The Digital Well-being
Data Exchange Platform For All

นโยบายและเงื่อนไขการใช้บริการของ NDID Platform
(NDID Platform Terms of Service)

ISO/IEC 27001 Information Security Management
IS 728377

ETDA Digital ID Exchange Service License No. 001-2566

Standard Security & Trust
มีมาตรฐาน มีความเชื่อมั่น และสามารถตรวจสอบได้

บันทึกการแก้ไข

ตารางในด้านล่างแสดงถึงรายการเปลี่ยนแปลงที่เกิดขึ้นกับเอกสารนี้

เวอร์ชั่น	วันที่	คำอธิบาย	จัดทำโดย
1.0	15 ต.ค. 67	เวอร์ชั่นเริ่มต้น – เอกสารฉบับนี้ที่ได้จัดทำขึ้นเพื่ออ้างอิงข้อมูลที่เกี่ยวข้องตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 (STATEMENT OF COMPLIANCE) ที่เกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (eKYC) และการลงลายมือชื่อทางอิเล็กทรอนิกส์ (eSignature) โดยมีการรับรองจากศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย (CHULA UNISEARCH)	NDID

ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย
CHULA UNISEARCH

STATEMENT OF COMPLIANCE

The deliverable has been developed in compliance with Thailand's Electronic Transaction Act, B.E. 2562 related to Electronic Know Your Customer (eKYC) and Electronic Signature (eSignature).

*Deliverable refers to the NDID Platform Terms of Service.

Issued by

Asc.Prof. Dr. Piyabutr Bunaramrueang
Faculty of Law,
Chulalongkorn University
15 October 2024

นโยบายและเงื่อนไขการใช้บริการของ NDID

(NDID Platform Term of Service)

สารบัญ

สารบัญ (ต่อ)

นโยบายและเงื่อนไขการใช้บริการของ NDID Platform

(NDID Platform Terms of Service)

1. บทนำ

1.1 ข้อมูลทั่วไป

เอกสารฉบับนี้เรียกว่า “**นโยบายและเงื่อนไขการใช้บริการของ NDID Platform**” โดยมีวัตถุประสงค์เพื่อชี้แจงแก่ทุกฝ่ายที่เกี่ยวข้องกับการให้บริการของ NDID ซึ่งประกอบด้วยการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (eKYC) บริการให้ความยินยอมในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์ (eConsent) และบริการลงลายมือชื่ออิเล็กทรอนิกส์ (eSignature) เพื่อการให้บริการแลกเปลี่ยนข้อมูลอย่างถูกต้อง ปลอดภัย มีมาตรฐาน และสร้างความเชื่อมั่นต่อทุกภาคส่วน

บริษัท เนชั่นแนลดิจิทัลไอดี จำกัด หรือ National Digital ID Co., Ltd. (“**NDID**”) เกิดจากการที่ภาครัฐได้ให้ความสำคัญของการใช้เทคโนโลยีดิจิทัลมาประยุกต์ใช้กับการให้บริการประชาชน และภาคธุรกิจให้มีประสิทธิภาพในเรื่องของการพัฒนาระบบการพิสูจน์และยืนยันตัวตนบนโลกดิจิทัล โดย NDID มีผู้ร่วมทุนหลากหลาย ซึ่งประกอบไปด้วย ธนาคารพาณิชย์ไทยทั้งภาครัฐและเอกชน บริษัทหลักทรัพย์ บริษัทจัดการกองทุน บริษัทประกันชีวิต บริษัทประกันวินาศภัย บริษัทผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ ตลาดหลักทรัพย์แห่งประเทศไทย บริษัทไปรษณีย์ไทย เป็นต้น ซึ่งล้วนเป็นองค์กรที่มีความน่าเชื่อถือสูงและส่วนใหญ่อยู่ภายใต้การกำกับดูแลของหน่วยงานที่มีอำนาจตามกฎหมาย เช่น ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) สำนักงานคณะกรรมการกำกับและส่งเสริมธุรกิจประกันภัย (คปภ.) และสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) เป็นต้น ดังนั้น NDID จึงมีนโยบายการทำงานในด้านต่าง ๆ ให้เทียบเท่ากับบริษัทและองค์กรที่มีการกำกับดูแลที่ดีดังกล่าวข้างต้น เช่น การบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) การปฏิบัติตามกฎหมายที่เกี่ยวข้อง เป็นต้น

เนื่องด้วยความไว้วางใจของลูกค้าที่มีต่อระบบจัดการของ NDID ที่ให้บริการต่อลูกค้าในปัจจุบัน NDID จึงให้ความสำคัญและตระหนักถึงความรับผิดชอบในการดำเนินการด้านต่าง ๆ เพื่อให้สอดคล้องและเป็นไปตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 (“**พ.ร.บ. ธุรกรรมฯ**”) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“**พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ**”) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2562 เป็นต้น รวมทั้ง NDID ได้รับอนุญาตในการประกอบธุรกิจบริการเกี่ยวกับระบบบริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID Service Exchange License) [1] ตามพระราชกฤษฎีกาว่าด้วย

[1] ธพส. 001-2566

การควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565 และได้แจ้งการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัล ตามพระราชกฤษฎีกาการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 (Digital Platform Service) เป็นที่เรียบร้อยแล้ว

1.2 คำนิยาม

นิยาม	คำอธิบาย
การพิสูจน์ตัวตน (Identity Proofing)	กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น
การยืนยันตัวตน (Authentication)	กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น
เจ้าของลายมือชื่อ (Signatory)	ผู้ซึ่งถือข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ และสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นในนามตนเองหรือแทนบุคคลอื่น (พ.ร.บ. ธุรกรรมฯ มาตรา 4)
ผู้ให้บริการแสดงตัวตน (IdP Agent)	ผู้ให้บริการพิสูจน์ตัวตนผ่านการอ่านบัตรประชาชน ณ ช่องทางที่กำหนด โดยมีจุดบริการเสียบบัตรประชาชน (Dip Chip) และ/หรือ ทำการเปรียบเทียบใบหน้าบนเครื่อง
ผู้ใช้บริการ (User)	ผู้สมัครใช้บริการ (User) ที่ได้มีการลงทะเบียนพิสูจน์ตัวตน และยืนยันตัวตนจากสิ่งที่ใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนแล้ว
ผู้บริหารจัดการโครงสร้างพื้นฐานกุญแจสาธารณะและมาตรฐานที่เกี่ยวข้อง	ผู้บริหารจัดการและควบคุมหน่วยงานสมาชิกที่มีหน้าที่จัดการและดูแลลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 26 แห่ง พ.ร.บ. ธุรกรรมฯ
ผู้พิสูจน์และยืนยันตัวตน (IdP)	ผู้ให้บริการซึ่งประมวลผลข้อมูลจากกระบวนการรวบรวม และตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลอัตลักษณ์นั้นจากกระบวนการพิสูจน์และยืนยันตัวตน โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ซึ่งกล่าวอ้างนั้นเป็นของบุคคลนั้นจริง

นิยาม	คำอธิบาย
ผู้สมัครใช้บริการ (Applicant)	ผู้ที่สมัครใช้บริการกับผู้พิสูจน์และยืนยันตัวตน
ผู้ให้ข้อมูลที่น่าเชื่อถือ (AS)	แหล่งข้อมูลที่มีข้อมูลที่น่าเชื่อถือ
ผู้ให้บริการ (RP)	หน่วยงานที่อาศัยผลการยืนยันตัวตนจากผู้พิสูจน์และยืนยันตัวตน (IdP) หรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้วในการตัดสินใจจะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ
พรฎ. แพลตฟอร์มดิจิทัลฯ	พระราชกฤษฎีกาการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565
พรฎ. การพิสูจน์และยืนยันตัวตนฯ	พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565
พ.ร.บ. ธุรกรรมฯ	พระราชบัญญัติว่าด้วยธุรกรรมทางเล็กทรอนิกส์ พ.ศ. 2544
หน่วยงานผู้ให้บริการระบบทำการแทน (Proxy)	หน่วยงานที่เชื่อมระบบกับผู้ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล แทนหน่วยงานสมาชิก
ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล	เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยงข้อมูลระหว่างบุคคลใด ๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตนและการทำธุรกรรมอื่น ๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน
ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)	อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์

นิยาม	คำอธิบาย
	ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น
สิ่งที่ใช้ยืนยันตัวตน (Authenticator)	สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ยืนยันตัวตน โดยสิ่งนั้นแสดงถึงความเชื่อมโยงระหว่างอัตลักษณ์กับบุคคล ซึ่งรวมถึงแต่ไม่จำกัดเพียง OTP, PIN, Username and Password, Token, Face ID, Finger Print และอื่น ๆ ซึ่งสามารถใช้เป็นลายมือชื่ออิเล็กทรอนิกส์อันมีผลผูกพันตามกฎหมาย[2] โดยให้ถือสิ่งที่ใช้ยืนยันตัวตน (authenticators) เป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ที่เป็นเครื่องมือในขั้นตอนการยืนยันตัวตนได้[3]
สิ่งที่ใช้รับรองตัวตน (Credential)	ข้อมูล วัตถุ เอกสาร ที่เชื่อมโยงอัตลักษณ์เข้ากับสิ่งที่ใช้ยืนยันตัวตน เช่น บัตรประจำตัวประชาชน ใบรับรอง เป็นต้น
หน่วยงานสมาชิก (Member)	สมาชิกที่มีนิติสัมพันธ์กับ NDID ได้แก่ ผู้พิสูจน์และยืนยันตัวตน (IdP) ผู้ให้บริการ (RP) ผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) และหน่วยงานผู้ให้บริการระบบทำการแทน (Proxy)
อัตลักษณ์ (Identity)	คุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลหรือภายในกรณีหรือบริบทที่กำหนด

[2] ID Enabling Environment Assessment: Guidance Note, WORLD BANK, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/881991559312326936/ID-Enabling-Environment-Assessment-Guidance-Note (last visited May 15, 2024).

[3] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures (repealed), HTTP://WWW.NATIONALARCHIVES.GOV.UK/WEBARCHIVE/, https://www.legislation.gov.uk/eudr/1999/93/article/1#reference-c000002 (last visited May 13, 2024).

นิยาม	คำอธิบาย
อัตลักษณ์ดิจิทัล (Digital Identity)	ข้อมูลอัตลักษณ์ที่ถูกรวบรวมและบันทึกไว้ในรูปแบบดิจิทัล ซึ่งใช้ระบุถึงหรือจำแนกบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์
ETDA	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
NDID MQA	NDID Member Qualification Assessment Framework (MQA)
NDID Platform	ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลโดย NDID ซึ่งให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลระหว่างหน่วยงานสมาชิก
NIST	National Institute of Standards and Technology

2. บริการของเรา

การให้บริการของ NDID ภายใต้นโยบายและเงื่อนไขการใช้บริการฉบับนี้ ได้แก่ บริการพิสูจน์และยืนยันตัวตนทางดิจิทัล (eKYC) บริการให้ความยินยอมในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์ (eConsent) และบริการลงลายมือชื่ออิเล็กทรอนิกส์ (eSignature) เพื่อรองรับการให้บริการแลกเปลี่ยนข้อมูลเพื่อให้หน่วยงานสมาชิกส่งมอบบริการที่ดีที่สุดแก่ลูกค้าของตนเพื่อคุณภาพชีวิตที่ดีของทุกภาคส่วน ภายใต้มาตรฐานความปลอดภัย กฎหมาย และกฎระเบียบที่เกี่ยวข้อง ตาม NDID Positioning “The Digital Well-being Data Exchange Platform for All” นอกจากนี้ บริการของ NDID ถูกออกแบบภายใต้มาตรฐานและความปลอดภัยตามหลักการ Data Security and Privacy by Design และสอดคล้องตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง

NDID จะให้การช่วยเหลือและสนับสนุนตามรายละเอียดข้อตกลงการให้บริการของ NDID โดย NDID จะใช้ความพยายามตลอดระยะเวลาเพื่อบำรุงรักษาและดำเนินการให้ NDID Platform เป็นไปตามมาตรฐานที่เกี่ยวข้อง และเราจะใช้ความพยายามเพื่อช่วยเหลือหน่วยงานสมาชิกและให้คำแนะนำแก่หน่วยงานสมาชิกเกี่ยวกับการทำงานร่วมกันของระบบ ทั้งนี้ เป็นไปตามข้อกำหนดใน Membership Agreement

2.1 บริการเกี่ยวกับการพิสูจน์และยืนยันตัวตน

- eKYC
  - eKYC
    - บริการการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อการนำข้อมูลเกี่ยวกับอัตลักษณ์ที่รวบรวมไว้ไปตรวจสอบได้ โดยตรวจสอบจากความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง
    - การยืนยันตัวตนตามอัตลักษณ์นั้นประกอบกับการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อให้มั่นใจว่าบุคคลที่กล่าวอ้างเป็นผู้ที่ครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง โดยระดับความน่าเชื่อถือของการพิสูจน์ตัวตนและการยืนยันตัวตนจะขึ้นอยู่กับความเสี่ยงของแต่ละบริการ
  - eConsent
    - บริการการให้ความยินยอมในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์ เพื่อการแลกเปลี่ยนข้อมูลในการทำธุรกรรมได้อย่างต่อเนื่อง โดยการได้รับความยินยอมจากผู้ใช้บริการในการเปิดเผยข้อมูลให้แก่หน่วยงานสมาชิกก่อนการทำธุรกรรมซึ่งผู้ใช้บริการสามารถตรวจสอบข้อมูลและรายละเอียดต่าง ๆ ได้ผ่านทางดิจิทัล ซึ่งสามารถให้ความยินยอมได้โดยใช้ eSignature
    - เนื่องจากกระบวนการพิสูจน์และยืนยันตัวตนจำเป็นต้องมีการตรวจสอบตัวตนผู้ใช้บริการ และตรวจสอบหลักฐานประกอบการยืนยันตัวตน เช่น บัตรประจำตัวประชาชน รวมถึงการเก็บข้อมูลย่อมต้องมีการขอความยินยอมจากผู้ใช้บริการก่อน ดังนั้น บริการ eConsent จึงเป็นส่วนหนึ่งของ eKYC และมีความสำคัญต่อการทำธุรกรรมต่าง ๆ เพื่อให้การดำเนินงานและการใช้ข้อมูลของหน่วยงานสมาชิกเป็นไปตามกฎหมายกำหนด

- eSignature [4]
  - บริการการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อการทำธุรกรรมต่าง ๆ โดยการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ เชื่อมโยงไปยังเจ้าของลายมือชื่อได้และอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อแต่เพียงผู้เดียว โดยอาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) เป็นวิธีการเหมาะสำหรับความรัดกุมและมั่นคงปลอดภัย และเชื่อถือได้ ซึ่งใช้ลายมือชื่ออิเล็กทรอนิกส์ในการยืนยันตัวตนผ่าน eKYC ได้

2.2 บริการเกี่ยวกับการลงลายมือชื่ออิเล็กทรอนิกส์

- eSignature
  - บริการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือตามหลักเกณฑ์ที่กฎหมายกำหนด เพื่อให้ผู้ใช้บริการสามารถลงลายมือชื่อในรูปแบบดิจิทัลได้ โดยการลงลายมือชื่อด้วยกุญแจส่วนตัว (Private Key) และสามารถตรวจสอบกับกุญแจสาธารณะ (Public Key) ที่อยู่บน NDID Platform ได้ เป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ตาม พ.ร.บ. ธุรกรรมฯ มาตรา 26
  - สัญญาทางอิเล็กทรอนิกส์ที่ลงลายมือชื่ออิเล็กทรอนิกส์แล้วมีผลผูกพันและบังคับใช้ตามกฎหมาย[5] และจัดเก็บเอกสารตามมาตรฐาน PDF/A-3 ซึ่งผู้ที่เกี่ยวข้องสามารถตรวจสอบถึงรายละเอียดและการเปลี่ยนแปลงของเอกสารสัญญาได้
  - เฉพาะผู้ให้บริการ (RP) กับผู้ใช้บริการและผู้ลงลายมือชื่อเท่านั้น ที่เห็นเนื้อหาของสัญญา โดยผู้พิสูจน์และยืนยันตัวตน (IdP) และ NDID ไม่เห็นเนื้อหาในสัญญา
  - การลงลายมือชื่ออิเล็กทรอนิกส์ มีผลบังคับใช้ในทางกฎหมายเนื่องด้วยเป็นไปตามเงื่อนไข[6] ดังต่อไปนี้
    - ผู้ลงลายมือชื่อสามารถลงลายมือชื่อในสัญญาด้วยลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งเป็นรูปแบบที่ได้รับการยอมรับ (Electronic Form of Signature)

[4] ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ตาม พ.ร.บ. ธุรกรรมฯ มาตรา 26 จึงหมายถึงลายมือชื่อที่มีลักษณะดังต่อไปนี้
(1) ข้อมูลที่ใช้สร้างลายมือชื่อสามารถเชื่อมโยงไปยังเจ้าของลายมือชื่อได้โดยไม่เชื่อมโยงไปยังบุคคลอื่น
(2) ข้อมูลที่ใช้สร้างลายมือชื่ออยู่ภายใต้การควบคุมของเจ้าของลายมือชื่ออิเล็กทรอนิกส์ในขณะสร้างลายมือชื่อนั้นโดยไม่มีบุคคลอื่นเข้ามาควบคุม
(3) สามารถตรวจพบการแก้ไขเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับลายมือชื่ออิเล็กทรอนิกส์ นับตั้งแต่สร้างลายมือชื่อขึ้น
(4) สามารถตรวจพบการแก้ไขเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับข้อความ นับตั้งแต่เวลาที่ลงลายมือชื่อ ซึ่งคุณลักษณะที่สามารถตรวจสอบการเปลี่ยนแปลงของลายมือชื่อและข้อความอิเล็กทรอนิกส์ได้ รวมถึงการที่เจ้าของลายมือชื่อเป็นผู้ควบคุมการลงลายมือชื่อของตัวเอง

[5] พ.ร.บ. ธุรกรรมฯ มาตรา 7

[6] Use of Electronic Signature in Federal Organization Transactions

- ผู้ลงลายมือชื่อมีเจตนาในการลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์ จากการแสดงข้อความให้ผู้ลงลายมือชื่อได้รับทราบและยอมรับเนื้อหาในเอกสาร (Intent to Sign)
- ลายมือชื่ออิเล็กทรอนิกส์ที่ได้ลงลายมือชื่อเป็นส่วนหนึ่งหรือได้แนบไปกับเอกสารอิเล็กทรอนิกส์ (Association of Signature to the Record) ซึ่งสามารถแสดงได้อย่างชัดเจนว่าเอกสารที่ลงลายมือชื่อเป็นเอกสารใดและยืนยันข้อมูลในเอกสารนั้น พร้อมทั้งมีความเชื่อมโยงกันระหว่างเอกสารและลายมือชื่อที่ลงลายมือชื่อในเอกสาร เพื่อการตรวจสอบการเปลี่ยนแปลงได้ในภายหลัง
- มีช่องทางในการพิสูจน์ตัวตนและยืนยันตัวตนของผู้ลงลายมือชื่อก่อนการลงลายมือชื่อในสัญญาผ่าน eKYC (Identification and Authentication of the Signer)
- มีช่องทางในการรักษาความถูกต้องของการลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์ (Integrity of Signed Record)

- นอกจากลายมือชื่ออิเล็กทรอนิกส์จะต้องมีความเกี่ยวข้องเชื่อมโยงกับเอกสารอิเล็กทรอนิกส์แล้ว ยังจะต้องมีความเกี่ยวข้องกับตัวผู้ลงลายมือชื่อด้วย ดังนั้น ในการยืนยันถึงความบังคับใช้ได้ของลายมือชื่ออิเล็กทรอนิกส์ที่ลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์จะต้องเริ่มจากการพิสูจน์ตัวตนและยืนยันตัวตนผู้ลงลายมือชื่อก่อน เพื่อเป็นหลักฐานว่าลายมือชื่อในรูปแบบอิเล็กทรอนิกส์นั้นเป็นของใคร และใครเป็นผู้เข้ามาข้องเกี่ยวกับธุรกรรมนั้น ฉะนั้นแล้ว การพิสูจน์ตัวตนและการยืนยันตัวตนจึงเป็นสิ่งสำคัญในกระบวนการลงลายมือชื่อ

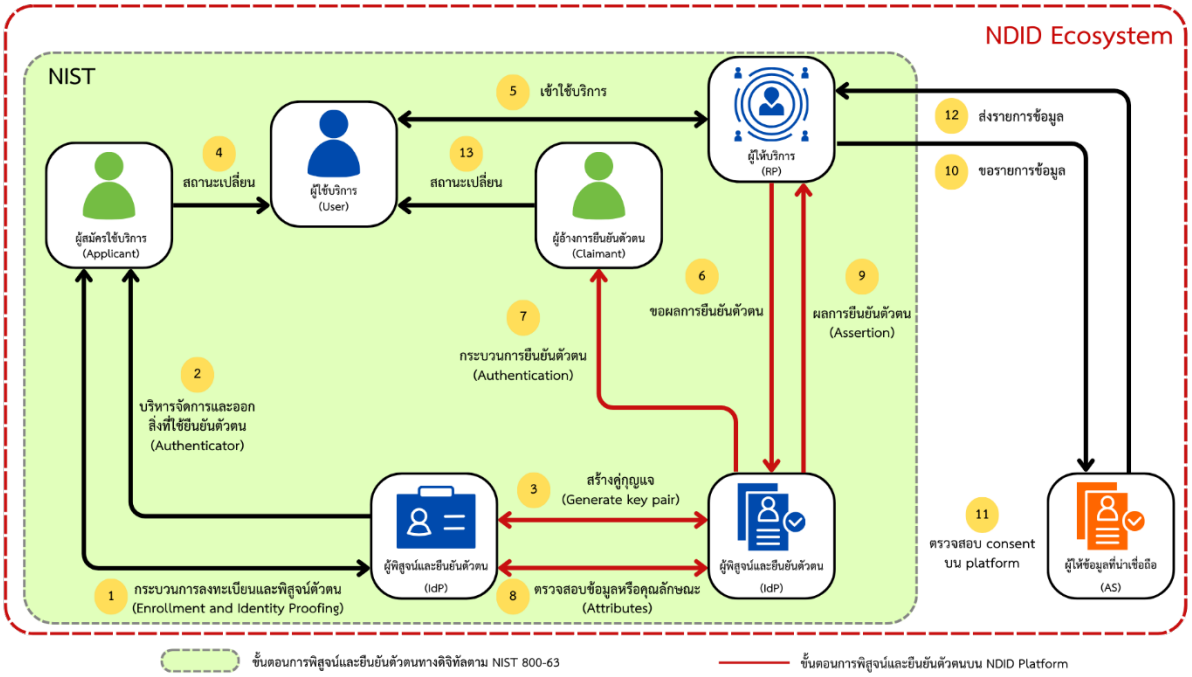
3. บทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้อง

NDID ออกแบบและพัฒนาระบบการเชื่อมโยงข้อมูลระหว่างหน่วยงานสมาชิกกับ NDID Platform และให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยใช้ระบบ Blockchain ซึ่งเป็นเทคโนโลยี Distributed Ledger Technology (DLT) โดยใช้หลักการ Cryptography และความสามารถของ Distributed Computing เพื่อสร้างกลไกความน่าเชื่อถือของแพลตฟอร์ม [7] ด้วยคุณสมบัติของ Distributed Ledger Technology และ Cryptography ทำให้การเข้าถึงข้อมูล การบริหารความมั่นคงปลอดภัย และความน่าเชื่อถือของบริการสอดรับกับหลักการ Data Security and Privacy by Design เนื่องจากเป็นบริการที่มีความปลอดภัยสูงด้วยการใช้เทคโนโลยีแฮชและการเข้ารหัสในการรับส่งข้อมูล (Hash – SHA-256,

[7] Yermack, David. “Corporate Governance and Blockchains*.” *Review of Finance* 21, no. 1 (March 1, 2017): 7–31. https://doi.org/10.1093/rof/rfw074.

AES-256 & Distributed PKI) [8] ดังนั้น NDID Platform จึงเข้ามาเป็นหน่วยงานกลางในการเชื่อมโยงข้อมูลและให้บริการแลกเปลี่ยนข้อมูลการพิสูจน์และยืนยันตัวตนระหว่างหน่วยงานสมาชิก ผู้พิสูจน์และยืนยันตัวตน (IdP) ผู้ให้บริการ (RP) และผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) ให้มีความสะดวกยิ่งขึ้น

ภาพที่ 1 NDID Ecosystem



เทียบเคียง : NIST SP 800-63 Digital Identity Guidelines, *Digital Identity Model*. VS NDID Ecosystem

3.1 NDID Platform

1) NDID Platform ได้รับใบอนุญาตในการเป็นผู้ให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่อให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัลระหว่างหน่วยงานสมาชิก กับระบบ NDID Platform ที่สามารถให้บริการระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้มีมาตรฐานเดียวกัน โดย NDID จะไม่สามารถเข้าแทรกแซงเนื้อหาของข้อมูลที่มีการแลกเปลี่ยนระหว่างหน่วยงานสมาชิกด้วยกันได้

[8] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.), BLOCKCHAIN FOR GOVERNMENT SERVICES - การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ, https://www.oper.navy.mi.th/upload/pdf/Manual/BlockChain-for-Government-Services.pdf.

2) เมื่อมีการส่งข้อมูลผ่าน NDID Platform ระหว่างหน่วยงานสมาชิกจะมีการบันทึกข้อมูลการใช้งาน (log) และข้อมูล Timestamp ตามชุดข้อมูลและระดับความเสี่ยงในการพิสูจน์และยืนยันตัวตน (IAL, AAL) ซึ่งมีการเข้ารหัสและทำการแฝงข้อมูลไว้

3) NDID Platform บริหารจัดการโครงสร้างพื้นฐานกุญแจสาธารณะและมาตรฐานที่เกี่ยวข้องของหน่วยงานสมาชิกโดยการประเมินคุณสมบัติ ตรวจสอบการทำงานและกำกับดูแลเพื่อให้เป็นไปตามหลักมาตรฐานสากล ผ่านการประเมิน NDID Member Qualification Assessment Framework (NDID MQA) และการตรวจสอบการได้รับอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตามหลักเกณฑ์และเงื่อนไขที่ ETDA กำหนด

3.2 ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)

ผู้พิสูจน์และยืนยันตัวตน (“Identity Provider” หรือ “IdP”) หมายถึง นิติบุคคลหรือหน่วยงานซึ่งทำหน้าที่เป็นผู้พิสูจน์และยืนยันตัวตนของผู้ใช้บริการ ผ่านการตรวจสอบข้อมูลอัตลักษณ์ของบุคคลและตรวจสอบความเชื่อมโยงกันระหว่างเจ้าของข้อมูลกับข้อมูลอัตลักษณ์นั้น ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องได้รับใบอนุญาตประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตาม พ.ร.ฎ. การพิสูจน์และยืนยันตัวตนฯ ตามแต่ละประเภทการให้บริการของผู้พิสูจน์และยืนยันตัวตน (IdP) ได้แก่ บริการพิสูจน์ตัวตน บริการยืนยันตัวตน และบริการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

โดยผู้พิสูจน์และยืนยันตัวตน (IdP) ทำหน้าที่ในการออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและรับรองความถูกต้องของสิ่งที่ใช้ยืนยันตัวตน รวมถึงสร้างและบริหารกุญแจเพื่อการพิสูจน์และยืนยันตัวตนและลงลายมือชื่ออิเล็กทรอนิกส์ ซึ่งผู้พิสูจน์และยืนยันตัวตน (IdP) มีหน้าที่ดังต่อไปนี้

1) รับลงทะเบียน (enrollment) โดยการเก็บรวบรวมข้อมูลส่วนบุคคลและเอกสารหลักฐานเท่าที่จำเป็นสำหรับการตรวจสอบความเชื่อมโยงของผู้สมัครใช้บริการกับข้อมูลอัตลักษณ์นั้น พร้อมการแจ้งนโยบายคุ้มครองข้อมูลส่วนบุคคลให้ผู้สมัครใช้บริการทราบก่อนหรือขณะเก็บรวบรวมข้อมูล โดยคำนึงถึงหลักการธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความพร้อมใช้งาน (availability)

2) พิสูจน์ตัวตน (identity proofing) ผู้สมัครใช้บริการที่ประสงค์จะพิสูจน์ตัวตนเพื่อสร้างอัตลักษณ์ดิจิทัล (Digital ID) โดยมีมาตรฐานในการดำเนินงาน ดังนี้

   2.1) จัดให้มีกลไกหรือช่องทางในการแก้ไขข้อมูลให้ถูกต้อง ในกรณีที่ผู้สมัครใช้บริการที่ประสงค์จะพิสูจน์ตัวตนร้องเรียนหรือแจ้งปัญหาจากกระบวนการพิสูจน์ตัวตนเข้ามา โดยดำเนินการให้ช่องทางดังกล่าวเข้าถึงและใช้งานได้โดยง่าย เพื่อแก้ปัญหาหรือข้อร้องเรียนได้อย่างมีประสิทธิภาพ

2.2) ตรวจสอบข้อมูลของผู้สมัครใช้บริการ โดยอาจตรวจสอบกับผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) และตรวจสอบการเปลี่ยนแปลงของเอกสารหลักฐาน และรูปแบบมาตรฐานของเอกสารที่เก็บรวบรวม

2.3) อาจใช้ระบบเปรียบเทียบรูปภาพ (facial recognition) ด้วยระบบเทคโนโลยีสารสนเทศที่เป็นไปตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน กฎเกณฑ์และมาตรฐานที่ ETDA กำหนด

2.4) จัดให้ผู้สมัครใช้บริการรับทราบเงื่อนไขและข้อกำหนดการใช้บริการต่าง ๆ และยอมรับ NDID Terms & Conditions และรวมทั้งผลกระทบกรณีไม่ให้ความยินยอมในการใช้ระบบเปรียบเทียบรูปภาพ (facial recognition)

2.5) เก็บข้อมูลการใช้งานในกระบวนการพิสูจน์ตัวตน (audit logs) และมีขั้นตอนการบริหารจัดการความเสี่ยงทั้งในด้านความเป็นส่วนตัวและมาตรการรักษาความมั่นคงปลอดภัย และมีกระบวนการการรับมือในกรณีการพิสูจน์ตัวตนไม่สำเร็จ (handles proofing errors)

3) ออกสิ่งที่ใช้ยืนยันตัวตนแก่ผู้ใช้บริการ (authenticator) และบริหารจัดการสิ่งที่ใช้รับรองตัวตน (credential)

4) เก็บรักษาข้อมูลเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนและข้อมูลการลงทะเบียนของผู้ใช้บริการให้ปลอดภัยและอยู่ในสภาพพร้อมใช้งาน

5) กำหนดมาตรฐานในการให้บริการตามลักษณะของการให้บริการ

6) ในกรณีที่ผู้พิสูจน์และยืนยันตัวตน (IdP) มีการเชื่อมต่อกับ NDID ผ่าน Proxy ผู้พิสูจน์และยืนยันตัวตน (IdP) จะต้องเข้าทำ (1) สัญญา Membership Agreement หรือ สัญญาการเป็นสมาชิกภาครัฐ กับ NDID และ (2) สัญญา Service Agreement หรือ สัญญาให้บริการ กับ Proxy (รวมเป็น 2 สัญญา) ให้ครบถ้วนและถูกต้อง เพื่อให้การดำเนินงานอยู่มาตรฐานเดียวกันทั้ง Ecosystem

7) ผู้พิสูจน์และยืนยันตัวตน (IdP) สามารถให้บริการได้หลายรูปแบบ เช่น ให้บริการเฉพาะภายในองค์กรตนเอง (Private IdP) / ให้บริการเป็นการทั่วไป (Public IdP) / ให้บริการเฉพาะกลุ่มบริษัทในเครือ และ/หรือ พันธมิตรทางธุรกิจ (Exclusive IdP) หรือรูปแบบอื่นใดตามที่ NDID อาจกำหนดให้มีขึ้น

ทั้งนี้ หน้าที่เพิ่มเติมของผู้พิสูจน์และยืนยันตัวตน (IdP) ให้เป็นไปตามข้อกำหนดใน Membership Agreement

3.3 ผู้ให้บริการ (Relying Party: RP)

ผู้ให้บริการ (“Relying Party” หรือ “RP”) หมายถึง หน่วยงานที่อาศัยผลการยืนยันตัวตนจากผู้พิสูจน์และยืนยันตัวตน (IdP) หรือสิ่งที่ใช้ยืนยันตัวตน (authentication) และผลการยืนยันตัวตน (assertion) หรือสิ่งที่ใช้รับรองตัวตน (credential) ที่ผู้ใช้บริการ (User) มีอยู่ก่อนแล้ว ในการตัดสินใจอนุญาตให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ โดยไม่ต้องดำเนินกระบวนการพิสูจน์และยืนยันตัวตนใหม่ ซึ่งผู้ให้บริการ (RP) มีหน้าที่ดังต่อไปนี้

1) จัดให้มีการยืนยันตัวตนของผู้ใช้บริการ
2) นำทางหรือแนะนำให้ผู้ใช้บริการทำการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) ที่ผู้ใช้บริการได้ลงทะเบียนและพิสูจน์ตัวตนไว้
3) ตรวจสอบความครบถ้วนสมบูรณ์ (integrity) ของผลการยืนยันตัวตน (assertion) ก่อนนำผลการยืนยันตัวตนไปใช้งานให้บริการ [9]
4) ตรวจสอบความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ [10]
5) ในกรณีที่ผู้ให้บริการ (RP) มีการเชื่อมต่อกับ NDID ผ่าน Proxy ผู้ให้บริการ (RP) จะต้องเข้าทำ (1) สัญญา Membership Agreement หรือ สัญญาการเป็นสมาชิกภาครัฐ กับ NDID และ (2) สัญญา Service Agreement หรือ สัญญาให้บริการ กับ Proxy (รวมเป็น 2 สัญญา) ให้ครบถ้วนและถูกต้อง เพื่อให้การดำเนินงานอยู่มาตรฐานเดียวกันทั้ง Ecosystem

ทั้งนี้ หน้าที่เพิ่มเติมของผู้ให้บริการ (RP) ให้เป็นไปตามข้อกำหนดใน Membership Agreement

3.4 ผู้ให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS)

ผู้ให้ข้อมูลที่น่าเชื่อถือ (“Authoritative Source” หรือ “AS”) หมายถึง แหล่งข้อมูลที่มีข้อมูลที่น่าเชื่อถือ เพื่อตรวจสอบ หรือยืนยันความถูกต้องของข้อมูลได้ [11] ซึ่งผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) มีหน้าที่ดังต่อไปนี้

1) ให้ข้อมูล หรือจัดทำข้อมูลอย่างมีเหตุผล มีหลักเกณฑ์ หรือมีการอ้างอิง เพื่อให้ผู้ร้องขอสามารถตรวจสอบหรือทราบข้อมูลต่าง ๆ ได้
2) รับรองข้อมูลที่ได้จัดทำขึ้นว่าข้อมูลส่วนบุคคลนั้นมีที่มาของข้อมูลซึ่งได้รับมาด้วยวิธีการหรือแนวทางที่ถูกต้องและเป็นไปตามกับหลักเกณฑ์ที่กฎหมายกำหนด

[9] มธอ. 11-2566 เล่ม 1

[10] UNCITRAL 2001, Article 11

[11] มธอ. 11-2566 เล่ม 1, NIST SP 800-63-3

3) ตรวจสอบข้อมูลของผู้ใช้บริการที่จัดทำไว้ให้ถูกต้องอยู่เสมอตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้อง และจัดให้มีแผนการบริหารจัดการข้อมูลภายในองค์กรเพื่อสามารถให้บริการได้อย่างมีประสิทธิภาพ

4) ตรวจสอบสถานะการพิสูจน์และยืนยันตัวตนและการให้ความยินยอมในการเปิดเผยข้อมูลของผู้ใช้บริการที่ได้รับจากผู้พิสูจน์และยืนยันตัวตน (IdP) ก่อนเปิดเผยข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลของผู้ใช้บริการ

5) ตรวจสอบข้อมูลตามคำขอของผู้ให้บริการ (RP)

6) ส่งรายการข้อมูลตามที่ผู้ให้บริการ (RP) ได้ร้องขอข้อมูล

7) ในกรณีที่ผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) มีการเชื่อมต่อกับ NDID ผ่าน Proxy ผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) จะต้องเข้าทำ (1) สัญญา Membership Agreement หรือ สัญญาการเป็นสมาชิกภาครัฐกับ NDID และ (2) สัญญา Service Agreement หรือ สัญญาให้บริการ กับ Proxy (รวมเป็น 2 สัญญา) ให้ครบถ้วนและถูกต้อง เพื่อให้การดำเนินงานอยู่มาตรฐานเดียวกันทั้ง Ecosystem

ทั้งนี้ หน้าที่เพิ่มเติมของผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) ให้เป็นไปตามข้อกำหนดใน Membership Agreement

3.5 ผู้ใช้บริการ (User) และผู้ลงลายมือชื่อ (Signatory)

ผู้ใช้บริการ (User) และผู้ลงลายมือชื่อ (Signatory) หมายถึง บุคคลที่ผู้สมัครใช้บริการที่ได้มีการลงทะเบียนพิสูจน์ตัวตนและยืนยันตัวตนจากสิ่งที่ใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) แล้ว และเป็นผู้ที่ต้องยืนยันตัวตนก่อนการเข้าใช้บริการของผู้ให้บริการ (RP) รวมถึงเป็นบุคคลที่ใช้ข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์กระทำการในนามตนเอง หรือในนามตัวแทนของบุคคลอื่น ดังนั้น ผู้ใช้บริการ (User) และผู้ลงลายมือชื่อ (Signatory) จึงเป็นบุคคลเดียวกันที่ได้เข้าใช้บริการ NDID Platform โดยมีเจตนาที่จะเข้าสู่ระบบหรือเข้าทำธุรกรรมกับผู้พิสูจน์และยืนยันตัวตน (IdP) หรือผู้ให้บริการ (RP) ซึ่งจำเป็นต้องมีการพิสูจน์และยืนยันตัวตนก่อนได้รับอนุญาตเข้าสู่ระบบหรือเข้าถึงบริการต่าง ๆ โดยผู้ใช้บริการ (User) และผู้ลงลายมือชื่อ (Signatory) มีหน้าที่ดังต่อไปนี้

1) ได้ลงทะเบียนเพื่อการพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) ก่อนการใช้บริการ NDID Platform และตกลงผูกพันตามการพิสูจน์และยืนยันตัวตนทางดิจิทัล และ/หรือธุรกรรมใด ๆ ที่ได้ดำเนินการผ่าน NDID Platform

2) รับรองว่าข้อมูลที่ใช้เพื่อการพิสูจน์และยืนยันตัวตนนั้นเป็นข้อมูลจริง ถูกต้อง และเก็บรักษาสิ่งที่ใช้ยืนยันตัวตนให้ปลอดภัย อยู่ภายใต้การควบคุมของผู้ใช้บริการและผู้ลงลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

3) ใช้ความระมัดระวังตามสมควรในการสร้างลายมือชื่ออิเล็กทรอนิกส์ เพื่อหลีกเลี่ยงการสร้างลายมือชื่ออิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต [12]
4) แจ้งแก่บุคคลใด ๆ ที่เกี่ยวข้องกับการใช้ลายมือชื่ออิเล็กทรอนิกส์โดยไม่ชักช้า เมื่อผู้ลงลายมือชื่อทราบว่าข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อาจถูกทำลาย สูญหาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ [13] หรือมีความเสี่ยงอย่างมีนัยยะสำคัญที่ข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อาจถูกทำลาย สูญหาย ถูกแก้ไข ถูกเปิดเผยโดยมิชอบ หรือถูกล่วงรู้โดยไม่สอดคล้องกับวัตถุประสงค์ [14]
5) ใช้ความระมัดระวังตามสมควรกรณีมีการใช้ใบรับรองอิเล็กทรอนิกส์เพื่อให้แน่ใจว่าลายมือชื่ออิเล็กทรอนิกส์ยังได้รับการรับรองความถูกต้องและสมบูรณ์ของเนื้อหาทั้งหมด ที่ได้ดำเนินการโดยผู้ใช้บริการและผู้ลงลายมือชื่อเกี่ยวกับใบรับรองนั้นตลอดอายุใบรับรอง หรือตามที่มีการกำหนดในใบรับรอง [15]
6) ใช้ความระมัดระวังตามสมควรในการพิสูจน์และยืนยันตัวตนในการทำธุรกรรมต่าง ๆ โดยสามารถขอข้อมูลในการทำรายการพิสูจน์และยืนยันตัวตน (Transaction Log) การดำเนินการของผู้พิสูจน์และยืนยันตัวตน (IdP) และผู้ให้บริการ (RP) เพื่อเป็นหลักฐานได้ตามกฎหมายเมื่อมีการร้องขอ รวมถึงควรมีรายการตรวจสอบอื่น ๆ เพิ่มเติมจาก Log ด้วย เช่น นโยบายหรือกระบวนการเก็บรักษากุญแจส่วนตัว [16] เครื่องมือหรืออุปกรณ์ที่ใช้เก็บรักษากุญแจส่วนตัวมีความปลอดภัย เป็นต้น [17]

[12] UNCITRAL 2001, Article 8(1)(a) สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 27(1)

[13] UNCITRAL 2001, Article 8(1)(b)(i) สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 27(2)(ก)

[14] UNCITRAL 2001, Article 8(1)(b)(ii) สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 27(2)(ข)

[15] UNCITRAL 2001, Article 8(1)(c) สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 27(3)

[16] IO Moonwalkers, Inc. v. Banc of Am. Merch. Servs., LLC 814 S.E.2d 583 (N.C. Ct. App. 2018).

[17] สามารถดูรายละเอียดรายการตรวจสอบเพื่อการใช้งานลายมือชื่ออิเล็กทรอนิกส์ประเภทที่เชื่อถือได้และที่ได้รับการรับรองเพิ่มเติมได้ที่ คู่มือลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature), โครงการจัดทำเนื้อหาหลักสูตรเพื่อสร้างความรู้ความเข้าใจด้านกฎหมายและเทคโนโลยีดิจิทัล ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย

4. เงื่อนไขการให้บริการ

4.1 มาตรฐานการใช้บริการ NDID Platform

บริการ NDID Platform เป็นการให้บริการด้วยการพิสูจน์และยืนยันตัวตนดิจิทัล (eKYC) การแลกเปลี่ยนข้อมูลภายใต้ความยินยอมของเจ้าของข้อมูล (eConsent) และการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ (eSignature) โดยได้มีการกำหนดมาตรฐานระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) สำหรับการให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับ NDID Platform ที่ระดับ IAL 2 และระดับ AAL 2 ขึ้นไป โดยอ้างอิงตามการกำหนดระดับความน่าเชื่อถือตามมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ในส่วนระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของหน่วยงานสมาชิกที่ใช้งาน NDID Platform นั้น NDID จะทำการพิจารณาระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนแยกออกไปเฉพาะราย โดยสมาชิกต้องคำนึงถึงหน่วยงานกำกับดูแล โดยพิจารณาจากกฎเกณฑ์ของหน่วยงานกำกับดูแลนั้น ๆ เช่น ผู้ให้บริการ (RP) เป็นธนาคาร ซึ่งมีธนาคารแห่งประเทศไทยเป็นหน่วยงานกำกับดูแลที่กำหนดระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนที่ระดับ IAL 2.3 และระดับ AAL 2.2

กรณีไม่มีหน่วยงานกำกับดูแล ผู้ให้บริการ (RP) ต้องพิจารณาระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนจากความเสี่ยงของธุรกรรมของหน่วยงานตนเอง โดยประเมินความเสี่ยงตามระดับความน่าเชื่อถือที่ ETDA กำหนด [18]

4.2 การระงับและการยกเลิกการให้บริการ

ในกรณีที่หน่วยงานสมาชิกดำเนินการใดอันเป็นการผิดสัญญาที่หน่วยงานสมาชิกทำไว้กับ NDID หรือละเมิดต่อหลักเกณฑ์ของกฎหมายที่เกี่ยวข้อง NDID อาจดำเนินการอย่างใดอย่างหนึ่งหรือหลายอย่างประกอบกันดังนี้

1) ระงับการให้บริการไม่ว่าบางส่วนหรือทั้งหมด
2) ยกเลิกสัญญา Membership Agreement กับหน่วยงานสมาชิกรายนั้น

อย่างไรก็ดี ในกรณีที่ NDID พิจารณาแล้วเห็นว่าหน่วยงานสมาชิกอาจแก้ไขเหตุการณ์ที่ระบุไว้ตามวรรคก่อนได้ NDID อาจดำเนินการให้มีการตักเตือนเป็นหนังสือไปยังหน่วยงานสมาชิกรายนั้น เพื่อให้หน่วยงานสมาชิกดำเนินการแก้ไขภายในระยะเวลาที่กำหนด ทั้งนี้ เป็นไปตามข้อกำหนดใน Membership Agreement

[18] มธอ. 11-2566

4.3 การรักษาความมั่นคงปลอดภัยทางเทคนิค

NDID มีนโยบายและกระบวนการที่มีประสิทธิภาพในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ สำหรับใช้ในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ NDID Platform ตลอดจนบทบาทและหน้าที่ของแต่ละส่วนงานในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามข้อกำหนดตามมาตรฐานสากล ISO/IEC 27001 เช่น การรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ (Information Security) ความมั่นคงปลอดภัยระบบคลาวด์ (Cloud Security) การจัดการระบบเครือข่าย (Network Management) การมีแผนความต่อเนื่องทางธุรกิจ (BCP) การมี Governance ของเครือข่าย (การเข้าร่วมระบบ) ของหน่วยงานสมาชิกเพื่อเชื่อมต่อบน Platform เป็นต้น นอกจากนี้โครงสร้างพื้นฐานของระบบเครือข่ายภายในได้รับการแบ่งแยกเป็นระบบพัฒนา (Development environment) ระบบปฏิบัติงานจริง (Production) และการใช้งานของผู้ใช้บริการอย่างชัดเจน โดยแบ่งทางกายภาพ (Physical) และทางตรรกะ (Logical)

NDID บริหารจัดการ NDID Platform จากการควบคุมความมั่นคงปลอดภัยทางเทคนิคบนระบบ (Technical Security Controls) โดยได้เทียบเคียงมาตรฐานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำนโยบายและแนวปฏิบัติของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ พ.ศ. 2552 [19]

อย่างไรก็ดี NDID Platform เป็นระบบที่ออกแบบด้วยเทคโนโลยี Blockchain ซึ่งมีการจัดเก็บข้อมูลซึ่งมีการเข้ารหัสและแบ่งเป็นบล็อค เพื่อการเชื่อมโยงข้อมูลระหว่างหน่วยงานสมาชิกกับ NDID Platform และให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล ดังนั้น รายการข้อมูลที่ปรากฏบน NDID Platform จึงมีความจำเป็นต่อการทำงานของระบบซึ่งไม่สามารถแก้ไขหรือลบข้อมูลได้

[19] เทียบเคียงมาตรฐานตามแนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) บทที่ 6 การควบคุมความมั่นคงปลอดภัยด้านเทคนิค (Technical Security Controls) ในเรื่องต่อไปนี้ ได้แก่ การสร้างและติดตั้งคู่กุญแจ (Key Pair Generation and Installation), การป้องกันกุญแจส่วนตัว (Private Key Protection) รายละเอียดอื่นเกี่ยวกับการจัดการคู่กุญแจ (Others Aspect of Key Pair Management), การควบคุมความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ (Computer Security Controls) และข้อกำหนดสำหรับการประทับเวลาในการบันทึกต่าง ๆ (Time-stamping)

5. การรับรองและรับประกัน

NDID จะให้คำรับรองและรับประกันเฉพาะกรณีที่หน่วยงานสมาชิกและผู้ใช้บริการปฏิบัติตามนโยบายและเงื่อนไขการใช้บริการเท่านั้น

NDID ปฏิเสธความรับผิดชอบในการรับประกันใด ๆ นอกเหนือไปจากที่ได้ให้ไว้ตามนโยบายและเงื่อนไขการใช้บริการ และไม่รับประกันว่า NDID Platform จะปราศจากข้อผิดพลาด จะไม่มีการหยุดชะงัก จะปราศจาก สปายแวร์ มัลแวร์ แอดแวร์ ไวรัส หนอนคอมพิวเตอร์ หรือโค้ดประสงค์ร้าย หรือจะสามารถทำงานได้ตามข้อกำหนดเฉพาะของหน่วยงานสมาชิกซึ่งไม่ใช่มาตรฐานที่ NDID จัดเตรียมให้ NDID ไม่สามารถและไม่รับประกันว่า ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจะทำงานได้บนฮาร์ดแวร์ของหน่วยงานสมาชิก ด้วยระบบปฏิบัติการของหน่วยงานสมาชิก หรือด้วยซอฟต์แวร์อื่น ๆ ที่ติดตั้งบนคอมพิวเตอร์ของหน่วยงานสมาชิก

ทั้งนี้ การรับรองและรับประกันของ NDID และหน่วยงานสมาชิก รวมถึงการปฏิเสธการรับประกันของ NDID ให้เป็นไปตามข้อกำหนดใน Membership Agreement

6. ข้อจำกัดความรับผิด

NDID จะไม่ต้องรับผิดชอบต่อการสูญเสียหรือความเสียหายใด ๆ ที่เกิดขึ้นกับหน่วยงานสมาชิก ผู้ใช้งาน และ/หรือบุคคลอื่นใดอันเป็นผลมาจากหรือเนื่องจากการให้บริการของ NDID ยกเว้นแต่ความสูญหายหรือเสียหายนั้นมาจากกลฉ้อฉล ความประมาทเลินเล่ออย่างร้ายแรง หรือการกระทำผิดโดยตั้งใจหรือเจตนาของ NDID หรือกรรมการ พนักงาน หรือตัวแทนของ NDID

หน่วยงานสมาชิกจะต้องรับผิดชอบต่อสมาชิกรายอื่น ๆ ของ NDID หรือบุคคลอื่นใดเนื่องจากการไม่ปฏิบัติตาม Membership Agreement และ/หรือกฎหมายที่เกี่ยวข้อง หรือเนื่องจากการกระทำการดำเนินงาน หรือการละเว้นการกระทำของหน่วยงานสมาชิก กรรมการ พนักงาน ตัวแทน และ/หรือผู้รับจ้างของตน

6.1 สิทธิและข้อจำกัดการใช้งาน

NDID จะไม่รับผิดชอบในความล่าช้า ผิดพลาด หรือความเสียหายที่เกิดจากการถ่ายโอนข้อมูลผ่านเครือข่ายการสื่อสาร เทคโนโลยี หรือสิ่งอำนวยความสะดวกใด ๆ ที่อยู่นอกเหนือความควบคุมของ NDID และผู้ใช้บริการรับทราบได้ว่าอาจเกิดปัญหาจากการใช้งานผ่านเครือข่ายการสื่อสาร เทคโนโลยี หรือสิ่งอำนวยความสะดวกต่าง ๆ ได้

6.2 ข้อกำหนดที่เกี่ยวข้องกับบุคคลภายนอก

NDID Platform อาจมีการเชื่อมโยงกันระหว่างเว็บไซต์หรือฐานข้อมูล ซึ่งข้อมูลดังกล่าวไม่ได้ถูกเขียนหรือตรวจสอบโดย NDID ซึ่ง NDID ไม่มีส่วนรับผิดชอบในความพร้อมสำหรับการใช้งาน หรือเนื้อหา ผลิตภัณฑ์ หรือความถูกต้องของเนื้อหาข้อมูลอื่น ๆ บนแหล่งข้อมูลภายนอกนั้น

กรณีที่ผู้ใช้หรือบุคคลอื่นใดประสบความเสียหายหรือสูญหายจากการให้บริการของ NDID โดยการใช้ NDID Platform นั้น เบื้องต้น หน่วยงานสมาชิกตกลงยินยอมว่าจะเป็นผู้รับผิดชอบต่อความสูญหายหรือเสียหาย และในการจัดการประเด็นต่าง ๆ ที่เกี่ยวข้องกับผู้ใช้หรือบุคคลอื่นดังกล่าวโดยตรง

ทั้งนี้ ข้อจำกัดความรับผิดให้เป็นไปตามข้อกำหนดใน Membership Agreement

7. การคุ้มครองข้อมูลส่วนบุคคล

การเก็บ รักษาข้อมูล และนโยบายคุ้มครองข้อมูลส่วนบุคคล

การออกแบบและการปรับใช้ระบบ บริการ ผลิตภัณฑ์ และแนวปฏิบัติของ NDID ได้คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ NDID นำหลักการคุ้มครองข้อมูลส่วนบุคคลมาเป็นส่วนสำคัญในกระบวนการทำงานหลักของการประมวลผลระบบต่าง ๆ และการให้บริการของ NDID และใช้เทคโนโลยีเพิ่มความเป็นส่วนตัว เพื่อช่วยในการปฏิบัติตามการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบให้เป็นไปตามหลักการ Data protection by design [20] ซึ่งการออกแบบระบบโดยคำนึงถึงหลักการ Data Security and Privacy by design จะช่วยลดผลกระทบหรือความเสียหายที่จะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล เช่น การประมวลผลข้อมูลเท่าที่จำเป็น การนำมาตรการมาประยุกต์ใช้ เช่น การใช้เทคโนโลยีแฮช การเข้ารหัสข้อมูล (Encryption) การปิดทับข้อมูล (Masking) การแฝงข้อมูล (Pseudonymization) การจัดทำข้อมูลนิรนาม (Anonymization) เป็นต้น

NDID ได้ตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กฎหมายกำหนด โดยผู้ใช้บริการสามารถศึกษานโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ใช้บริการของ NDID Platform ได้ที่ [https://ndid.co.th/laws/]

[20] GDPR, Article 25 Data Protection by design and by default.

8. ทรัพย์สินทางปัญญา

หน่วยงานสมาชิกจะเป็นเจ้าของสิทธิ สิทธิความเป็นเจ้าของและผู้ทรงสิทธิ และประโยชน์ทั้งหมดในทรัพย์สินทางปัญญาของหน่วยงานสมาชิกที่มีอยู่ก่อน Membership Agreement มีผลบังคับใช้ และ/หรือทรัพย์สินทางปัญญาที่พัฒนาขึ้นอย่างอิสระโดยหน่วยงานสมาชิกหรือเพื่อหน่วยงานสมาชิก โดยไม่ได้อาศัย ใช้หรือเข้าถึงทรัพย์สินทางปัญญาของ NDID

NDID จะเป็นเจ้าของสิทธิ สิทธิความเป็นเจ้าของและผู้ทรงสิทธิ และประโยชน์ทั้งหมด (รวมถึงแต่ไม่จำกัดอยู่เพียงสิทธิในทรัพย์สินทางปัญญาทั้งหมดของ NDID) ใน

1) ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมทั้ง "บล็อกเชน" หรือ Distributed Ledger Technology (DLT) ที่ NDID พัฒนาขึ้นหรือที่พัฒนาให้ กับ NDID
2) เครื่องมือของ NDID ตลอดจนงานดัดแปลง และการรวบรวมผลงานตามที่กล่าวมาก่อนหน้านี้ (รวมทั้ง API)
3) ระบบ ฮาร์ดแวร์ ซอฟต์แวร์ และบริการของ NDID
4) ชื่อ ชื่อทางการค้า เครื่องหมายการค้า เครื่องหมายบริการ คำโฆษณา (สโลแกน) ตราสัญลักษณ์ (โลโก้) ชื่อโดเมน หรือเครื่องหมายบ่งชี้อื่น ๆ ทั้งหมดของ NDID
5) ข้อมูลทั้งหมดที่ NDID ได้รับ รวบรวม และ/หรือจัดเก็บที่เกี่ยวข้องกับการที่หน่วยงานสมาชิกใช้งานระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล รวมถึงแต่ไม่จำกัดอยู่เพียงข้อมูลเชิงสถิติ บันทึก (logs) และข้อมูลการวิเคราะห์ทราฟฟิก (traffic analysis data)
6) การดัดแปลง (derivatives) การปรับแต่ง การเสริม หรือการปรับปรุงรายการตาม ข้อ (1) ถึง (5)

การอนุญาตและข้อจำกัดการใช้งาน NDID Platform และบริการอื่นของ NDID ที่เกี่ยวเนื่อง รวมถึงการใช้ทรัพย์สินโอเพนซอร์ซ ให้เป็นไปตามข้อตกลงและเงื่อนไขใน Membership Agreement

9. กฎหมายที่ใช้บังคับและเขตอำนาจศาล

เงื่อนไขการใช้บริการฉบับนี้จะถูกตีความและบังคับใช้ตามกฎหมายของประเทศไทย หากมีความแตกต่าง ข้อพิพาท ข้อขัดแย้ง หรือความขัดโต้เถียงใด ๆ ที่เกิดขึ้นจากหรือเกี่ยวข้องกับเงื่อนไขการใช้บริการหรือการปฏิบัติตามเงื่อนไขการใช้บริการ รวมถึงข้อพิพาทใด ๆ เกี่ยวกับการมีอยู่ ความสมบูรณ์ การยุติสิทธิ หรือหน้าที่ของ NDID และหน่วยงานสมาชิก ทั้งสองฝ่ายจะพยายามระงับข้อพิพาทอย่างฉันมิตร เป็นระยะเวลา 30 วัน หลังจากได้รับหนังสือบอกกล่าวการมีข้อพิพาทเป็นลายลักษณ์อักษรจากอีกฝ่าย

กรณี NDID และหน่วยงานสมาชิกไม่สามารถตกลงระงับข้อพิพาทกันได้ภายในระยะเวลา 30 วัน ดังกล่าว ให้ศาลในประเทศไทยเป็นผู้ระงับข้อพิพาทนั้น

10. การเปลี่ยนแปลงข้อกำหนดนี้

NDID ขอสงวนสิทธิในการเปลี่ยนแปลง หรือเพิ่มเติมรายละเอียดตามที่ระบุในนโยบายและเงื่อนไขการใช้บริการฉบับนี้ เพื่อให้สอดคล้องตามนโยบายการให้บริการ และ/หรือ เพื่อปฏิบัติให้เป็นไปตามหลักเกณฑ์ของกฎหมายที่เกี่ยวข้อง โดยจะแจ้งให้หน่วยงานสมาชิกทราบล่วงหน้า

ในกรณีที่ต้องมีการตีความรายละเอียดที่ระบุไว้นโยบายและเงื่อนไขการใช้บริการฉบับนี้ หรือในกรณีที่ปรากฏข้อเท็จจริงว่าข้อความใดในนโยบายและเงื่อนไขการใช้บริการฉบับนี้ขัดหรือแย้งกันเอง NDID ขอสงวนสิทธิในการตีความ โดยหน่วยงานสมาชิกต้องปฏิบัติตามแนวการตีความหรือคำวินิจฉัยของ NDID เป็นสำคัญ

เอกสารแนบท้าย

1. บทนำ

1.1 ข้อมูลทั่วไป

เอกสารแนบท้ายนี้เป็นคำอธิบายประกอบนโยบายและเงื่อนไขการใช้บริการของ NDID Platform เพื่ออธิบายถึงมาตรฐานของ NDID Platform ว่าเป็นไปตามที่กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนด โดยเอกสารแนบท้ายนี้ไม่ใช่เงื่อนไขการใช้บริการ และไม่มีผลผูกพันทางกฎหมาย หน่วยงานสมาชิกและผู้ใช้บริการควรอ่านและทำความเข้าใจนโยบายและเงื่อนไขการใช้บริการเป็นสำคัญ

1.2 คำนิยาม

นิยาม	คำอธิบาย
ข้อมูลอิเล็กทรอนิกส์ (Data Message)	ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร (พ.ร.บ. ธุรกรรมฯ มาตรา 4)
ธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transaction)	ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน (พ.ร.บ. ธุรกรรมฯ มาตรา 4)
ผู้อ้างการยืนยันตัวตน (Claimant)	ผู้ที่กล่าวอ้างการยืนยันตัวตนจากผู้พิสูจน์และยืนยันตัวตนจากสิ่งที่ใช้ยืนยันตัวตน
มธอ. 11-2566 เล่ม 1 (Digital Identity – Framework)	มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ 11-2566 เล่ม 1 กรอบการทำงาน
มธอ. 11-2566 เล่ม 2 (Digital Identity – Identity Proofing Requirements)	มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ 11-2566 เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
มธอ. 11-2566 เล่ม 3 (Digital Identity – Authentication requirements)	มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เลขที่ 11-2566 เล่ม 3 ข้อกำหนดของการยืนยันตัวตน

นิยาม	คำอธิบาย
วิธีการลงลายมือชื่อ (Signing Method/Process)	กระบวนการ วิธีการ และองค์ประกอบต่าง ๆ ที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์เพื่อให้เป็นที่ยอมรับ
PKI	Public Key Infrastructure
UNCITRAL 1996	UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998
UNCITRAL 2001	UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

2. ภาพรวมการทำงานของ NDID Platform

การให้บริการของ NDID Platform เพื่อการเข้าสู่ระบบหรือทำธุรกรรม ที่มีการพิสูจน์และยืนยันตัวตนและการลงลายมือชื่อเป็นสิ่งยืนยันว่าได้มีการรับรองความถูกต้องของข้อความโดยผู้ใช้บริการและผู้ลงลายมือชื่อแล้ว ซึ่งการทำธุรกรรมทางอิเล็กทรอนิกส์บน NDID Platform นี้ มีการลงลายมือชื่ออิเล็กทรอนิกส์เพื่อผูกพันการทำธุรกรรมต่าง ๆ โดยกฎหมายได้รับรองและคุ้มครองการดำเนินการทางอิเล็กทรอนิกส์นี้ให้มีผลทางกฎหมายบนพื้นฐานของ**หลักความเท่าเทียมกัน (Functional Equivalence)** ระหว่างการใช้ข้อความที่อยู่ในรูปของกระดาษกับข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ให้สามารถกระทำทางอิเล็กทรอนิกส์ได้และมีผลทางกฎหมายเทียบเท่ากับวิธีการเดิม (paper-based) [1] ประกอบกับการนำเทคโนโลยีมาใช้ในการดำเนินการใด ๆ ต้องไม่กระทบต่อความแน่นอนทางกฎหมาย เป็นไปตาม**หลักความแน่นอนทางกฎหมาย (Legal certainty)** กฎหมายและเทคโนโลยีสามารถปรับใช้ด้วยกันได้และกลมกลืนกันบนพื้นฐานของความเป็นกลางทางเทคโนโลยี ความแน่นอนทางกฎหมายของธุรกรรมทางอิเล็กทรอนิกส์จะยกระดับให้กฎเกณฑ์ต่าง ๆ และการมีผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์สามารถอยู่บนพื้นฐานของความเป็นกลางทางเทคโนโลยี โดยการประเมินวิธีการทางเทคโนโลยีที่เป็นกลาง ความน่าเชื่อถือในทางปฏิบัติ และเทคนิคในการสร้างลายมือชื่ออิเล็กทรอนิกส์ประกอบกัน[2] นอกจากนี้ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ ไม่ควรมีการเลือกปฏิบัติท่ามกลางเทคโนโลยี หรือวิธีการทางเทคนิคต่าง ๆ ที่อาจนำไปใช้ได้อย่างเท่าเทียมกันเพื่อสื่อสารหรือจัดเก็บข้อมูลอิเล็กทรอนิกส์ เป็นไปตาม**หลักความเป็นกลางทางเทคโนโลยี (Technology neutrality)**[3]

[1] UNCITRAL 2001. Article 6.1 และ Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce, paras. 15-18

[2] UNCITRAL 2001, The General Assembly and Article 7

[3] UNCITRAL 2001, Article 3

เพื่อให้กฎหมายไม่แบ่งแยกความแตกต่างในเรื่องรูปแบบของเทคโนโลยี หรือปิดกั้นการพัฒนาของเทคโนโลยี หรือให้ความสำคัญกับเทคโนโลยีใดเทคโนโลยีหนึ่ง เพื่อให้ทุกลายมือชื่ออิเล็กทรอนิกส์สามารถใช้บังคับได้เหมือนกันหมดอย่างเท่าเทียมไม่ว่าจะใช้เทคโนโลยีใด[4]

ดังนั้น NDID จึงได้ออกแบบและพัฒนาระบบการเชื่อมโยงข้อมูลระหว่างหน่วยงานสมาชิกกับ NDID Platform และให้บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยใช้เทคโนโลยี Blockchain และ Distributed Ledger Technology (DLT) ซึ่งทำงานบนหลักการของ Cryptography และ Distributed Computing เพื่อสร้างกลไกความน่าเชื่อถือของแพลตฟอร์ม [5] ด้วยคุณสมบัติของ Distributed Ledger Technology และ Cryptography ทำให้การเข้าถึงข้อมูล การบริหารความมั่นคงปลอดภัย และความน่าเชื่อถือของบริการสอดรับกับหลักการ Data Security and Privacy by Design เนื่องจากเป็นบริการที่มีความปลอดภัยสูงด้วยการใช้เทคโนโลยีแฮชและการเข้ารหัสในการรับส่งข้อมูล (Hash – SHA-256, AES-256 & Distributed PKI)[6] และสามารถรองรับเทคโนโลยีในอนาคต

3. รายละเอียดการให้บริการ

3.1 eKYC

การให้บริการพิสูจน์และยืนยันตัวตนทางดิจิทัลหรือบริการ eKYC ให้บริการเพื่อการตรวจสอบจากความเชื่อมโยงของข้อมูลระหว่างผู้ใช้บริการกับอัตลักษณ์นั้น ซึ่งช่วยให้การพิสูจน์และยืนยันตัวตนสามารถทำได้อย่างสะดวกรวดเร็วยิ่งขึ้นผ่านข้อมูลที่ได้มีการจัดเก็บไว้ โดยบริการ eKYC สามารถใช้บริการได้ผ่านหน่วยงานสมาชิกของ NDID Platform ประกอบด้วย ผู้พิสูจน์และยืนยันตัวตน (IdP) และผู้ให้บริการ (RP) ซึ่งได้ผ่านเกณฑ์การประเมินคุณสมบัติตามที่ทาง NDID กำหนด (NDID MQA) และได้รับอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ตามหลักเกณฑ์และเงื่อนไขของ ETDA โดยบริการ eKYC บน NDID Platform ได้ยกระดับการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการ (User) ในการรับบริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพ ซึ่งผู้พิสูจน์และยืนยันตัวตน (IdP) และผู้ให้บริการ (RP) สามารถตรวจสอบถามถูกต้อง ความแท้จริง และตัวตนของผู้ใช้บริการ (User)[7] ที่ทำรายการผ่าน NDID Platform เพื่อให้สันนิษฐานได้ว่าผู้ใช้บริการ (User) ที่ได้รับการพิสูจน์และยืนยัน

[4] Use of Electronic Signature in Federal Organization Transactions

[5] Yermack, David. “Corporate Governance and Blockchains*.” *Review of Finance* 21, no. 1 (March 1, 2017): 7–31. https://doi.org/10.1093/rof/rfw074.

[6] สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.), *supra* note 9.

[7] ผู้ใช้บริการ (User) หมายความรวมถึง Subscriber ตาม NIST SP 800-63A Digital Identity Guidelines Enrollment and Identity Proofing Requirements

ตัวตนเป็นบุคคลนั้นจริง เป็นไปตาม พ.ร.บ. ธุรกรรมฯ มาตรา 34/3 โดยมีภาพรวมการให้บริการ eKYC ผ่านกระบวนการดังต่อไปนี้

การลงทะเบียน (Enrollment) และการพิสูจน์ตัวตน (Identity proofing)

ขั้นตอนของการการลงทะเบียน (enrollment) และการพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่เกิดขึ้นนอก NDID Platform เป็นกระบวนการที่ดำเนินการโดยผู้พิสูจน์และยืนยันตัวตน (IdP) กับผู้สมัครใช้บริการ (Applicant)

ภาพที่ 2 การลงทะเบียน (enrollment) และการพิสูจน์ตัวตน (identity proofing)

ที่มา: NIST SP 800-63A Digital Identity Guidelines Enrollment and Identity Proofing Requirements

1. [Resolution] ผู้สมัครใช้บริการ (Applicant) ที่ประสงค์จะใช้บริการหรือทำธุรกรรมต้องดำเนินการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) เพื่อตรวจสอบข้อมูลอัตลักษณ์และความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น
2. [Validation] ผู้พิสูจน์และยืนยันตัวตน (IdP) จะพิสูจน์ตัวตนของบุคคลโดยดำเนินการตรวจสอบหลักฐานแสดงตน และข้อมูลเกี่ยวกับอัตลักษณ์นั้น รวมถึงตรวจสอบคุณสมบัติของผู้สมัครใช้บริการ (Applicant) ตามเกณฑ์กฎหมายที่เกี่ยวข้องและระดับความน่าเชื่อถือของการพิสูจน์ตัวตนที่กำหนด

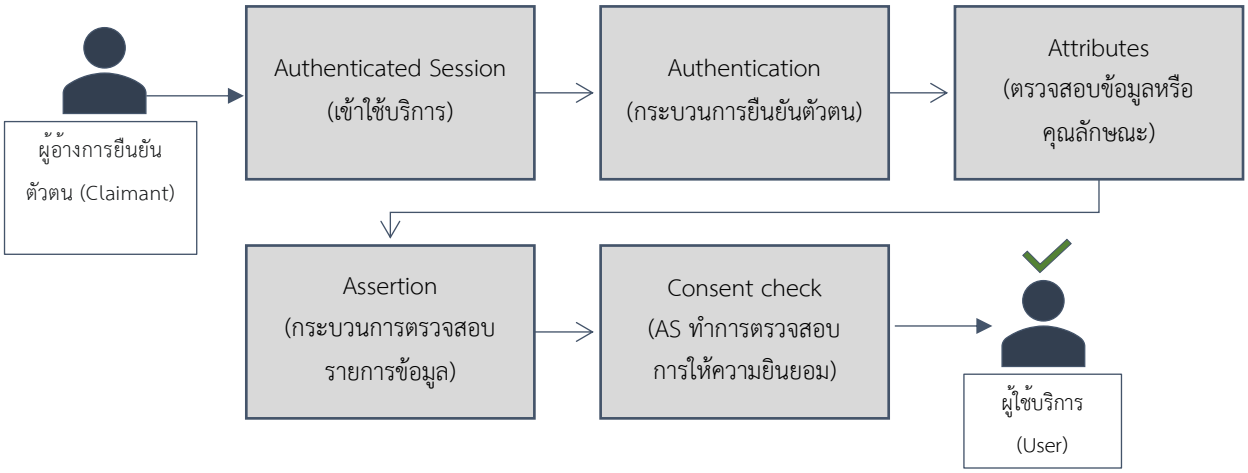
3. [Verification] ผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องยืนยันความเชื่อมโยงระหว่างข้อมูลกับบุคคลว่ามีตัวตนจริง เมื่อพิสูจน์ตัวตนสำเร็จ ผู้พิสูจน์และยืนยันตัวตน (IdP) จะออกสิ่งที่ใช้ยืนยันตัวตน (authenticator) ให้แก่ผู้สมัครใช้บริการ (Applicant) ซึ่งจะเปลี่ยนสถานะเป็นผู้ใช้บริการ (User) เพื่อใช้ในการยืนยันตัวตนผ่านระบบ NDID Platform ได้

โดยผู้พิสูจน์และยืนยันตัวตน (IdP) สามารถบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) ได้ตามแต่ละหลักเกณฑ์และเงื่อนไขของตน เป็นไปตามที่มาตรฐานระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนตามที่ มธอ. 11-2566 รวมทั้งผู้ให้บริการ (RP) อาจกำหนดปัจจัยของการยืนยันตัวตนตามที่หน่วยงานกำกับดูแลกำหนด ซึ่งอาจเป็นการรวบรวมข้อมูลที่เกี่ยวกับอัตลักษณ์ การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ หรือข้อบังคับของหน่วยงานกำกับดูแลที่เกี่ยวข้อง เป็นต้น โดยอาจกำหนดจากปัจจัยและสิ่งที่ใช้ยืนยันตัวตน (authenticator) ได้ทั้งสิ่งที่ผู้ใช้บริการรู้ (something you know) สิ่งที่ผู้ใช้บริการมี (something you have) และสิ่งที่ผู้ใช้บริการเป็น (something you are)

การยืนยันตัวตน (authentication) [8]

ขั้นตอนของการยืนยันตัวตน (authentication) เป็นกระบวนการที่เกิดขึ้นบน NDID Platform เพื่อให้ผู้ใช้บริการ (User) ได้ยืนยันตัวตนก่อนการใช้บริการผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ให้บริการ (RP)

ภาพที่ 3 การยืนยันตัวตน (authentication)



เทียบเคียง : NIST SP 800-63 Digital Identity Guidelines, *Digital Identity Model*. VS NDID Ecosystem

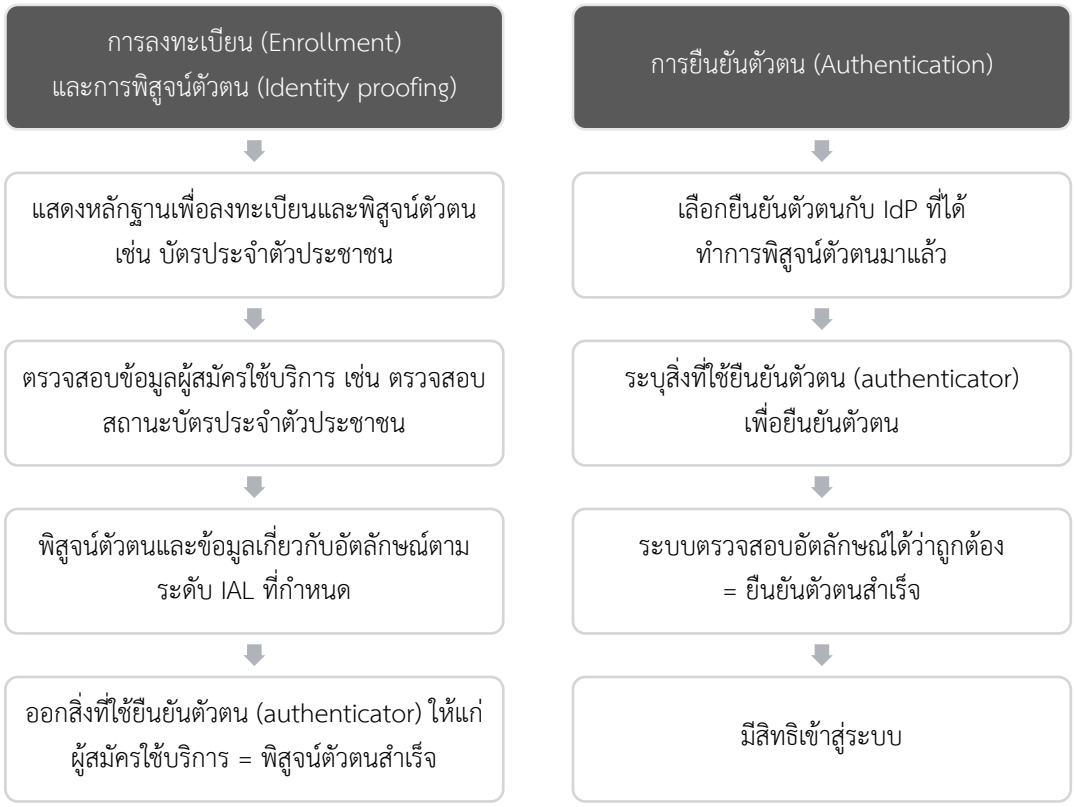
[8] พ.ร.บ. ธุรกรรมฯ มาตรา 34/3

1. [RP Session] ผู้อ้างการยืนยันตัวตน (claimant) ประสงค์จะเข้าใช้บริการหรือทำธุรกรรมใด ๆ บนระบบของผู้ให้บริการ (RP) ต้องยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) ก่อนการใช้บริการตามระดับความน่าเชื่อถือของการยืนยันตัวตนที่ผู้ให้บริการ (RP) กำหนด
2. [Authenticated Session] ผู้อ้างการยืนยันตัวตน (claimant) ต้องเลือกผู้พิสูจน์และยืนยันตัวตน (IdP) บนระบบของผู้ให้บริการ (RP) เพื่อทำการยืนยันตัวตน โดยผู้ให้บริการ (RP) จะทำการร้องขอหรือนำทาง (redirect) ไปยังผู้พิสูจน์และยืนยันตัวตน (IdP) ที่ผู้ใช้บริการเลือก ผ่าน NDID Platform
3. [Authentication] ผู้พิสูจน์และยืนยันตัวตน (IdP) จะส่งคำร้องขอยืนยันตัวตนไปยังผู้อ้างการยืนยันตัวตน (claimant) ผ่านแจ้งเตือนโดยระบบของผู้พิสูจน์และยืนยันตัวตน (IdP) เพื่อให้ผู้อ้างการยืนยันตัวตน (claimant) ทำการพิสูจน์ว่าได้ครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตน เช่น การยืนยันตัวตนด้วย PIN (memorized secrets) หรือสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตามที่ผู้พิสูจน์และยืนยันตัวตน (IdP) ได้ออกให้
4. [Attributes] ผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องตรวจสอบความถูกต้องของข้อมูลหรือคุณลักษณะและสถานะของสิ่งที่ใช้ยืนยันตัวตน โดยอาจให้ผู้อ้างการยืนยันตัวตน (claimant) ถ่ายรูปตนเอง (selfie) เพื่อทำการเปรียบเทียบกับภาพตนเองตอนที่ทำการลงทะเบียนและพิสูจน์ตัวตนครั้งแรกกับผู้พิสูจน์และยืนยันตัวตน (IdP)
5. [Assertion] เมื่อยืนยันตัวตนสำเร็จผู้พิสูจน์และยืนยันตัวตน (IdP) จะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการ (RP) และเมื่อได้รับสถานะของการยืนยันตัวตน ผู้ให้บริการ (RP) จะส่งคำร้องขอข้อมูลไปยังผู้ให้ข้อมูลที่น่าเชื่อถือ (AS)
6. [Consent check] ผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) ทำการตรวจสอบการให้ความยินยอมและสถานะการยืนยันตัวตนของผู้ใช้บริการ (User) บนระบบ NDID Platform และส่งข้อมูลกลับไปยังผู้ให้บริการ (RP) ตามรายการที่ผู้ให้บริการ (RP) ร้องขอ นอก NDID Platform
7. ผู้ให้บริการ (RP) ให้ผู้อ้างการยืนยันตัวตน (claimant) กรอกข้อมูลเพิ่มเติม ตรวจสอบความถูกต้องอีกครั้ง และยืนยันข้อมูล เมื่อการยืนยันตัวตนสำเร็จ ผู้ใช้บริการ (User) จึงสามารถเข้าสู่ระบบหรือทำธุรกรรมของผู้ให้บริการ (RP) ได้ต่อไป

จากการให้บริการ eKYC บน NDID Platform จะมีการประมวลผลข้อมูลของการทำรายการพิสูจน์และยืนยันตัวตนที่มีการดำเนินการโดยผู้พิสูจน์และยืนยันตัวตน (IdP) และผู้ให้บริการ (RP) โดย **ข้อมูลการทำรายการ** ประกอบด้วย RP Node/ ID Mode/ Request ID/ MIN AAL/ MIN IAL/ Request Timeout/ Min IDP/ IDP ID List/ AS ID List/ Service ID/ Min AS เป็นต้น ทั้งนี้ ข้อมูลที่อยู่บน NDID Platform จะอยู่ในรูปแบบรหัสที่ใช้เทคโนโลยี Hash SHA-256 ทำให้ข้อมูลรหัสนั้นไม่สามารถคำนวณย้อนกลับเป็น

ข้อความที่สามารถเข้าใจได้ รายละเอียดในการคุ้มครองข้อมูลเพิ่มเติมสามารถดูได้ที่นโยบายคุ้มครองข้อมูลส่วนบุคคลสำหรับผู้ใช้บริการ NDID Platform

ภาพที่ 4 กระบวนการใช้บริการ eKYC [9]



[ระดับความน่าเชื่อถือ Level of Assurance (LoA)] ในกระบวนการพิสูจน์และยืนยันตัวตนหน่วยงานสมาชิกในฐานะผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องมีการกำหนดระดับความน่าเชื่อถือเพื่อการพิสูจน์และยืนยันตัวตนผู้ใช้บริการด้วย ซึ่งระดับความน่าเชื่อถือ Level of Assurance (LoA) เป็นแนวคิดที่สำคัญสำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัลและการทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากช่วยให้หน่วยงานสามารถประเมินความเสี่ยงที่เกี่ยวข้องกับอัตลักษณ์ดิจิทัล และกำหนดระดับความน่าเชื่อถือที่จำเป็นต่อการยืนยันตัวตนได้ ซึ่งระดับความน่าเชื่อถือ (LoA) คือการวัดระดับความความถูกต้องและความน่าเชื่อถือของอัตลักษณ์ดิจิทัลได้ผ่านการกำหนดขอบเขตการตรวจสอบการพิสูจน์และการยืนยันความถูกต้องของ

[9] ผู้ใช้บริการ (User) สามารถเลือกยืนยันตัวตนได้ด้วยสิ่งที่ใช้ยืนยันตัวตน (authenticator) 3 ประเภท ทั้งนี้ เป็นไปตามที่ผู้พิสูจน์และยืนยันตัวตน (IdP) กำหนด

1. สิ่งที่ผู้ใช้บริการรู้ (something you know) เช่น รหัสผ่าน password หรือ PIN เป็นต้น
2. สิ่งที่ผู้ใช้บริการมี (something you have) เช่น รหัส OTP หรือ กุญแจส่วนตัว (private key) เป็นต้น
3. สิ่งที่ผู้ใช้บริการเป็น (something you are) เช่น ภาพใบหน้า หรือ ลายนิ้วมือ เป็นต้น

อัตลักษณ์ดิจิทัล ยิ่งระดับความน่าเชื่อถือสูง ระดับของความไว้วางใจและความเชื่อมั่นในอัตลักษณ์ดิจิทัลก็จะยิ่งมากขึ้น และความเสี่ยงในการละเมิดหรือขโมยข้อมูลอัตลักษณ์ก็จะลดลงด้วยเช่นกัน

ทั้งนี้ สามารถแบ่งระดับความน่าเชื่อถือออกได้เป็น 2 ส่วน ได้แก่ ระดับความน่าเชื่อของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ซึ่งหน่วยงานสมาชิกควรมีการประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือนี้เหมาะสมกับการให้บริการของตน โดยการประเมินผลกระทบที่อาจเกิดจากการพิสูจน์และยืนยันตัวตนที่ผิดพลาด และทำการเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อที่เหมาะสม[10] ซึ่งทุกบริการหรือธุรกรรมที่ต้องมีการพิสูจน์และยืนยันตัวตนจำเป็นต้องกำหนดระดับความน่าเชื่อถือ [11]

- ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) แบ่งออกเป็น 3 ระดับ ตามระดับความเข้มงวด ซึ่งหน่วยงานสมาชิกของ NDID ควรกำหนดระดับ IAL ไว้อย่างน้อยระดับ IAL 2 ขึ้นไป
  - การพิสูจน์ตัวตนระดับ IAL 2 กำหนดให้มีการพิจารณาหลักฐานการแสดงตน โดยผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องตรวจสอบว่าอัตลักษณ์ที่ผู้สมัครกล่าวอ้างมีอยู่จริง และต้องตรวจสอบความถูกต้องแท้จริงของข้อมูลอัตลักษณ์ และ ความเชื่อมโยงระหว่างบุคคลกับข้อมูลอัตลักษณ์ด้วย การพิสูจน์ตัวตนที่ระดับ IAL 2 สามารถแสดงตัวได้ทั้งแบบต่อหน้า (face-to-face) หรือแบบไม่ต่อหน้า (non face-to-face) ก็ได้ เช่น ผ่านตู้ให้บริการพิสูจน์ตัวตน (kiosk) สำหรับลงทะเบียน หรือทางแอพพลิเคชันพร้อมหลักฐานแสดงตัวตน ได้แก่ บัตรประจำตัวประชาชน หรือหนังสือเดินทาง โดยบัตรประจำตัวประชาชนที่ใช้เพื่อพิสูจน์ตัวตนจะตรวจสอบข้อมูลจากเครื่องอ่านบัตรประชาชนร่วมด้วย เพื่อตรวจสอบความแท้จริงของข้อมูล และเปรียบเทียบจากรูปภาพหรือใบหน้าของบุคคลประกอบกัน
- ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) แบ่งออกเป็น 3 ระดับตามระดับความเข้มงวด ซึ่งหน่วยงานสมาชิกของ NDID ควรกำหนดระดับ AAL ไว้อย่างน้อยระดับ AAL 2 ขึ้นไป
  - การยืนยันตัวตนระดับ AAL 2 กำหนดให้การยืนยันตัวตนต้องมี 2 ปัจจัยที่แตกต่างกันเป็นอย่างน้อย โดยสามารถดำเนินการได้ 2 วิธี วิธีแรกคือใช้การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authenticator) จำนวน 1 อย่าง เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor

[10] NIST Special Publication 800-63-3 (Digital Identity Guidelines)

[11] มธอ. 11-2566

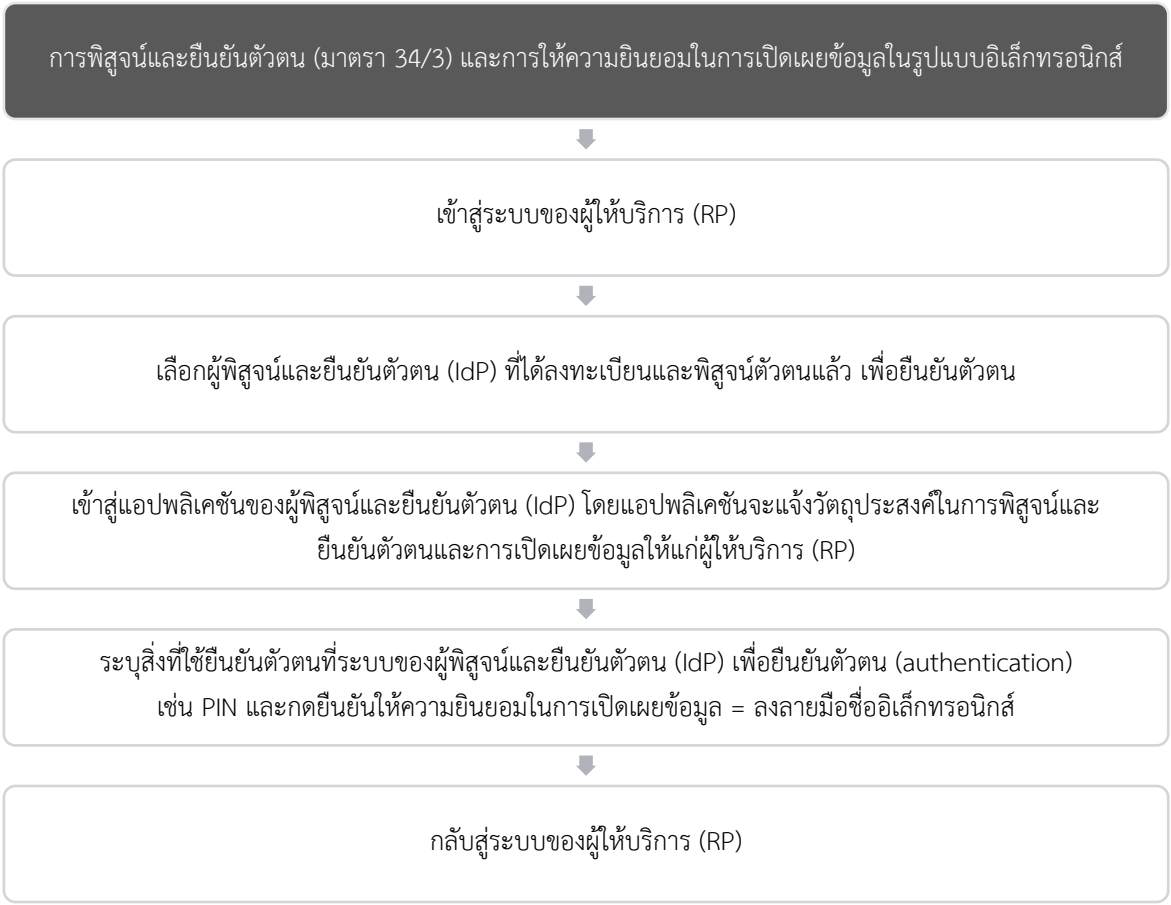
cryptographic software) เป็นต้น หรือวิธีที่สองคือใช้สิ่งยืนยันตัวตนแบบปัจจัยเดียว (single-factor authenticator) ที่แตกต่างกันจำนวน 2 อย่าง เช่น รหัสลับจดจำ (memorized secret) ร่วมกับอุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) หรือรหัสลับจดจำ (memorized secret) ร่วมกับอุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) หรือรหัสลับจดจำ (memorized secret) ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) เป็นต้น นอกจากระดับ AAL 2 จะป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance) ได้แล้ว ยังป้องกันการนำข้อมูลที่ได้ไปกระทำการเลียนแบบซ้ำ (replay resistance) อีกด้วย เช่น เข้าสู่ระบบซ้ำจาก Username และรหัสผ่านที่ได้มา เป็นต้น

3.2 eConsent

การให้บริการให้ความยินยอมในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์หรือ eConsent บน NDID Platform เป็นการขอความยินยอมจากผู้ใช้บริการ (User) ก่อนที่หน่วยงานสมาชิกจะเปิดเผยข้อมูลให้แก่กัน ซึ่งการให้ความยินยอมนี้จำเป็นต่อการดำเนินการบน NDID Platform เพื่อการแลกเปลี่ยนข้อมูลในการทำธุรกรรมได้อย่างต่อเนื่อง NDID Platform จึงได้ออกแบบบริการ eConsent เพื่อเป็นช่องทางที่รองรับการให้ความยินยอมในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์ผ่านทางดิจิทัล และสามารถตรวจสอบข้อมูลได้ทันที บริการ eConsent จึงมีความสำคัญต่อการทำธุรกรรมต่าง ๆ เพื่อให้การดำเนินงานและการใช้ข้อมูลของหน่วยงานสมาชิกเป็นไปตามกฎหมายกำหนด

สำหรับการขอความยินยอมบนบริการ eConsent จากผู้ใช้บริการ (User) ในการเปิดเผยข้อมูลให้แก่หน่วยงานสมาชิกก่อนการทำธุรกรรม ผู้ใช้บริการ (User) สามารถตรวจสอบข้อมูลและรายละเอียดต่าง ๆ ได้ผ่านทางหน้าจอแสดงข้อความที่ปรากฏบนระบบหรือแอพพลิเคชั่นของผู้พิสูจน์และยืนยันตัวตน (IdP) ซึ่งข้อมูลดังกล่าวจำเป็นต่อการให้บริการของผู้ให้บริการ (RP) ซึ่งการให้ความยินยอมผ่าน eConsent มีความน่าเชื่อถือจากกระบวนการที่ผู้ใช้บริการ (User) จำเป็นต้องมีการตรวจสอบตัวตนผู้ใช้บริการ (User) ผ่านการพิสูจน์และยืนยันตัวตนทางดิจิทัลโดย eKYC มาก่อน ซึ่งสันนิษฐานได้ว่าผู้ใช้บริการ (User) มีตัวตนจริงและได้ให้ความยินยอมเปิดเผยข้อมูลของตนเองในการทำธุรกรรม ประกอบกับผู้ใช้บริการ (User) สามารถให้ความยินยอมได้โดยใช้ eSignature ได้ด้วยตนเอง ซึ่ง eSignature ดังกล่าวได้เชื่อมโยงไปยังผู้ใช้บริการ (User) ซึ่งเป็นผู้ลงลายมือชื่อ (Signatory) ได้

ภาพที่ 5 ขั้นตอนการให้ความยินยอมของผู้ใช้บริการ (User) ในการเปิดเผยข้อมูลในรูปแบบอิเล็กทรอนิกส์ผ่าน eConsent

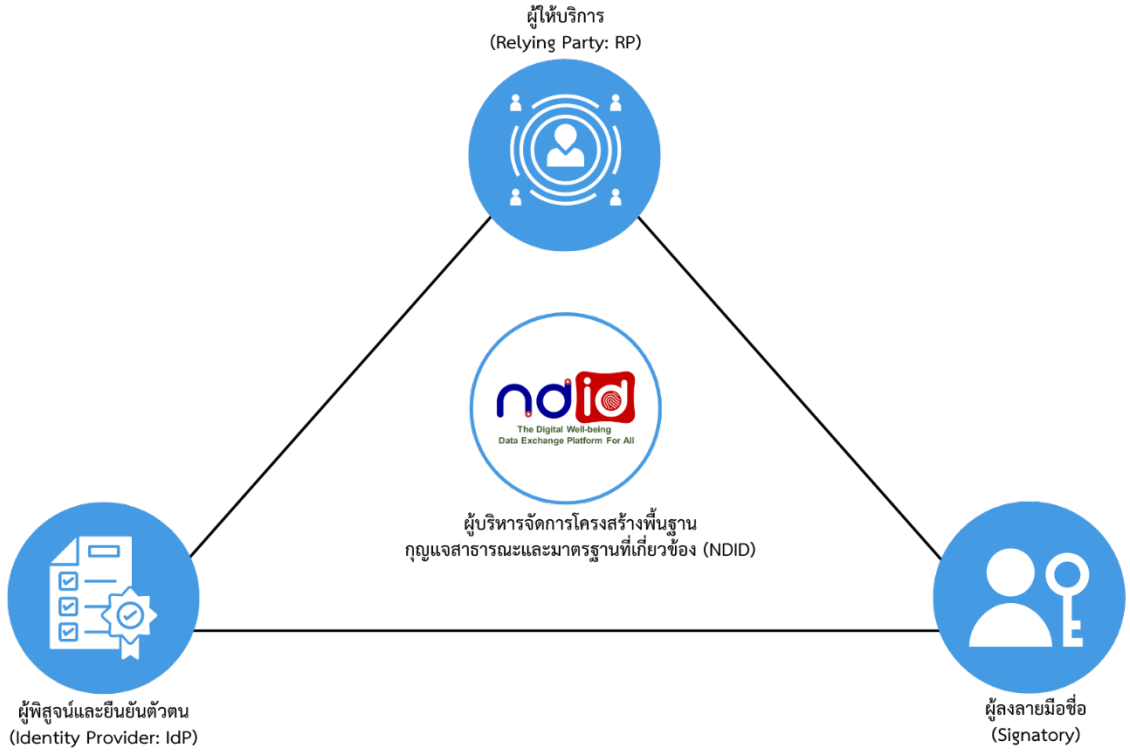


3.3 eSignature

การให้บริการลงลายมือชื่ออิเล็กทรอนิกส์หรือ eSignature บน NDID Platform เป็นการให้บริการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือเพื่อใช้ในการลงลายมือชื่อสำหรับการทำธุรกรรมในรูปแบบดิจิทัล NDID ได้นำเทคโนโลยีที่มีมาตรฐานเพื่อนำมาสร้างลายมือชื่ออิเล็กทรอนิกส์ที่มีผลบังคับใช้ตามกฎหมายและเป็นไปตามหลักเกณฑ์ของมาตรฐานทั้งในประเทศไทยและสากล เพื่อให้หน่วยงานสมาชิกและผู้ใช้บริการ (User) สามารถมั่นใจได้ว่าการทำธุรกรรมทางอิเล็กทรอนิกส์หรือการลงลายมือชื่อในสัญญาอิเล็กทรอนิกส์สามารถเชื่อถือได้และมีผลบังคับใช้ตามกฎหมาย

สำหรับบริการ eSignature หน่วยงานสมาชิกยังคงมีบทบาทเกี่ยวเนื่องกับการลงลายมือชื่ออิเล็กทรอนิกส์ผ่าน NDID Platform ทั้งผู้พิสูจน์และยืนยันตัวตน (IdP) และผู้ให้บริการ (RP) รวมถึง NDID ในฐานะผู้บริหารจัดการโครงสร้างพื้นฐานกุญแจสาธารณะและมาตรฐานที่เกี่ยวข้องที่ได้จัดให้บริการ eSignature รองรับการลงลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ เพื่อให้ผู้ลงลายมือชื่อ (Signatory) หรือผู้ใช้บริการ (User) NDID Platform สามารถลงลายมือชื่อได้อย่างมีผลบังคับทางกฎหมาย

ภาพที่ 6 ผู้เกี่ยวข้องกับบริการ eSignature



เทียบเคียง : โครงสร้างการลงลายมือชื่ออิเล็กทรอนิกส์ตาม UNCITRAL2001 VS การลงลายมือชื่ออิเล็กทรอนิกส์ผ่านบริการ eSignature บน NDID Ecosystem

ตารางที่ 1 การให้บริการลงลายมือชื่ออิเล็กทรอนิกส์	
องค์ประกอบลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ	**รายละเอียดการให้บริการ eSignature**
การแสดงเจตนาของเจ้าของลายมือชื่อ (Person's approval) [12]	✓ มีการใช้วิธีการหรือเทคโนโลยีที่ทำให้สามารถแสดงให้เห็นได้ว่าเป็นการแสดงเจตนาโดยเจ้าของลายมือชื่อ
ความเชื่อมโยงไปยังเจ้าของลายมือชื่อ (Unique) [13]	✓ มีการพิสูจน์และยืนยันตัวตนเจ้าของลายมือชื่อก่อนลงลายมือชื่อด้วยมาตรฐานระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนที่เหมาะสมโดยกำหนดเป็นระดับ IAL และ AAL 2 ขึ้นไป

[12] UNCITRAL 1996, Article 7(a)

[13] UNCITRAL 2001, Article 6.3(a), สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 26(1)

ตารางที่ 1 การให้บริการลงลายมือชื่ออิเล็กทรอนิกส์	
องค์ประกอบลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ	**รายละเอียดการให้บริการ eSignature**
การควบคุมของเจ้าของลายมือชื่อ (Sole Control)[14]	✓ มีการใช้เทคโนโลยีคู่กุญแจในการลงลายมือชื่อเพื่อให้สามารถตรวจสอบถึงความเชื่อมโยงไปยังเจ้าของลายมือชื่อโดยจะมีกระบวนการเข้าถึงที่ใช้เพื่อพิสูจน์ว่าเป็นเจ้าของลายมือชื่อจริงและเพื่อยืนยันความถูกต้องแท้จริงของข้อมูล
การตรวจสอบและติดตามรายการที่เกิดขึ้นกับลายมือชื่อ (Traceability) [15]	✓ มีการใช้กุญแจสาธารณะในการตรวจสอบรายละเอียดของลายมือชื่อได้ว่าถูกแก้ไขหรือเปลี่ยนไปหรือไม่
การตรวจพบการเปลี่ยนแปลงที่เกิดขึ้นแก่ข้อความ (Proof of Integrity and Original of Data) [16]	✓ มีการใช้เทคโนโลยี cryptographic hash function และเทคโนโลยี Blockchain จึงทำให้สามารถตรวจสอบได้ว่าข้อความที่ถูกบันทึกไว้ได้ถูกแก้ไขหรือเปลี่ยนแปลงหรือไม่ ✓ มีการใช้เทคโนโลยีไฟล์ PDF A/3 และกระบวนการเพื่อตรวจสอบการเปลี่ยนแปลงได้ เช่น การลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนเอกสารที่ถูก hash หรือ Smart Contract หรือสัญญาฉบับเต็ม ทำให้สามารถตรวจพบการเปลี่ยนแปลงที่เกิดขึ้นแก่ข้อความได้

[14] UNCITRAL 2001, Article 6.3(b), สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 26(2)

[15] UNCITRAL 2001, Article 6.3(c), สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 26(3)

[16] UNCITRAL 2001, Article 6.3(d), สอดคล้องกับ พ.ร.บ. ธุรกรรมฯ มาตรา 26(4)

โดยบริการ eSignature เป็นไปตามองค์ประกอบลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือที่กฎหมายกำหนด ดังนี้

1) การแสดงเจตนาของเจ้าของลายมือชื่อ (Person's approval)

การให้บริการลงลายมือชื่ออิเล็กทรอนิกส์มีการนำเทคโนโลยีคู่กุญแจ (Key Pair) มาใช้เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งนำมาใช้ในการลงนามสำหรับการทำธุรกรรมแบบดิจิทัล ทำให้ข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ดังกล่าวสามารถเชื่อมโยงกลับไปยังเจ้าของลายมือชื่อได้ พร้อมทั้งสามารถพิสูจน์เพื่อยืนยันได้ว่าข้อมูลที่ทำให้เกิดลายมือชื่ออิเล็กทรอนิกส์นั้นถูกควบคุมโดยเจ้าของลายมือชื่อเท่านั้น ซึ่งสะท้อนให้เห็นถึงการแสดงเจตนาของเจ้าของลายมือชื่อในการลงนามในธุรกรรมอย่างชัดเจน โดยการแสดงเจตนาในการลงลายมือชื่อในเอกสารอิเล็กทรอนิกส์ของเจ้าของลายมือชื่อมักเกิดขึ้นผ่านกระบวนการที่ผู้ใช้บริการ (User) อ่านและกดรับทราบเงื่อนไขและนโยบายการใช้บริการ และขั้นตอนที่ผู้ใช้บริการ (User) ใส่รหัสเพื่ออ่านสัญญาโดยสามารถพิจารณายืนยันหรือยกเลิกรายการได้

2) ความเชื่อมโยงไปยังเจ้าของลายมือชื่อ (Unique)

การพิสูจน์และยืนยันตัวตนของผู้ลงลายมือชื่อ (signatory) สามารถทำได้ผ่านการใช้เทคโนโลยีการจับคู่กุญแจ (Key Pair) โดยมีกระบวนการเข้าถึงตัวตนซึ่งใช้เพื่อพิสูจน์ว่าเป็นเจ้าของลายมือชื่อจริงและเพื่อยืนยันความถูกต้องแท้จริงของข้อมูล โดยการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือต้องจัดให้มีการพิสูจน์และยืนยันตัวตนในระดับที่เหมาะสมกับการทำธุรกรรม โดย NDID Platform อาศัยการสร้างลายมือชื่อด้วยเทคโนโลยีการจับคู่กุญแจ (Key Pair) เพื่อเสริมสร้างความเชื่อมโยงระหว่างลายมือชื่ออิเล็กทรอนิกส์กับเจ้าของลายมือซึ่งโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้งาน ประกอบกับการนำเทคโนโลยีการใช้อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device) [17] มาใช้เพื่อทำให้มั่นใจได้ว่าข้อมูลที่ถูกควบคุมเพื่อใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นถูกทำขึ้นโดยเจ้าของลายมือชื่อ เช่น การกรอกรหัสลับ เป็นต้น ประกอบกับผู้ลงลายมือชื่อได้ผ่านการพิสูจน์และยืนยันตัวตนด้วยบริการ eKYC มาก่อนลงลายมือชื่อตามมาตรฐานระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน IAL และ AAL ที่กำหนดด้วย เป็นไปตามหลักเกณฑ์ใน พ.ร.บ. ธุรกรรมฯ มาตรา 26 (1) และ UNCITRAL 2001 Article 6 (a)

[17] มธอ. 11-2566 เล่ม 3 ข้อ 3

3) การควบคุมของเจ้าของลายมือชื่อ (Sole Control)

การลงนามด้วยลายมือชื่ออิเล็กทรอนิกส์ผ่านฟังก์ชั่น eSignature เพื่อให้สามารถมั่นใจได้ว่าข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ถูกควบคุมโดยเจ้าของลายมือชื่อเท่านั้น โดยการควบคุมนั้นปราศจากการควบคุมโดยบุคคลอื่นที่ไม่ใช่เจ้าของลายมือชื่อ เจ้าของลายมือชื่อจะต้องเป็นผู้มีหน้าที่บริหารจัดการและรู้ถึงวิธีการเข้าถึงข้อมูลที่ใช้สร้างลายมือชื่อ เช่น รู้วิธีการเข้าถึงกุญแจส่วนตัวที่ใช้ในการสร้างลายมือชื่ออิเล็กทรอนิกส์แต่เพียงผู้เดียว เนื่องด้วยความเฉพาะตัวของการเข้าถึงกุญแจส่วนตัวสะท้อนให้เห็นว่าผู้ที่เป็นเจ้าของข้อมูลหรือเจ้าของกุญแจเท่านั้นที่จะสามารถนำกุญแจส่วนตัวนั้นมาใช้จับคู่เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ได้ เพราะหากกุญแจส่วนตัวนั้นสามารถถูกเข้าถึงหรือควบคุมโดยบุคคลอื่นได้ก็จะส่งผลให้การพิสูจน์ความแท้จริงของกระบวนการสร้างลายมือชื่ออิเล็กทรอนิกส์ไม่สามารถกระทำได้ [18] การใช้งานอยู่ภายใต้วัตถุประสงค์ของผู้ใช้บริการ (User) ซึ่งเป็นเจ้าของลายมือชื่อ ส่งผลให้สามารถใช้เป็นเครื่องพิสูจน์เพื่อยืนยันได้ว่าข้อมูลที่ทำให้เกิดลายมือชื่ออิเล็กทรอนิกส์นั้นถูกควบคุมโดยเจ้าของลายมือชื่อเท่านั้น และปราศจากการควบคุมหรือการแทรกแซงของบุคคลอื่น [19] ซึ่งเป็นไปตามหลักเกณฑ์ใน พ.ร.บ. ธุรกรรมฯ มาตรา 26 (2) และ UNCITRAL 2001 Article 6 (b)

ในการบริหารจัดการคู่กุญแจ ผู้พิสูจน์และยืนยันตัวตน (IdP) มีหน้าที่เป็นผู้สร้างคู่กุญแจที่ใช้สำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์ หลังจากที่ผู้ใช้บริการ (User) ได้มีการพิสูจน์และยืนยันตัวตนเรียบร้อยแล้ว โดยผู้พิสูจน์และยืนยันตัวตน (IdP) จะมอบกุญแจสาธารณะ (Public Key) ที่ถูกสร้างขึ้นไว้บน NDID Platform เพื่อใช้ในการลงทะเบียนผู้ใช้งาน (enrolled) เข้าสู่ระบบ ส่วนกุญแจส่วนตัว (Private Key) ผู้พิสูจน์และยืนยันตัวตน (IdP) จะเป็นผู้ดูแลและบริหารจัดการ สำหรับมาตรฐานการสร้างคู่กุญแจ NDID ได้กำหนดให้ใช้เทคโนโลยี Hardware Security Module (HSM) สำหรับกระบวนการสร้างกุญแจให้เป็นไปตามมาตรฐาน Federal Information Processing Standard (FIPS) 140-2 ที่ออกโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) โดยมาตรฐานนี้เข้ามากำหนดมาตรการรักษาความปลอดภัยโดยใช้เทคโนโลยี Cryptographic Module สำหรับการเข้ารหัสข้อมูลที่มีความอ่อนไหวแต่ไม่ได้จำแนกประเภทข้อมูล (Sensitive But Unclassified Information) [20]

---

[18] Vieira, Bárbara. “Remote (Digital) Signatures and eIDAS Regulation.” *Medium* (blog), July 9, 2021. https://b-vieira.medium.com/remote-digital-signatures-and-the-eidas-regulation-af4384be679d.

[19] NDID ได้กำหนดให้หน่วยงานสมาชิกจัดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปตามระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (Sole Control) เพื่อเป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล Remote Signing Service (ขมธอ. 36-2566) รายละเอียดปรากฏตาม NDID MQA

[20] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (Supercedes FIPS PUB 140-1, 1994 January 11) SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, Security Level 3, Page 10, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.140-2.pdf

4) การตรวจสอบและติดตามรายการที่เกิดขึ้นกับลายมือชื่อ (Traceability)

NDID Platform มีวิธีการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือ โดยได้นำเทคโนโลยีคู่กุญแจ (Key Pair) มาใช้เป็นองค์ประกอบที่สำคัญสำหรับการสร้างลายมือชื่ออิเล็กทรอนิกส์ให้มีคุณสมบัติที่สามารถตรวจสอบได้ว่าลายมือชื่ออิเล็กทรอนิกส์ที่ถูกสร้างขึ้นถูกแก้ไขหรือเปลี่ยนแปลงหรือไม่ และขั้นตอนของการลงลายมือชื่อด้วยเทคโนโลยีคู่กุญแจ (Key Pair) เพื่อให้เกิดเป็นลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือเป็นการให้บริการที่ได้มาตรฐานของ NDID Platform โดยได้ดำเนินการให้เป็นไปตามกฎหมายและหลักเกณฑ์ทั้งในประเทศไทยและในระดับสากล เพราะนอกจากคู่กุญแจสาธารณะและคู่กุญแจส่วนตัวเมื่อนำมาจับคู่กันแล้วจะสามารถสร้างลายมือชื่ออิเล็กทรอนิกส์ที่มีคุณสมบัติตามที่กฎหมายกำหนดได้ ในด้านการทำงานของเทคโนโลยีคู่กุญแจยังส่งเสริมให้เกิดความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์ว่ามีความถูกต้อง แม่นยำ และลดข้อโต้แย้งด้านความไม่แท้จริงของข้อมูลที่ใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ เนื่องจากคู่กุญแจส่วนตัวจะทำหน้าที่ในการลงลายมือชื่อในรูปแบบดิจิทัล และคู่กุญแจสาธารณะจะทำหน้าที่เป็นสิ่งที่ใช้พิสูจน์ความถูกต้องแท้จริงในตัวตนของเจ้าของลายมือชื่อ ด้วยเหตุนี้ การลงลายมือชื่อในรูปแบบดิจิทัลโดยใช้เทคโนโลยีคู่กุญแจจึงทำให้ความถูกต้องแท้จริงของข้อมูลมีความน่าเชื่อถือมากยิ่งขึ้นตาม FIPS 186-5 Digital Signature Standard (DSS) และมาตรฐาน NIST SP 800-63 Digital Identity Guidelines และการลงลายมือชื่อในรูปแบบดิจิทัลดังกล่าวยังมีผลบังคับใช้ทางกฎหมายด้วย [21] เนื่องจากเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ลงบนเอกสารสัญญาอิเล็กทรอนิกส์ทำให้ลายมือชื่ออิเล็กทรอนิกส์ถูกแนบไปหรือมีส่วนเกี่ยวข้องกับข้อมูลหรือเอกสารสัญญาอิเล็กทรอนิกส์ เพื่อให้สามารถตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ได้

นอกจากนี้ NDID ได้จัดให้มีการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์โดยการนำไฟล์เอกสารสัญญา PDF มาตรวจสอบกับรายการข้อมูลที่แนบอยู่กับไฟล์เอกสารสัญญา เช่น การตรวจสอบหมายเลขการทำรายการใน NDID Platform (request Id) หรือการตรวจสอบลำดับของบล็อกที่ทำรายการ (blockHeight) เป็นต้น โดย NDID ได้จัดเตรียมระบบสำหรับการตรวจสอบเพื่ออำนวยความสะดวกในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์สำหรับผู้ใช้บริการ (User) ซึ่งผู้ใช้บริการ (User) สามารถร้องขอการตรวจสอบข้อมูลไปยังผู้ให้บริการ (RP) เมื่อผู้ให้บริการ (RP) ได้รับคำร้องดังกล่าว จะดำเนินการตรวจสอบข้อมูลผ่านระบบสำหรับการตรวจสอบที่ NDID ได้จัดเตรียมไว้ โดยการกรอกรายละเอียดรายการข้อมูลตามที่ NDID กำหนด และเมื่อเสร็จสิ้นการตรวจสอบข้อมูลจึงจะแจ้งผลการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ให้กับผู้ใช้บริการ (User) ถึงความถูกต้องของเลขประจำตัวประชาชนผู้ลงลายมือชื่อ ข้อความในการลงนาม รวมถึงเอกสารแนบต่าง ๆ ทั้งนี้ NDID ได้กำหนดวิธีการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์นี้เพื่อให้สอดรับกับหลักการการตรวจสอบการเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ที่เกิดขึ้นหลังจากเวลาที่ลายมือชื่อตามหลักเกณฑ์ใน พ.ร.บ. ธุรกรรมฯ มาตรา 26 (3) และ UNCITRAL 2001 Article 6 (c)

[21] Use of Electronic Signatures in Federal Organization Transactions, General Services Administration and Federal Chief Information Officers Council, Version 1.0, 25 January 2013.

5) การตรวจพบการเปลี่ยนแปลงที่เกิดขึ้นแก่ข้อความ (Proof of Integrity and Original of Data)

การลงลายมือชื่ออิเล็กทรอนิกส์บนเอกสารสัญญาอิเล็กทรอนิกส์ คือการลงลายมือชื่อบนเอกสารรูปแบบดิจิทัลที่ได้มาตรฐานและมีคุณสมบัติเป็นต้นฉบับตามหลักเกณฑ์ที่กฎหมายกำหนด โดย NDID กำหนดให้จัดทำเอกสารสัญญาให้อยู่ในรูปแบบ Portable Document File (PDF) เพื่อแสดงผลข้อความที่ถูกต้องตรงกับข้อความที่อยู่ในรูปแบบกระดาษ (Hard copy) ซึ่ง NDID Platform ได้จัดให้มีช่องทางในการรักษาความถูกต้องสมบูรณ์ของลายมือชื่อและข้อความบนเอกสารสัญญาอิเล็กทรอนิกส์ โดยการจัดทำเอกสารสัญญาให้อยู่ในรูปแบบตามมาตรฐาน PDF A/3 ซึ่งมีคุณสมบัติในการบันทึกจัดเก็บข้อมูลที่อยู่ในไฟล์ได้อย่างถาวรโดยที่ข้อมูลไม่เปลี่ยนแปลงไป รวมถึงจัดให้มีกระบวนการเพื่อตรวจสอบการเปลี่ยนแปลงของเอกสารสัญญาอิเล็กทรอนิกส์ ทำให้ตรวจสอบได้ถึงการเปลี่ยนแปลงของลงลายมือชื่อและข้อความบนเอกสารสัญญาอิเล็กทรอนิกส์ได้ จึงทำให้การลงลายมือชื่ออิเล็กทรอนิกส์นี้มีผลบังคับใช้ทางกฎหมาย [22]

นอกจากนี้ NDID ยังได้จัดให้มีช่องทางตรวจสอบรายละเอียดและความเปลี่ยนแปลงที่เกิดขึ้นกับข้อความบนเอกสารสัญญาอิเล็กทรอนิกส์ได้ เพื่อให้มั่นใจว่าข้อความที่ถูกแสดงอยู่บนเอกสารสัญญาอิเล็กทรอนิกส์ฉบับปัจจุบันมีความถูกต้องและไม่ถูกแก้ไข ปรับปรุง หรือเปลี่ยนแปลง หรือหากกรณีเอกสารถูกแก้ไข ปรับปรุง หรือเปลี่ยนแปลง ก็สามารถตรวจสอบถึงรายละเอียดการแก้ไข ปรับปรุง หรือเปลี่ยนแปลงนั้นได้ โดยการจัดให้มีกระบวนการตรวจสอบเอกสารผ่านระบบสำหรับการตรวจสอบที่ NDID ได้จัดเตรียมไว้ โดยการนำไฟล์เอกสารสัญญา PDF มาตรวจสอบกับรายการข้อมูลที่แนบอยู่กับไฟล์เอกสารสัญญาอิเล็กทรอนิกส์ ดังนั้น เอกสารสัญญาอิเล็กทรอนิกส์นี้จึงถือได้ว่ามีการนำเสนอหรือเก็บรักษาให้เป็นเอกสารสัญญาต้นฉบับตามหลักเกณฑ์ใน พ.ร.บ. ธุรกรรมฯ มาตรา 10 ประกอบกับการให้บริการในทุกขั้นตอนผู้ใช้บริการ (User) และผู้ให้บริการ (RP) สามารถตรวจสอบรายละเอียดที่แสดงถึงความครบถ้วนหรือรายการที่เปลี่ยนแปลงไปได้ทั้งหมด ทั้งนี้ NDID ได้กำหนดวิธีการตรวจสอบข้อความบนเอกสารสัญญาอิเล็กทรอนิกส์นี้เพื่อให้สอดรับกับหลักการการตรวจพบการเปลี่ยนแปลงที่เกิดขึ้นแก่ข้อความ ตามหลักเกณฑ์ใน พ.ร.บ. ธุรกรรมฯ มาตรา 26 (4) และ UNCITRAL 2001 Article 6 (d)

3.4 ตัวอย่างบริการของ NDID Platform

3.4.1 บริการเปิดบัญชี

บริการเปิดบัญชีเป็นบริการที่สามารถดำเนินการทางออนไลน์ได้ผ่าน NDID Platform เช่น บัญชีธนาคาร บัญชีหลักทรัพย์ หรือบัญชีอื่น ๆ ทำให้ผู้ใช้บริการสามารถเปิดบัญชีออนไลน์ได้สะดวกและ

[22] Use of Electronic Signatures in Federal Organization Transactions, General Services Administration and Federal Chief Information Officers Council, Version 1.0, 25 January 2013.

รวดเร็วยิ่งขึ้น โดย NDID Platform ได้รองรับให้มีการพิสูจน์และยืนยันตัวตนผ่าน eKYC และการลงลายมือชื่ออิเล็กทรอนิกส์ผ่าน eSignature ซึ่งเป็นกระบวนการลงลายมือชื่อและวิธีการที่น่าเชื่อถือเพื่อให้การเปิดบัญชีออนไลน์นี้มีผลบังคับได้ตามกฎหมาย โดยคำนึงถึงหลักเกณฑ์และเงื่อนไขตามที่กฎหมาย ประกาศ คำสั่ง ข้อบังคับ และระเบียบของหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการให้บริการนั้นกำหนด รวมถึงสามารถรองรับการให้บริการลงลายมือชื่ออิเล็กทรอนิกส์เพื่อการเปิดบัญชีที่แตกต่างกันตามแต่ละประเภทบัญชี เช่น การเปิดบัญชีธนาคาร เป็นไปตามประกาศธนาคารแห่งประเทศไทย ที่ สนส.19/2562 เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน หรือการเปิดบัญชีหลักทรัพย์เป็นไปตามประกาศแนวปฏิบัติสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ นป.4/2566 เรื่อง แนวทางปฏิบัติในการนำเทคโนโลยีมาใช้ในการทำความรู้จักลูกค้า เป็นต้น

โดยการเปิดบัญชี ผู้ให้บริการ (RP) ต้องจัดให้ผู้ใช้บริการที่ขอเปิดบัญชีทำการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (IdP) ก่อนเสมอ รวมถึงกำหนดวิธีการที่น่าเชื่อถือเพื่อแสดงเจตนาโดยการลงลายมือชื่ออิเล็กทรอนิกส์โดยคำนึงถึงลักษณะ หรือประเภทของธุรกรรม ซึ่งผู้พิสูจน์และยืนยันตัวตน (IdP) อาจกำหนดวิธีการลงลายมือชื่อได้ตามความเหมาะสม เช่น การกดปุ่ม “ยอมรับ” หรือ “ตกลง” หรือ “ยืนยัน” [23] หรือการใส่ PIN หรือการระบุ OTP ก่อนกดยืนยันการทำรายการ เป็นต้น

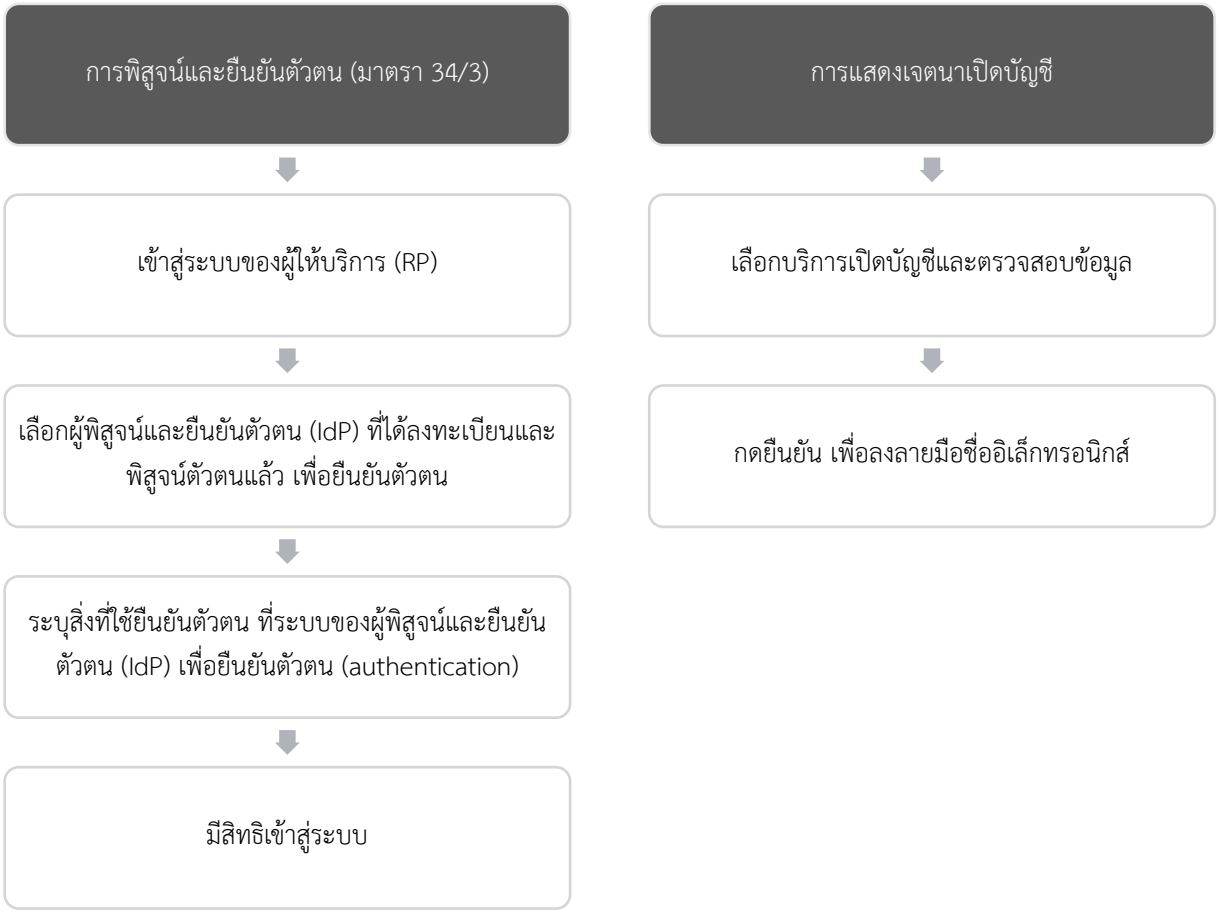
เมื่อการพิสูจน์และยืนยันตัวตนเป็นองค์ประกอบที่สำคัญเพราะลายมือชื่ออิเล็กทรอนิกส์นำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น [24] ดังนั้น ความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์จะเชื่อมโยงกันกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของบุคคลด้วย บริการเปิดบัญชีผ่าน NDID Platform จึงได้นำฟังก์ชั่น eKYC เพื่อพิสูจน์และยืนยันตัวตน และ eSignature เพื่อลงลายมือชื่ออิเล็กทรอนิกส์มาใช้ เมื่อการพิสูจน์และยืนยันตัวตนเป็นองค์ประกอบที่สำคัญเพราะลายมือชื่ออิเล็กทรอนิกส์นำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยสามารถระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่อที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น [25] ดังนั้น ความน่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์จะเชื่อมโยงกันกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตนของบุคคลด้วย บริการเปิดบัญชีผ่าน NDID Platform จึงได้นำฟังก์ชั่น eKYC เพื่อพิสูจน์และยืนยันตัวตน และ eSignature เพื่อลงลายมือชื่ออิเล็กทรอนิกส์มาใช้

[23] Bassano v Toft & Ors [2014] EWHC 377 (QB)

[24] UNCITRAL 1996, Article 7(1)(a)

[25] UNCITRAL 1996, Article 7(1)(a)

ภาพที่ 7 การเปิดบัญชีผ่าน NDID Platform [26]



[26] ผู้ใช้บริการสามารถเลือกยืนยันตัวตนได้ด้วยสิ่งที่ใช้ยืนยันตัวตน (authenticator) 3 ประเภท ทั้งนี้ เป็นไปตามที่ผู้พิสูจน์และยืนยันตัวตน (IdP) กำหนด

1. สิ่งที่ผู้ใช้บริการรู้ (something you know) เช่น รหัสผ่าน password หรือ PIN เป็นต้น
2. สิ่งที่ผู้ใช้บริการมี (something you have) เช่น รหัส OTP หรือ กุญแจส่วนตัว (private key) เป็นต้น
3. สิ่งที่ผู้ใช้บริการเป็น (something you are) เช่น ภาพใบหน้า หรือ ลายนิ้วมือ เป็นต้น

ตัวอย่างการเปิดบัญชีธนาคารกับสถาบันการเงินผ่าน NDID Platform

ผู้ใช้บริการ (User) ที่ต้องการสมัครบริการเปิดบัญชีธนาคารใหม่กับผู้ให้บริการ (RP) ที่เป็นธนาคารพาณิชย์ที่ตนไม่เคยมีบัญชีมาก่อน ผู้ใช้บริการ (User) ต้องเลือกผู้พิสูจน์และยืนยันตัวตน (IdP) ที่ตนเคยได้ทำการลงทะเบียนและพิสูจน์ตัวตนไว้แล้วเพื่อทำการยืนยันตัวตนผ่าน NDID Platform ก่อนสมัครบริการเปิดบัญชีธนาคาร

เมื่อผู้ใช้บริการ (User) เลือกช่องทางการยืนยันตัวตน eKYC ผ่าน NDID Platform หน้าต่างจะแสดงข้อกำหนดและเงื่อนไขการให้บริการเพื่อให้ผู้ใช้บริการ (User) ได้ศึกษารายละเอียดและเงื่อนไขการให้บริการยืนยันตัวตน ผู้ใช้บริการ (User) จะได้รับแจ้งเตือนจากผู้พิสูจน์และยืนยันตัวตน (IdP) โดยผู้ใช้บริการ (User) ต้องพิสูจน์และยืนยันตัวตนว่าเป็นบุคคลนั้นจริง ผ่านสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตามที่ธนาคารกำหนด เช่น ใส่ PIN หรือรหัส OTP เพื่อเข้าสู่ระบบของผู้พิสูจน์และยืนยันตัวตน (IdP)

เมื่อเข้าสู่ระบบสำเร็จ ผู้พิสูจน์และยืนยันตัวตน (IdP) จะแจ้งวัตถุประสงค์เพื่อการเปิดบัญชีธนาคารของผู้ให้บริการ (RP) พร้อมแจ้งรายการข้อมูลที่จำเป็นต่อการเชื่อมโยงข้อมูลผ่าน NDID Platform และเพื่อส่งข้อมูลให้ธนาคารผู้ให้บริการ (RP) เมื่อผู้ใช้บริการ (User) อ่านรายละเอียดตามที่ปรากฏในเอกสารเสร็จสิ้นจึงกดรับทราบและให้ความยินยอมในการประมวลผลข้อมูลเพื่อไปสู่ขั้นตอนถัดไป

ผู้ใช้บริการ (User) ต้องใส่รหัส (PIN) เพื่อตรวจสอบและยืนยันข้อมูล ซึ่งการยืนยันตัวตนผ่าน NDID Platform เพื่อการเปิดบัญชีธนาคารจะใช้การแสดงข้อมูลบนบัตรประจำตัวประชาชนประกอบกับเทคโนโลยีการจดจำใบหน้าของผู้ใช้บริการ (User) เป็นไปตามประกาศธนาคารแห่งประเทศไทย ที่ สนส. 19/2562 เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน

ทั้งนี้ โดยกระบวนการเปิดบัญชีในขั้นตอนการใส่รหัส PIN หรือกดปุ่มยืนยันผ่านฟังก์ชั่น eSignature เป็นการนำลายมือชื่ออิเล็กทรอนิกส์มาใช้เป็นหนึ่งในขั้นตอนในการยืนยันตัวตน เนื่องจากลายมือชื่ออิเล็กทรอนิกส์ที่เกิดขึ้นสามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อได้ จึงทำให้การยืนยันตัวตนมีความน่าเชื่อถือเชื่อมโยงกันกับลายมือชื่ออิเล็กทรอนิกส์ [27]

[27] พ.ร.บ. ธุรกรรมฯ มาตรา 34/3

ภาพที่ 8 การเปิดบัญชีธนาคาร [28]

[28] ผู้ใช้บริการสามารถเลือกยืนยันตัวตนได้ด้วยสิ่งที่ใช้ยืนยันตัวตน (authenticator) 3 ประเภท ทั้งนี้ เป็นไปตามที่ผู้พิสูจน์และยืนยันตัวตน (IdP) กำหนด

1. สิ่งที่ผู้ใช้บริการรู้ (something you know) เช่น รหัสผ่าน password หรือ PIN เป็นต้น
2. สิ่งที่ผู้ใช้บริการมี (something you have) เช่น รหัส OTP หรือ กุญแจส่วนตัว (private key) เป็นต้น
3. สิ่งที่ผู้ใช้บริการเป็น (something you are) เช่น ภาพใบหน้า หรือ ลายนิ้วมือ เป็นต้น

3.4.2 บริการ dContract

บริการ dContract เป็นบริการลงลายมือชื่ออิเล็กทรอนิกส์บน NDID Platform ที่ให้บริการสร้างลายมือชื่ออิเล็กทรอนิกส์ที่น่าเชื่อถือเพื่อใช้ในการลงลายมือชื่อสำหรับการทำธุรกรรมในรูปแบบดิจิทัล การลงลายมือชื่อบนเอกสารหรือสัญญาอิเล็กทรอนิกส์ เช่น สัญญากู้ยืมเงิน ใบสมัครใช้บริการ หรือการจัดทำหนังสือมอบอำนาจ รวมทั้งการลงลายมือชื่อเพื่อรับรองความถูกต้องของข้อมูลหรือเอกสารที่ได้นำส่งผ่านช่องทางอิเล็กทรอนิกส์ ผ่านฟังก์ชั่น eSignature ประกอบกับการนำฟังก์ชั่น eKYC มาใช้งานเพื่อให้ผู้ใช้บริการ (User) ทำการยืนยันตัวตนก่อนลงนามในสัญญา ซึ่งจะช่วยลดต้นทุนและลดความเสี่ยงในการดำเนินการเกี่ยวกับการลงลายมือชื่อในเอกสารสัญญาอิเล็กทรอนิกส์ โดยการให้บริการดังกล่าวทำให้ข้อมูลที่ใช้สำหรับสร้างลายมือชื่ออิเล็กทรอนิกส์นั้นมีความสามารถในการเชื่อมโยงไปยังเจ้าของลายมือชื่อทั้งในด้านความเชื่อมโยงกันของข้อมูลและอำนาจในการควบคุมข้อมูลนั้น นอกจากนี้ บริการ dContract ได้จัดให้มีวิธีการตรวจสอบความถูกต้องแท้จริงของลายมือชื่ออิเล็กทรอนิกส์ที่ถูกสร้างขึ้นว่ามีการเปลี่ยนแปลงหรือแก้ไขเกิดขึ้นกับลายมือชื่ออิเล็กทรอนิกส์หรือข้อความหรือไม่ ด้วยลักษณะการสร้างลายมือชื่ออิเล็กทรอนิกส์ตามคุณสมบัติดังกล่าวจึงทำให้การให้บริการนี้สอดคล้องตามหลักเกณฑ์ที่ระบุใน พ.ร.บ. ธุรกรรมฯ มาตรา 26

ทั้งนี้ เอกสารหรือสัญญาบางประเภทมีเนื้อหาจำนวนมากทำให้มีข้อจำกัดในการแสดงข้อความหรือเนื้อหาของเอกสารหรือสัญญาทั้งหมดแก่ผู้ใช้บริการ (User) เพื่อลงลายมือชื่อผ่านช่องทางอุปกรณ์สื่อสาร เช่น Mobile Banking ดังนั้น ด้วยพัฒนาการทางเทคโนโลยีและเทคนิคในปัจจุบัน ทำให้มีการใช้เทคโนโลยีและเทคนิคในรูปแบบต่าง ๆ ที่สามารถแสดงข้อมูลเพื่อการลงลายมือชื่ออิเล็กทรอนิกส์ผ่านบริการ dContract ได้ โดยมีการให้บริการในปัจจุบัน 3 รูปแบบ ดังนี้

1) การลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนสัญญาฉบับเต็ม

รูปแบบการลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนสัญญาฉบับเต็ม เป็นการจัดทำสัญญาฉบับเต็มในรูปแบบอิเล็กทรอนิกส์ให้ผู้ใช้บริการ (User) อ่านและรับทราบรายละเอียดทั้งหมดของสัญญา เช่น การแสดงสัญญาฉบับเต็มบนหน้าจอผ่านทาง Mobile Banking Application และผู้ใช้บริการ (User) ดำเนินการยืนยันตัวตนเพื่อลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนสัญญาฉบับเต็ม ทำให้คู่กุญแจ (PKI) ซึ่งเป็นลายมือชื่ออิเล็กทรอนิกส์ของผู้ใช้บริการ (User) กลายเป็นส่วนหนึ่งหรือแนบไปกับสัญญาฉบับเต็มนั้น และไม่สามารถแก้ไขหรือเปลี่ยนแปลงได้

2) การลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนเอกสารที่ถูก hash

รูปแบบการลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนเอกสารที่ถูก hash เป็นการจัดทำสัญญาในรูปแบบอิเล็กทรอนิกส์ให้ผู้ใช้บริการ (User) อ่านและรับทราบรายละเอียดทั้งหมดของสัญญาผ่านช่องการสื่อสาร เช่น

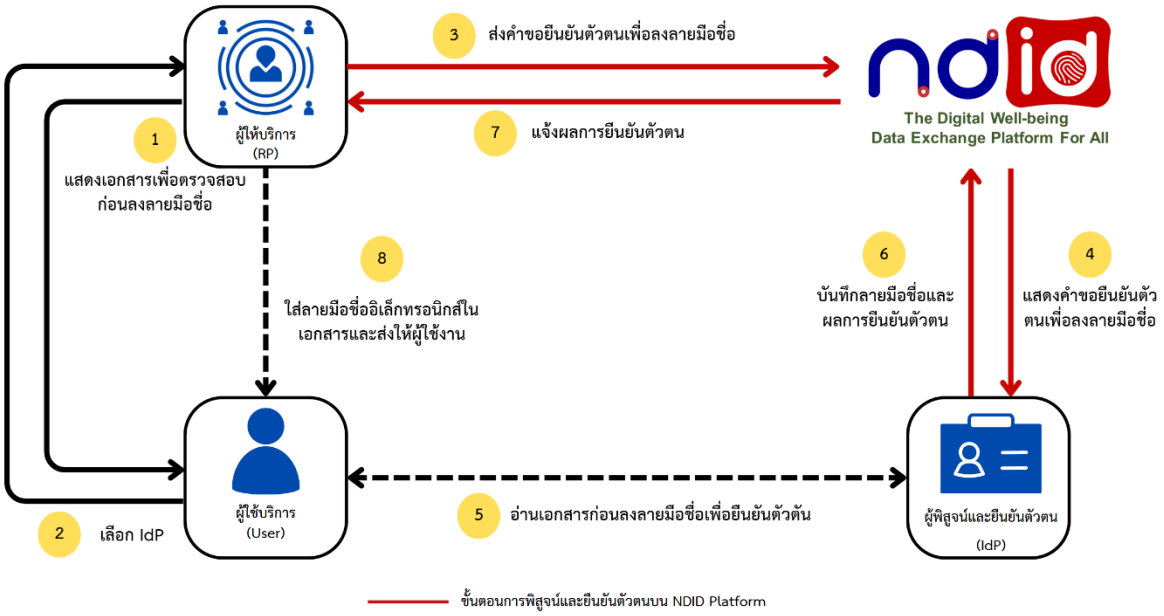
ส่งผ่านทาง verified e-mail ของผู้ใช้บริการ (User) เพื่ออ่านและรับทราบรายละเอียดทั้งหมดของสัญญาผ่านหน้าจอคอมพิวเตอร์ จากนั้นเอกสารหรือสัญญาอิเล็กทรอนิกส์สำหรับการลงลายมือชื่อดังกล่าวจะถูกทำการ hash (การหาตัวเลขทางคณิตศาสตร์แทนเอกสารสัญญา โดยสามารถตรวจสอบการเปลี่ยนแปลงแก้ไขเอกสารสัญญานั้นได้ แม้เป็นเพียงการแก้ไขตัวอักษรในเอกสารสัญญา หรือการเว้นวรรค ซึ่งตัวเลขคณิตศาสตร์จะแสดงผลที่เปลี่ยนแปลงไป) และถูกเข้ารหัสในการรับส่งข้อมูลไว้ ก่อนให้ผู้ใช้บริการ (User) ดำเนินการยืนยันตัวตนเพื่อลงลายมือชื่อ เมื่อผู้ใช้บริการ (User) พิจารณาลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนเอกสารที่ถูก hash เรียบร้อยแล้วนั้น จะทำให้คู่กุญแจ (PKI) ซึ่งเป็นลายมือชื่ออิเล็กทรอนิกส์แนบไปกับเอกสารที่ถูก hash โดยทั้งเอกสารและลายมือชื่ออิเล็กทรอนิกส์ของผู้ใช้บริการ (User) จะถูก hash และถูกเข้ารหัสในการรับส่งข้อมูลอีกครั้ง ทั้งนี้ในการขึ้นระบบ (implementation) สามารถมีได้หลายรูปแบบ เช่น hash เอกสารโดยตรง หรือ hash link เป็นต้น

3) การลงลายมือชื่อด้วยกุญแจ (PKI) บน Smart Contract

รูปแบบการลงลายมือชื่อด้วยคู่กุญแจ (PKI) บน Smart Contract เป็นการจัดทำสัญญาในรูปแบบอิเล็กทรอนิกส์ที่ประกอบด้วย 2 ส่วน คือ ส่วนแรกเป็นข้อสัญญาฉบับมาตรฐานซึ่งแต่ละประเภทสัญญาจะมีหมายเลขอ้างอิงเฉพาะของแต่ละสัญญานั้น ๆ (template ID) แยกตามแต่ละ version ของสัญญามาตรฐาน โดยมีเงื่อนไขที่เป็นไปตามกฎหมายกำหนดและมีข้อตกลงที่สำคัญเดียวกัน (มีการจัดเก็บที่สามารถตรวจสอบย้อนกลับข้อความได้ (Long-term validation material) และส่วนที่สองเป็นข้อมูลส่วนบุคคลเฉพาะของแต่ละรายผู้ใช้บริการ (User) เช่น ชื่อ นามสกุล จำนวนเงินที่กู้ยืม อัตราดอกเบี้ย เป็นต้น

โดยองค์ประกอบทั้ง 2 ส่วนนี้จะรวมกันแสดงหมายเลขอ้างอิงเฉพาะ (template ID) และเวอร์ชั่น (version) ของสัญญามาตรฐานพร้อมข้อมูลส่วนบุคคลเฉพาะของแต่ละรายผู้ใช้บริการ (User) ให้ผู้ใช้บริการ (User) อ่านและรับทราบรายละเอียดของสัญญา เช่น การแสดงสัญญาผ่านทาง Mobile Banking Application ก่อนที่จะดำเนินการยืนยันตัวตน และลงลายมือชื่อด้วยคู่กุญแจ (PKI) บน Smart Contract ต่อไป

ภาพที่ 9 การลงลายมือชื่อในเอกสารหรือสัญญาอิเล็กทรอนิกส์



[Creation] สำหรับการสร้างลายมือชื่ออิเล็กทรอนิกส์ในบริการ dContract โดย NDID นำเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) มาใช้เป็นส่วนสำคัญในการรักษาความถูกต้องและความมั่นคงปลอดภัยของข้อมูลที่ใช้ประกอบกันเพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ให้มีคุณสมบัติที่น่าเชื่อถือตามองค์ประกอบที่กฎหมายกำหนด โดยเทคโนโลยี PKI นี้ มีวิธีการดำเนินการเพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ผ่านการจับคู่กุญแจสาธารณะและกุญแจส่วนตัวซึ่งมีคุณสมบัติที่สามารถเข้ากันได้ นอกจากนี้ ยังนำเทคโนโลยีที่ใช้เพื่อสร้างลายมือชื่ออิเล็กทรอนิกส์ให้มีคุณสมบัติในการยืนยันตัวตนผู้ใช้บริการ (User) มาประกอบการให้บริการ เช่น การใช้ Verifiable Credentials [29] เพื่อยืนยันตัวตนผู้ใช้บริการ (User)

[29] Verifiable Credential (VC) สำหรับการลงลายมือชื่ออิเล็กทรอนิกส์เป็นมาตรฐานในการแสดงข้อมูลประจำตัวที่สามารถตรวจสอบความถูกต้องได้ทางดิจิทัล โดยมีคุณสมบัติหลักดังนี้:

1. Self-sovereign Identity: เจ้าของข้อมูล (เช่น บุคคลหรือองค์กร) สามารถควบคุมข้อมูลประจำตัวของตนเองได้
2. Issuers, Holders, and Verifiers: ข้อมูลใน VC ถูกออกโดยหน่วยงานที่น่าเชื่อถือ เช่น รัฐบาล สถาบันการศึกษา หรือบริษัท ซึ่งข้อมูลนี้ถูกลงนามด้วยเทคโนโลยีคู่คีย์ (PKI) เพื่อป้องกันการแก้ไข, ผู้ถือข้อมูล (Holder) และผู้ตรวจสอบข้อมูล (Verifier) ซึ่งสามารถตรวจสอบได้ว่าข้อมูลประจำตัวเป็นของจริงและยังไม่ถูกแก้ไข
3. Cryptographic Signatures: ข้อมูลใน VC จะถูกลงนามโดยใช้เทคโนโลยีคู่คีย์ (PKI) ทำให้สามารถตรวจสอบได้ว่าใครเป็นผู้ออกและไม่มีการแก้ไขข้อมูลตั้งแต่ถูกออก
4. Decentralization: ประยุกต์ใช้เทคโนโลยีบล็อกเชนหรือโครงสร้างแบบกระจาย (Decentralized) เพื่อลดความเสี่ยงของการควบคุมจากศูนย์กลาง

ก่อนการสร้างลายมือชื่ออิเล็กทรอนิกส์ให้มีองค์ประกอบที่น่าเชื่อถือตามหลักเกณฑ์ที่กฎหมายกำหนด เพื่อให้ผู้ใช้บริการ (User) เท่านั้นที่สามารถลงนามในเอกสารสัญญาอิเล็กทรอนิกส์ได้

[Validation] สำหรับการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์จากบริการ eSignature ภายหลังจากที่ได้ลงลายมือชื่อแล้วว่าถูกแก้ไขหรือเปลี่ยนแปลงหรือไม่ NDID มีกระบวนการในการสร้างและเพิ่มความน่าเชื่อถือให้กับลายมือชื่อ (Signature Augmentation) เพื่อให้ลายมือชื่อมีข้อมูลการตรวจสอบความถูกต้องในระยะยาว (signature with long-term validation material) เป็นลายมือชื่อที่มีข้อมูลตรวจสอบความถูกต้องลายมือชื่อมีความพร้อมใช้ระยะยาว โดย NDID ได้จัดให้มีระบบสำหรับการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์โดยการนำเอกสารอิเล็กทรอนิกส์ มาตรวจสอบกับรายการข้อมูลที่แนบอยู่กับเอกสารสัญญาอิเล็กทรอนิกส์ โดย NDID ได้กำหนดรายการข้อมูลที่ผู้ให้บริการ (RP) ต้องระบุเพื่อการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ผ่านการนำไฟล์เอกสารสัญญามาตรวจสอบกับรายการข้อมูลที่ปรากฏในลายมือชื่ออิเล็กทรอนิกส์ที่แนบอยู่กับไฟล์ในเอกสารสัญญา ซึ่งใช้สำหรับการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ให้กับผู้ให้บริการ (RP) ที่ได้รับคำร้องตรวจสอบลายมือชื่ออิเล็กทรอนิกส์จากผู้ใช้บริการ (User) แล้ว NDID จะทำการตรวจสอบข้อมูลตามที่ผู้ให้บริการ (RP) ระบุไว้ และแจ้งผลการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ให้ผู้ให้บริการ (RP) และผู้ใช้บริการ (User) ทราบ

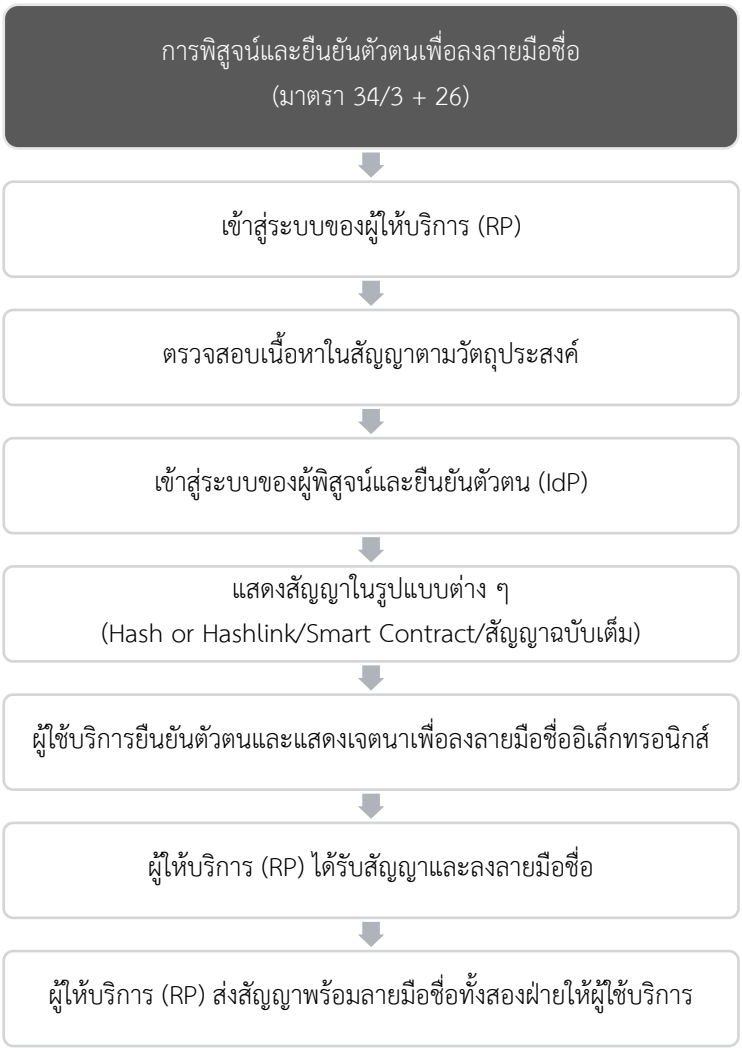
โดยตัวอย่างการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ มีรายการตรวจสอบอย่างน้อย ดังนี้

5. Privacy-preserving: VC ช่วยในการปกป้องความเป็นส่วนตัว ผู้ถือข้อมูลสามารถเลือกที่จะแชร์เฉพาะข้อมูลที่จำเป็นต่อการตรวจสอบ เช่น การยืนยันคุณสมบัติโดยไม่ต้องเปิดเผยข้อมูลส่วนตัวทั้งหมด

เทคโนโลยี VC สามารถนำมาใช้เพื่อการลงนามอิเล็กทรอนิกส์ในลักษณะที่เจ้าของข้อมูลสามารถยืนยันสิทธิ์หรืออำนาจของตนในรูปแบบดิจิทัลโดยไม่จำเป็นต้องใช้ข้อมูลประจำตัวแบบดั้งเดิม

ตารางที่ 2 ตัวอย่างรายการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์จากบริการ dContract		
ลำดับ	**รายการ**	**คำอธิบาย**
1.	requestId	หมายเลขการทำรายการใน NDID Platform
2.	requestMessage	ข้อความที่ผู้ให้บริการ (RP) ต้องการแสดงให้ผู้ใช้บริการ (User) เห็นผ่านผู้พิสูจน์และยืนยันตัวตน (IdP)
3.	salt	เลขสุ่มเพื่อเพิ่มความปลอดภัยสำหรับ request Message ก่อนที่จะทำการแฮชข้อมูล (hash)
4.	blockHeight	ลำดับของ Block ที่ทำรายการ
5.	chainId	ชื่อของ Blockchain ที่ทำรายการ
6.	createdAt	เวลาที่สร้างรายการ
7.	signature	ลายมือชื่ออิเล็กทรอนิกส์ของผู้ใช้บริการ (signatory)
8.	verifiyMethod	วิธีการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์
9.	rpTimeStamp	เวลาที่ทำรายการใน server/website ของผู้ให้บริการ (RP) และชื่อผู้ให้บริการ (RP)
10.	idpTimeStamp	เวลาที่ทำรายการใน server/website ของผู้พิสูจน์และยืนยันตัวตน (IdP) และชื่อผู้พิสูจน์และยืนยันตัวตน (IdP)
11.	asTimeStamp	เวลาที่ทำรายการใน server/website ของผู้ให้ข้อมูลที่น่าเชื่อถือ (AS) และชื่อผู้ให้ข้อมูลที่น่าเชื่อถือ (AS)
12.	templateId	หมายเลขของ template สัญญา
13.	documentType	ประเภทเอกสาร
14.	citizenId	หมายเลขประจำตัวประชาชน
15.	dynamicData	Field ข้อมูล ซึ่งแปรผันไปตาม template ที่เลือก

ภาพที่ 10 ตัวอย่างขั้นตอนการลงลายมือชื่อผ่านบริการ dContract



ดังนั้น การทำสัญญาทางอิเล็กทรอนิกส์ผ่านบริการ dContract ผ่านกระบวนการสร้างลายมือชื่ออิเล็กทรอนิกส์ในรูปแบบเทคโนโลยี PKI ตามหลักเกณฑ์ที่ระบุใน พ.ร.บ. ธุรกรรมฯ มาตรา 26 ทั้ง 3 รูปแบบ การลงลายมือชื่อด้วยคู่กุญแจ (PKI) บนเอกสารฉบับเต็มบนเอกสารที่ถูกเข้ารหัส (hash) และบนเอกสาร Smart Contract เช่น สัญญากู้ยืมเงิน ใบสมัครใช้บริการ หรือการจัดทำหนังสือมอบอำนาจ รวมทั้งการลงลายมือชื่อเพื่อรับรองความถูกต้องของข้อมูลหรือเอกสารที่ได้นำส่งผ่านช่องทางอิเล็กทรอนิกส์ จึงมีผลผูกพันและบังคับใช้ทางกฎหมายได้ตาม พ.ร.บ. ธุรกรรมฯ มาตรา 7 รวมถึงสามารถเป็นเอกสารสัญญาต้นฉบับตามมาตรา 10 และใช้เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายได้ ตามมาตรา 11

4. การคุ้มครองข้อมูลส่วนบุคคล

NDID Platform ได้ออกแบบตามหลัก Data Security and Privacy by design [30] ซึ่งคำนึงถึงหลักการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ ในการให้บริการต่าง ๆ รวมถึงการกำหนดแนวนโยบายเพื่อการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการทำงานต่าง ๆ ดังนี้

- เราได้คาดการณ์ความเสี่ยงและเหตุการณ์ที่อาจละเมิดความเป็นส่วนตัวไว้ล่วงหน้าและดำเนินการเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล
- เรารับรองว่าข้อมูลส่วนบุคคลได้รับการปกป้องโดยอัตโนมัติในทุกระบบ บริการ ผลิตภัณฑ์และ/หรือแนวปฏิบัติทางธุรกิจ ดังนั้นเจ้าของข้อมูลจึงไม่จำเป็นต้องกระทำการใด ๆ เพื่อปกป้องข้อมูลของด้วยตัวเองอีก
- เราได้แจ้งข้อมูลการติดต่อของผู้รับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคลให้กับบุคลากรภายในองค์กรและเจ้าของข้อมูลส่วนบุคคล
- เราใช้ นโยบายภาษาที่เข้าใจง่าย สำหรับเอกสารที่ใช้ประกาศกับสาธารณะเพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าใจได้ง่ายว่าเรากำลังทำอะไรกับข้อมูลส่วนบุคคลอยู่
- เราได้จัดเตรียมเครื่องมือและวิธีการต่าง ๆ เพื่อให้เจ้าของข้อมูลสามารถกำหนดวิธีในการประมวลผลข้อมูลส่วนบุคคลของเขาได้ และให้เจ้าของข้อมูลได้ตรวจสอบว่านโยบายของเราถูกบังคับใช้อย่างเหมาะสมหรือไม่
- เราได้ตั้งค่าเริ่มต้นด้านความเป็นส่วนตัวอย่างเข้มงวด รวมถึงจัดให้มีตัวเลือกและการควบคุมตามความต้องการของผู้ใช้งานที่สามารถใช้งานได้โดยง่าย
- เราไม่มีการใช้ผู้ประมวลผลข้อมูลส่วนบุคคล หากมีเราจะเลือกเฉพาะแต่ผู้ประมวลผลข้อมูลส่วนบุคคลที่รับประกันได้ว่ามีมาตรการทางเทคนิคและมาตรการทางองค์กรที่เหมาะสมสำหรับหลักการ Data protection by design
- เมื่อเราใช้ระบบ บริการ หรือผลิตภัณฑ์อื่นในกิจกรรมการประมวลผลข้อมูลของเรา เราได้ตรวจสอบให้แน่ใจแล้วว่าเรามีการใช้เฉพาะแต่ผู้ออกแบบและผู้ผลิตที่คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล
- เราใช้เทคโนโลยีเพิ่มความเป็นส่วนตัว (privacy-enhancing technologies: PET) เพื่อช่วยในการปฏิบัติตามการคุ้มครองข้อมูลส่วนบุคคลโดยการออกแบบ (Data protection by design)

[30] GDPR, Article 25 and Information Commissioner's Office, *Data Protection by Design and Default*, (2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-by-design-and-default/ (last visited Mar 5, 2024).

5. การประเมิน Member Qualification Assessment Framework (NDID MQA)

NDID เป็นผู้บริหารจัดการโครงสร้างพื้นฐานกุญแจสาธารณะและมาตรฐานที่เกี่ยวข้อง โดยใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ซึ่งจะจัดเก็บกุญแจสาธารณะ (public key) ของหน่วยงานสมาชิกไว้บน Blockchain เพื่อตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของหน่วยงานสมาชิกในการทำธุรกรรม [31] และเพื่อการรักษาความปลอดภัยและมาตรฐานของการใช้บริการ NDID Platform โดย NDID ได้กำหนดมาตรฐานของการดำเนินการของหน่วยงานสมาชิก ผ่านการประเมิน Member Qualification Assessment Framework (MQA) ก่อนการอนุญาตให้เข้าเป็นหน่วยงานสมาชิกและเชื่อมต่อระบบกับ NDID Platform ด้วยการตรวจสอบมาตรฐานในด้านต่าง ๆ เพื่อบริหารจัดการ (manage) และควบคุม (control) หน่วยงานสมาชิกในการออกและจัดเก็บคู่กุญแจสาธารณะ (public key) และกุญแจส่วนบุคคล (private key) [32] ซึ่งอยู่ในความครอบครองของผู้ลงลายมือชื่อ [33] เพื่อการลงลายมือชื่ออิเล็กทรอนิกส์ และเพื่อยืนยันตัวตน และรับประกันความถูกต้องและความสมบูรณ์ของข้อมูลอย่างการลงลายมือชื่ออิเล็กทรอนิกส์ในเอกสารหรือสัญญาอิเล็กทรอนิกส์

การประเมินและตรวจสอบคุณสมบัติของผู้พิสูจน์และยืนยันตัวตน (IdP) ดำเนินการตาม Member Qualification Assessment Framework (MQA) ตามเงื่อนไขที่ NDID กำหนด รวมถึงการได้รับอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) โดยก่อนการเข้าร่วมเป็นหน่วยงานสมาชิก ผู้พิสูจน์และยืนยันตัวตน (IdP) ต้องดำเนินการประเมินและตรวจติดตามระบบของผู้พิสูจน์และยืนยันตัวตน (IdP) และการให้บริการผ่าน NDID Platform อย่างสม่ำเสมอ การประเมินผ่าน MQA นั้น NDID ได้ทำการตรวจสอบมาตรการของหน่วยงานสมาชิกทั้งในเรื่องการระบุ (Identify) ป้องกัน (Protect) ตรวจสอบ (Detect) รับมือ (Response) กู้คืน (Recover) ความเสี่ยงทางไซเบอร์ในด้านต่าง ๆ รวมถึงการตรวจสอบการออกและจัดเก็บคู่คีย์ (Cryptographic Key generation and storage) ของหน่วยงานสมาชิกด้วย ซึ่งทำให้มั่นใจได้ว่าการให้บริการ eKYC และ eSignature ผ่าน NDID Platform จึงมีความน่าเชื่อถือและมั่นคงปลอดภัย

ทั้งนี้ รายละเอียดการประเมินและตรวจสอบเป็นไปตามข้อกำหนดใน NDID Member Qualification Assessment Framework และ Membership Agreement

---

[31] การตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์ที่ดำเนินการโดยหน่วยงานสมาชิกเป็นกระบวนการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์โดยอ้างอิงจากข้อความต้นฉบับและคู่กุญแจที่สอดคล้องกัน โดย NDID Platform จะยืนยันความถูกต้องเมื่อกุญแจสาธารณะของผู้ลงลายมือชื่อเข้าได้กับลายมือชื่ออิเล็กทรอนิกส์ที่สร้างด้วยกุญแจส่วนตัวของผู้ลงลายมือชื่อ โดยลายมือชื่อและข้อความไม่มีการเปลี่ยนแปลงไป ทั้งนี้ เทียบเคียงหลักการตรวจสอบตามเงื่อนไขของลายมือชื่ออิเล็กทรอนิกส์ตาม พ.ร.บ. ธุรกรรมฯ มาตรา 26 และ UNCITRAL 2001, Part 2 Guide to Enactment, at 43 - 44.

[32] NIST SP 800-63-3, Appendix A.

[33] เทียบเคียงหลักการตรวจสอบตามเงื่อนไขของลายมือชื่ออิเล็กทรอนิกส์ตาม พ.ร.บ. ธุรกรรมฯ มาตรา 26 และ UNCITRAL 2001, Part 2 Guide to Enactment, at 48.

The Digital Well-being
Data Exchange Platform For All