ขอเชิญรับฟังความคิดเห็นต่อ

ร่างแนวปฏิบัติ การลงลายมือชื่ออิเล็กทรอนิกส์

สำหรับเจ้าหน้าที่ของรัฐ

วันที่ 17 พ.ค. 65 | 13.30 - 15.30 น.

สแกน QR Code
เพื่อรับ Link เข้าร่วมการประชุม
และร่วมแสดงความคิดเห็น

ลงนามสะดวก ปลอดภัย และถูกต้อง
ด้วยลายมือชื่ออิเล็กทรอนิกส์

กำหนดการจัดงานรับฟังความคิดเห็นต่อร่างแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ

วันอังคารที่ 17 พฤษภาคม 2565 เวลา 13.30 – 15.30 น. ผ่านการประชุมออนไลน์

เวลา	หัวข้อบรรยาย/เสวนา	วิทยากร/ผู้ทรงคุณวุฒิ
13.00 – 13.30 น.	ลงทะเบียน	
13.30 – 13.35 น.	ประธานกล่าวเปิดงาน	**นางไอรดา เหลืองวิไล** รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
13.35 - 14.15 น.	การเสวนาในหัวข้อ **“ลงนามสะดวก ปลอดภัย และถูกต้อง ด้วยลายมือชื่ออิเล็กทรอนิกส์”**	1) **รศ. ดร.เกริก ภิรมย์โสภา** ประธานคณะทำงานเทคนิคด้านมาตรฐาน ความมั่นคงปลอดภัยภาครัฐ 2) **ดร.อุรัชฎา เกตุพรหม** ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล 3) **นายณัฏฐา พาชัยยุทธ** ผู้อำนวยการกองกิจการองค์การมหาชนและหน่วยงานของรัฐรูปแบบอื่น สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) 4) **นางสาวพลอย เจริญสม** ผู้ช่วยผู้อำนวยการสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์
14.15 – 14.30 น.	**พัก 15 นาที**	
14.30 – 15.00 น.	การนำเสนอร่างแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ	1) **ดร.ธีรวัฒน์ โรจนไพฑูรย์** ผู้เชี่ยวชาญมาตรฐานดิจิทัลภาครัฐ สำนักงานพัฒนารัฐบาลดิจิทัล 2) **นางสาวพิมพ์ชนก เจ็กภู่** นักวิเคราะห์อาวุโส สำนักงานพัฒนารัฐบาลดิจิทัล
15.00 – 15.25 น.	ตอบข้อซักถาม	
15.25 – 15.30 น.	ประธานกล่าวปิดงาน	**นางไอรดา เหลืองวิไล** รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

สามารถแสดงความคิดเห็นได้ ระหว่างวันที่ 30 เมษายน – 29 พฤษภาคม 2565

ช่องทางติดต่อเพื่อสอบถามข้อมูล รับข่าวสาร หรือร่วมพัฒนามาตรฐาน

ประกอบด้วย 2 ช่องทาง ได้แก่

เว็บไซต์

- https://standard.dga.or.th

ติดต่อ DGA Contact Center:

- โทร : (+66) 02 612 6060
- อีเมล: contact@dga.or.th
- เว็บไซต์ : https://www.dga.or.th/contact-dga/

ไอรดา เหลืองวิไล

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

กรณีศึกษาในร่างแนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของรัฐ

เพื่อใช้เป็นแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ และลายมือชื่อดิจิทัลที่เหมาะสมกับการปฏิบัติงาน**ของเจ้าหน้าที่ของรัฐ** ให้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ที่มี**ความมั่นคงปลอดภัย น่าเชื่อถือ และเป็นไปตามกฎหมาย**

1

ระบบใบรับรองผลการศึกษาอิเล็กทรอนิกส์
(Digital Transcript)

2

ระบบสารบรรณอิเล็กทรอนิกส์
(e-Saraban)

การเสวนาในหัวข้อ

“ลงนามสะดวก ปลอดภัย และถูกต้อง ด้วยลายมือชื่ออิเล็กทรอนิกส์”

รศ.ดร.เกริก ภิรมย์โสภา
ประธานคณะทำงานเทคนิค
ด้านความมั่นคงปลอดภัยภาครัฐ

ดร.อุรัชฎา เกตุพรหม
ผู้อำนวยการฝ่ายมาตรฐานดิจิทัลภาครัฐ
สำนักงานพัฒนารัฐบาลดิจิทัล

นายณัฏฐา พาชัยยุทธ
ผู้อำนวยการกองกิจการองค์การมหาชน
และหน่วยงานของรัฐรูปแบบอื่น
สำนักงานคณะกรรมการพัฒนาระบบราชการ

นางสาวพลอย เจริญสม
ผู้ช่วยผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทาง
อิเล็กทรอนิกส์

แนะนำ

“คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ”

โดย รศ.ดร.เกริก ภิรมย์โสภา

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ประธานคณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

หน้าที่และอำนาจ คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

- ศึกษาและจัดทำมาตรฐานและหลักเกณฑ์เกี่ยวกับการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เกี่ยวกับความมั่นคงปลอดภัยภาครัฐ
- ให้ข้อเสนอแนะแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล
- เชิญผู้แทนจากหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เข้าชี้แจงหรือขอให้สนับสนุนข้อมูลใด ๆ ต่อคณะทำงานได้ตามความเหมาะสม
- ดำเนินการอื่นใดตามที่ผู้อำนวยการหรือคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 มอบหมาย

การเสวนาในหัวข้อ

“ลงนามสะดวก ปลอดภัย และถูกต้อง ด้วยลายมือชื่ออิเล็กทรอนิกส์”

Q & A

พัก 15 นาที

การนำเสนอ

“ร่างแนวปฏิบัติ การลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ”

ดร.ธีรวัฒน์ โรจนไพฑูรย์
ผู้เชี่ยวชาญมาตรฐานดิจิทัลภาครัฐ
สำนักงานพัฒนารัฐบาลดิจิทัล

นางสาวพิมพ์ชนก เจ็กภู่
นักวิเคราะห์อาวุโส
สำนักงานพัฒนารัฐบาลดิจิทัล

เจ้าหน้าที่รัฐต้องรู้!

5 ประโยชน์ดีๆ ของ E-Signature

ช่วยให้การทำงานสบายขึ้นเป็นเท่าตัว!

- ลงนามผ่านอุปกรณ์อิเล็กทรอนิกส์ได้ทุกที่ทุกเวลา
- ลดการจัดเก็บเอกสารรูปแบบกระดาษ
- วิเคราะห์ข้อมูลได้รวดเร็วผ่านระบบคอมพิวเตอร์
- เพิ่มประสิทธิภาพในการทำงานของเจ้าหน้าที่ภาครัฐ
- ตรวจสอบความถูกต้องได้ด้วยการประมวลผลอัตโนมัติ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
“นำภาครัฐสู่การเป็นรัฐบาลดิจิทัล”
DGA Digital Government Development Agency

คนภาครัฐ มาทางนี้!

ทำความรู้จักกับ

หัวใจสำคัญ ของ E-Signature

- ต้องระบุตัวตนเจ้าของ E-Signature ได้
- แสดงเจตนาของเจ้าของ E-Signature ได้
- ใช้วิธีที่น่าเชื่อถือและถูกต้องตามกฎหมาย

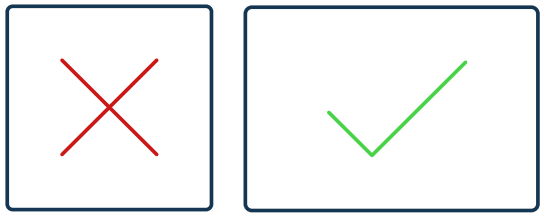
สาระสำคัญของ (ร่าง) แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์ สำหรับเจ้าหน้าที่ของรัฐ

1) e-Signature Act

กฎหมายที่เกี่ยวข้อง

2) e-Signature Overview

ภาพรวมการลงลายมือชื่ออิเล็กทรอนิกส์

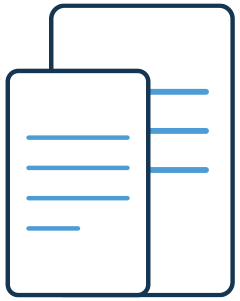


3) e-Signature Guideline

แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์

4) e-Signature Platform

ระบบลงลายมือชื่ออิเล็กทรอนิกส์



5) Case Study

กรณีศึกษาการลงลายมือชื่ออิเล็กทรอนิกส์

กฎหมายที่เกี่ยวข้องและภาพรวมของลายมือชื่ออิเล็กทรอนิกส์

e-Signature Act and Overview

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ประเภทและคุณสมบัติของลายมือชื่ออิเล็กทรอนิกส์ ตาม พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

มาตรา 9: ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

- ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้
- แสดงเจตนาของเจ้าของลายมือชื่อกับข้อความที่ลงลายมือชื่อได้
- ใช้วิธีการที่เชื่อถือได้ โดยคำนึงถึง
  - ความมั่นคงและรัดกุมของวิธีการที่ใช้
  - ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ ฯลฯ
  - ความรัดกุมของระบบติดต่อสื่อสาร

มาตรา 26:

- ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ข้อมูลที่ใช้สร้างลายมือชื่อเชื่อมโยงไปยังเจ้าของลายมือชื่อได้
- ข้อมูลที่ใช้สร้างลายมือชื่อ อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อ
- สามารถตรวจพบการเปลี่ยนแปลงของลายมือชื่อและข้อความได้

มาตรา 28: คุณสมบัติของผู้ให้บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์

ภาระการพิสูจน์ถึงความน่าเชื่อถือของลายมือชื่อ

เปรียบเทียบ มาตรา 9 กับ มาตรา 26

ประเภทลายมือชื่ออิเล็กทรอนิกส์	ข้อสันนิษฐานของลายมือชื่ออิเล็กทรอนิกส์	
	ผู้ที่กล่าวอ้างว่า ลายมือชื่อนั้นน่าเชื่อถือ	**ผู้ที่โต้แย้งหรือคัดค้านว่า ลายมือชื่อนั้นไม่น่าเชื่อถือ**
ทั่วไป (มาตรา 9)	ผู้ที่กล่าวอ้างมีภาระการพิสูจน์ถึงความน่าเชื่อถือนั้น	ผู้ที่โต้แย้งหรือคัดค้านมิได้มีภาระการพิสูจน์ถึงความไม่น่าเชื่อถือนั้น
ที่เชื่อถือได้ (มาตรา 26)	ผู้ที่กล่าวอ้างพิสูจน์เพียงว่าตนได้ปฏิบัติตามเงื่อนไขแห่งมาตรา 26 แล้ว โดยได้รับประโยชน์จากข้อสันนิษฐานความน่าเชื่อถือนั้น	ผู้ที่โต้แย้งหรือคัดค้านมีภาระการพิสูจน์ถึงความไม่น่าเชื่อถือนั้น

มาตรฐานการลงลายมือชื่ออิเล็กทรอนิกส์ในประเทศไทย

ขมธอ. 23-2563 ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Guideline)

ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

ประเภทที่ 1

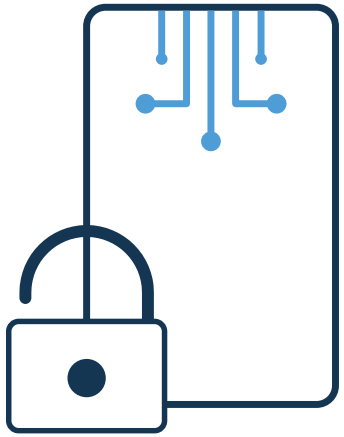
ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป

มาตรา 9

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

ประเภทที่ 2

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้



มาตรา 26

ประเภทที่ 3

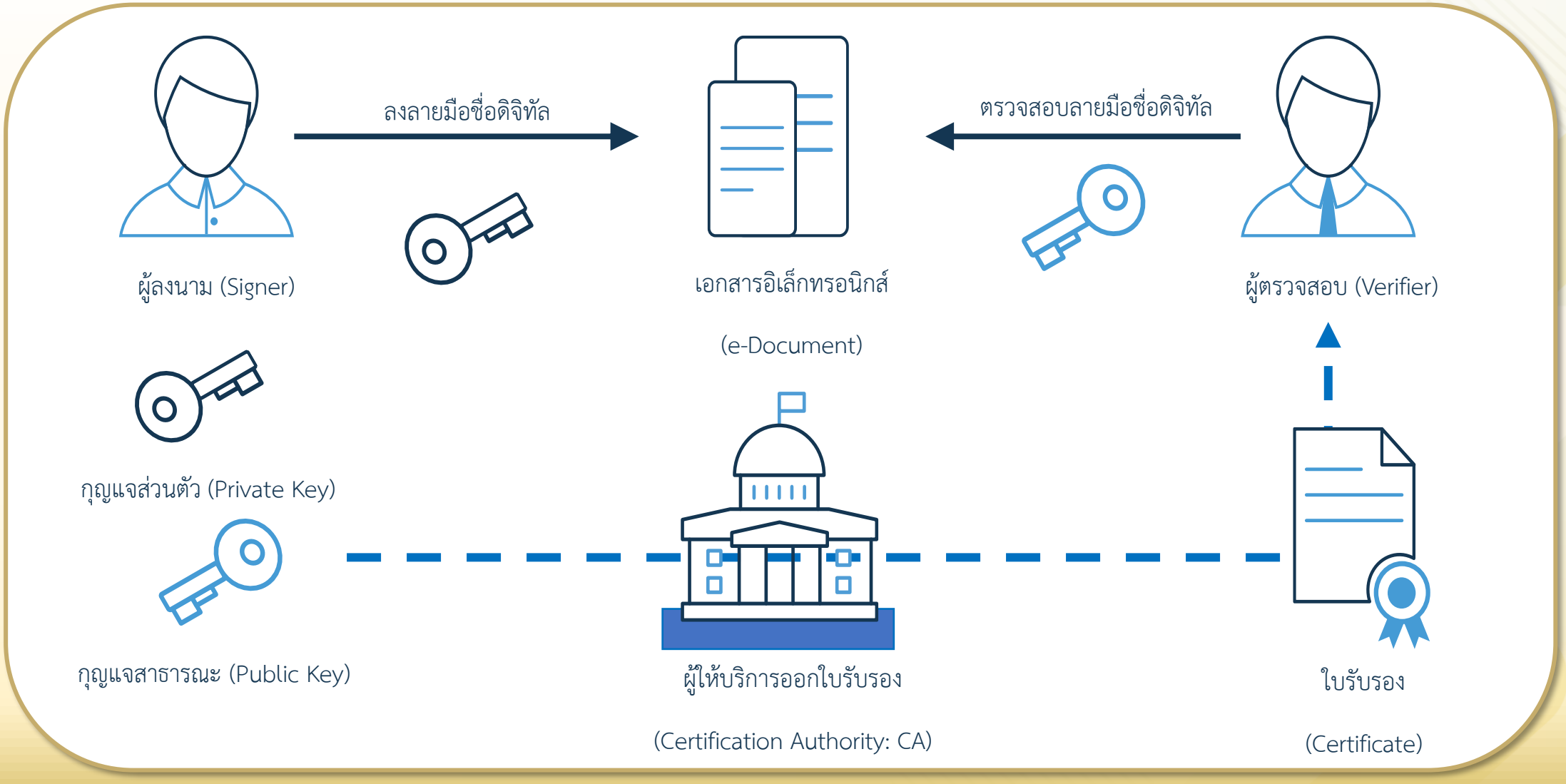
ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ซึ่งใช้

ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง

มาตรา 26 และ 28

ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ หรือลายมือชื่อดิจิทัล (Digital Signature)

ลายมือชื่อดิจิทัลเป็นลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ด้วยระบบรหัสแบบอสมมาตร (Asymmetric Cryptography)



คุณสมบัติของลายมือชื่อดิจิทัล (Digital Signature)

Authentication

สามารถยืนยันตัวเจ้าของลายมือชื่อ

Data Integrity

ตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้

Non-repudiation

เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้

ใบรับรอง (Certificate)

โดยสามารถขอออกใบรับรองได้ ในรูปแบบ CD, Smartcard และ USB Token

ใช้กับลายมือลายมือชื่ออิเล็กทรอนิกส์ ประเภทที่ 3 ออกโดยผู้ให้บริการออกใบรับรอง เช่น TDID INET (NRCA Subordinate)

ใบรับรองทำหน้าที่รับรองกุญแจสาธารณะให้กับผู้ลงนาม แบ่งได้เป็น 3 ประเภท ได้แก่

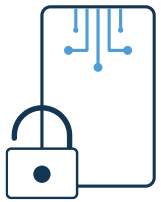
- ใบรับรองบุคคล
- ใบรับรองเจ้าหน้าที่นิติบุคคล (กรณีหน่วยงานออกเอกสารอิเล็กทรอนิกส์ที่ต้องระบุว่า ให้บุคคลใดเป็นผู้ลงนามเท่านั้น)
- ใบรับรองนิติบุคคล

ผู้ให้บริการออกใบรับรองมีหน้าที่ทำการเผยแพร่ใบรับรองและทำรายการเพิกถอนใบรับรอง เพื่อให้ผู้ใช้งานทั่วไปได้เข้ามาตรวจสอบสถานะใบรับรอง

ผู้ให้บริการออกใบรับรองแห่งชาติ (Thailand National Root Certification Authority: NRCA) ได้อยู่ในรายชื่อผู้ให้บริการที่น่าเชื่อถือ หรือที่เรียกว่า Trust List ของผู้ให้บริการเอกสารอิเล็กทรอนิกส์ เช่น Adobe Approved Trust List และ Microsoft Trusted Root Program ทำให้เอกสารที่ได้มีการลงลายมือชื่อดิจิทัลด้วยใบรับรองจากทาง NRCA ได้รับการรับรองความน่าเชื่อถือและสามารถนำไปใช้งานได้ทั่วโลก

การใช้งานและตรวจสอบลายมือชื่ออิเล็กทรอนิกส์

ขมธอ. 23-2563 ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature Guideline)

	ตัวอย่างวิธีการจัดทำ	ตัวอย่างแนวทางการตรวจสอบหลักฐาน
ลายมือชื่ออิเล็กทรอนิกส์ 	• การพิมพ์ชื่อไว้ที่ท้ายเนื้อหาของอีเมล	• ตรวจสอบ**ที่อยู่อีเมล**ว่ามาจากชื่อโดเมนของส่วนราชการ
	• การสแกนภาพลายมือชื่อที่เขียนด้วยมือและแนบไว้กับเอกสาร	• ตรวจสอบ**ภาพลายมือชื่อและหลักฐานอื่น**ที่แสดงถึงบริบทสำคัญเกี่ยวกับการลงลายมือชื่อ เช่น บุคคลที่สาม ลายมือชื่อในเอกสารก่อนหน้า
	• การใช้ระบบอัตโนมัติที่มีการยืนยันตัวตนประกอบกับลายมือชื่อประเภทที่ 1	• ตรวจสอบ**รายละเอียด** เช่น บันทึกเหตุการณ์ (log) การเข้าระบบและการกดยอมรับเพื่อลงลายมือชื่อ ซึ่งอาจมีได้อยู่ในรูปแบบของชื่อหรือลายมือชื่อ
	• การเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์โดยอาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI)	• ตรวจสอบผ่านเว็บไซต์หรือแอปพลิเคชันสำหรับการตรวจสอบลายมือชื่อ • ตรวจสอบผ่านโปรแกรมที่ใช้ในการเปิดเอกสารอิเล็กทรอนิกส์ ซึ่งรองรับการตรวจสอบลายมือชื่อดิจิทัล

แนวปฏิบัติการลงลายมือชื่ออิเล็กทรอนิกส์

e-Signature Guideline

ลำดับความเสี่ยงของธุรกรรม (Criticality Levels)

ระดับธรรมดา (Standard): ธุรกรรมทั่วไป ซึ่งอาจหมายรวมถึงการแลกเปลี่ยนหรือเข้าถึงข้อมูลอย่างจำกัด เช่น ธุรกรรมส่วนบุคคลที่มีผลกระทบในระดับต่ำต่อองค์กร การแลกเปลี่ยนข้อมูลภายในองค์กรตามลำดับชั้นของข้อมูลที่กำหนด — เสนอแนะให้ใช้**ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1**

ระดับขั้นสูง (Advanced): ธุรกรรมที่ต้องมีการพิจารณาอย่างรอบคอบถึงเงื่อนไขหรือข้อควรระวังเบื้องต้น — เสนอแนะให้ใช้**ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 2**

ระดับอ่อนไหว (Sensitive): ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่มีความละเอียดอ่อน เช่น ธุรกรรมที่เกี่ยวข้องกับข้อมูลที่เป็นความลับขององค์กร ธุรกรรมที่ก่อให้เกิดผลกระทบในวงกว้าง — เสนอแนะให้ใช้**ลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 3**

การเลือกใช้ประเภทลายมือชื่ออิเล็กทรอนิกส์

ตามชนิดของหนังสือราชการ

ชนิดของหนังสือราชการ ตามข้อ 10 แห่งระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. 2526

1) **หนังสือภายนอก:** หนังสือตราครุฑเพื่อติดต่อระหว่างส่วนราชการ หรือมีถึงหน่วยงานอื่นใดซึ่งมิใช่ส่วนราชการ หรือมีถึงบุคคลภายนอก

2) **หนังสือภายใน:** หนังสือติดต่อภายในกระทรวง ทบวง กรม หรือจังหวัดเดียวกัน

3) **หนังสือประทับตรา:** ใช้เฉพาะกรณีไม่ใช่เรื่องสำคัญ เช่น การขอรายละเอียดเพิ่มเติม การส่งสำเนาหนังสือ สิ่งของ เอกสาร หรือบรรณสาร การตอบรับทราบที่ไม่เกี่ยวกับราชการสำคัญ หรือการเงิน การแจ้งผลงานที่ได้ดำเนินการไปแล้วให้ส่วนราชการที่เกี่ยวข้องทราบ การเตือนเรื่องที่ค้าง

4) **หนังสือสั่งการ:** คำสั่ง ระเบียบ และข้อบังคับ

5) **หนังสือประชาสัมพันธ์:** ประกาศ แถลงการณ์ และข่าว

6) **หนังสือที่เจ้าหน้าที่จัดทำขึ้นหรือรับไว้เป็นหลักฐานในราชการ:** หนังสือรับรอง รายงานการประชุม บันทึก และหนังสืออื่น

ประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

รูปแบบการลงลายมือชื่ออิเล็กทรอนิกส์	ประเภทของผู้ลงนาม	ประเภทลายมือชื่อที่แนะนำ
1) หนังสือภายนอก	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกระทรวง	ประเภทที่ 3
2) หนังสือภายใน	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกรมหรือเทียบเท่า	ประเภทที่ 3
3) หนังสือประทับตรา	ในนามส่วนราชการ โดยหัวหน้าส่วนราชการระดับกองหรือเจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ 3
4) หนังสือสั่งการ		
4.1) มีผลบังคับใช้ในระดับภายในส่วนราชการ	ผู้บริหารระดับสูงหรือในนามส่วนราชการ	ประเภทที่ 2
4.2) มีผลบังคับใช้ในวงกว้าง เช่น ระหว่างส่วนราชการ เอกชน ภาคประชาชน ฯลฯ	ผู้บริหารระดับสูงหรือในนามส่วนราชการ	ประเภทที่ 3
5) หนังสือประชาสัมพันธ์	ในนามส่วนราชการ	ประเภทที่ 3
6) หนังสือที่เจ้าหน้าที่จัดทำขึ้น หรือรับไว้เป็นหลักฐานราชการ		
6.1) หนังสือที่ใช้ในการปฏิบัติงานในลักษณะเป็นประจำทั่วไป เช่น แบบคำร้อง คำขอ	เจ้าหน้าที่ธุรการหรือระบบอัตโนมัติ	ประเภทที่ 1
6.2) บันทึกเพื่อการติดต่อภายในส่วนราชการ เช่น บันทึกข้อความรายงานการประชุม	เจ้าหน้าที่ทั่วไป	ประเภทที่ 2
6.3) หนังสือที่จัดทำขึ้นตามอำนาจที่ได้รับมอบหมาย เช่น หนังสือรับรอง	เจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ 3
6.4) หนังสือที่มีพยานร่วมลงนาม	ผู้ลงนาม: ในนามส่วนราชการโดยผู้มีอำนาจลงนาม พยาน: เจ้าหน้าที่ผู้ได้รับมอบหมาย	ประเภทที่ 3

การเลือกใช้ประเภทลายมือชื่ออิเล็กทรอนิกส์ตามลักษณะการลงนาม

การลงลายมือชื่อ แบ่งออกได้เป็น 2 ลักษณะ ได้แก่ การลงลายมือชื่อโดยบุคคลเดียวในเอกสาร (Single Signing) และการลงลายมือชื่อหลายบุคคล (Multiple Signing)

การลงลายมือชื่อโดยบุคคลเดียว

- ❑ **การลงลายชื่อในนามบุคคลธรรมดา โดยเจ้าหน้าที่ภาครัฐ** เช่น การลงนามในบันทึกข้อความเพื่อการปฏิบัติหน้าที่ต่าง ๆ
- ❑ **การมอบอำนาจให้ลงลายมือชื่อ โดยผู้รับมอบอำนาจ** เช่น การลงนามแทนตามภารกิจที่ได้รับมอบหมาย การลงนามรับรองโดยนายทะเบียนผู้รับมอบอำนาจ
- ❑ **การลงลายมือชื่อในนามนิติบุคคล โดยผู้มีอำนาจตามกฎหมาย** เช่น หัวหน้าส่วนราชการระดับกรมขึ้นไป ผู้ว่าราชการจังหวัด และผู้มีอำนาจลงนามแต่เพียงผู้เดียวของนิติบุคคล

การลงลายมือชื่อหลายบุคคล

- ❑ **การลงลายมือชื่อหลายคน จากการจัดตั้งคณะบุคคลตามภารกิจ** เช่น การลงนามของคณะกรรมการบริหารโครงการ
- ❑ **การลงลายมือชื่อที่ต้องอาศัยพยาน** เช่น การลงนามในสัญญาจัดซื้อจัดจ้าง การลงนามในบันทึกข้อตกลงระหว่างนิติบุคคล

*หมายเหตุ การลงนามหลายบุคคล ควรใช้ลายมือชื่ออิเล็กทรอนิกส์ประเภทเดียวกัน

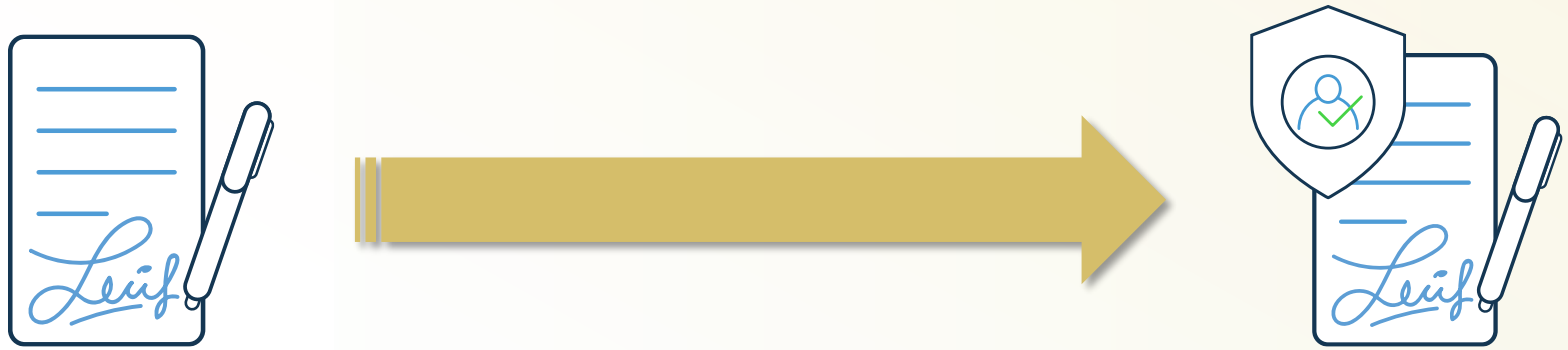
แนวทางการลงลายมือชื่อระหว่างสถานการณ์ฉุกเฉิน

1) ก่อนเกิดสถานการณ์ฉุกเฉิน

ควรมีการ**จัดทำแผน**สำหรับรองรับสถานการณ์ฉุกเฉิน หรือสภาวะวิกฤติที่อาจเกิดขึ้นในพื้นที่ปฏิบัติงาน

2) เมื่อเกิดสถานการณ์ฉุกเฉิน

ควรมี**การแจ้งเหตุฉุกเฉิน**ไปยังไปยังส่วนราชการ หรือผู้ที่เกี่ยวข้อง เช่น หน่วยงานต้นสังกัด หน่วยงานที่มีการติดต่อประสานงานเป็นประจำ และประชาชนผู้ใช้บริการ เพื่อให้รับทราบถึงข้อจำกัดในการดำเนิน



3) ระหว่างสถานการณ์ฉุกเฉิน

ส่วนราชการอาจใช้วิธีการทำงานที่ไม่ต้องพึ่งพาระบบ (manual work) คือ **การลงลายมือชื่อบนเอกสารกระดาษ** ตามที่เคยปฏิบัติมา

4) หลังจากสถานการณ์ฉุกเฉินสิ้นสุดลง

ควรมีการ**สร้างข้อมูลอิเล็กทรอนิกส์กลับขึ้นมาใหม่** โดยใช้ความระมัดระวังไม่ให้เกิดการทำซ้ำหรือขาดตกบกพร่อง ซึ่งส่วนราชการควรจัดให้มีลายมือชื่ออิเล็กทรอนิกส์ของหน่วยงานเพื่อการรับรองสำเนาที่แปลงมาโดยเจ้าหน้าที่ผู้ที่ได้รับมอบหมาย

แนวทางการลงลายมือชื่อสำหรับส่วนราชการที่ไม่มีความพร้อม

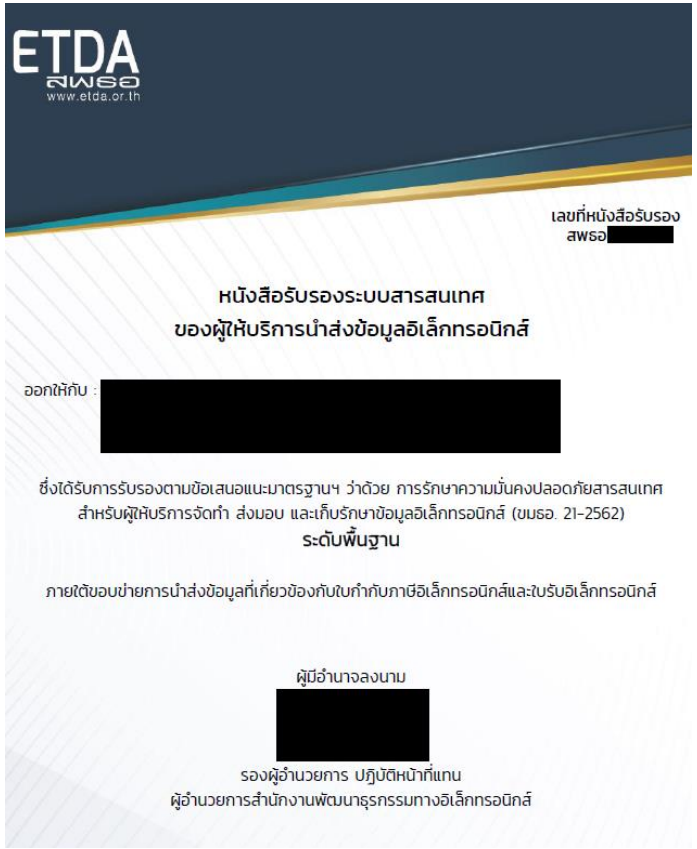
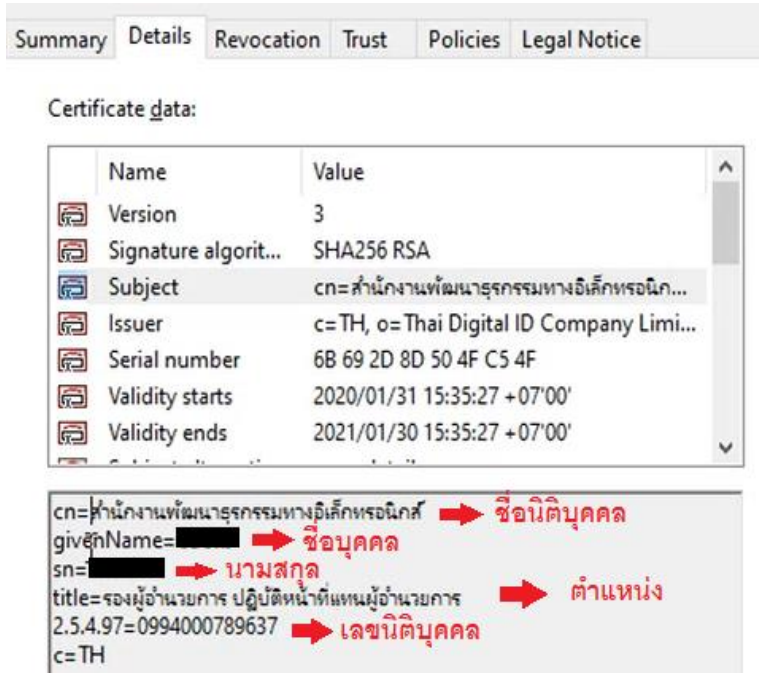
เช่น กรณีอยู่ในพื้นที่ห่างไกล ไม่สามารถเข้าถึงเครือข่ายอินเทอร์เน็ต หรือขาดระบบเทคโนโลยีสารสนเทศ

- ปฏิบัติตาม แนวปฏิบัติการรับ-ส่งหนังสือราชการทางอิเล็กทรอนิกส์ระหว่างส่วนราชการที่เป็นนิติบุคคล (สำนักงาน ก.พ.ร.) ศึกษาเพิ่มเติมที่ https://www.opdc.go.th/content/NjM4Ng
- หากไม่มี Email ของหน่วยงานให้แจ้งความประสงค์กับ สพร.

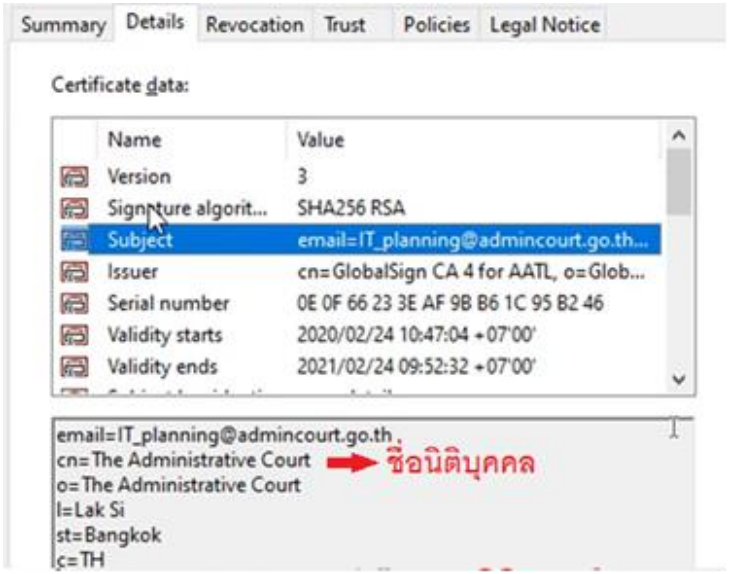
ข้อแนะนำสำหรับส่วนราชการที่ไม่มีความพร้อม

- การจัดทำและการส่ง หน่วยงานอาจขอใช้งานอุปกรณ์ในการจัดทำเอกสารอิเล็กทรอนิกส์ ลงลายมือชื่ออิเล็กทรอนิกส์และจัดส่ง ณ สำนักงานในเขตพื้นที่ใกล้เคียง เช่น สำนักงานในระดับอำเภอ หรือจังหวัด
- การรับ อาจแจ้งส่วนราชการผู้จัดส่งเอกสารเพื่อขอรับหนังสือในรูปแบบกระดาษ หรือจัดเจ้าหน้าที่ผู้รับผิดชอบการตรวจสอบการรับหนังสือราชการอิเล็กทรอนิกส์ ณ สำนักงานในเขตพื้นที่ใกล้เคียงที่ได้ขอใช้งานอุปกรณ์คอมพิวเตอร์และการสื่อสาร อาจพิมพ์ออกและลงลายมือชื่อด้วยหมึกเพื่อรับรองเอกสาร ก่อนที่จะส่งต่อไปยังส่วนราชการที่ไม่มีความพร้อม เพื่อให้สามารถดำเนินการต่อในรูปแบบกระดาษได้

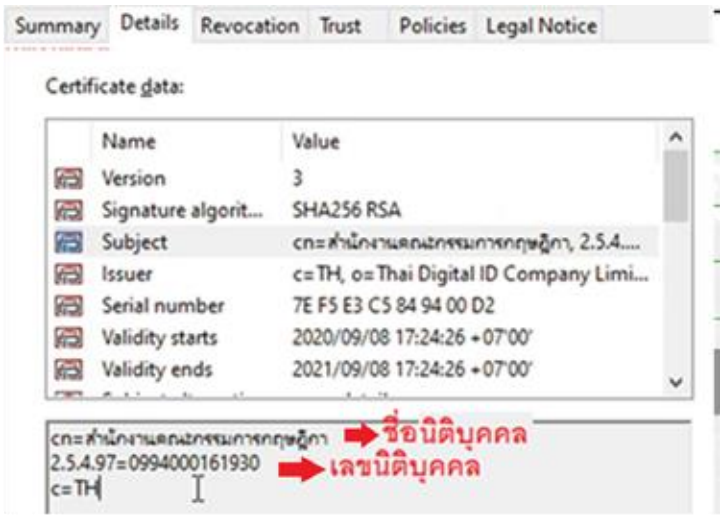
ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)
1. หนังสือรับรองระบบสารสนเทศของผู้ให้บริการนำส่งข้อมูลทางอิเล็กทรอนิกส์ของ สพธอ. แนวทางการใช้งานเอกสารต้นฉบับและการลงลายมือชื่อเป็นอิเล็กทรอนิกส์ตั้งแต่ต้น ซึ่งมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใช้ใบรับรองอิเล็กทรอนิกส์ของบุคคล (โดยระบุชื่อนามสกุล หน่วยงานที่สังกัด ตำแหน่งหน้าที่ชัดเจน)	 

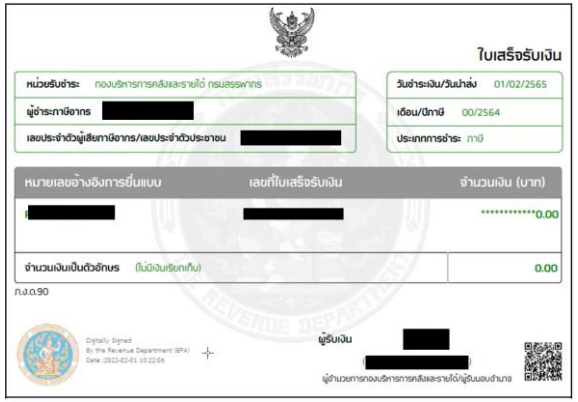
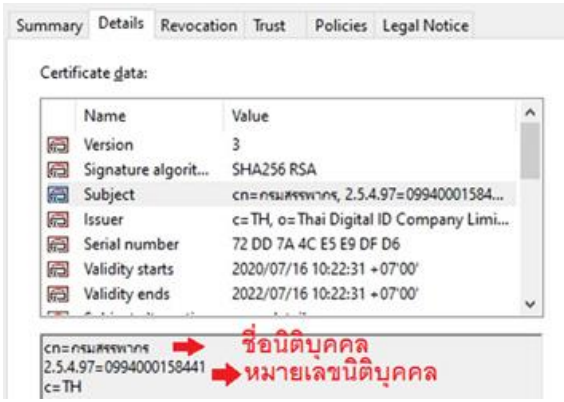
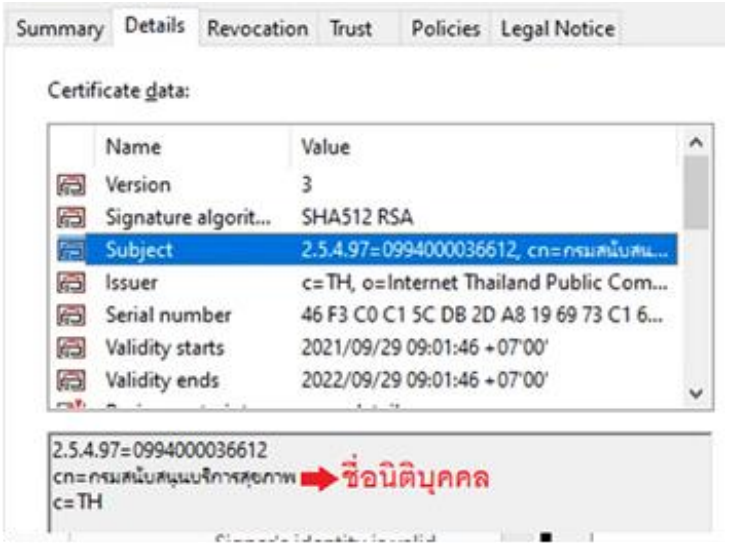
ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
2. เอกสารการขอคัดคำพิพากษาจากเว็บไซต์ของศาลปกครอง มีการลงลายมือชื่อบนกระดาษและสแกนเอกสารเป็นไฟล์อิเล็กทรอนิกส์ โดยมีการลงลายมือชื่ออิเล็กทรอนิกส์ทับลงไปในเอกสาร เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง โดยเป็นใบรับรองอิเล็กทรอนิกส์ที่ออกให้หน่วยงานหรือองค์กร (นิติบุคคล)		

ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
3. หนังสือเชิญประชุมจากสำนักงานกฤษฎีกา มีการลงลายมือชื่อบนกระดาษและสแกนเอกสารเป็นไฟล์อิเล็กทรอนิกส์ โดยมีการลงลายมือชื่ออิเล็กทรอนิกส์ทับลงไปในเอกสาร เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง โดยเป็นใบรับรองอิเล็กทรอนิกส์ที่ออกให้องค์กร (ใบรับรองนิติบุคคล โดยมีเลขนิติบุคคลขององค์กรแสดง)		

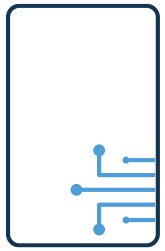
ตัวอย่างการใช้ลายมือชื่ออิเล็กทรอนิกส์ในเอกสารราชการ

เอกสาร	ภาพตัวอย่างเอกสารรูปแบบ PDF และข้อมูลที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ (CA)	
4. ใบเสร็จรับเงินอิเล็กทรอนิกส์โดยกรมสรรพากร มีการนำลายมือชื่อที่เป็นภาพมาการนำลายมือชื่อที่เป็นภาพมาวาง ก่อนมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใบรับรองอิเล็กทรอนิกส์ขององค์กร		
5. เอกสารใบอนุญาตโดยผู้มีอำนาจลงนาม 2 ท่าน ขึ้นไป เอกสารนี้เป็นลักษณะของเอกสารที่ผู้มีอำนาจหลายคนลงนามบนเอกสารเดียวกัน มีการนำลายมือชื่อที่เป็นภาพมาวาง ก่อนมีการลงลายมือชื่ออิเล็กทรอนิกส์โดยใบรับรองอิเล็กทรอนิกส์ขององค์กร (ใบรับรองนิติบุคคล) เพื่อไม่ให้เกิดการแก้ไขเปลี่ยนแปลงได้ในภายหลัง		

ระบบลงลายมือชื่ออิเล็กทรอนิกส์

e-Signature Platform

องค์ประกอบระบบลงลายมือชื่ออิเล็กทรอนิกส์



บริการเอกสารอิเล็กทรอนิกส์

e-Document Service

ทำหน้าที่บริหารจัดการเอกสารอิเล็กทรอนิกส์ตลอดวงจรชีวิต

ของเอกสาร (ขมธอ. 11-2560) เช่น ระบบ e-Saraban

บริการลงลายมือชื่อ

Signing Service

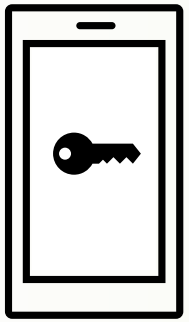
ทำหน้าที่อำนวยการลงลายมือชื่ออิเล็กทรอนิกส์บนเอกสาร

อิเล็กทรอนิกส์

บริการตรวจสอบลายมือชื่อ

Verification Service

ทำหน้าที่เชื่อมต่อกับระบบ PKI เพื่อตรวจสอบเอกสารและลายมือชื่อ

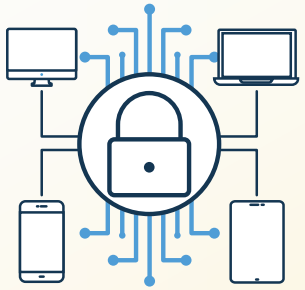


อุปกรณ์จัดเก็บกุญแจ

Key Storage

ทำหน้าที่จัดเก็บ บริหารจัดการ และใช้งานกุญแจส่วนตัว

เพื่อการลงลายมือชื่ออิเล็กทรอนิกส์



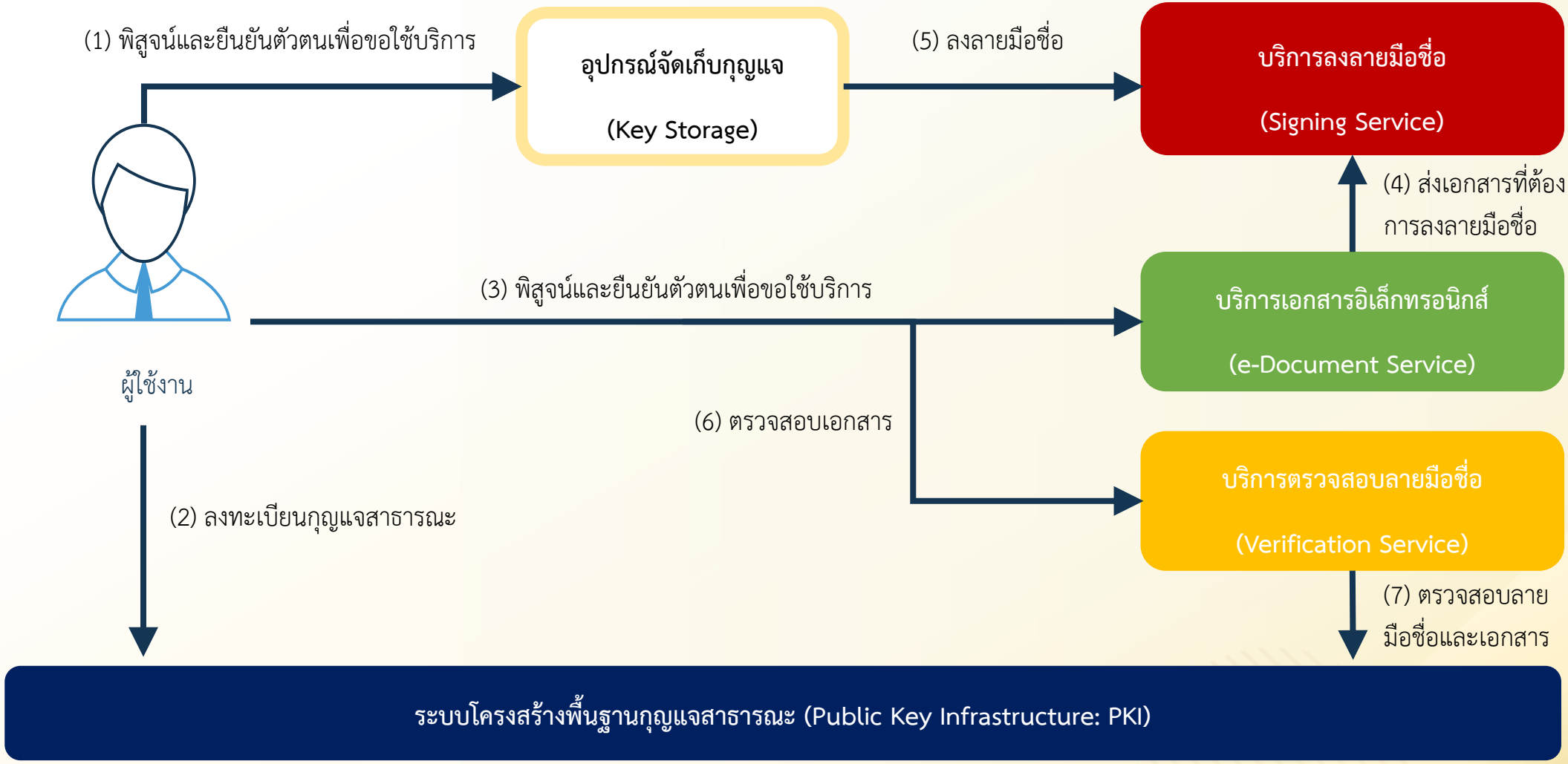
โครงสร้างพื้นฐานกุญแจสาธารณะ

Public Key Infrastructure (PKI)

ทำหน้าที่ให้บริการออกใบรับรองและรายการเพิกถอนใบรับรอง

เพื่อรับรองกุญแจสาธารณะ

ระบบลงลายมือชื่ออิเล็กทรอนิกส์



ระบบบริการและแนวทางการบรรเทาความเสี่ยง

บริการเอกสารอิเล็กทรอนิกส์ (e-Document Service)

- ทำหน้าที่เชื่อมต่อกับระบบอื่นเพื่ออำนวยให้เกิดการลงลายมือชื่ออิเล็กทรอนิกส์
- ทำหน้าที่เชื่อมต่อกับระบบอื่น ๆ เช่น บริการประทับรับรองเวลาอิเล็กทรอนิกส์ (e-Timestamping Service) และบริการอากรแสตมป์ (e-Stamp Duty Service)
- **อาจพิสูจน์และยืนยันตัวตนผู้ใช้งาน**ว่ามีอำนาจในการลงลายมือชื่อในเอกสารตามกฎเกณฑ์ของหน่วยงานหรือไม่
- ระบบควรบันทึกพยานหลักฐานที่เกี่ยวกับกับการลงลายมือชื่ออิเล็กทรอนิกส์ตาม ขมธอ. 23-2563

บริการลงลายมือชื่อ (Signing Service)

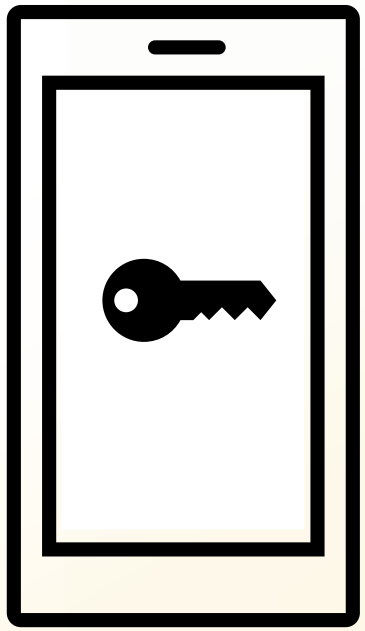
- ทำหน้าที่เชื่อมต่อกับ e-Document Service เพื่อรับเอกสาร และเชื่อมต่อกับ Key Storage เพื่อสร้างลายมือชื่อด้วยกุญแจส่วนตัว จากนั้นส่งเอกสารที่ถูกลงลายมือกลับมายัง e-Document Service
- **การสร้างลายมือชื่อควรเกิดขึ้นที่ Key Storage** โดย Signing Service ไม่ควรได้รับข้อมูลกุญแจส่วนตัวโดยตรง
- ระบบควรทำการลบข้อมูลเอกสารหรือข้อมูลส่วนบุคคลใด ๆ ภายหลังการลงลายมือชื่อ หากไม่มีเหตุจำเป็นต้องจัดเก็บข้อมูลดังกล่าว

บริการตรวจสอบลายมือชื่อ (Verification Service)

- ทำหน้าที่เชื่อมต่อกับระบบ PKI เพื่อตรวจสอบเอกสารและลายมือชื่อไม่ถูกปลอมแปลงหรือแก้ไข รวมทั้งระบุตัวตนและแสดงเจตนาของผู้ที่ลงลายมือชื่อ
- กรณีที่มีการลงลายมือชื่อหลายบุคคล ระบบสามารถตรวจสอบลำดับการลงลายมือชื่อ
- ระบบควรทำการลบข้อมูลเอกสารหรือข้อมูลส่วนบุคคลใด ๆ ภายหลังการตรวจสอบเอกสารและลายมือชื่อ หากไม่มีเหตุจำเป็นต้องจัดเก็บข้อมูลดังกล่าว

อุปกรณ์จัดเก็บกุญแจ

(Key Storage)



โครงสร้างพื้นฐานกุญแจสาธารณะ

(Public Key Infrastructure: PKI)

ประเภทอุปกรณ์จัดเก็บกุญแจ (Key Storage)

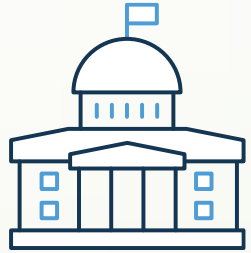
อุปกรณ์จัดเก็บกุญแจ (Key Storage) คือ ซอฟต์แวร์สำหรับบริหารจัดการกุญแจและข้อมูลอื่น ๆ ที่เกี่ยวข้อง รวมทั้งทำหน้าที่ในการเชื่อมต่อและแลกเปลี่ยนข้อมูลเข้ากับระบบอื่นเพื่ออำนวยให้เกิดการลงลายมือชื่ออิเล็กทรอนิกส์ โดยแบ่งออกเป็น 2 ประเภทหลักตามลักษณะการจัดเก็บกุญแจส่วนตัว ได้แก่

- กระเป๋าอิเล็กทรอนิกส์ในอุปกรณ์ส่วนตัว (Edge wallet): จัดเก็บกุญแจส่วนตัวภายในอุปกรณ์ที่ผู้ใช้งานครอบครอง
- กระเป๋าอิเล็กทรอนิกส์บนระบบคลาวด์ (Cloud wallet): จัดเก็บกุญแจส่วนตัวบนระบบคลาวน์คอมพิวเตอร์

ประเภท Key Storage	ข้อดี	ข้อเสีย
Edge Wallet	• **กุญแจส่วนตัวอยู่ภายใต้การควบคุมของผู้ใช้งาน** • มีความเสี่ยงต่ำในการเกิดปัญหาจากภัยคุกคามทางไซเบอร์	• ผู้ใช้งานมีภาระในการจัดเก็บและสำรองข้อมูล (backup) กุญแจส่วนตัวด้วยตนเอง • กุญแจส่วนตัวมีโอกาสสูญหายหากผู้ใช้งานไม่ระมัดระวัง
Cloud Wallet	• ผู้ใช้งานไม่มีภาระโดยตรงในการบริหารจัดการกุญแจส่วนตัว • ระบบคลาวน์ทำการสำรองข้อมูลกุญแจส่วนตัวโดยอัตโนมัติ	• **กุญแจส่วนตัวอยู่ภายใต้การควบคุมของผู้ให้บริการ** • ความปลอดภัยขึ้นกับความน่าเชื่อถือของผู้ให้บริการ

อ้างอิง: Preukschat, Alex, and Drummond Reed. *Self-sovereign identity*. Manning Publications, 2021

การบริหารจัดการกุญแจส่วนตัวสำหรับบุคคลและองค์กร



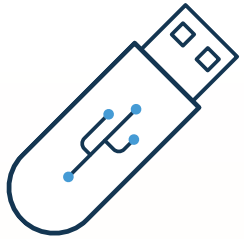
กุญแจส่วนตัวสำหรับบุคคล (natural person)	กุญแจส่วนตัวสำหรับองค์กร (legal person)
• ผู้ใช้งานต้องทำการยืนยันตัวตนก่อนการลงลายมือชื่อทุกครั้ง ด้วยวิธีการที่น่าเชื่อถือ เช่น การใช้รหัสผ่านที่มีความยาวเพียงพอหรือใช้ข้อมูลชีวมิติ (biometrics) • จัดเก็บกุญแจส่วนตัวด้วยการเข้ารหัสตามมาตรฐาน PKCS #12 หรือจัดเก็บภายในอุปกรณ์ที่น่าเชื่อถือ เช่น USB Authenticator และ Secure Enclave ตามมาตรฐาน FIPS 140-2 • จัดทำแนวทางการเพิกถอน (revocation) และ/หรือการกู้คืนข้อมูล (recovery) กุญแจส่วนตัวที่มีความปลอดภัยน่าเชื่อถือ • ทำการบันทึกประวัติการใช้งานกุญแจส่วนตัวสำหรับการลงลายมือชื่อ	• กำหนดนโยบายและมาตรการบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้งานที่ได้รับมอบอำนาจ ตามมาตรฐาน เช่น ISO/IEC 24760, ISO/IEC 29146 • กำหนดนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามมาตรฐานระดับสากล เช่น มาตรฐาน ISO/IEC 27001 • กำหนดนโยบายและมาตรการเพิกถอน (revocation) และ/หรือการกู้คืนข้อมูล (recovery) กุญแจส่วนตัว • จัดทำ Audit Trail เพื่อบันทึกการใช้งานกุญแจส่วนตัวโดยผู้ใช้งานทั้งหมด • ใช้อุปกรณ์ประเภท Cryptographic Modules ที่น่าเชื่อถือในการบริหารจัดการกุญแจส่วนตัว ตามมาตรฐาน เช่น NIST FIPS 140-2

อ้างอิง:

- NIST SP 800-57 Recommendation for Key Management: Part 1 – General
- NIST SP 800-57 Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations

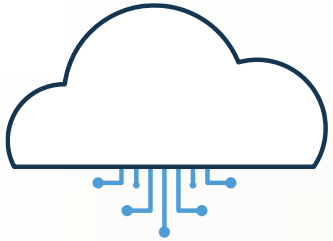
การกู้คืนและเพิกถอนกุญแจส่วนตัว

การบริหารจัดการกุญแจส่วนตัวควรกำหนดนโยบายและมาตรการกู้คืนข้อมูลกุญแจ (key recovery) และเพิกถอนกุญแจ (key revocation) เพื่อลดความเสี่ยงในการสูญเสียการเข้าถึงกุญแจและภัยคุกคามทางไซเบอร์ (อ้างอิง NIST SP 800-57 Part 1 Appendix B และ ITU X.509)



Offline Recovery

กู้คืนข้อมูลกุญแจจากอุปกรณ์ซึ่งไม่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยอุปกรณ์ที่ใช้สำรองข้อมูลควรมีอายุการใช้งานยาวนานเพียงพอต่อการใช้งานของกุญแจ (cryptoperiod)

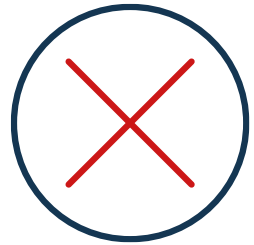


Online Recovery

กู้คืนข้อมูลกุญแจจากระบบคลาวด์ซึ่งเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต โดยควรเลือกใช้บริการจากผู้ให้บริการที่น่าเชื่อถือ และควรจัดเก็บกุญแจส่วนตัวที่ถูกเข้ารหัสแล้วด้วยกุญแจอื่นหรือใช้รหัสผ่าน (PKCS #12)

Social Recovery

กู้คืนข้อมูลกุญแจจากบุคคลหรือองค์กรอื่น (trustees) ที่ผู้ใช้งานเชื่อถือ เช่น การใช้กระบวนการ key sharding เพื่อแบ่งข้อมูลกุญแจส่วนตัวเป็นหลายส่วนให้ trustees จัดเก็บ

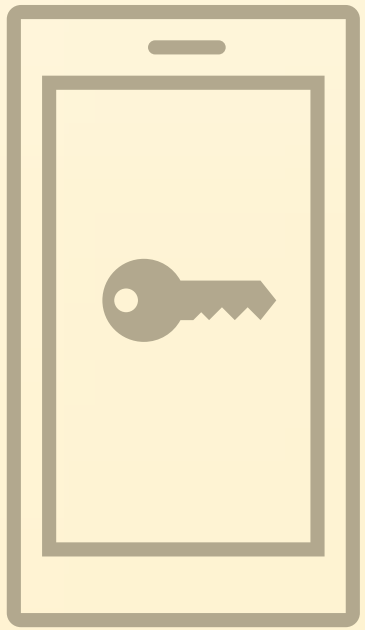


Revocation

เพิกถอนกุญแจส่วนตัวหากถูกเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาตหรือสูญหายโดยไม่สามารถกู้คืนได้ โดยแจ้ง CA ให้บันทึกการเพิกถอนกุญแจดังกล่าวลงรายการเพิกถอนใบรับรอง (Certificate Revocation List: CRL) หรือแก้ไขข้อมูลใน DID Document ในกรณีที่ใช้ DPKI

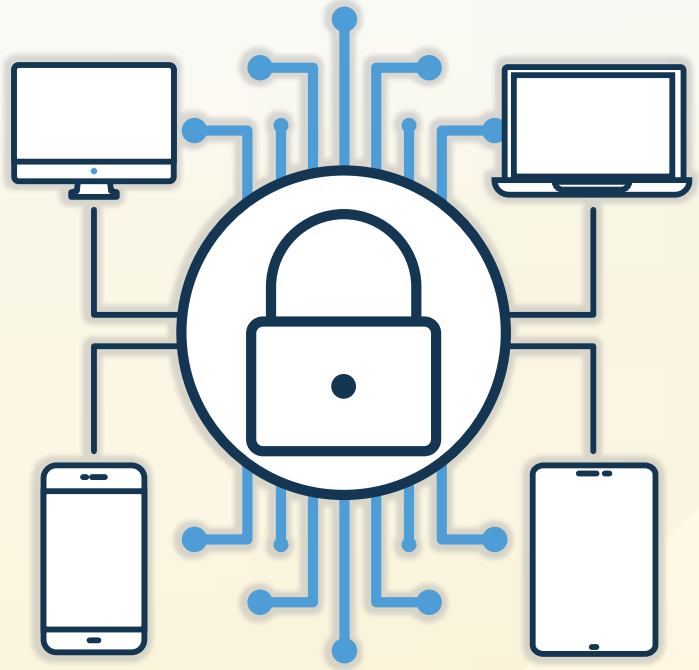
อุปกรณ์จัดเก็บกุญแจ

(Key Storage)



โครงสร้างพื้นฐานกุญแจสาธารณะ

(Public Key Infrastructure: PKI)

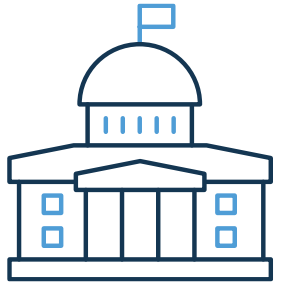


โครงสร้างพื้นฐานกุญแจสาธารณะ

โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) เป็นระบบสำหรับให้บริการออกใบรับรอง (Certificate) และรายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL) โดยใช้มาตรฐาน เช่น X.509 เพื่อรับรองว่ากุญแจสาธารณะนั้นมีความน่าเชื่อถือ สามารถนำไปใช้เพื่อตรวจสอบว่าลายมือชื่อนั้นถูกสร้างโดยผู้ลงนามตามที่กล่าวอ้าง รวมทั้ง ตรวจสอบว่าลายมือชื่อและเอกสารที่ถูกลงนามไม่มีการเปลี่ยนแปลง PKI ประกอบด้วย 4 องค์ประกอบใหญ่ๆ ที่สำคัญ ได้แก่

ผู้ใช้บริการ: End Entity

เป็นผู้ซึ่งประสงค์จะขอใช้บริการใบรับรองอิเล็กทรอนิกส์



ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์:

Certification Authority (CA)

ซึ่งทำหน้าที่ในการให้บริการเกี่ยวกับการออกใบรับรองอิเล็กทรอนิกส์

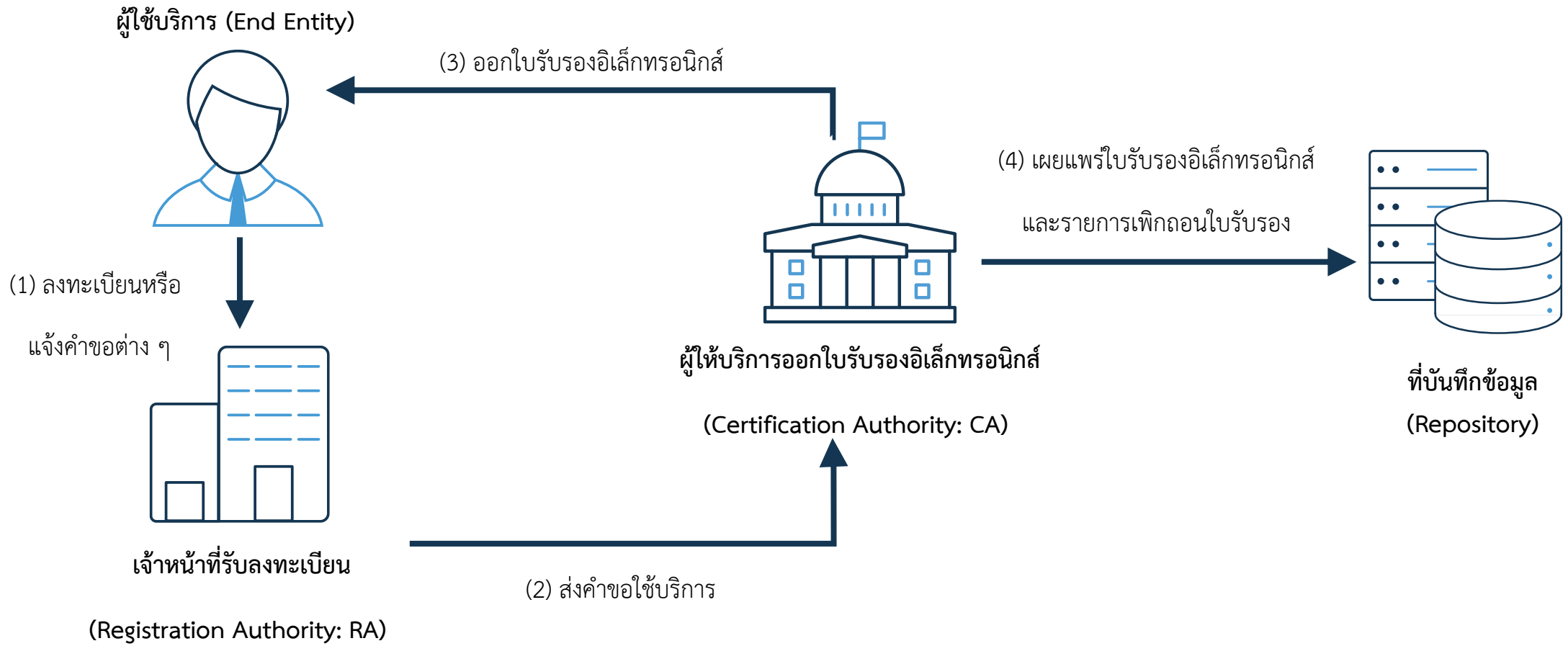
เจ้าหน้าที่รับลงทะเบียน: Registration Authority (RA)

ทำหน้าที่รับลงทะเบียน แจ้งเพิกถอน หรือต่ออายุใบรับรองอิเล็กทรอนิกส์ รวมทั้ง ตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ใช้บริการ

ที่บันทึกข้อมูล: Repository

เป็นระบบคอมพิวเตอร์สำหรับสืบค้นใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการ

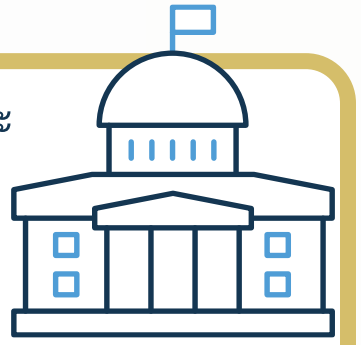
องค์ประกอบของโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์



ประเภทของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์

ผู้ให้บริการออกใบรับรองสาธารณะ

Publicly-trusted CA



- e-signature ประเภท 3

- เป็นผู้ให้บริการออกใบรับรองที่ให้บริการต่อสาธารณะ รวมถึงประชาชนทั่วไป บริษัทเอกชน และหน่วยงานของรัฐ

- กำกับดูแลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ซึ่งมีผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์แห่งชาติ (Thailand National Root Certification Authority: NRCA) เป็นผู้ให้บริการออกใบรับรองลำดับชั้นบนสุด (root CA) ซึ่งรับรองผู้ให้บริการออกใบรับรองในลำดับชั้นถัดลงมา (subordinate CA)

ผู้ให้บริการออกใบรับรองส่วนตัว

Privately-trusted CA

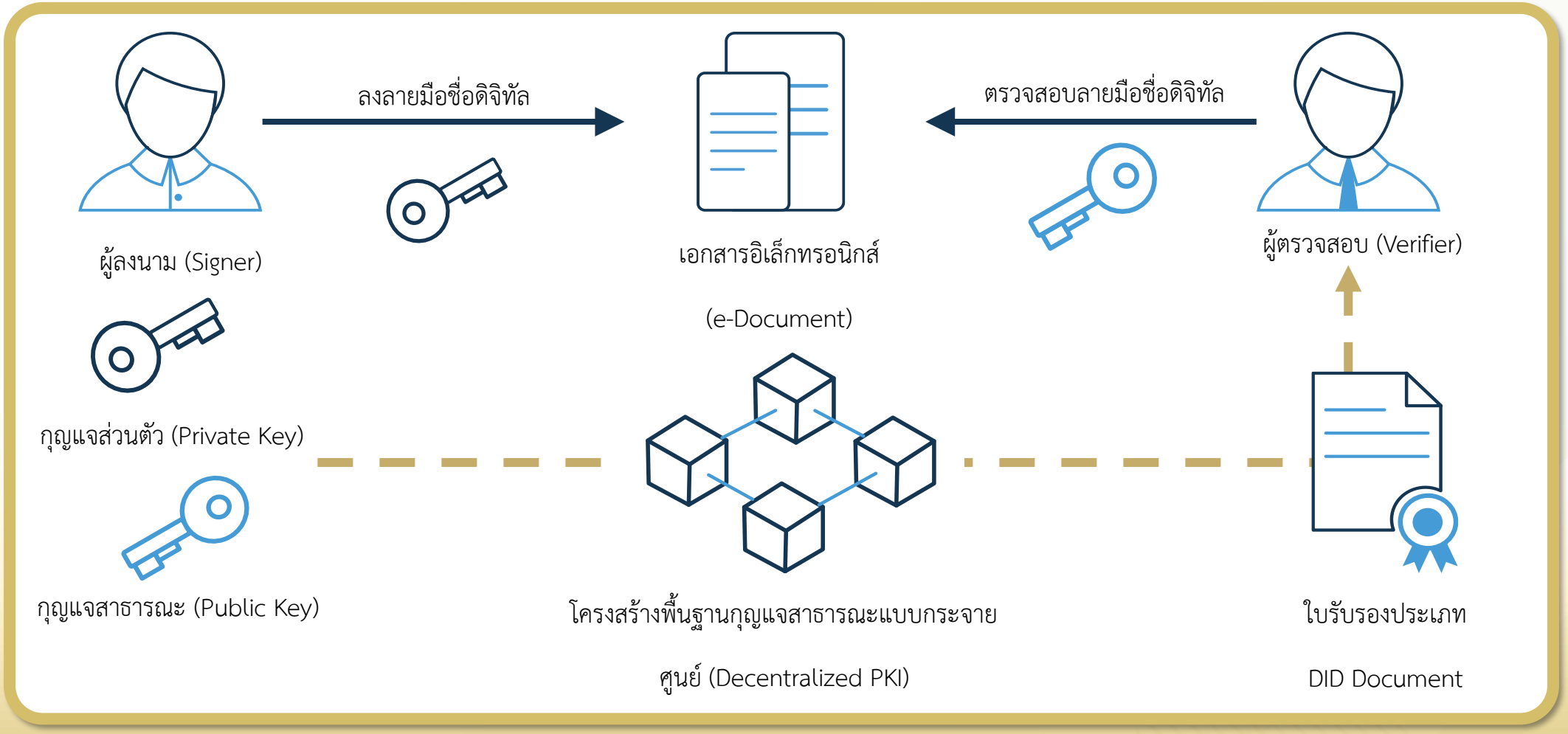
- e-signature ประเภท 2

- เป็นผู้ให้บริการออกใบรับรองที่ให้บริการภายในองค์กร หรือหน่วยงาน
- มีการพิสูจน์ตัวตนผู้ใช้งานก่อนออกใบรับรองตามความเหมาะสมของประเภทธุรกรรม
- ออกใบรับรองและรายการเพิกถอนใบรับรองตามมาตรฐาน ขมธอ. 15-2560 และ ITU X.509 และ IETF RFC5280 เป็นต้น
- บริหารจัดการกุญแจส่วนตัวและกุญแจสาธารณะตลอดวงจรชีวิตรวมทั้งการสำรองข้อมูลกุญแจตามมาตรฐาน เช่น NIST SP 800-57
- กำหนดนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามมาตรฐานความปลอดภัยทางไซเบอร์ เช่น ISO/IEC 27001
- ผู้ใช้งานภายในองค์กรควรเป็นผู้สร้างและถือครองกุญแจส่วนตัวด้วยตนเอง โดยส่งคำร้องขอใบรับรอง (Certificate Signing Request) มายังระบบออกใบรับรอง ตามมาตรฐาน PKCS#10 (IETF RFC 2986)

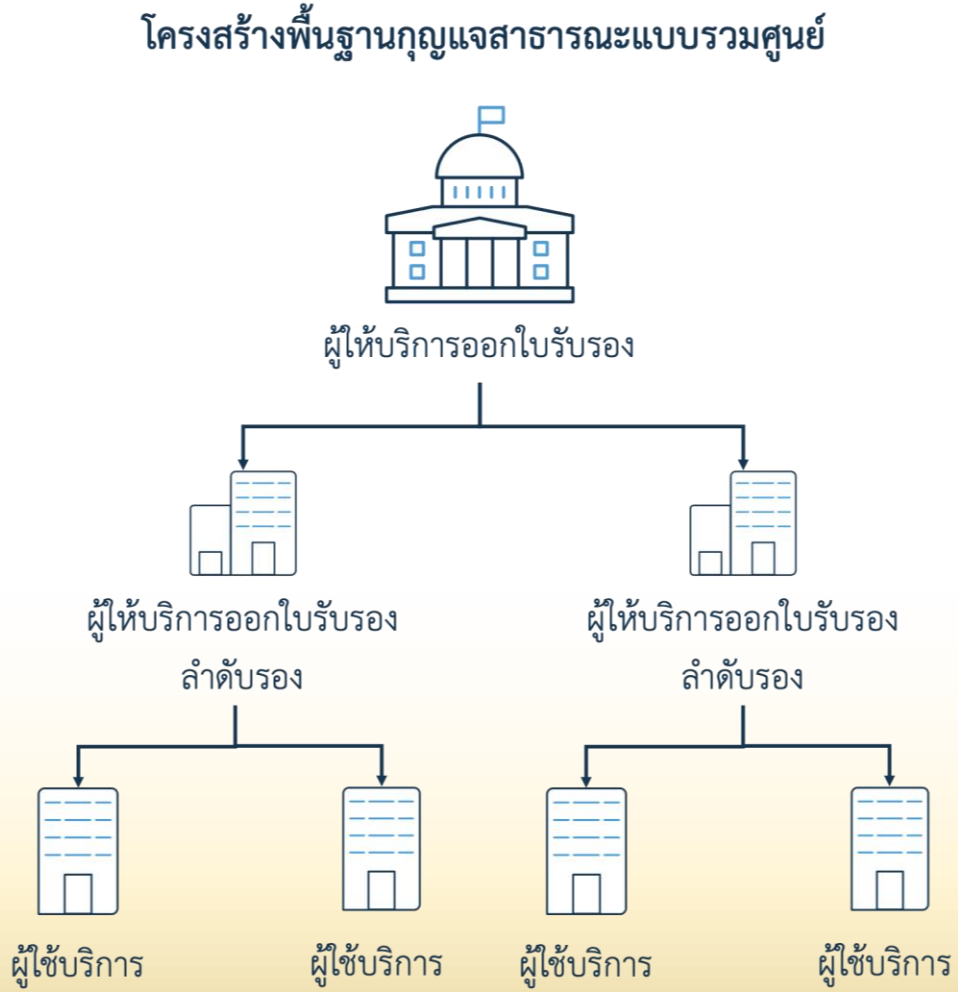
อ้างอิง: Thailand National Root Certification Authority , Certification Practice Statement

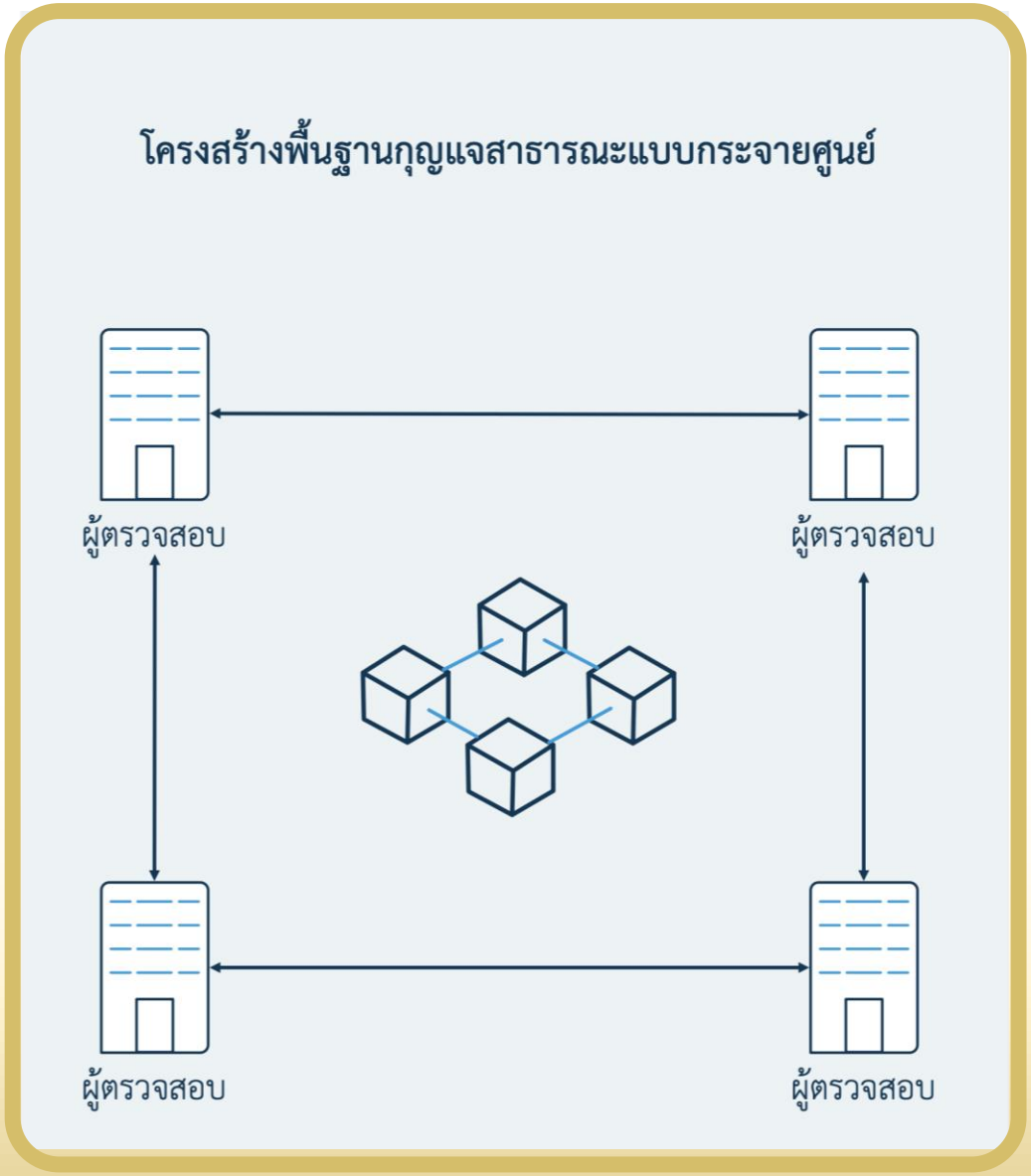
โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์

โครงสร้างพื้นฐานกุญแจสาธารณะแบบกระจายศูนย์ (Decentralized Public Key Infrastructure: DPKI) ใช้เทคโนโลยี distributed ledger มาประยุกต์ใช้เป็นโครงสร้างพื้นฐานกุญแจสาธารณะซึ่งไม่มีตัวกลางเป็นบุคคลหรือองค์กร โดยใช้ตัวระบุแบบกระจายศูนย์ (decentralized identifier: DID) และใบรับรองประเภท DID Document ทดแทนการออกใบรับรองประเภท X.509 โดย CA



เปรียบเทียบโครงสร้างพื้นฐานกุญแจสาธารณะแบบรวมศูนย์และกระจายศูนย์





แนวทางการใช้งานระบบโครงสร้างพื้นฐานกุญแจสาธารณะ

ประเภท PKI	ข้อดี	ข้อเสีย	ประเภทธุรกรรมที่เหมาะสม
Publicly-trusted CA	✓ รับรองลายมือชื่อประเภทที่ 3 ✓ หน่วยงานไม่จำเป็นต้องติดตั้งและดูแลระบบ PKI ด้วยตนเอง ✓ หน่วยงานไม่จำเป็นต้องพัฒนาบริการตรวจสอบลายมือชื่อ	○ ใบรับรองมีราคาแพง หากมีความต้องการใช้งานกุญแจเป็นจำนวนมาก ○ การออกใบรับรองและเปลี่ยนกุญแจใหม่มีราคาแพง	➢ การลงลายมือชื่อในเอกสารที่ใช้ตรวจสอบจากภายนอกองค์กร ➢ การลงลายมือชื่อในนามส่วนราชการหรือผู้บริหารระดับสูง
Privately-trusted CA	✓ รับรองลายมือชื่อประเภทที่ 2 ✓ องค์กรสามารถออกใบรับรองให้บุคลากรของตนได้อย่างอิสระ	○ องค์กรต้องจัดทำนโยบายและมาตรการบริหารจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์	➢ การลงลายมือชื่อในเอกสารที่ใช้ภายในองค์กรโดยบุคลากรจำนวนมาก
Decentralized PKI	✓ รับรองลายมือชื่อประเภทที่ 2 ✓ องค์กรสามารถออกใบรับรองให้บุคลากรของตนได้อย่างอิสระ	○ เป็นเทคโนโลยีใหม่ที่ยังไม่มีการใช้งานอย่างแพร่หลาย มีมาตรฐานและกรณีศึกษาสำหรับการอ้างอิงยังมีจำนวนน้อย	➢ การลงลายมือชื่อในเอกสารที่ใช้ภายในองค์กรโดยบุคลากรจำนวนมาก ➢ การทำธุรกรรมภายในภาคีความร่วมมือ (consortium) ระหว่างองค์กร

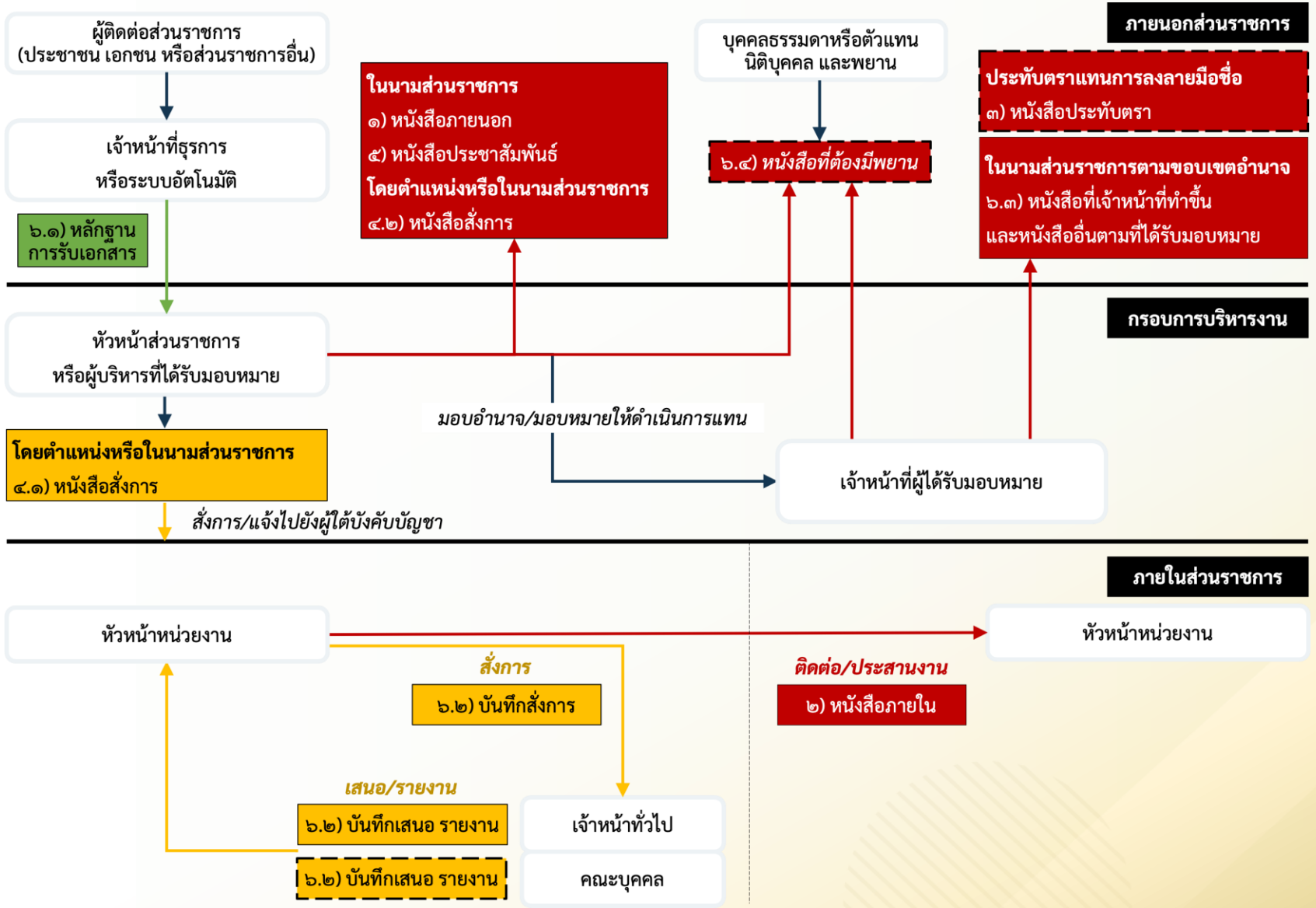
กรณีศึกษา

Case Study

แผนภาพการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับงานสารบรรณ (e-Saraban)

คำอธิบายแผนภาพ

แผนภาพแบ่งออกเป็น 3 ส่วนหลัก ได้แก่
(๑) ภายนอกส่วนราชการ หมายถึงบุคคลภายนอก หน่วยงานอื่นใดซึ่งมิใช่ส่วนราชการและส่วนราชการอื่น ที่มีหนังสือมายังส่วนราชการและที่ส่วนราชการออกหนังสือไปถึง
(๒) กรอบการบริหารงาน หมายถึง กระบวนการพิจารณาถึงการดำเนินงานที่เกี่ยวข้องกับหนังสือที่ได้รับ
(๓) ภายในส่วนราชการ หมายถึงเจ้าหน้าที่ภายในส่วนราชการเดียวกัน



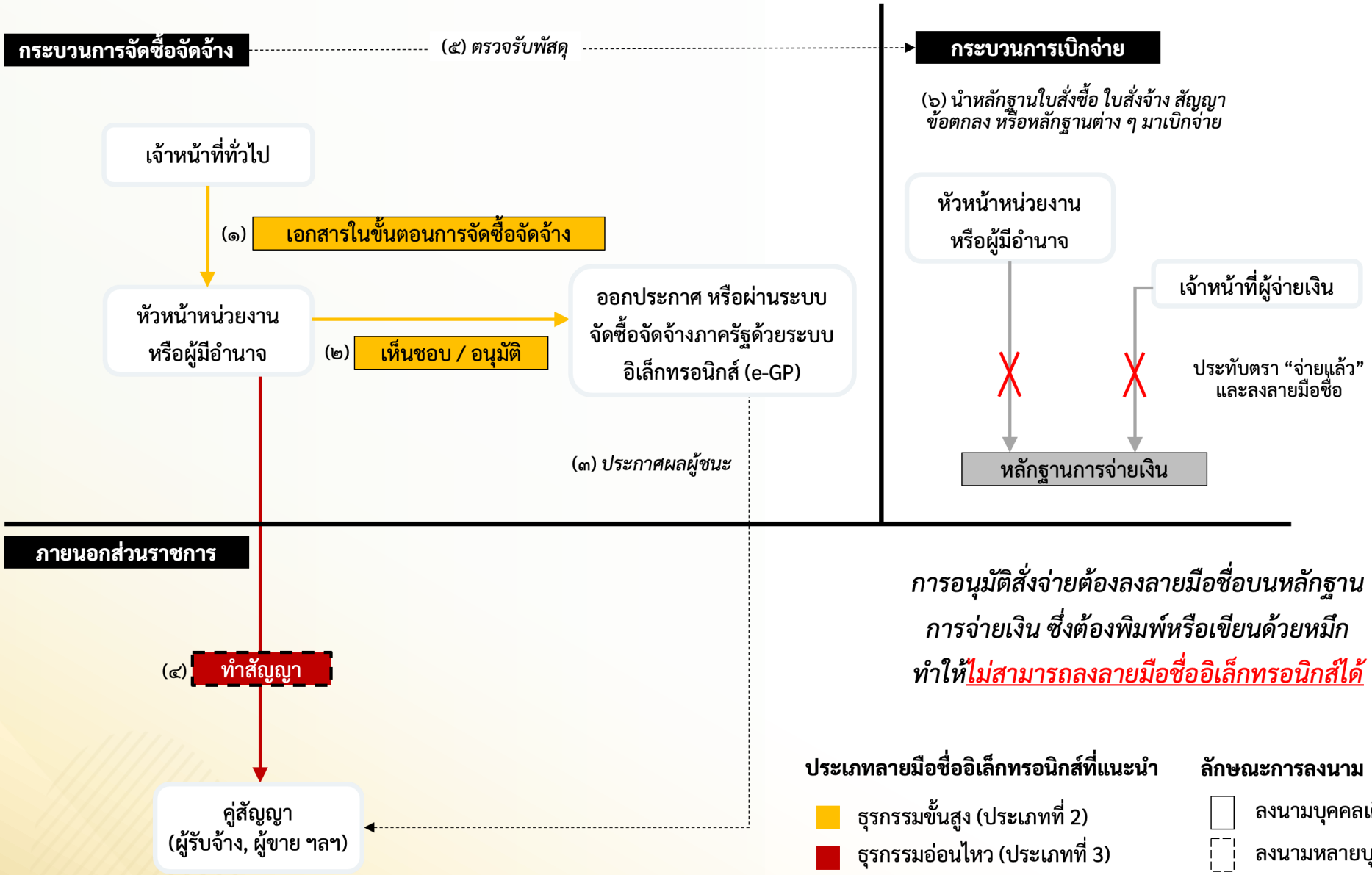
ประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

- ธุรกรรมธรรมดา (ประเภทที่ ๑)
- ธุรกรรมขั้นสูง (ประเภทที่ ๒)
- ธุรกรรมอ่อนไหว (ประเภทที่ ๓)

ลักษณะการลงนาม

- ลงนามบุคคลเดียว
- ลงนามหลายบุคคล

แผนภาพแสดงข้อจำกัดของการใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารทางการเงิน



การอนุมัติสั่งจ่ายต้องลงลายมือชื่อบนหลักฐานการจ่ายเงิน ซึ่งต้องพิมพ์หรือเขียนด้วยหมึก ทำให้ไม่สามารถลงลายมือชื่ออิเล็กทรอนิกส์ได้

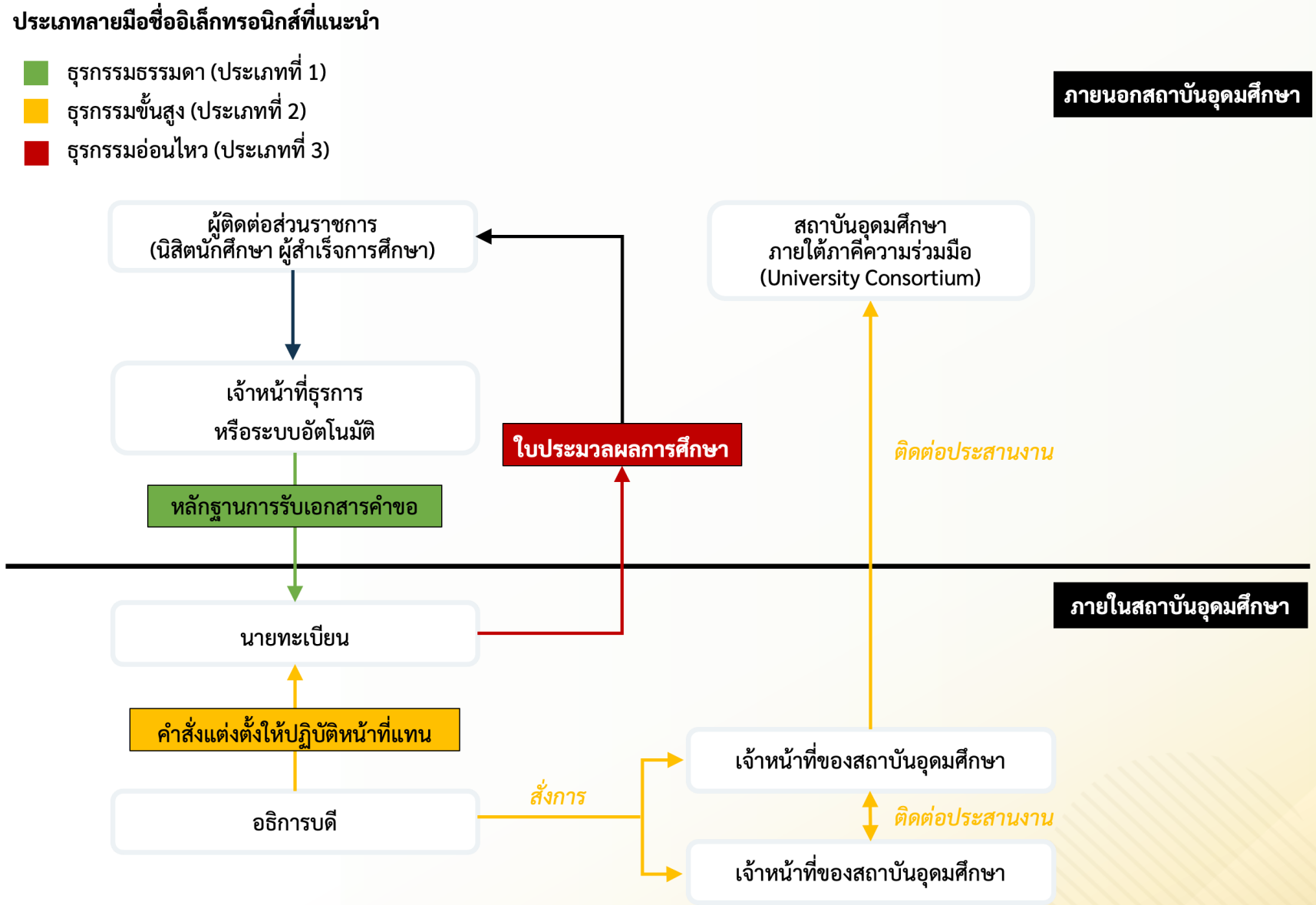
ประเภทลายมือชื่ออิเล็กทรอนิกส์ที่แนะนำ

- ธุรกรรมขั้นสูง (ประเภทที่ 2)
- ธุรกรรมอ่อนไหว (ประเภทที่ 3)

ลักษณะการลงนาม

- ลงนามบุคคลเดียว
- ลงนามหลายบุคคล

แผนภาพตัวอย่างการเลือกใช้ลายมือชื่ออิเล็กทรอนิกส์สำหรับเอกสารของสถาบันการศึกษา



Q & A

THANK YOU