
กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
ETDA
กิจกรรมถ่ายทอดความรู้
บริการลงลายมือชื่อดิจิทัล
ที่ใช้การควบคุมจากระยะไกล
Remote Signing Service
วันพฤหัสบดีที่ 15 มิถุนายน 2566 เวลา 10.00 - 12.00 น.
ผ่านโปรแกรม Microsoft Teams
แบบสำรวจ
โดย คณะที่ปรึกษาโครงการฯ
จุฬาลงกรณ์มหาวิทยาลัย
ร่วมตอบแบบสำรวจ
Remote Signing Service
https://bit.ly/ETDA_RS_Survey

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

กำหนดการของกิจกรรมถ่ายทอดความรู้มีรายละเอียด ดังนี้

เวลา	รายละเอียดกิจกรรม
10:00 - 10:15 น.	กล่าวเปิดการอบรม/สัมมนา โดยผู้แทน จากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
10:15 - 11:45 น.	ความเข้าใจใน Remote Signing • ความเข้าใจประเด็นสำคัญของ กฎหมายไทยและกฎหมายสหภาพยุโรปที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์ • ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S) เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล • มาตรฐานที่เกี่ยวข้องกับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล • ข้อกำหนดด้านความมั่นคงปลอดภัยที่สำคัญ • ทิศทางด้านมาตรฐานสำหรับลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย
11:45 - 12:00 น.	ถาม/ตอบ และแลกเปลี่ยนเรียนรู้ร่วมกัน

ความเข้าใจประเด็นสำคัญของ กฎหมายไทย และ กฎหมายสหภาพยุโรป ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

กฎหมายไทย : พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
หมวด 1 ธุรกรรมอิเล็กทรอนิกส์ และ หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

กฎหมายไทย : พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
หมวด 1 ธุรกรรมอิเล็กทรอนิกส์ และ หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

มาตรา ๔ ในพระราชบัญญัตินี้

“ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

“ลายมือชื่ออิเล็กทรอนิกส์” หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

กฎหมายไทย : พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
หมวด 1 ธุรกรรมอิเล็กทรอนิกส์ และ หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

หมวด 1 ธุรกรรมอิเล็กทรอนิกส์

มาตรา ๙[๑๑] ในกรณีที่กฎหมายกำหนดให้มีการลงลายมือชื่อ หรือกำหนดผลทางกฎหมาย กรณีที่ไม่มีการลงลายมือชื่อไว้ ให้ถือว่าได้มีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความในข้อมูลอิเล็กทรอนิกส์ และ

(๒) ใช้วิธีการในลักษณะอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(ก) วิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมทั้งปวง รวมถึงข้อตกลงใด ๆ ที่เกี่ยวข้อง หรือ

(ข) วิธีการอื่นใดที่สามารถยืนยันตัวเจ้าของลายมือชื่อและสามารถแสดงเจตนาของเจ้าของลายมือชื่อ ตาม (๑) ได้ด้วยวิธีการนั้นเองหรือประกอบกับพยานหลักฐานอื่น

กฎหมายไทย : พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
หมวด 1 ธุรกรรมอิเล็กทรอนิกส์ และ หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

ETDA

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

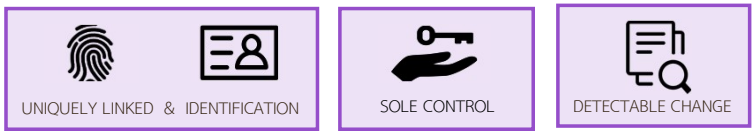
มาตรา ๒๖ ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังต่อไปนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

(๑) ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้

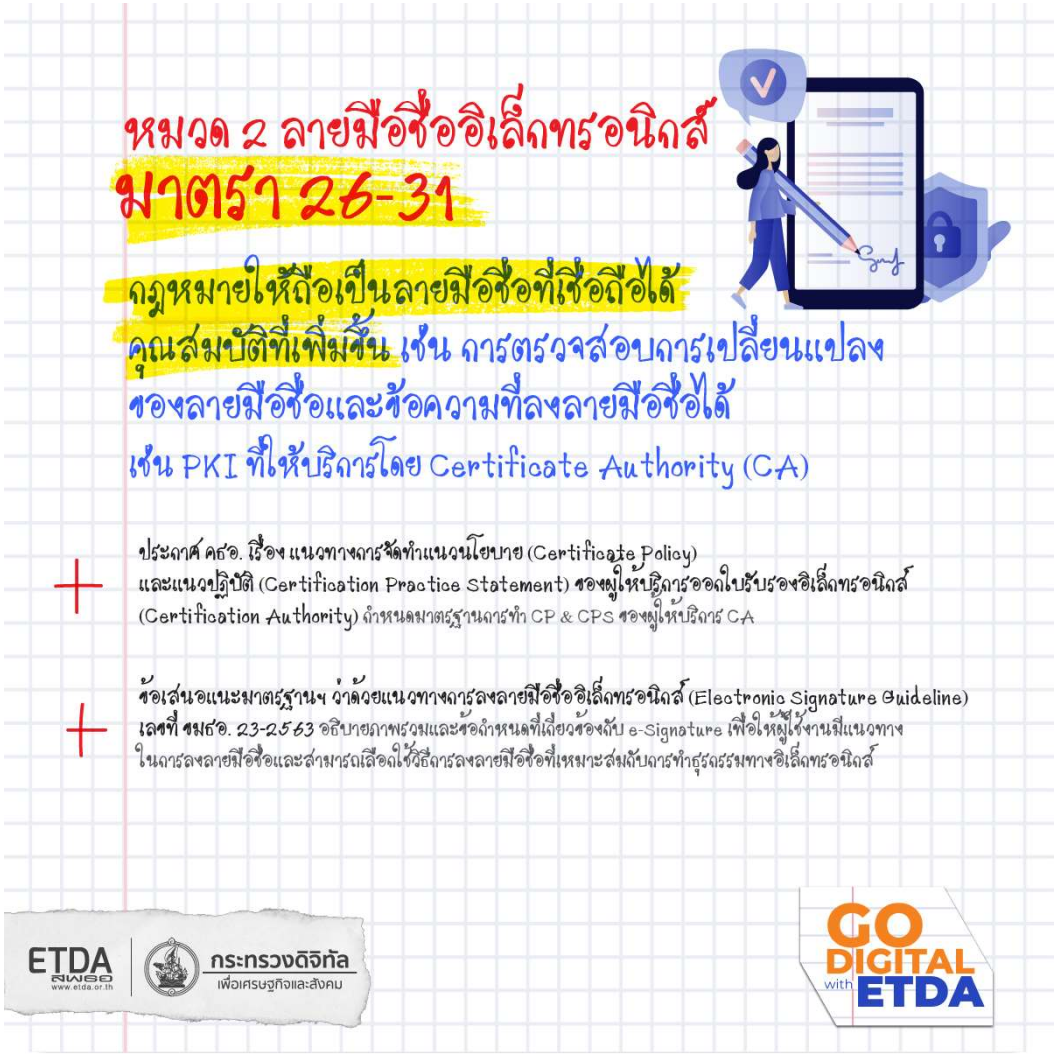
(๒) ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น

(๓) การเปลี่ยนแปลงใด ๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้

(๔)[๑๙] ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อเป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์



กฎหมายไทย : พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
หมวด 1 ธุรกรรมอิเล็กทรอนิกส์ และ หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์



มาตรา 26	ลักษณะของ ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้
มาตรา 27	เจ้าของลายมือชื่อต้องดำเนินการอะไรบ้าง เพื่อให้ลายมือชื่ออิเล็กทรอนิกส์มีผลทางกฎหมาย
มาตรา 28	ผู้ให้บริการออกใบรับรองต้องดำเนินการอะไรบ้าง เพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ให้มีผลทางกฎหมาย
มาตรา 29	ความเชื่อถือได้ของระบบ วิธีการ และบุคลากร ตามมาตรา 28 (6) ต้องคำนึงถึงสิ่งใดบ้าง
มาตรา 30	คู่กรณีที่เกี่ยวข้องต้องดำเนินการสิ่งใดบ้าง
มาตรา 31	ใบรับรองหรือลายมือชื่ออิเล็กทรอนิกส์ให้ถือว่ามีผลทางกฎมาย โดยไม่ต้องคำนึงถึงสถานที่ออกใบรับรอง และสถานที่ทำการของผู้ออกใบรับรอง

กฎหมายสหภาพยุโรป : กฎหมายเอดาส (eIDAS) เป็นข้อบังคับของสหภาพยุโรปเกี่ยวกับบริการระบุตัวตนทางอิเล็กทรอนิกส์และความน่าเชื่อถือสำหรับธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2014

eIDAS Timelines

2014

Regulation in Force

The EU regulation 910/2014 on electronic Identification and trust Services (eIDAS) in the EU.

2015

Technical Specification

EU announced eID Interoperability framework and eIDAS technical specifications on AdES (Advanced Electronic Signature) formats & QSCD (Qualified Electronic Signature Creation Device) , etc.

2018

GO LIVE!

EU-Wide eID – Recognition to support EU Digital Single Market, eID schemes has covered around 59% of the EU population

2021

Revise the regulation

Add EU digital identity wallets (W3C VC standard), Remote Server Signature Signing (CEN standard), distributed digital id (wallet) and electronic ledgers.

กฎหมายสหภาพยุโรป : กฎหมายเอดาส (eIDAS) เป็นข้อบังคับของสหภาพยุโรปเกี่ยวกับบริการระบุตัวตนทางอิเล็กทรอนิกส์และความน่าเชื่อถือสำหรับธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2014

- บทที่ 1 ข้อกำหนดทั่วไป (General Provisions)
- บทที่ 3 บริการที่เชื่อถือได้ (Trust Services) ในหมวด 4 ลายมือชื่ออิเล็กทรอนิกส์ (Electronic signatures)

บทที่ 1 ข้อกำหนดทั่วไป (General Provisions)

Article 3

SES (Simple Electronic Signature)

(10) Electronic signature means 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

AdES (Advanced Electronic Signature)

(11) Advanced electronic signature means an electronic signature which meets the requirements set out in Article 26

QES (Qualified Electronic Signature)

(12) Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures

กฎหมายสหภาพยุโรป : กฎหมายเอดาส (eIDAS) เป็นข้อบังคับของสหภาพยุโรปเกี่ยวกับบริการระบุตัวตนทางอิเล็กทรอนิกส์และความน่าเชื่อถือสำหรับธุรกรรมทางอิเล็กทรอนิกส์ ค.ศ. 2014

- บทที่ 1 ข้อกำหนดทั่วไป (General Provisions)
- บทที่ 3 บริการที่เชื่อถือได้ (Trust Services) ในหมวด 4 ลายมือชื่ออิเล็กทรอนิกส์ (Electronic signatures)

บทที่ 3 บริการที่เชื่อถือได้ (Trust Services)

Article26

AdES (Advanced Electronic Signature)

An advanced electronic signature shall meet the following requirements:

it is uniquely linked to the signatory;

it is capable of identifying the signatory;

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

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

Article25

QES (Qualified Electronic Signature) shall have the equivalent legal effect of a handwritten signature.

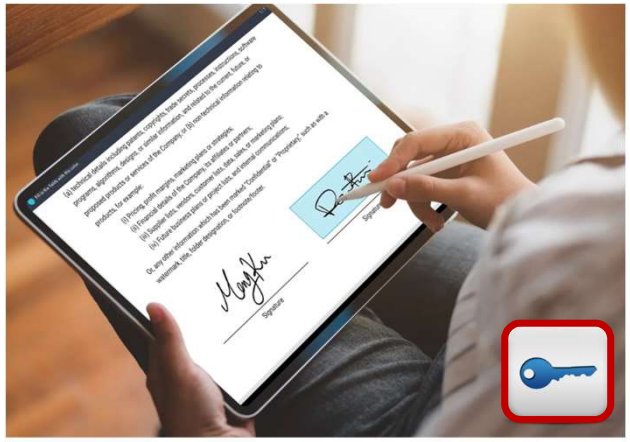
1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.
3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.

ลายมือชื่อดิจิทัล (Digital Signature)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S - trustworthy system supporting server signing)

เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)

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

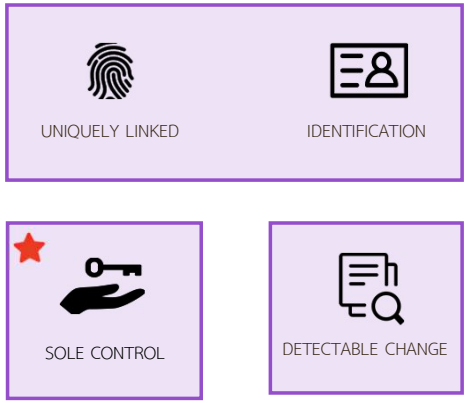
Remote Signing

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 หรือที่เรียกว่า **การลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)**

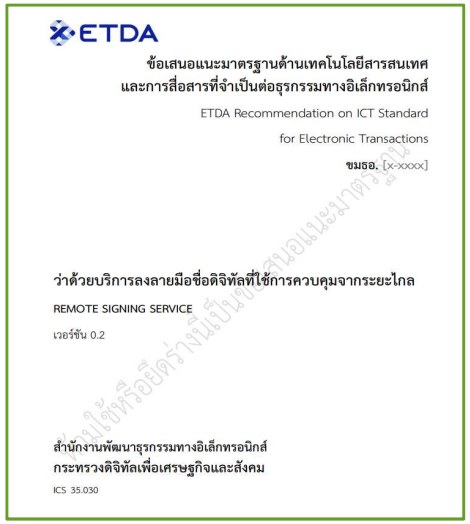
ประเด็นพิจารณา คือ การที่จะต้องมีกลไกในการยืนยันว่ากุญแจส่วนตัวนั้น ต้องอยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ โดยไม่มีการควบคุมของบุคคลอื่น (sole control)



มาตรฐานการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (remote signing service)

เพิ่มทางเลือกวิธีการลงลายมือชื่อดิจิทัลที่เชื่อถือได้

- อำนวยความสะดวกและลดอุปสรรคจากการจัดเก็บกุญแจส่วนตัวไว้กับเจ้าของลายมือชื่อ
- ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ สำหรับหน่วยงานที่ต้องการใช้ และ/หรือให้บริการ
- สร้างความเข้าใจที่ตรงกันระหว่างหน่วยงานที่เกี่ยวข้อง ผู้ให้บริการ เจ้าของลายมือชื่อและคู่กรณี


ETDA

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล

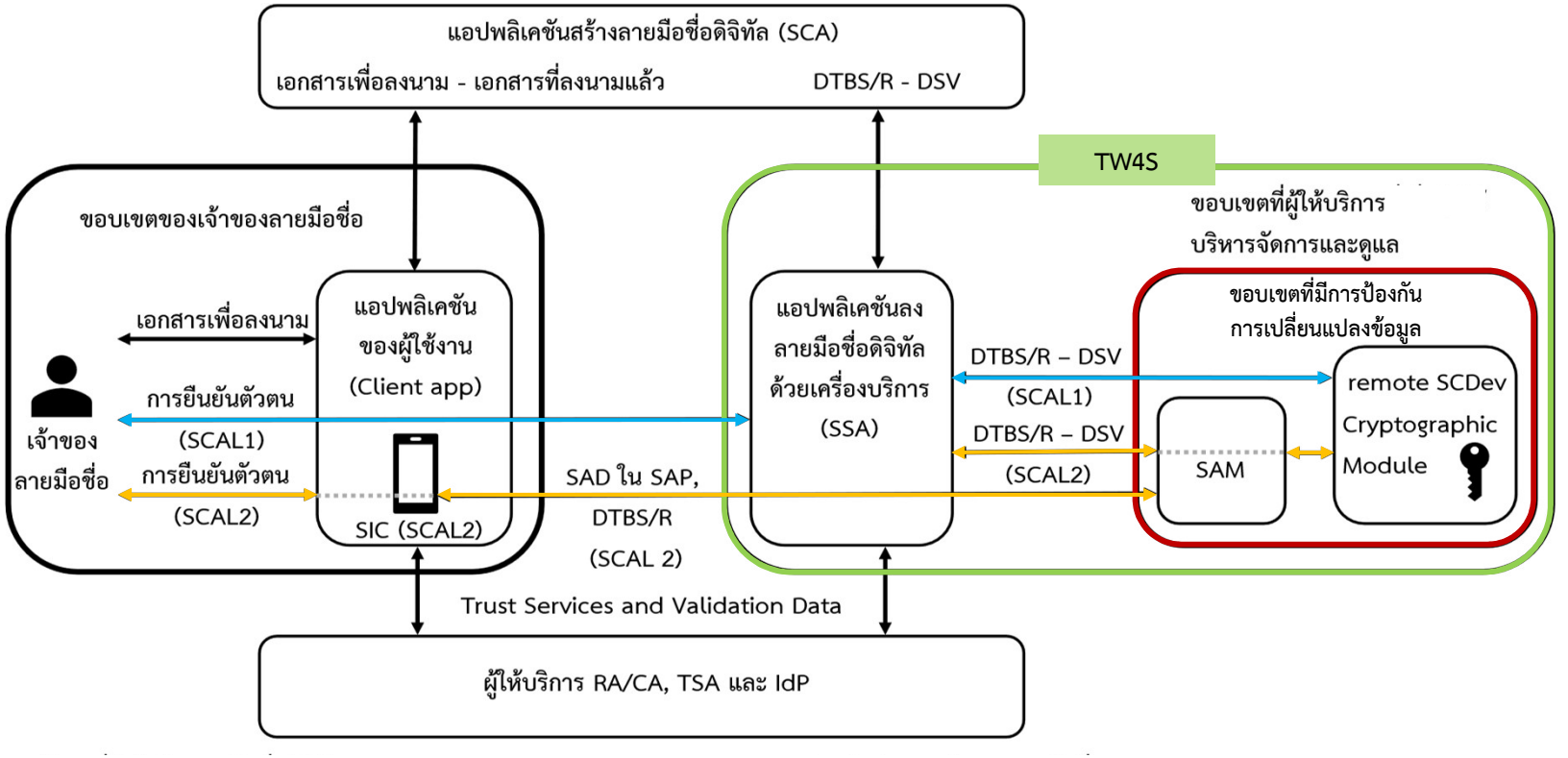
REMOTE SIGNING SERVICE

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

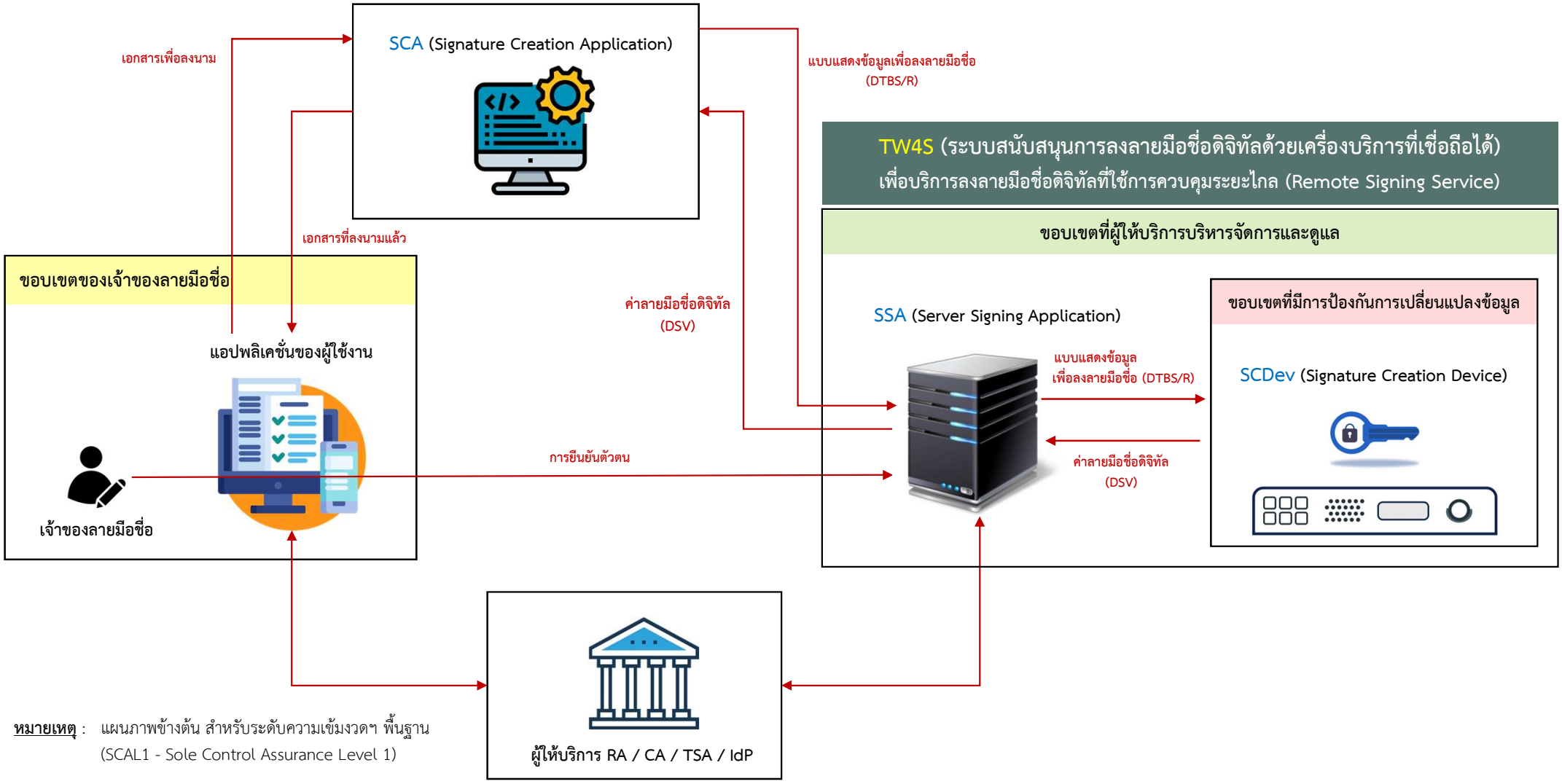
ICS 35.030

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



- 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)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



หมายเหตุ : แผนภาพข้างต้น สำหรับระดับความเข้มงวดฯ พื้นฐาน (SCAL1 - Sole Control Assurance Level 1)

มาตรฐานที่เกี่ยวข้องกับบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)

หน่วยงานมาตรฐานทางเทคนิคของสหภาพยุโรป ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

CEN	**The European Committee for Standardization (CEN)** The CEN Electronic Signature standards, which are part of the **EN 419** series, provide requirements and recommendations for the implementation of electronic signatures and related trust services. The EN 419 series covers a wide range of topics, including the legal framework for electronic signatures, the security of electronic signatures, and the interoperability of electronic signature systems.
ETSI	**The European Telecommunications Standards Institute (ETSI)** The ETSI Electronic Signature standards, which are part of the **TS 119** series, focus on the technical implementation of electronic signatures and related trust services, such as electronic seals and time-stamping. The ETSI standards provide detailed specifications for the creation, verification, and validation of electronic signatures, as well as for the provision of trust services.

- **The standards developed by CEN and ETSI are referenced in the EU's eIDAS Regulation.**
- **Both CEN and ETSI electronic signature standards have different scopes and focuses, they are complementary and often used together.**

หน่วยงานมาตรฐานทางเทคนิคของสหภาพยุโรป ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

CEN Document Codes

EN (European Standard)
a normative document that provides requirements, specifications, and guidelines for products, services, and processes that are intended to be used in Europe

TS (Technical Specification)
a normative document that provides detailed technical information and requirements for products, services, or processes, but is less formal than an EN

TR (Technical Report)
a non-normative document that provides informative or explanatory material, such as a literature review or a state-of-the-art report

ETSI Document Codes

EN (European Standard)
a normative document that provides requirements, specifications, and guidelines for products, services, and processes that are intended to be used in Europe.

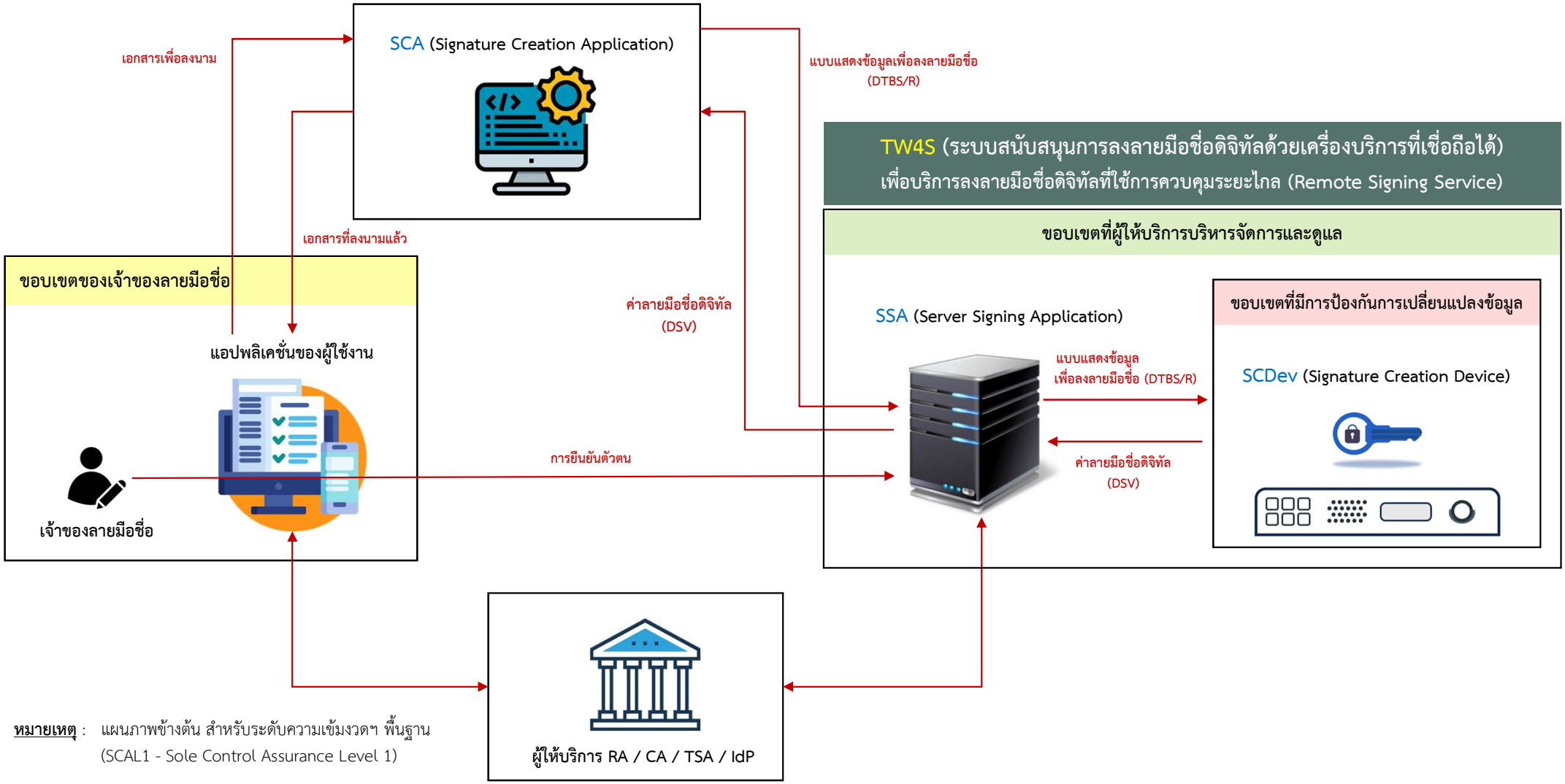
TS (Technical Specification)
a normative document that provides detailed technical information and requirements for products, services, or processes, but is less formal than an EN.

EG (ETSI Guide)
a non-normative document that provides guidance or recommendations on a specific topic.

ES (ETSI Standardization Publication)
a non-normative document that provides information on ETSI activities, initiatives, or events.

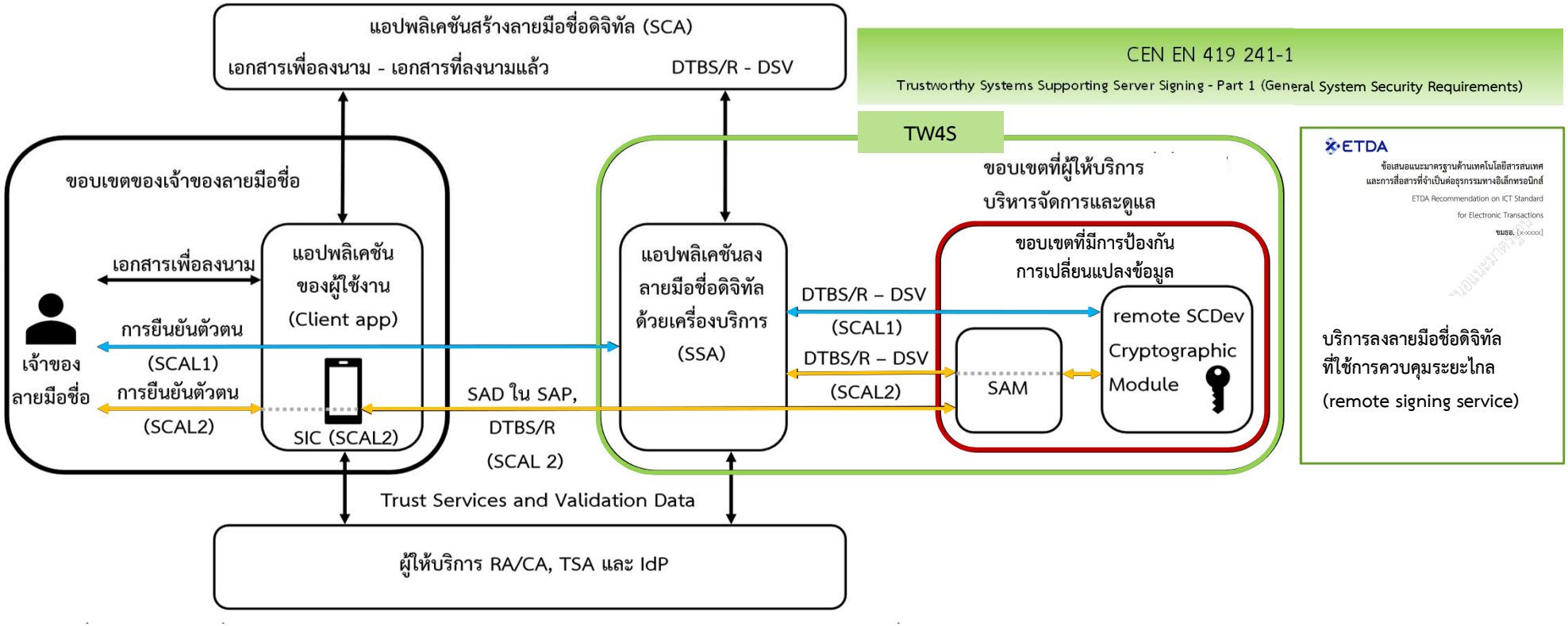
- Normative standards are often used in regulated industries, such as healthcare, aviation, and finance, to ensure compliance with specific regulations and standards
- Non-normative documents are often used to provide background information, clarify concepts or terminology, or provide guidance on best practices or new technologies, but they are not intended to be used as a basis for compliance or certification.

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



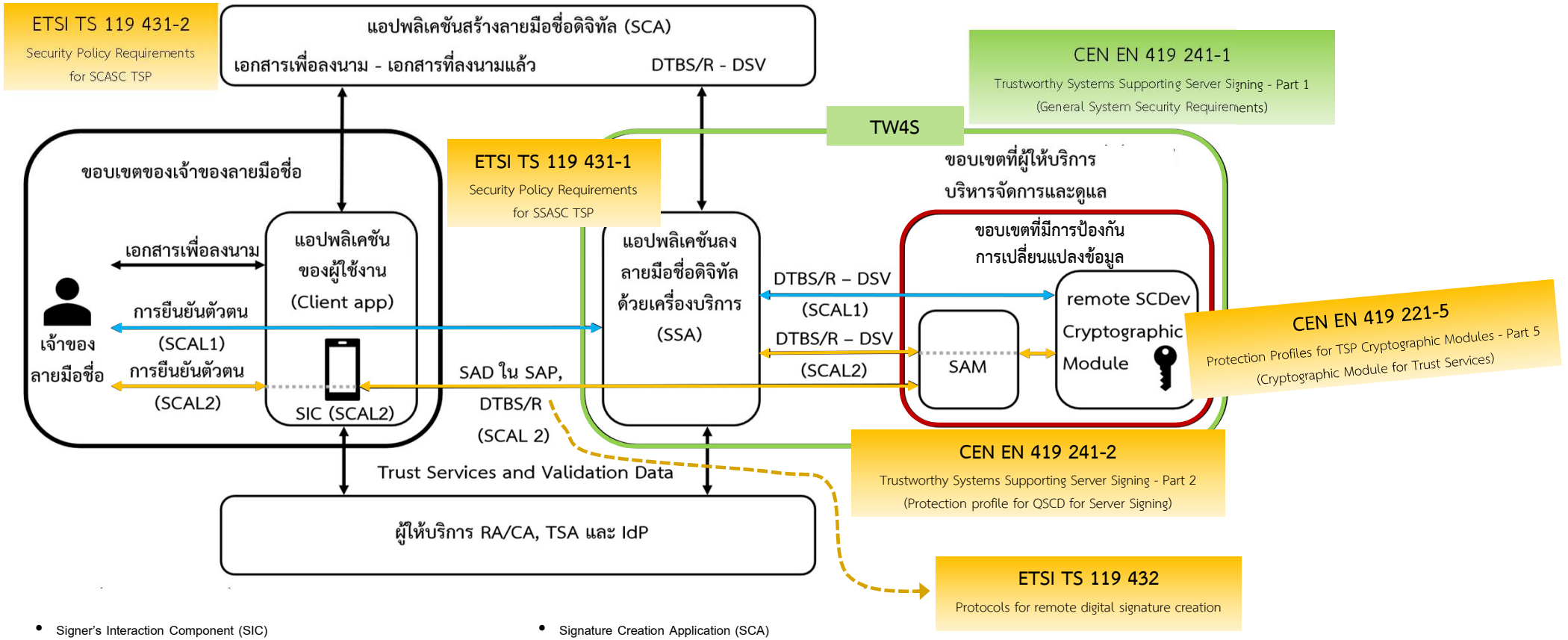
หมายเหตุ : แผนภาพข้างต้น สำหรับระดับความเข้มงวดฯ พื้นฐาน (SCAL1 - Sole Control Assurance Level 1)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



- 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)

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



- 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)

ข้อกำหนดด้านความมั่นคงปลอดภัยที่สำคัญ

ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้

กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ETDA

1) การบริหารจัดการ	การกำหนดบทบาทและสิทธิ์ของเจ้าหน้าที่และผู้ใช้งานอย่างเหมาะสมและปลอดภัย
2) ระบบและการปฏิบัติงาน	ระบบต้องตั้งค่าเวลาให้ตรงและถูกต้องเทียบกับแหล่งเวลาอ้างอิงที่เชื่อถือได้ เพื่อให้มีความมั่นใจว่าเวลาของการบันทึกกิจกรรมสำหรับการตรวจสอบมีความแม่นยำ รวมทั้งต้องจัดให้มีคู่มือการปฏิบัติงานและการบริหารจัดการดูแลระบบ
3) การระบุและยืนยันตัวตน	ระบบต้องมีกลไกการระบุและยืนยันตัวตนเพื่อป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่ได้รับอนุญาต
4) การควบคุมและจำกัดการเข้าถึงระบบ	ระบบต้องมีกลไกการควบคุมและจำกัดการเข้าถึงระบบ เพื่อป้องกันการเข้าถึงข้อมูลและส่วนประกอบสำคัญทั้งหมดของระบบ
5) การบริหารจัดการกุญแจ	ต้องมีการบริหารและจัดการกุญแจให้ความมั่นคงปลอดภัยตลอดวงจรชีวิตของกุญแจ ประกอบด้วย การสร้างกุญแจ, การจัดเก็บ สำรองและกู้คืนกุญแจ, การใช้กุญแจ, การเผยแพร่กุญแจ, การต่ออายุ ปรับปรุง และเปลี่ยนกุญแจ รวมทั้งการลบกุญแจ
6) การตรวจสอบ	ต้องบันทึกข้อมูลเหตุการณ์ต่างๆที่เกิดขึ้นภายในระบบ เพื่อใช้ในการตรวจสอบ
7) การสำรองและกู้คืนข้อมูล	ต้องมีการสำรองข้อมูลระบบ ข้อมูลผู้ใช้งาน และข้อมูลอื่นที่เกี่ยวข้องทั้งหมดที่จำเป็นต่อการกู้คืนระบบในภายหลังระบบล้มเหลวหรือเกิดเหตุภัยพิบัติต่อระบบ (ไม่รวมถึงข้อมูลสำรองและกู้คืนของกุญแจต่างๆ)

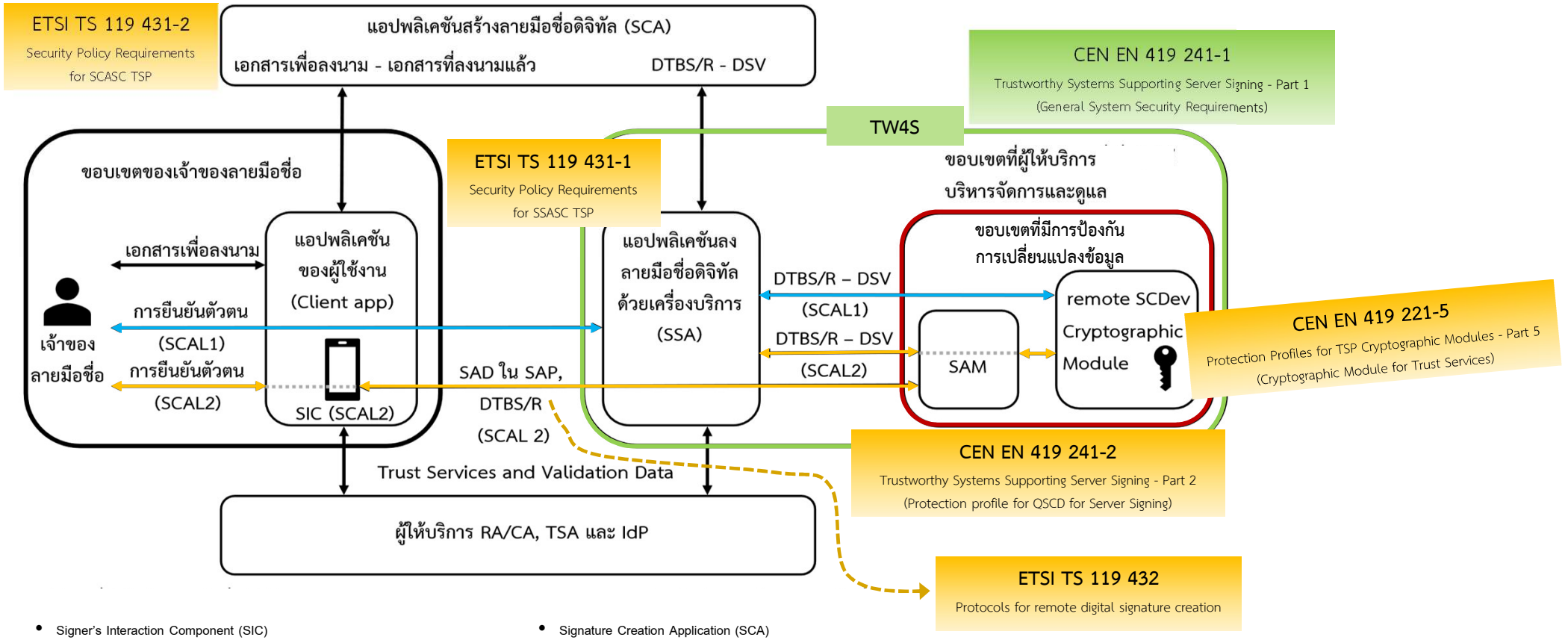
* การตั้งค่ากุญแจสำหรับใช้สร้างลายมือชื่อดิจิทัล และกุญแจรหัสลับ ต้องมีกระบวนวิธีเข้ารหัสลับ ที่มีความมั่นคงปลอดภัยเพียงพอตลอดช่วงอายุของใบรับรอง

* การยืนยันตัวตนเจ้าของลายมือชื่อ สำหรับระดับความเข้มงวดในการควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น ขั้นพื้นฐาน (SCAL1) ต้องมีที่ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน IAL1 ขึ้นไป และการยืนยันตัวตน AAL1 ขึ้นไป

* การสร้างลายมือชื่อดิจิทัล และกระบวนการระบบรหัสลับ ต้องมีความมั่นคงปลอดภัยเพียงพอในตลอดช่วงอายุของใบรับรอง

ทิศทางด้านมาตรฐาน สำหรับลายมือชื่ออิเล็กทรอนิกส์ในบริบทของประเทศไทย

ระบบสนับสนุนการลงลายมือชื่อดิจิทัลด้วยเครื่องบริการที่เชื่อถือได้ (TW4S)
เพื่อบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมระยะไกล (remote signing service)



- 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)

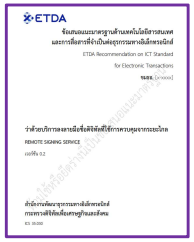
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ จนนำไปสู่ ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้และผ่านการรับรอง มี 3 องค์ประกอบ

ทิศทางด้านมาตรฐาน สำหรับลายมือชื่ออิเล็กทรอนิกส์ในบริบทของประเทศไทย

มาตรฐาน / เทคโนโลยี	ผู้ให้บริการ / กระบวนการ	ระบบ / อุปกรณ์

มาตรฐานสำหรับ Remote Signing

เพื่อให้ได้ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้



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

ผู้ให้บริการที่เชื่อถือได้ (TSP)

บริการ SSA / SCA / Protocols for Remote SIgning

ETSI TS 119 431-1
Security Policy Requirements for SSASC TSP

ETSI TS 119 431-2
Security Policy Requirements for SCASC TSP

ETSI TS 119 432
Protocols for remote digital signature creation

ระบบ/อุปกรณ์ที่เชื่อถือได้ (QSCD)

เกณฑ์ประเมินในส่วนของ QSCD (SAM และ SCDev)

CEN EN 419 221-5
Protection Profiles for TSP Cryptographic Modules - Part 5
(Cryptographic Module for Trust Services)

CEN EN 419 241-2
Trustworthy Systems Supporting Server Signing - Part 2
(Protection profile for QSCD for **Server Signing**)

ISO/IEC 15408
Evaluation criteria for IT security (Common Criteria)

ขมธอ. 23-2563
ประเภทของลายมือชื่ออิเล็กทรอนิกส์

QES
QUALIFIED ELECTRONIC SIGNATURE

มีผลทางกฎหมายเทียบเท่ากับลายเซ็นที่เขียนด้วยลายมือ

หมายเหตุ : แผนภาพข้างต้นเป็นการเสนอตามแนวทาง Qualified Electronic Signature (QES) ของสหภาพยุโรป ซึ่งอาจมีการเปลี่ยนแปลงได้ตามความเหมาะสมและบริบทที่อาจเปลี่ยนไปในอนาคต

Q&A

ร่วมตอบแบบสำรวจ https://bit.ly/ETDA_RS_Survey