณ์ดิจิทัลนั้นยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง

๒.๒ ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานชั่วคราว หรือยุติการใช้งานอัตลักษณ์ดิจิทัล ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อยดังนี้

๒.๒.๑ มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ

๒.๒.๒ ป้องกันไม่ให้มีการใช้งานอัตลักษณ์ดิจิทัลตามคำขอ

๒.๒.๓ มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานอัตลักษณ์ดิจิทัลได้ พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน

ข้อ ๓ กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๓.๑ ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตนที่สูงกว่าให้ครบถ้วน

๓.๒ ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตน

๓.๓ เมื่อดำเนินการยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการพิสูจน์ตัวตนดังกล่าว เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ

ข้อ ๔ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลผู้ใช้บริการอย่างน้อยดังนี้

๔.๑ ต้องรวบรวมหรือจัดเก็บข้อมูลเพื่อการพิสูจน์ตัวตนเพียงเท่าที่จำเป็น เหมาะสม และตรงตามวัตถุประสงค์ของการให้บริการ

๔.๒ ต้องจำกัดการเปิดเผยข้อมูลอัตลักษณ์ของผู้ใช้บริการต่อบุคคลอื่นเพื่อใช้ในการพิสูจน์ตัวตนตามที่ได้รับความยินยอมจากผู้ใช้บริการ เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

ส่วนที่ ๒ การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน

ข้อ ๕ ผู้รับใบอนุญาตต้องบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและกระบวนการยืนยันตัวตนให้สอดคล้องตามลักษณะและระดับความเสี่ยงของธุรกรรมหรือการประกอบธุรกิจ

ข้อ ๖ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนให้พิจารณาตามข้อกำหนดของการยืนยันตัวตนภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งครอบคลุมกระบวนการอย่างน้อยดังนี้

๖.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

๖.๒ การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน

๖.๓ การหมดอายุและการออกใหม่

๖.๔ การเพิกถอน หรือยุติการใช้งาน

ข้อ ๗ ชนิดของสิ่งที่ใช้ยืนยันตัวตนและข้อกำหนดเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนให้พิจารณาตามข้อกำหนดของการยืนยันตัวตนภายใต้มาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งครอบคลุมหัวข้ออย่างน้อยดังนี้

๗.๑ ชนิดของสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

๗.๒ ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

ข้อ ๘ ก่อนดำเนินการยืนยันตัวตนผู้รับใบอนุญาตต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนอย่างน้อยดังนี้

๘.๑ ตรวจสอบให้แน่ใจว่าสิ่งที่ใช้ยืนยันตัวตนที่แสดงนั้นถูกต้อง ใช้งานได้ และยังไม่หมดอายุหรือถูกเพิกถอน

๘.๒ ในกรณีที่ตรวจพบการทำธุรกรรมที่ผิดปกติต้องมีการตรวจสอบว่าสิ่งที่ใช้ยืนยันตัวตนนั้นยังอยู่ภายใต้ความควบคุมของเจ้าของอัตลักษณ์ดิจิทัลที่แท้จริง

ข้อ ๙ ในกรณีที่ผู้ใช้บริการร้องขอให้ระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนชั่วคราวหรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน ผู้รับใบอนุญาตต้องจัดให้มีกระบวนการอย่างน้อยดังนี้

๙.๑ มีการตรวจสอบความถูกต้องของคำขอก่อนที่จะดำเนินการตามคำขอ

๙.๒ มีการแจ้งให้ผู้ใช้บริการทราบว่าไม่สามารถใช้งานสิ่งที่ใช้ยืนยันตัวตนได้พร้อมระบุเหตุผล เช่น ระงับการใช้งานชั่วคราว ยุติการใช้งาน

ข้อ ๑๐ กรณีที่ระบบการให้บริการรองรับการยกระดับความน่าเชื่อถือของการยืนยันตัวตนผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๑๐.๑ ต้องดำเนินการให้สอดคล้องตามข้อกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตนที่สูงกว่าให้ครบถ้วน

๑๐.๒ ต้องจัดให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้นก่อนเริ่มกระบวนการยกระดับความน่าเชื่อถือของการยืนยันตัวตน

๑๐.๓ เมื่อดำเนินการยกระดับความน่าเชื่อถือของการยืนยันตัวตนเสร็จสิ้น ต้องส่งการแจ้งเตือนผู้ใช้บริการทราบผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้ยกระดับความน่าเชื่อถือของการยืนยันตัวตน เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ

ส่วนที่ ๓ การเชื่อมโยงและแลกเปลี่ยนข้อมูล

ข้อ ๑๑ ผู้รับใบอนุญาตต้องกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) สำหรับเชื่อมโยงคำขอและการตอบกลับ โดยต้องสามารถเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอได้และสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ ซึ่งต้องมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ

ข้อ ๑๒ ผู้รับใบอนุญาตต้องจัดให้มีนโยบายเกี่ยวกับการเปิดเผยข้อมูลอัตลักษณ์ที่สอดคล้องกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลและประกาศให้ผู้ที่เกี่ยวข้องได้รับทราบเป็นการทั่วไป

ข้อ ๑๓ ผู้รับใบอนุญาตต้องจัดให้มีรายการข้อมูลอัตลักษณ์ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลในระบบการให้บริการ โดยต้องมีชุดข้อมูลขั้นต่ำที่สามารถระบุตัวผู้ใช้บริการได้อย่างชัดเจนประกอบด้วย

๑๓.๑ เลขประจำตัวประชาชน

๑๓.๒ ชื่อ นามสกุล ภาษาไทย

๑๓.๓ ชื่อ นามสกุล ภาษาอังกฤษ (ถ้ามี)

๑๓.๔ วัน เดือน ปี เกิด

๑๓.๕ ที่อยู่ตามบัตรประจำตัวประชาชน

ข้อ ๑๔ ในกรณีที่ดำเนินการยืนยันตัวตนสำเร็จและมีการตอบกลับไปยังคำขอต้นทาง ผู้รับใบอนุญาตต้องดำเนินการอย่างน้อยดังนี้

๑๔.๑ ผลการยืนยันตัวตนประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ

๑๔.๒ ต้องจัดให้มีการรักษาความลับของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในกระบวนการดังกล่าวเพื่อให้มั่นใจว่าเฉพาะบุคคลที่เกี่ยวข้องและมีสิทธิเท่านั้นที่สามารถเข้าถึงข้อมูลได้

๑๔.๓ ต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัยเพื่อรักษาความครบถ้วนของผลหรือข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตน

ข้อ ๑๕ ห้ามมิให้ผู้รับใบอนุญาตส่งข้อมูลที่ใช้สำหรับการตรวจสอบสถานะของหลักฐานแสดงตนให้กับบุคคลอื่น โดยข้อมูลดังกล่าวได้แก่

๑๕.๑ เลขคำร้องขอมีบัตรประจำตัวประชาชน

๑๕.๒ หมายเลขชิปบัตรประจำตัวประชาชน

๑๕.๓ เลขควบคุมหลังบัตรประจำตัวประชาชน (เลเซอร์ ไอดี (laser ID))

เว้นแต่เป็นกรณีที่ผู้รับใบอนุญาตต้องปฏิบัติตามที่กฎหมายกำหนด

ส่วนที่ ๔ การพิสูจน์และยืนยันตัวตนโดยใช้เทคโนโลยีชีวมิติ

ข้อ ๑๖ ในกรณีที่ผู้รับใบอนุญาตมีการใช้งานข้อมูลชีวมิติในกระบวนการพิสูจน์และยืนยันตัวตนต้องมีการดำเนินการอย่างน้อยดังนี้

๑๖.๑ ต้องจัดให้มีการกำกับดูแลการใช้งานเทคโนโลยีชีวมิติตามหลักปฏิบัติดังนี้

๑๖.๑.๑ มีนโยบายและแนวปฏิบัติการนำเทคโนโลยีชีวมิติมาใช้ในระบบการให้บริการอย่างชัดเจน ซึ่งต้องคำนึงถึงการดำเนินงานที่สำคัญอย่างน้อยดังนี้

(๑) การประเมินความเสี่ยงการนำเทคโนโลยีชีวมิติมาใช้

(๒) การปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และ

(๓) การรักษาความมั่นคงปลอดภัยข้อมูลชีวมิติ

๑๖.๑.๒ มีการบริหารจัดการอัตลักษณ์เพื่อการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติที่สอดคล้องตามมาตรฐานการใช้งานเทคโนโลยีชีวมิติสำหรับการพิสูจน์และยืนยันตัวตน

๑๖.๑.๓ มีการจัดทำคู่มือหรือแนวปฏิบัติสำหรับบุคลากรที่ปฏิบัติงานเกี่ยวกับการใช้งานข้อมูลชีวมิติ

๑๖.๑.๔ มีการจัดทำคู่มือหรือการให้คำแนะนำผู้ใช้บริการในการใช้งานข้อมูลชีวมิติ

๑๖.๒ ต้องจำกัดการเข้าถึงการควบคุมข้อมูลชีวมิติให้สามารถเข้าถึงได้เฉพาะบุคลากรที่เกี่ยวข้องซึ่งผ่านการฝึกอบรมอย่างเหมาะสม และมีการสอบทานสิทธิอย่างสม่ำเสมอ

ส่วนที่ ๕ การตรวจสอบประวัติการใช้งาน

ข้อ ๑๗ ให้ผู้รับใบอนุญาตจัดเก็บข้อมูลประวัติการใช้งานเพื่อประโยชน์ในการสอบทานของผู้ใช้บริการ โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ผู้ใช้บริการเรียกดูข้อมูลย้อนหลังได้เป็นระยะเวลาไม่น้อยกว่า หกเดือน โดยอย่างน้อยควรมีข้อมูลดังต่อไปนี้

๑๗.๑ ประวัติกิจกรรมของผู้ใช้บริการที่ได้ดำเนินการผ่านระบบการให้บริการของผู้รับใบอนุญาต

๑๗.๒ ประวัติการให้ความยินยอมในการเปิดเผยข้อมูลอัตลักษณ์

ข้อ ๑๘ การแสดงผลการตรวจสอบประวัติการใช้งานต้องไม่มีการแสดงข้อมูลส่วนบุคคลของผู้ใช้บริการ

หมวด ๒
บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ส่วนที่ ๑ ข้อกำหนดทั่วไป

ข้อ ๑๙ ผู้รับใบอนุญาตต้องจัดให้มีมาตรการดูแลข้อมูลส่วนบุคคลอย่างน้อยดังนี้

๑๙.๑ ไม่นำข้อมูลส่วนบุคคลของผู้ใช้บริการมาใช้เป็นตัวระบุ (identifier) ผู้ใช้บริการ

๑๙.๒ ไม่จัดเก็บหรือคงไว้ซึ่งข้อมูลส่วนบุคคลของผู้ใช้บริการที่มีการส่งจากผู้รับใบอนุญาตไปยังผู้อาศัยการพิสูจน์และยืนยันตัวตน เว้นแต่เป็นการจัดเก็บโดยมั่นคงปลอดภัยในระหว่างเซสชันการพิสูจน์และยืนยันตัวตน และข้อมูลดังกล่าวต้องไม่สามารถเข้าถึงได้โดยบุคลากรของผู้รับใบอนุญาต

ข้อ ๒๐ ผู้รับใบอนุญาตต้องจัดให้มีการบันทึกประวัติกิจกรรม (log) สำหรับบริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้เพื่อการตรวจสอบ (audit log) โดยกรณีที่เป็นคำขอเพื่อการยืนยันตัวตนต้องมีการจัดเก็บประวัติกิจกรรมของการโต้ตอบทั้งหมดที่เกี่ยวข้องกับคำขอเพื่อการยืนยันตัวตนดังกล่าว โดยใช้ตัวระบุเฉพาะของการโต้ตอบเดียวกัน (unique interaction identifier) สำหรับแต่ละเหตุการณ์

ส่วนที่ ๒ ข้อกำหนดด้านความสอดคล้องของระบบการให้บริการ

ข้อ ๒๑ ในการกำหนดเงื่อนไขความสอดคล้องของระบบการให้บริการเพื่อให้บุคคลอื่นสามารถเชื่อมต่อได้อย่างมีประสิทธิภาพ ผู้รับใบอนุญาตต้องแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการอย่างน้อยในเรื่องดังต่อไปนี้

๒๑.๑ ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล (assurance level) ที่สามารถเชื่อมต่อกับระบบการให้บริการ

๒๑.๒ โพรโทคอล (protocol) สำหรับเชื่อมโยงคำขอ (request) และการตอบกลับ (response) ในระบบการให้บริการ

ข้อ ๒๒ ในการกำหนดความสอดคล้องของระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้รับใบอนุญาตต้องพิจารณาดำเนินการอย่างน้อยดังนี้

๒๒.๑ จัดให้มีรายชื่อและระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการของตน

๒๒.๒ จัดให้มีกลไกที่สามารถคัดแยกผู้รับใบอนุญาตที่เชื่อมต่อกับระบบการให้บริการที่มีระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ในระดับที่สอดคล้องตามคำขอหรือสูงกว่าคำขอของผู้ส่งคำขอได้

ข้อ ๒๓ การกำหนดโพรโทคอลที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลในระบบการให้บริการ (communication protocol) ต้องสามารถเชื่อมโยงคำขอและการตอบกลับ โดยเชื่อมโยงคำขอไปยังปลายทางที่ระบุโดยผู้ส่งคำขอและสามารถเชื่อมโยงการตอบกลับไปยังคำขอต้นทางได้ ซึ่งต้องมีการแจ้งให้ผู้เชื่อมต่อทราบเกี่ยวกับเงื่อนไขความสอดคล้องของระบบการให้บริการ

ข้อ ๒๔ ผู้รับใบอนุญาตต้องกำหนดส่วนต่อประสานโปรแกรมประยุกต์ (application programming interface) ที่ใช้สำหรับการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนในระบบการให้บริการ (ถ้ามี) โดยอย่างน้อยต้องสามารถเชื่อมโยงรายการต่อไปนี้เข้าด้วยกันได้อย่างถูกต้องและครบถ้วน

๒๔.๑ รายการข้อมูลที่กำหนดในคำขอและการตอบกลับ

๒๔.๒ ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามที่กำหนดในคำขอและการตอบกลับ

ส่วนที่ ๓ ข้อกำหนดด้านเทคนิค

ข้อ ๒๕ ผู้รับใบอนุญาตต้องจัดให้มีแผนการทดสอบ (testing plan) การเชื่อมโยงและแลกเปลี่ยนข้อมูลบนระบบการให้บริการที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยของระบบการให้บริการ โดยแผนการทดสอบดังกล่าวเป็นส่วนหนึ่งของรายงานผลการตรวจประเมินความพร้อมในการประกอบธุรกิจ

ข้อ ๒๖ ผู้รับใบอนุญาตต้องจัดให้มีการทดสอบการใช้งานตามแผนการทดสอบร่วมกับผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการก่อนเริ่มให้บริการแก่บุคคลดังกล่าว

ข้อ ๒๗ ห้ามมิให้เปิดให้บริการแก่ผู้ประสงค์จะเชื่อมต่อกับระบบการให้บริการของผู้รับใบอนุญาตที่ไม่สามารถทดสอบการใช้งานร่วมกันกับผู้รับใบอนุญาตหรือผลการทดสอบไม่สามารถดำเนินการได้โดยสมบูรณ์