กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ETDA

ประชุมรับฟังความคิดเห็นต่อ
ร่างข้อเสนอแนะมาตรฐาน

บริการลงลายมือชื่อดิจิทัล ที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)

วันพฤหัสบดีที่ 18 พฤษภาคม 2566 เวลา 13.30 - 15.30 น.
ผ่านโปรแกรม Microsoft Teams Meeting

รายละเอียดเพิ่มเติม

ร่วมแสดงความคิดเห็น
ภายในวันที่ 19 พฤษภาคม 2566

ผ่านทาง อีเมล: estandard.center@etda.or.th
สอบถามข้อมูลเพิ่มเติมได้ที่ โทร 02-123-1234 # 91510
www.etda.or.th/th/StandardNews/03052566.aspx

นำเสนอโดย คณะที่ปรึกษาโครงการฯ
จุฬาลงกรณ์มหาวิทยาลัย

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

หัวข้อการประชุม

- ทำไมต้องมีมาตรฐาน Remote Signing
- ร่างมาตรฐานฯ อ้างอิงมาจากแหล่งใด
- รายละเอียดสำคัญของ ร่างมาตรฐานฯ
- รับฟังข้อคิดเห็น ข้อเสนอแนะ และ ตอบข้อสงสัย

บริการลงลายมือชื่อดิจิทัล ที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)

ทำไมต้องมีมาตรฐาน Remote Signing

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔)[๑๙] ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อเป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

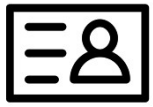
---

[๑๙] มาตรา ๒๖ วรรคหนึ่ง (๔) แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

UNIQUELY LINKED — Data that is uniquely linked to the signatory



IDENTIFICATION — Data that is capable to identify the signatory

SOLE CONTROL — Data that is sole control led by the signatory

DETECTABLE CHANGE — Data that any later change is detectable

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

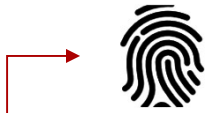
(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔)[๑๙] ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อเป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

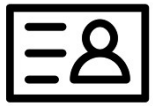
บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

---

[๑๙] มาตรา ๒๖ วรรคหนึ่ง (๔) แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒



UNIQUELY LINKED — Data that is uniquely linked to the signatory



IDENTIFICATION — Data that is capable to identify the signatory

SOLE CONTROL — Data that is sole control led by the signatory

DETECTABLE CHANGE — Data that any later change is detectable

พระราชบัญญัติ
ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
พ.ศ. ๒๕๔๔

หมวด ๒
ลายมือชื่ออิเล็กทรอนิกส์

มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และ

(๔)[๑๙] ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อเป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์

บทบัญญัติในวรรคหนึ่ง ไม่เป็นการจำกัดว่าไม่มีวิธีการอื่นใดที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือการแสดงพยานหลักฐานใดเกี่ยวกับความไม่น่าเชื่อถือของลายมือชื่ออิเล็กทรอนิกส์

---

[๑๙] มาตรา ๒๖ วรรคหนึ่ง (๔) แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒

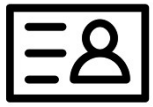
กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

DIGITAL SIGNATURE

UNIQUELY LINKED

Data that is uniquely linked to the signatory



IDENTIFICATION

Data that is capable to identify the signatory

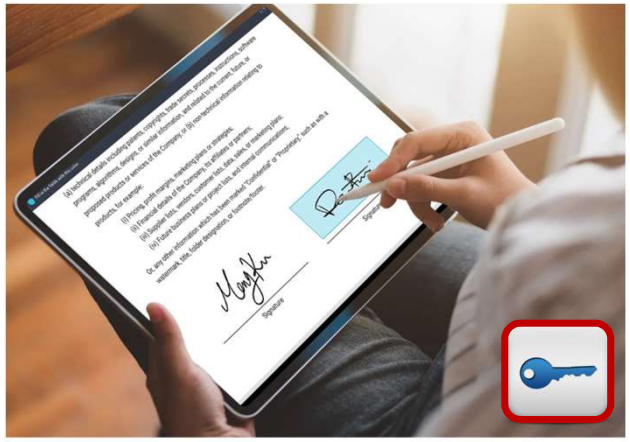
SOLE CONTROL

Data that is sole control led by the signatory

DETECTABLE CHANGE

Data that any later change is detectable

Local Signing



กุญแจสำหรับสร้างลายมือชื่อดิจิทัล ถูกเก็บไว้ที่เจ้าของลายมือชื่อ โดยอาจเก็บในอุปกรณ์อิเล็คทรอนิกส์ (hardware) เช่น USB Token หรือ ติดตั้งในรูปแบบซอฟต์แวร์ (software) บนอุปกรณ์คอมพิวเตอร์

- การลงนามอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อแต่เพียงผู้เดียว เนื่องจาก Signing Key เก็บไว้กับตัวเจ้าของลายมือชื่อ
- จำเป็นต้องมีอุปกรณ์ด้านความปลอดภัยเพิ่มเติม หรือต้องติดตั้งซอฟต์แวร์เพิ่มเติมที่อุปกรณ์คอมพิวเตอร์ของเจ้าของลายมือชื่อ
- การลงนาม Anywhere, Anytime, Any Device เป็นเรื่องท้าทาย เนื่องจากต้องพกพาอุปกรณ์ด้านความปลอดภัย /อุปกรณ์คอมพิวเตอร์ติดตัวตลอดเวลา

Remote Signing

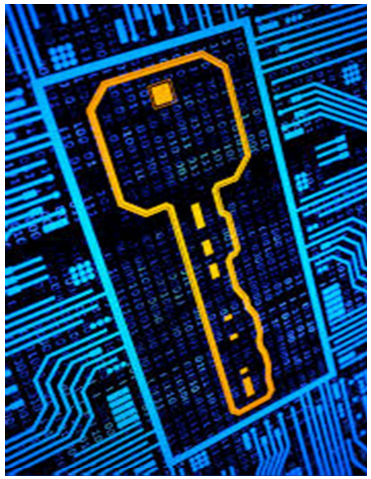
กุญแจสำหรับสร้างลายมือชื่อดิจิทัล มิได้เก็บไว้ที่เจ้าของลายมือชื่อ แต่ถูกเก็บไว้บนระบบ โดยเรียกใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์

- ต้องมีระบบ กระบวนการ และผู้ให้บริการที่เชื่อถือได้ เพื่อให้มั่นใจว่าการลงนามอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อแต่เพียงผู้เดียว
- ไม่จำเป็นต้องมี hardware พิเศษ หรือติดตั้ง software ใดๆเพิ่มเติม
- สะดวกสบายในการลงนาม Anywhere, Anytime, Any Device

ปัจจุบันระบบการลงลายมือชื่อดิจิทัลส่วนใหญ่ จะอำนวยความสะดวกให้กับผู้ใช้งาน โดยการเก็บรักษากุญแจส่วนตัว (private key) และสั่งให้สร้างลายมือชื่อดิจิทัลด้วยกุญแจส่วนตัวนั้น ผ่านระบบเครือข่ายคอมพิวเตอร์

ประเด็นพิจารณา คือ การที่จะต้องมีกลไกในการยืนยันว่ากุญแจส่วนตัวนั้น ต้องอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)

มาตรฐานการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service)



เพิ่มทางเลือกวิธีการลงลายมือชื่อดิจิทัลที่เชื่อถือได้

- อำนวยความสะดวกและลดอุปสรรคจากการจัดเก็บกุญแจส่วนตัวไว้กับเจ้าของลายมือชื่อ
- ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้สำหรับหน่วยงานที่ต้องการใช้ และ/หรือให้บริการ
- สร้างความเข้าใจที่ตรงกันระหว่างหน่วยงานที่เกี่ยวข้อง ผู้ให้บริการ เจ้าของลายมือชื่อและคู่กรณี

ร่างมาตรฐานฯ อ้างอิงมาจากแหล่งใด

การลงลายมือชื่ออิเล็กทรอนิกส์ที่ใช้การควบคุมจากระยะไกล (remote signing) ที่อำนวยความสะดวกให้กับผู้ใช้งานในการเก็บรักษาและเรียกใช้งานกุญแจส่วนตัว (private key) ผ่านระบบเครือข่ายคอมพิวเตอร์ นั้น

โดยในปัจจุบันรูปแบบนี้ได้รับการยอมรับในทางกฎหมายในสหภาพยุโรปตามข้อกำหนดใน **กฎหมายเอดาส (eIDAS)** ซึ่งได้ออกข้อกำหนดเทคนิค วิธีการ และรูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์ที่ใช้การควบคุมระยะไกล (remote signing หรือ server signing) ไว้เป็นมาตรฐานทางเทคนิคของสหภาพยุโรปแล้ว

ซึ่งคณะกรรมการด้านมาตรฐานของสหภาพยุโรป (CEN) ได้กำหนดมาตรฐานความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy systems supporting server signing) โดยข้อกำหนดเกี่ยวกับระบบการลงลายมือชื่อที่ใช้การควบคุมจากระยะไกล **CEN EN 419 241** ถูกนำมาใช้เป็นแนวทางในการจัดทำ ร่างข้อเสนอแนะมาตรฐานบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service) ฉบับของทาง ETDA นี้

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014

On electronic identification and trust services for electronic transactions in the internal market

Electronic Identification – eIDAS

Article 3 *(summary....)*

- Simple Electronic Signature (SES)

  data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

- Advanced Electronic Signature (AdES)

  an electronic signature which is additionally:

  uniquely linked to and capable of identifying the signatory;

  created in a way that allows the signatory to retain control;

  linked to the document in a way that any subsequent change of the data is detectable.

- Qualified Advanced Electronic Signature (QES)

  an advanced electronic signature which is additionally:

  created by a qualified signature creation device; and is based on a qualified certificate for electronic signatures.

Article 26

An advanced electronic signature (AdES) shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements

This document specifies security requirements and recommendations for **Trustworthy Systems Supporting Server Signing (TW4S)** that generate digital signatures. The TW4S is composed at least of one Server Signing Application (SSA) and one Signature Creation Device (SCDev) or one remote Signature Creation Device. A remote SCDev is a SCDev extended with remote control provided by a Signature Activation Module (SAM) executed in a tamper protected environment. This module uses the Signature Activation Data (SAD), collected through a Signature Activation Protocol (SAP), in order to guarantee with a high level of confidence that the signing keys are used under sole control of the signer.

The SSA uses a SCDev or a remote SCDev in order to generate, maintain and use the signing keys under the sole control of their authorized signer. Signing key import from CAs is out of scope. So when the SSA uses a remote SCDev, the authorized signer remotely controls the signing key with a high level of confidence. A TW4S is intended to deliver to the signer or to some other application, a digital signature created based on the data to be signed.

This standard:

- provides commonly recognized functional models of TW4S;
- specifies overall requirements that apply across all of the services identified in the functional model;
- specifies security requirements for each of the services identified in the TW4S;
- specifies security requirements for sensitive system components which may be used by the TW4S.

This standard is technology and protocol neutral and focuses on security requirements.

บริการลงลายมือชื่อดิจิทัล ที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)

รายละเอียดสำคัญของ ร่างมาตรฐานฯ

เนื้อหาทั้งหมด ของ ร่างมาตรฐานฯ

1. ขอบข่าย
2. บทนิยาม
3. อักษรย่อ
4. ภาพรวมของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S)
    - 4.1 ภาพรวมของกระบวนการสร้างลายมือชื่อ
    - 4.2 ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อ โดยไม่มีการควบคุมของบุคคลอื่น
    - 4.3 การพิสูจน์และยืนยันตัวตนของเจ้าของลายมือชื่อ
    - 4.4 กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และโมดูลเข้ารหัสลับ
    - 4.5 ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล
    - 4.6 โพรโทคอลเพื่อสั่งให้สร้างลายมือชื่อดิจิทัล
    - 4.7 ส่วนติดต่อของเจ้าของลายมือชื่อดิจิทัล
    - 4.8 โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล
    - 4.9 ขอบเขตสภาพแวดล้อม
5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้
    - 5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น
    - 5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ
    - 5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติม สำหรับระดับความเข้มงวดขั้นสูง
    - 5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ TW4S

1. ขอบข่าย

- อธิบายส่วนประกอบและหลักการทำงานของระบบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S) รวมถึงการบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจตรงกัน
- กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยที่จำเป็นต่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกลด้วยระบบ TW4S ให้หน่วยงานที่ต้องการใช้ และ/หรือให้บริการนำไปปฏิบัติเพื่อให้บริการมีความน่าเชื่อถือและอ้างอิงตามมาตรฐานของสหภาพยุโรป

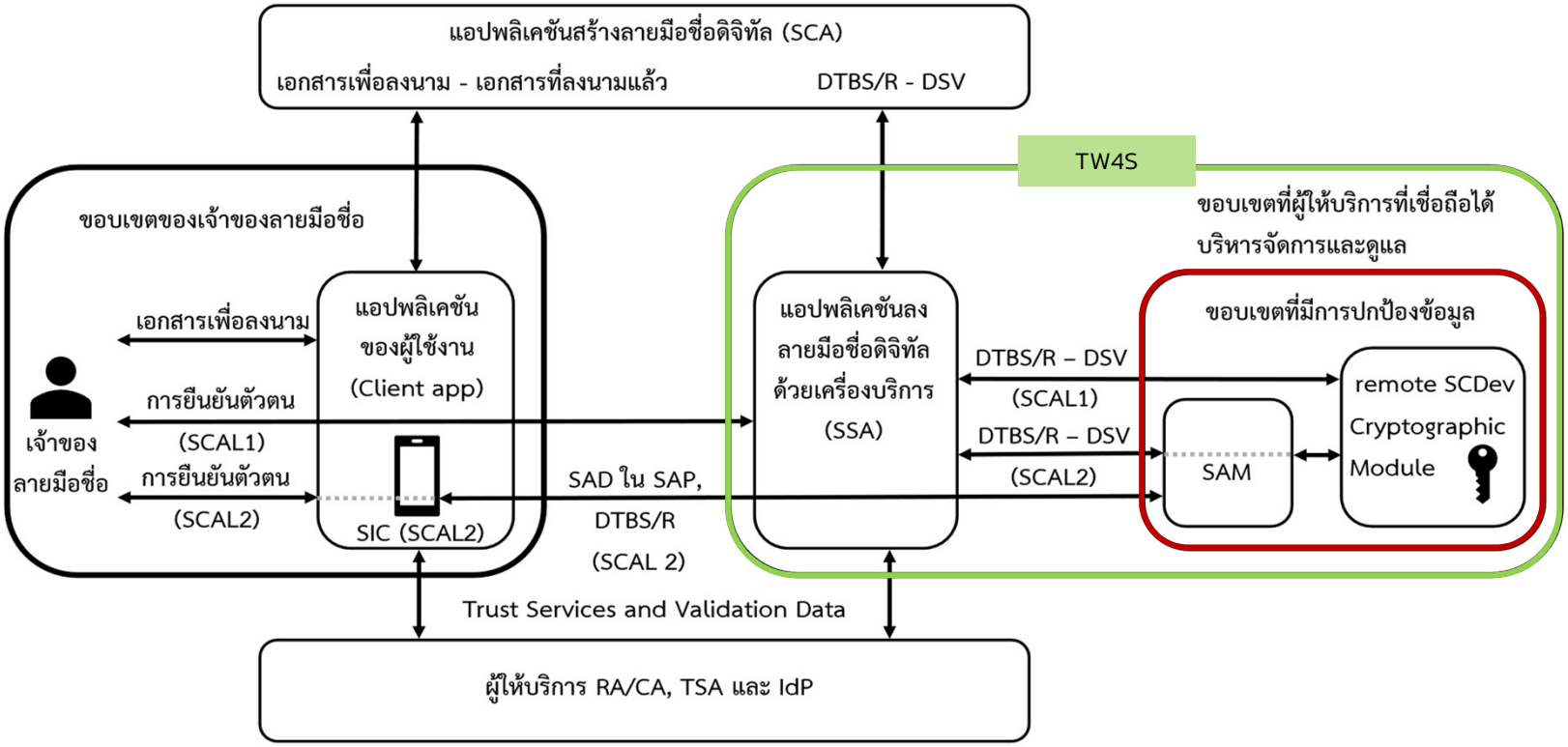
2. บทนิยาม

- การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing หรือ server signing) หมายถึง การสร้างลายมือชื่อดิจิทัล โดยเจ้าของลายมือชื่ออาศัย **ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)** ในการควบคุมกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) และสามารถรับรองได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) นั้น อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control)
- **อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signature creation device: remote SCDev)** หมายถึง อุปกรณ์หรือซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัลที่เจ้าของลายมือชื่อสามารถควบคุมได้จากระยะไกลผ่านโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) ที่สามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) นั้นอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น
- **โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (signature activation module: SAM)** หมายถึง ซอฟต์แวร์ที่ใช้ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ซึ่งสามารถรับประกันความเชื่อมั่นในระดับสูงได้ว่าการใช้กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น
- **แอปพลิเคชันสร้างลายมือชื่อดิจิทัล (signature creation application: SCA)** หมายถึง แอปพลิเคชันที่ใช้ลงนามในเอกสารอิเล็กทรอนิกส์ด้วยลายมือชื่อดิจิทัลที่สร้างจากอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)
- **ส่วนติดต่อของเจ้าของลายมือชื่อ (signer's interaction component: SIC)** หมายถึง ส่วนประกอบในรูปแบบซอฟต์แวร์ และ/หรือฮาร์ดแวร์ที่ทำงานร่วมกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) โดยเจ้าของลายมือชื่อเป็นผู้สั่งการใช้งาน

3. อักษรย่อ

อักษรย่อ	คำเต็ม	คำภาษาไทย
TW4S	Trustworthy System Supporting Server Signing	ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้
SCDev	Signature Creation Device	อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล
SAM	Signature Activation Module	โมดูลสั่งให้สร้างลายมือชื่อดิจิทัล
SSA	Server Signing Application	แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ
SCA	Signature Creation Application	แอปพลิเคชันสร้างลายมือชื่อดิจิทัล
SIC	Signer's Interaction Component	ส่วนติดต่อของเจ้าของลายมือชื่อ
SCAL	Sole Control Assurance Level	ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น
DTBS/R	Data to Be Signed Representation	แบบแสดงข้อมูลเพื่อลงลายมือชื่อ
DSV	Digital Signature Value	ค่าลายมือชื่อดิจิทัล

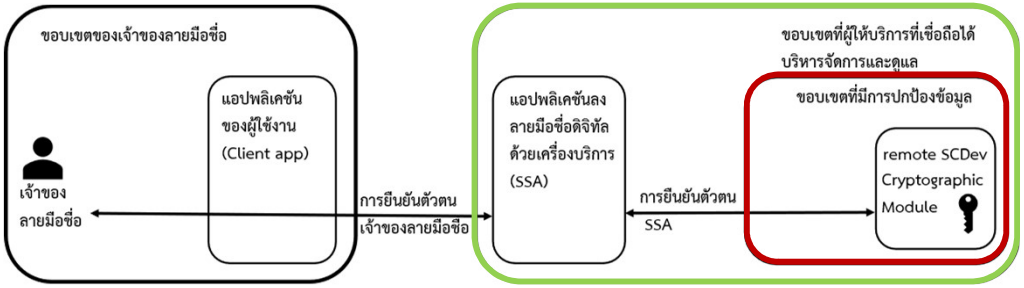
4. ภาพรวมของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S)



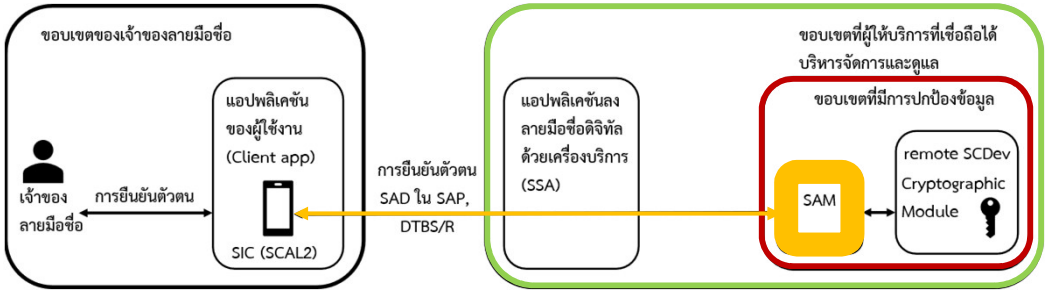
- Signer's Interaction Component (SIC)
- Server Signing Application (SSA)
- Remote Signature Creation Device (remote SCDev)
- Signature Activation Protocol (SAP)
- Data to Be Signed Representation (DTBS/R)
- Signature Creation Application (SCA)
- Signature Activation Module (SAM)
- Sole Control Assurance Level (SCAL)
- Signature Activation Data (SAD)
- Digital Signature Value (DSV)

4. ภาพรวมของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (trustworthy system supporting server signing: TW4S)

ระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น (sole control assurance level: SCAL)



การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ พื้นฐาน SCAL1



การยืนยันตัวตนเพื่อสั่งให้สร้างลายมือชื่อดิจิทัลระดับความเข้มงวดฯ ขั้นสูง SCAL2

ระดับความเข้มงวดฯ พื้นฐาน **SCAL1**

- เจ้าของลายมือชื่อต้องยืนยันตัวตนกับแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) จนสำเร็จก่อน จึงจะได้รับอนุญาตให้เข้าถึงส่วนปฏิบัติงานเกี่ยวข้องกับลายมือชื่อดิจิทัล
- แอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) ต้องเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (signing key) ของเจ้าของลายมือชื่อไปยังปัจจัยของการยืนยันตัวตน (authentication factor) ของเจ้าของลายมือชื่อ
- ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน อย่างน้อย: IAL1 และ AAL1

ระดับความเข้มงวดฯ ขั้นสูง **SCAL2**

- ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกสร้างขึ้น หรือเป็นผลลัพธ์ที่เกิดจากการติดต่อที่มีความมั่นคงปลอดภัยระหว่างโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) กับส่วนติดต่อของเจ้าของลายมือชื่อ (SIC) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่ออนุญาตให้สร้างลายมือชื่อดิจิทัลในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev)
- ข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) ต้องถูกส่งให้กับโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ผ่านแอปพลิเคชันลงลายมือชื่อดิจิทัลด้วยเครื่องบริการ (SSA) เพื่ออนุญาตให้อุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) สร้างลายมือชื่อดิจิทัลด้วยแบบแสดงข้อมูลเพื่อลงลายมือชื่อ (DTBS/R) เฉพาะที่ระบุไว้
- ระดับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน อย่างน้อย: IAL2 และ AAL2

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น (general security requirements: SRG)

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (core component security requirements: SRC)

5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับความเข้มงวดฯ ขั้นสูง SCAL2 (additional security requirements: SRA)

5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ TW4S

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น (general security requirements: SRG)

5.1.1 การบริหารจัดการ (SRG_M)

การกำหนดบทบาทและสิทธิ์ของเจ้าหน้าที่และผู้ใช้งานอย่างเหมาะสมและปลอดภัย

5.1.2 ระบบและการปฏิบัติงาน (SRG_O)

ระบบ TW4S ต้องตั้งค่าเวลาให้ตรงและถูกต้องเทียบกับแหล่งเวลาอ้างอิงที่เชื่อถือได้ รวมทั้งต้องจัดให้มีคู่มือการปฏิบัติงานที่เกี่ยวข้องกับระบบ และคู่มือการบริหารจัดการระบบสำหรับผู้ใช้งานที่มีสิทธิสูง

5.1.3 การระบุและยืนยันตัวตน (SRG_IA)

ระบบ TW4S ต้องมีกลไกการระบุและยืนยันตัวตนเพื่อป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่ได้รับอนุญาต

5.1.4 การควบคุมและจำกัดการเข้าถึงระบบ (SRG_SA)

ระบบ TW4S ต้องมีความสามารถในการควบคุมและจำกัดผู้ใช้งานที่ระบุไว้ ในการเข้าถึงข้อมูล หรือส่วนประกอบของระบบ

5.1.5 การบริหารจัดการกุญแจ (SRG_KM)

การสร้างกุญแจ, การจัดเก็บ สำรอง และกู้คืนกุญแจ, การใช้กุญแจ, การเผยแพร่กุญแจ, การต่ออายุ ปรับปรุง และเปลี่ยนกุญแจ, การจัดเก็บกุญแจเพื่อเป็นข้อมูลที่เก็บไว้เป็นหลักฐานในระยะยาว และ การลบกุญแจ

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.1 ข้อกำหนดด้านความมั่นคงปลอดภัยพื้นฐานที่จำเป็น (general security requirements: SRG) ... *ต่อ .....*

5.1.6 การตรวจสอบ (SRG_AA)

ต้องบันทึกข้อมูลเหตุการณ์ต่างๆที่เกิดขึ้นภายในระบบ TW4S เพื่อใช้ในการตรวจสอบ

5.1.7 การจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาว (SRG_AR)

ต้องจัดเก็บข้อมูลไว้เป็นหลักฐานในระยะยาวบนสื่อบันทึกข้อมูลภายนอก โดยสื่อบันทึกข้อมูลนี้ควรมีการจัดเก็บอย่างเหมาะสมให้สามารถนำมาใช้ได้ในภายหลัง และสามารถใช้เป็นหลักฐานในทางกฎหมายเพื่อรับรองลายมือชื่อดิจิทัลที่สร้างขึ้นในระบบ TW4S แต่ต้องไม่จัดเก็บพารามิเตอร์ที่สำคัญต่อความมั่นคงปลอดภัย เช่น รหัสผ่านของผู้ใช้งานระบบ TW4 เป็นต้น

5.1.8 การสำรองและกู้คืนข้อมูล (SRG_BK)

ครอบคลุมถึงข้อมูลระบบ ข้อมูลผู้ใช้งาน และข้อมูลอื่นที่เกี่ยวข้องทั้งหมดที่จำเป็นต่อการกู้คืนระบบในภายหลังระบบล้มเหลวหรือเกิดเหตุภัยพิบัติต่อระบบ แต่ไม่รวมถึงข้อมูลสำรองและกู้คืนของกุญแจต่างๆ

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.2 ข้อกำหนดด้านความมั่นคงปลอดภัยของส่วนประกอบหลักของระบบ (core component security requirements: SRC)

5.2.1 การตั้งค่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และกุญแจระบบรหัสลับ (SRC_SKS.1)

พารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วยระบบ TW4S ต้องมีความมั่นคงปลอดภัยเพียงพอตลอดช่วงอายุของใบรับรอง รวมทั้งต้องรักษาความครบถ้วนสมบูรณ์ของข้อมูลที่เกี่ยวข้องกับการเชื่อมโยงกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัลของเจ้าของลายมือชื่อกับใบรับรอง

5.2.2 การยืนยันตัวตนเจ้าของลายมือชื่อ (SRC_SA)

การยืนยันตัวตนเจ้าของลายมือชื่อให้มีระดับความเข้มงวดพื้นฐาน SCAL1 รวมทั้งต้องมีมาตรการจัดการเมื่อการยืนยันตัวตนเพื่อเข้าถึงระบบไม่สำเร็จหรือเกิดความผิดพลาด

5.2.3 การสร้างลายมือชื่อดิจิทัล และกระบวนการระบบรหัสลับ (SRC_DSC)

พารามิเตอร์ของอัลกอริทึมที่ใช้สำหรับการสร้างลายมือชื่อด้วยระบบ TW4S ต้องถูกกำหนดให้มีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรอง

5.3 ข้อกำหนดด้านความมั่นคงปลอดภัยเพิ่มเติมสำหรับระดับความเข้มงวดฯ ขั้นสูง SCAL2 (additional security requirements: SRA)

5.3.1 โพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัลและข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SRA_SAP)

ต้องมีมาตรการควบคุมตามจำเป็นกับระดับความเสี่ยงเพื่อรับมือและโต้ตอบต่อภัยคุกคามกับโพรโทคอลสั่งให้สร้างลายมือชื่อดิจิทัล (SAP) และข้อมูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAD) รวมทั้งโมดูลสั่งให้สร้างลายมือชื่อดิจิทัล (SAM) ต้องติดตั้งและใช้งานภายใต้ขอบเขตที่ผู้ให้บริการที่เชื่อถือได้บริหารจัดการและมีการป้องกันการเปลี่ยนแปลงข้อมูล ซึ่งเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการประเมินทั่วไปด้านความมั่นคงปลอดภัยในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป ตามมาตรฐาน ISO/IEC 15408 หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องและเทียบเคียงกัน

5.3.2 การบริหารจัดการกุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล (SRA_SKM)

กุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล ต้องถูกสร้างขึ้นและใช้งานภายในอุปกรณ์/ระบบสร้างลายมือชื่อดิจิทัล (SCDev) โดยต้องเป็นอุปกรณ์/ระบบที่เชื่อถือได้และผ่านการประเมินทั่วไปด้านความมั่นคงปลอดภัยในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป ตามมาตรฐาน ISO/IEC 15408 หรือมาตรฐานอื่นในระดับประเทศที่เกี่ยวข้องและเทียบเคียงกัน

5. ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

5.4 ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยสำหรับระบบ TW4S

เพื่อให้บริการระบบ TW4S มีความน่าเชื่อถือ ผู้ให้บริการต้องใช้ผลิตภัณฑ์ระบบ TW4S ที่ผ่านการตรวจรับรองเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Common Criteria หรือ CC) ตามมาตรฐาน ISO/IEC 15408 ด้วย ข้อกำหนดป้องกันการดัดแปลงแก้ไข (Protection Profile) ในระดับความเข้มงวดในการประเมินตามเกณฑ์ประเมินทั่วไปด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (EAL) ที่ระดับ 4 ขึ้นไป

ข้อกำหนดการป้องกันการดัดแปลงแก้ไข (Protection Profile) สำหรับระบบ TW4S เพื่อใช้เป็นเกณฑ์ประเมินด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของผลิตภัณฑ์ให้เป็นไปตามมาตรฐาน CEN EN 419 241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing หรือข้อเสนอแนะ หรือประกาศของหน่วยงานในระดับประเทศที่รับผิดชอบ

บริการลงลายมือชื่อดิจิทัล ที่ใช้การควบคุมจากระยะไกล (Remote Signing Service)

รับฟังข้อคิดเห็น ข้อเสนอแนะ และ ตอบข้อสงสัย

Q&A

https://www.etda.or.th/th/StandardNews/03052566.aspx