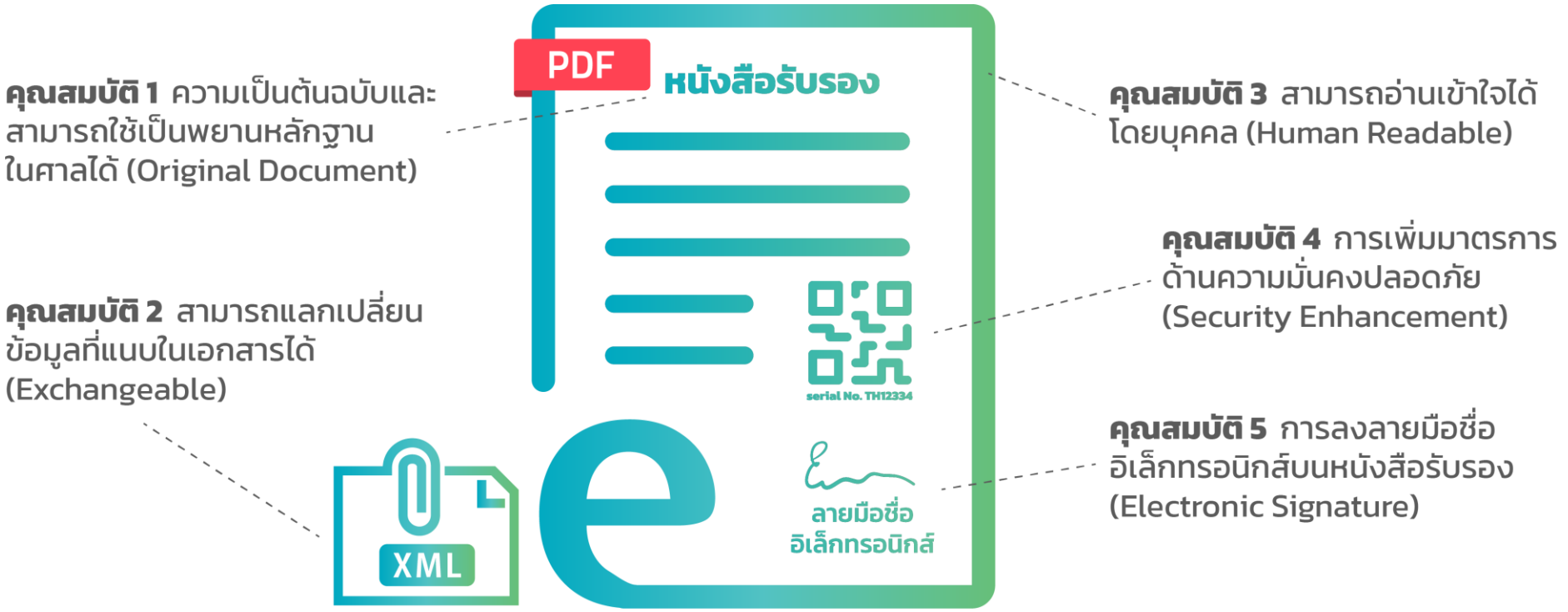
ETDA สพธอ www.etda.or.th

ประชุมเชิงปฏิบัติการ โครงการ Digital Transcript

Technology PKI and e-Timestamp

การสร้างเอกสารอิเล็กทรอนิกส์ที่มีความน่าเชื่อถือ



Source: https://www.etda.or.th/th/Our-Service/Digital-Trusted-services-Infrastructure/TEDA/Speed-up-e-Licensing.aspx

การลงลายมือชื่ออิเล็กทรอนิกส์

ประเภทของลายมือชื่ออิเล็กทรอนิกส์	ตัวอย่างของรูปแบบของลายมือชื่ออิเล็กทรอนิกส์	องค์ประกอบของลายมือชื่ออิเล็กทรอนิกส์		
		การพิสูจน์และยืนยันตัวตน	เจตนาในการลงลายมือชื่อ	การรักษาความครบถ้วนของข้อมูล
ประเภทที่ 1 ลายมือชื่ออิเล็กทรอนิกส์ทั่วไป	– การพิมพ์ชื่อไว้ท้ายเนื้อหาของอีเมล – การสแกนภาพของลายมือชื่อที่เขียนด้วยมือและแนบไปกับเอกสาร – การใช้สไตลัส (stylus) เขียนลายมือชื่อด้วยมือลงบนหน้าจอและบันทึกไว้ – การใช้ระบบงานอัตโนมัติที่มีการยืนยันตัวผู้ใช้งานมาประกอบกับรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ประเภทที่ 1	มีการพิสูจน์และยืนยันตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรม	มีกระบวนการหรือหลักฐานที่แสดงได้ว่าบุคคลได้ยอมรับการแสดงเจตนาที่ตนได้ลงลายมือชื่ออย่างชัดเจน	มีหลักฐานหรือใช้บุคคลที่สามที่เชื่อถือได้ เพื่อแสดงว่าไม่มีการเปลี่ยนแปลงความหมายของข้อความที่ลงลายมือชื่อ และรับรองความครบถ้วนของข้อมูล
ประเภทที่ 2 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้	– ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI)	– มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือมีการพิสูจน์ตัวตนที่ระดับ IAL2 ขึ้นไป – มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป ซึ่งเป็นการยืนยันตัวตนแบบหลายปัจจัยและมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลในการลงลายมือชื่อต่อข้อความ
ประเภทที่ 3 ลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ ซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง	– ลายมือชื่อดิจิทัลที่อาศัยโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) และใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรอง	– มีการพิสูจน์ตัวตนที่น่าเชื่อถือและเหมาะสมกับความเสี่ยงของธุรกรรมหรือมีการพิสูจน์ตัวตนที่ระดับ IAL2 ขึ้นไป – มีการยืนยันตัวตนที่ระดับ AAL2 ขึ้นไป ซึ่งเป็นการยืนยันตัวตนแบบหลายปัจจัยและมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในการลงลายมือชื่อต่อข้อความที่ตนแสดงเจตนา	ใช้ลายมือชื่อดิจิทัลซึ่งใช้ใบรับรองที่ออกโดยผู้ให้บริการออกใบรับรองในการลงลายมือชื่อต่อข้อความ

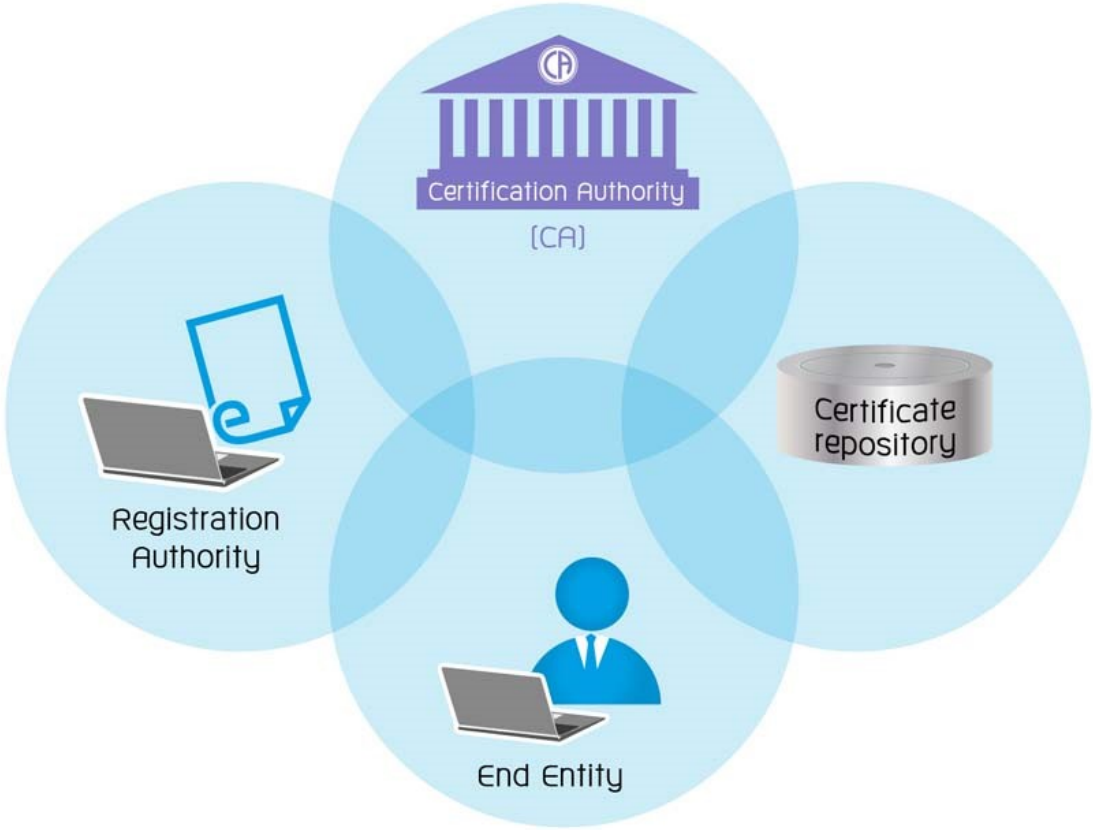
Source: https://standard.etda.or.th/wp-content/uploads/2020/06/20200529-ER-E-Signature-Guideline-V08-36F.pdf

PKI คืออะไร

Public Key Infrastructure (PKI)

เป็นเทคโนโลยีที่ใช้ในการรักษาความปลอดภัยของข้อมูลในปัจจุบัน ซึ่งเทคโนโลยีดังกล่าวประกอบด้วยกุญแจ 2 ดอก คือ **กุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key)** โดยที่บุคคลหรือเอ็นทิตี้หนึ่งๆ จะมีกุญแจทั้ง 2 ดอกดังกล่าว แต่เนื่องด้วยตัวของเทคโนโลยีเพียงอย่างเดียวนั้นไม่สามารถระบุได้ว่าบุคคลนั้นเป็นเจ้าของกุญแจซึ่งอ้างถึงจริงหรือไม่ ดังนั้น โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) จึงเป็นโครงสร้างที่ก่อให้เกิดความน่าเชื่อถือในการระบุถึงความเป็นเจ้าของกุญแจสาธารณะว่าเป็นของบุคคลนั้นจริง

โดยการสร้างความน่าเชื่อถือของกุญแจสาธารณะจึงจำเป็นที่จะต้องมีหน่วยงานที่มีความน่าเชื่อถือ เพื่อทำหน้าที่ในการรับรองกุญแจสาธารณะว่าเป็นของบุคคลซึ่งอ้างถึงจริง ซึ่งหน่วยงานดังกล่าวก็คือ **ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority : CA)**

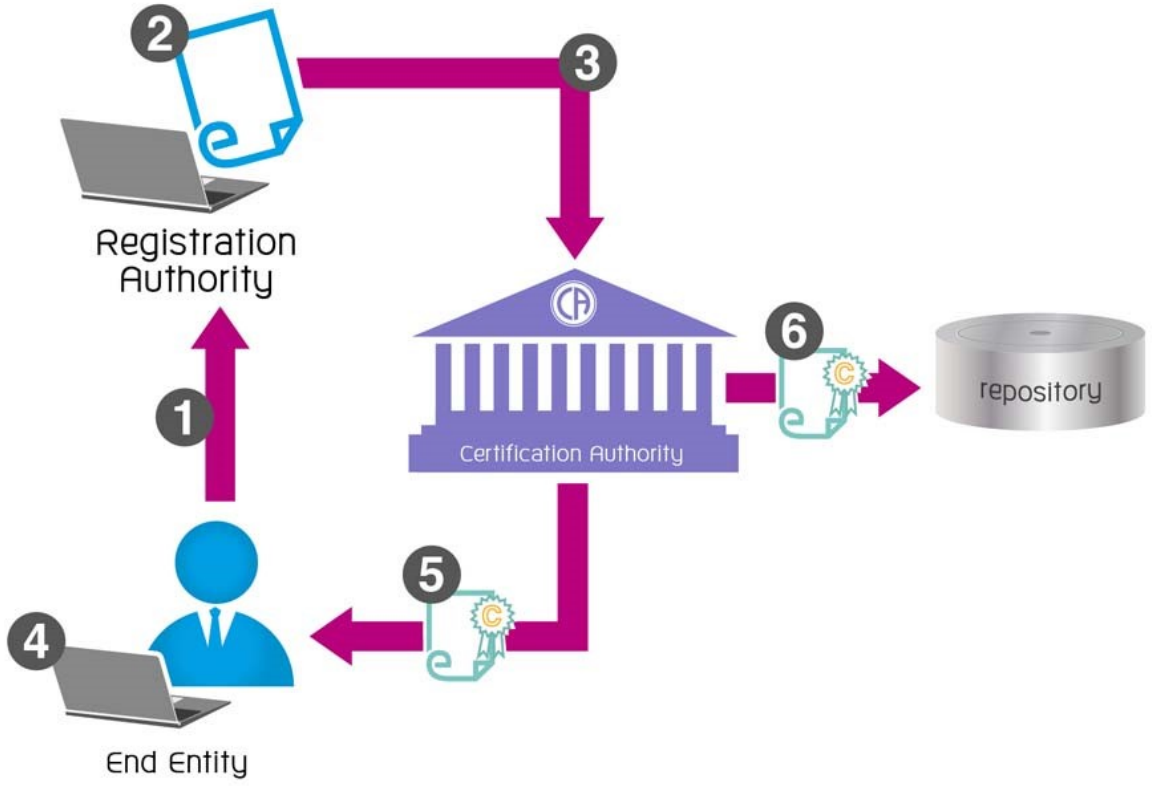


องค์ประกอบของ Public Key Infrastructure

Source: https://www.nrca.go.th/content/02-2.html

CA รับรองความน่าเชื่อถือผ่านใบรับรองอิเล็กทรอนิกส์ (Certificate)

1. ผู้ขอใช้บริการแจ้งความจำนงในการขอใช้ใบรับรองอิเล็กทรอนิกส์ไปยังเจ้าหน้าที่รับลงทะเบียน
2. เจ้าหน้าที่รับลงทะเบียนตรวจสอบและยืนยันความถูกต้องของข้อมูลที่ผู้ขอใช้บริการได้ให้ไว้ตามแบบคำขอใบรับรองอิเล็กทรอนิกส์
3. เจ้าหน้าที่รับลงทะเบียนส่งคำขอใช้ใบรับรองอิเล็กทรอนิกส์ของผู้ขอใช้บริการไปยังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
4. ผู้ขอใช้บริการทำการสร้างคู่กุญแจส่วนตัวและกุญแจสาธารณะ โดยกุญแจสาธารณะที่สร้างขึ้นนั้นจะถูกส่งไปยังผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์
5. ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ทำการรับรองข้อมูลและกุญแจสาธารณะของผู้ขอใช้บริการ และส่งผลที่ได้จากการรับรองกลับไปยังผู้ขอใช้บริการในรูปแบบของใบรับรองอิเล็กทรอนิกส์
6. ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์นำใบรับรองอิเล็กทรอนิกส์ที่ออกใหม่เผยแพร่ในที่บันทึกข้อมูล เพื่อให้บุคคลอื่นสามารถสืบค้นใบรับรองอิเล็กทรอนิกส์ของผู้ขอใช้บริการได้

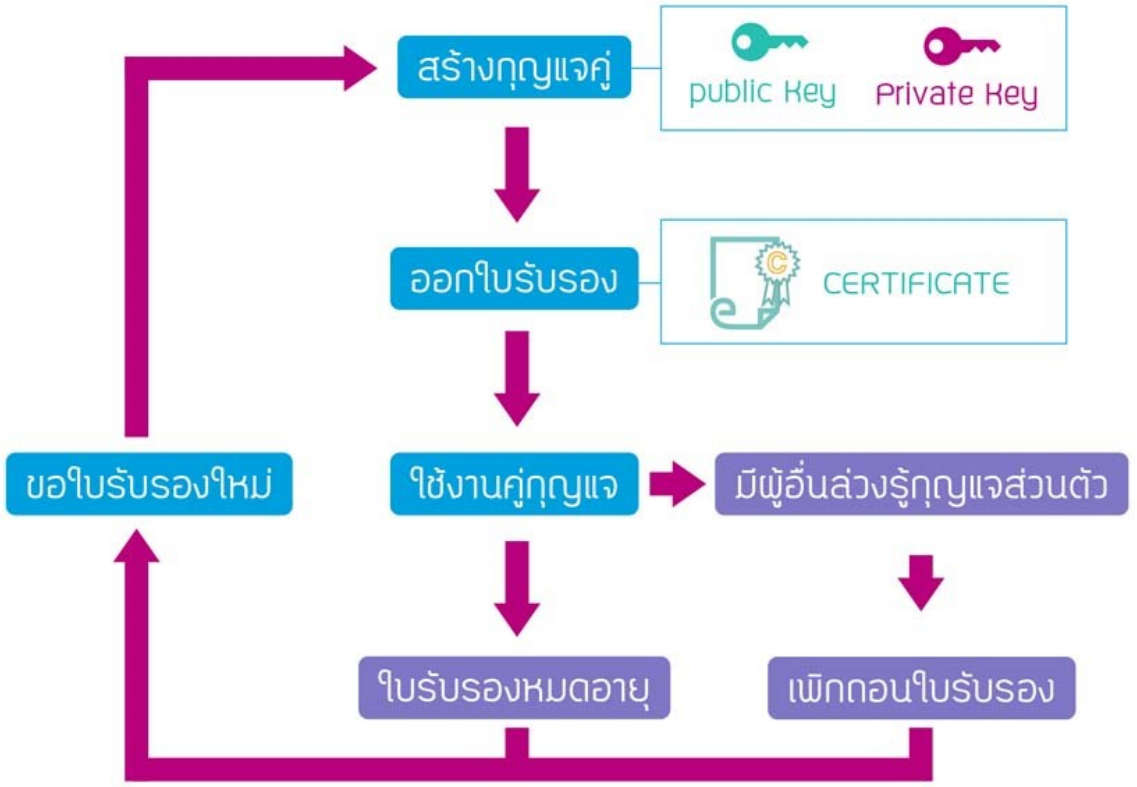


ขั้นตอนการขอใช้ใบรับรองอิเล็กทรอนิกส์

Source: https://www.nrca.go.th/content/02-2.html

วงจรชีวิตของใบรับรองอิเล็กทรอนิกส์

1. ผู้ขอใช้บริการสร้างกุญแจคู่ ซึ่งประกอบไปด้วยกุญแจส่วนตัวและกุญแจสาธารณะ
2. ผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์จะทำการรับรองกุญแจสาธารณะและข้อมูลของเจ้าของกุญแจสาธารณะ โดยออก**ใบรับรองอิเล็กทรอนิกส์ตามมาตรฐาน X.509**
3. การใช้งานใบรับรองอิเล็กทรอนิกส์และกุญแจส่วนตัว ในกรณีที่ไม่ต้องการใช้ใบรับรองอิเล็กทรอนิกส์ เช่นการรั่วของ Private key หรือมีการเปลี่ยนแปลงตำแหน่งหรือรายละเอียดในใบรับรองอิเล็กทรอนิกส์ ผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์จะต้องแจ้ง CA เพื่อทำการขอเพิกถอนใบรับรองอิเล็กทรอนิกส์ โดย**ใบรับรองอิเล็กทรอนิกส์ที่ถูกเพิกถอนนั้นจะปรากฏอยู่ในรายการเพิกถอนใบรับรอง (Certificate Revocation List : CRL)** หลังจากนั้นผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์จะต้องทำการขอใบรับรองอิเล็กทรอนิกส์ใหม่
4. เมื่อใบรับรองอิเล็กทรอนิกส์หมดอายุ ผู้ที่เป็นเจ้าของใบรับรองอิเล็กทรอนิกส์ดังกล่าวจะต้องทำการขอใบรับรองอิเล็กทรอนิกส์ใหม่

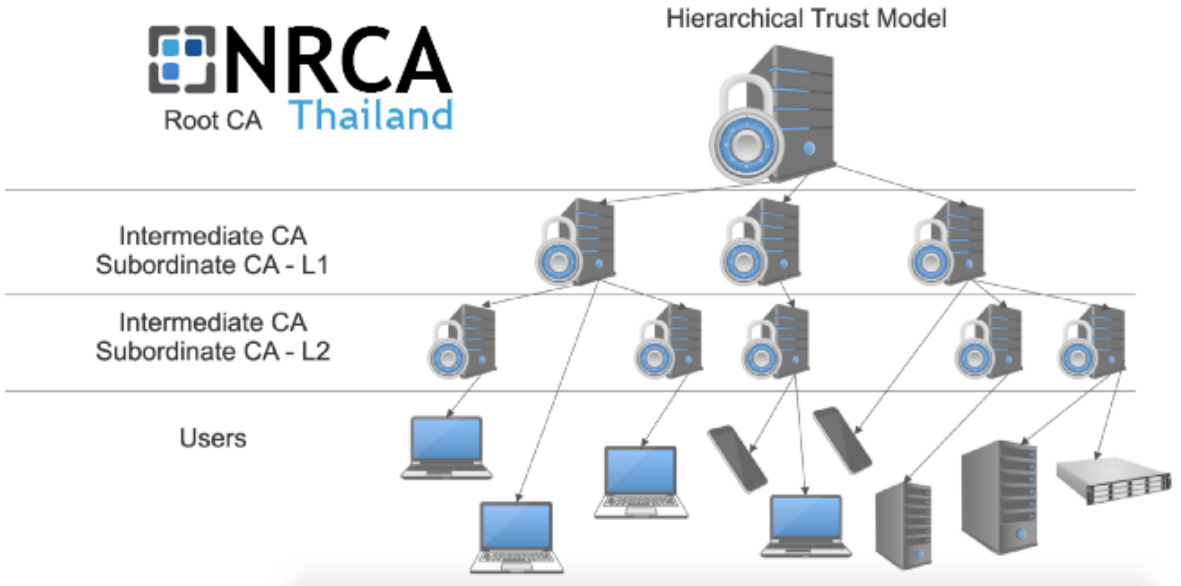


วงจรชีวิตของใบรับรองอิเล็กทรอนิกส์

Source: https://www.nrca.go.th/content/02-2.html

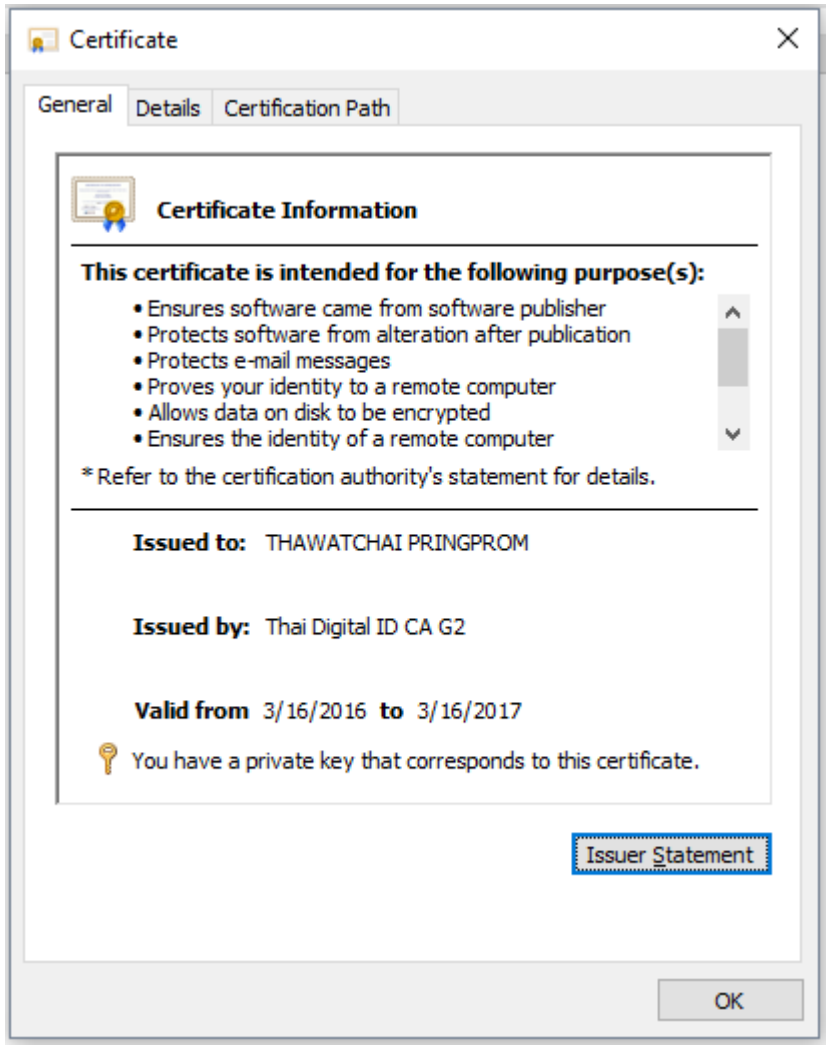
รูปแบบของ PKI Trust Model

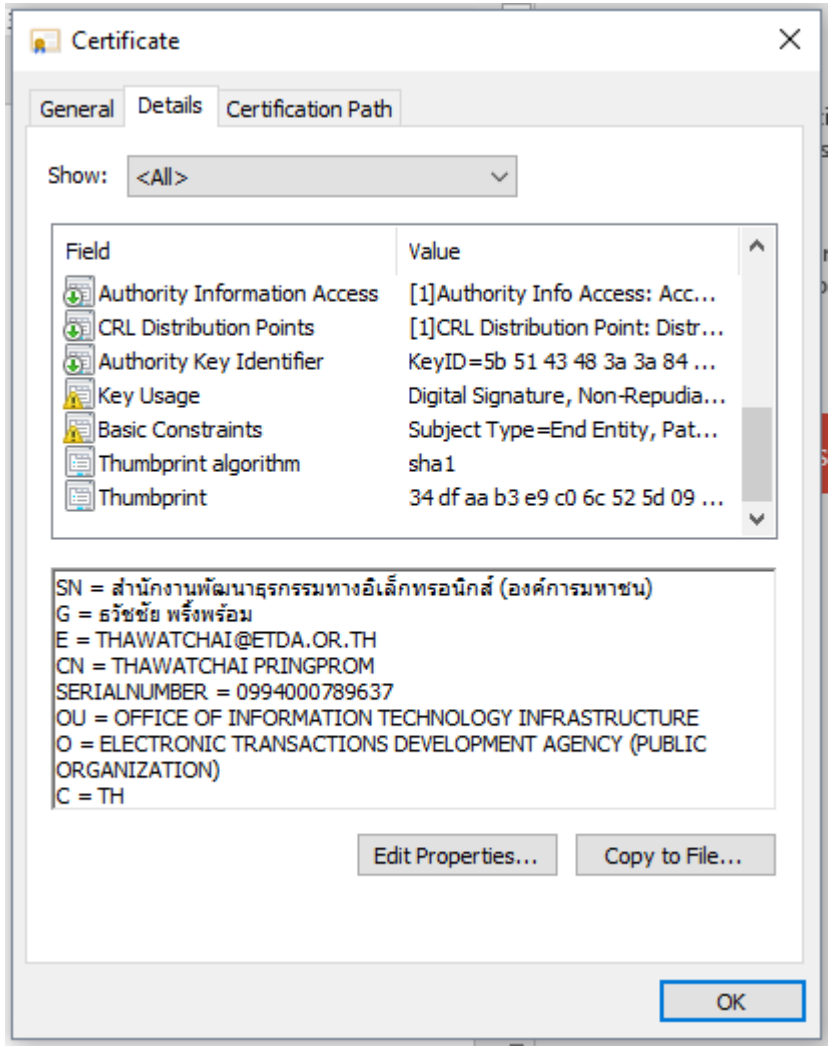
- รูปแบบการสร้างความเชื่อในการใช้งานผ่าน PKI ที่เป็นที่นิยมคือการสร้างสายความเชื่อ (Chain of trust) ในรูปแบบลำดับชั้น (Hierarchy trust model)
- โดยจะมี CA รายหนึ่งทำหน้าที่รับรองใบรับรองอิเล็กทรอนิกส์ของ CA รายอื่นๆ และจะอยู่ในลำดับชั้นสูงสุดที่นิยมเรียกกันว่า Root CA
- คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ผู้ซึ่งดูแลด้านการวางนโยบายเกี่ยวกับธุรกรรมอิเล็กทรอนิกส์ของประเทศ ได้เห็นชอบให้มีการใช้ระบบ Trust Model ในรูปแบบ Root CA ขึ้นในประเทศไทย
- National Root CA (NRCA) จะทำหน้าที่เป็นศูนย์กลางในการสร้างความเชื่อมั่นของการใช้งานระบบ PKI เพื่อให้เกิดการทำงานร่วมกัน (Interoperability) ระหว่าง CA ในประเทศ รวมไปถึงเป็นศูนย์กลางในการติดต่อกับ CA ต่างประเทศ

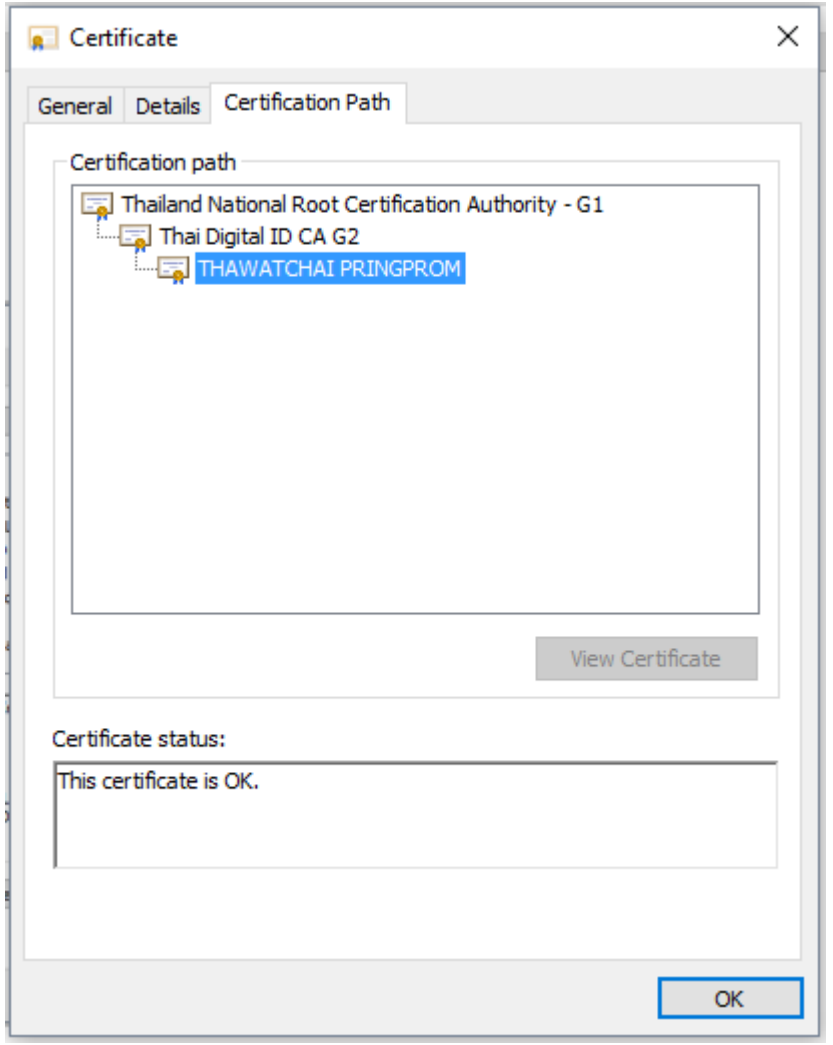


รูปแบบความเชื่อแบบลำดับชั้น

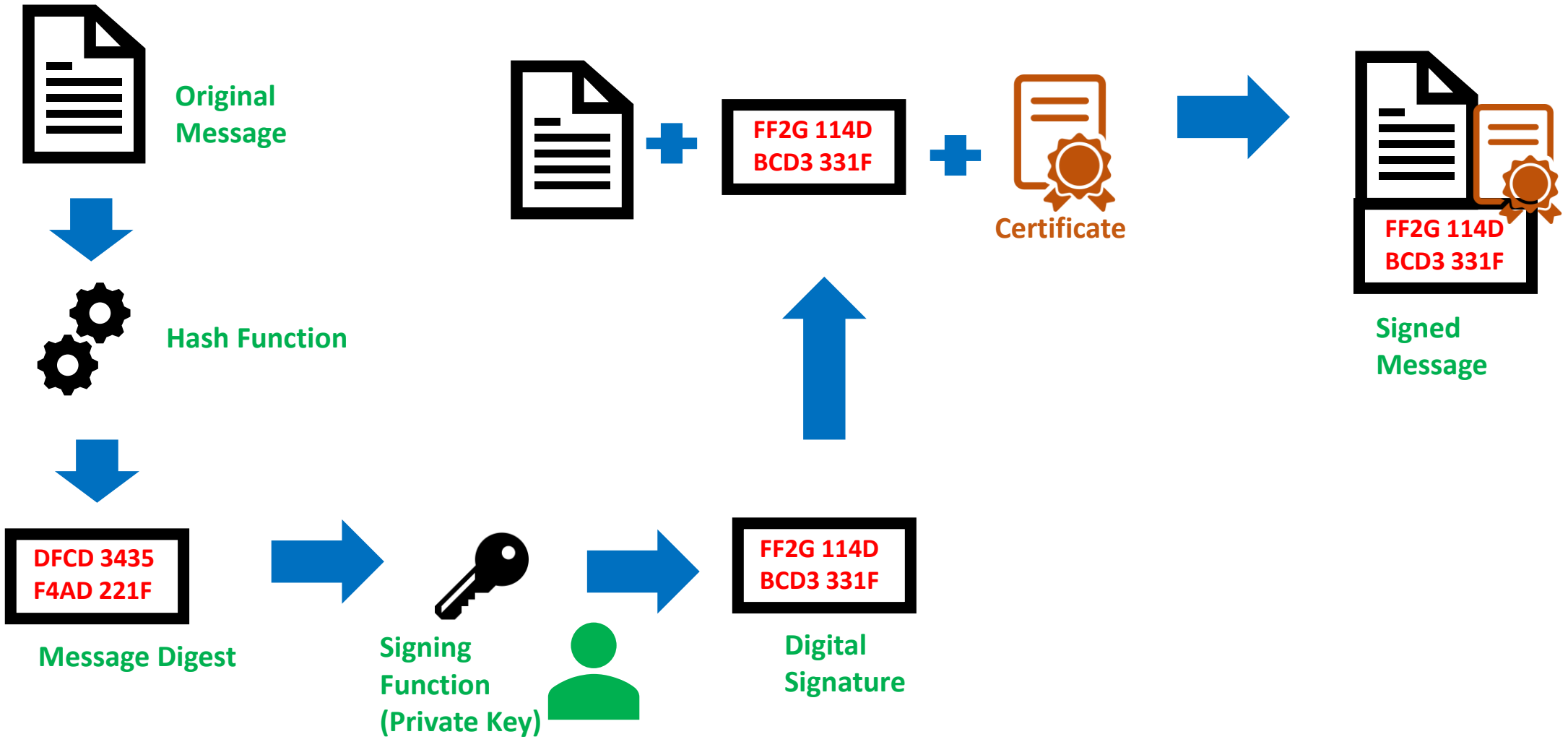
ตัวอย่างใบรับรองอิเล็กทรอนิกส์





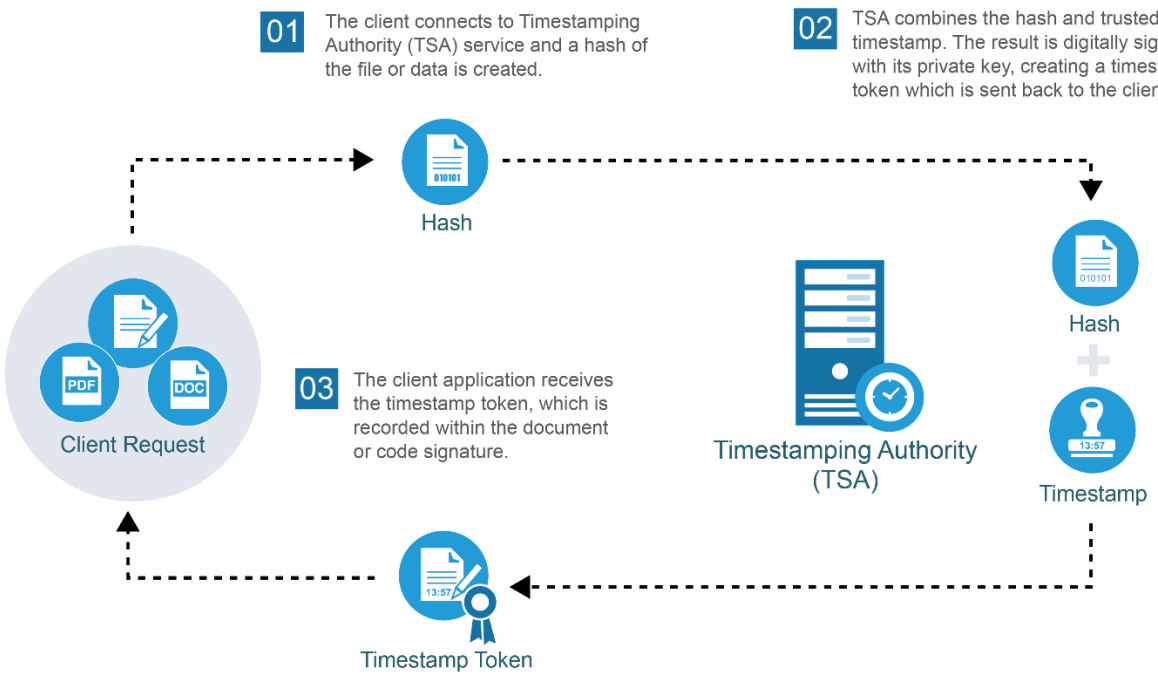


การใช้ใบรับรองอิเล็กทรอนิกส์ในการลงลายมือชื่อ



e-Timestamp ทำให้เอกสารอิเล็กทรอนิกส์มีความน่าเชื่อถือได้อย่างไร

- การให้บริการประทับรับรองเวลา (e-Timestamp) เป็นการเพิ่มความเชื่อมั่นและรับรองการมีอยู่ของเอกสารอิเล็กทรอนิกส์ ณ เวลานั้น โดยการอ้างเวลาของ Trust service ผ่านกลไกตาม**มาตรฐานสากล RFC 3161**
- เนื่องจากเวลามาจากเวลาของสาผู้รับรอง (Time Stamp Authority หรือ TSA) การประทับเวลาจะสร้างความมั่นใจให้กับผู้ใช้เอกสารว่า**เป็นเอกสารจริงที่มีตัวตน ณ เวลาประทับ และมารถตรวจสอบความครบถ้วนของเอกสาร (Integrity)**
- การประทับเวลาเป็น**องค์ประกอบที่สำคัญของการตรวจสอบความถูกต้องในระยะยาว (long-term validation หรือ LTV)** โดยเฉพาะกรณีที่ต้องการตรวจสอบความถูกต้องของเอกสารในกรณีที่ใบรับรองอิเล็กทรอนิกส์ของผู้ลงนามหมดอายุแล้ว
- e-Timestamp เป็นรูปแบบการใช้เทคโนโลยี PKI โดยเป็นการใช้ใบรับรองอิเล็กทรอนิกส์ของ TSA ในการรับรองเอกสาร



กระบวนการทำงานของ e-Timestamp

THANK YOU