คู่มืออบรม Active Dirrectory (AD) และ Certificate Authority (CA)

สำหรับผู้ใช้งาน

สำนักงาน ป.ป.ท

17 กันยายน 2563

เวลา 9:00 น.-16:00 น.

สารบัญ

1. Active Directory

Active Directory คืออะไร???

AD ให้บริการจัดเก็บ directory ของ server(เครือข่าย) เสมือนแหล่งรวบรวมรายชื่อ User(ผู้ใช้) รายชื่อทรัพยากรใน ไว้ด้วยกัน บัญชีผู้ใช้ไปยังรายชื่อเครื่องคอมพิวเตอร์ต่างๆ ที่ทำงานบนเครือข่าย(server) รายชื่อที่ shared folder บน file sever โดยที่ AD จะมีฐานข้อมูลสำหรับจัดการ Directory บน Server

ประโยชน์ของ Active Directory

ถ้าองค์กรที่มี User จำนวนมาก ๆ สามารถนำ Active Directory มาใช้งาน จะช่วยลดภาระค่าใช้จ่ายในการบริหารจัดการทรัพยากรของ User อีกทั้งยังเพิ่มความปลอดภัยให้กับระบบโดยรวมโดยที่ไม่ต้องซื้อเครื่องมือเพิ่มเติม นอกจากจะช่วยจัดการทรัพยากรในระบบแล้ว Active Directory ทำหน้าที่จัดเก็บข้อมูลเกี่ยวกับ object ต่างๆ เช่น ผู้ใช้ (User), กลุ่ม (Group) คอมพิวเตอร์ (Computer) หรือ นโยบายรักษาความปลอดภัย (Security Policy) เป็นต้น

Active directory กับความสำคัญต่อองค์กร

Active Directory ถือได้ว่าเป็นหัวใจในการบริหารจัดการทรัพยากรในเน็ตเวิร์กขององค์กรหลายๆ องค์กรในปัจจุบัน เนื่องจากมันทำหน้าที่เก็บข้อมูลของทรัพยากรต่างๆ ช่วยให้ง่ายต่อการค้นหา จัดการและบริหาร เช่น ข้อมูลของเครื่องคอมพิวเตอร์ในระบบ Printer, Server แชร์โฟลเดอร์ รายชื่อของ UserและPassword รวมไปถึงสิทธิ์ในการใช้ทรัพยากรในองค์กรและคุณสมบัติของผู้ใช้งาน การบริหารจัดการทั้งหมดสามารถทำได้อย่างสะดวกโดยไม่จำเป็นต้องเดินไปเซตที่หน้าเครื่องคอมพิวเตอร์ของผู้ใช้งานทีละเครื่อง

ทำไมต้องมี ระบบActive Directory

เนื่องด้วยพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2)

<u>มาตรา ๒๖</u>

ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

**ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์
คือ ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัท หรือสถาบันการศึกษา

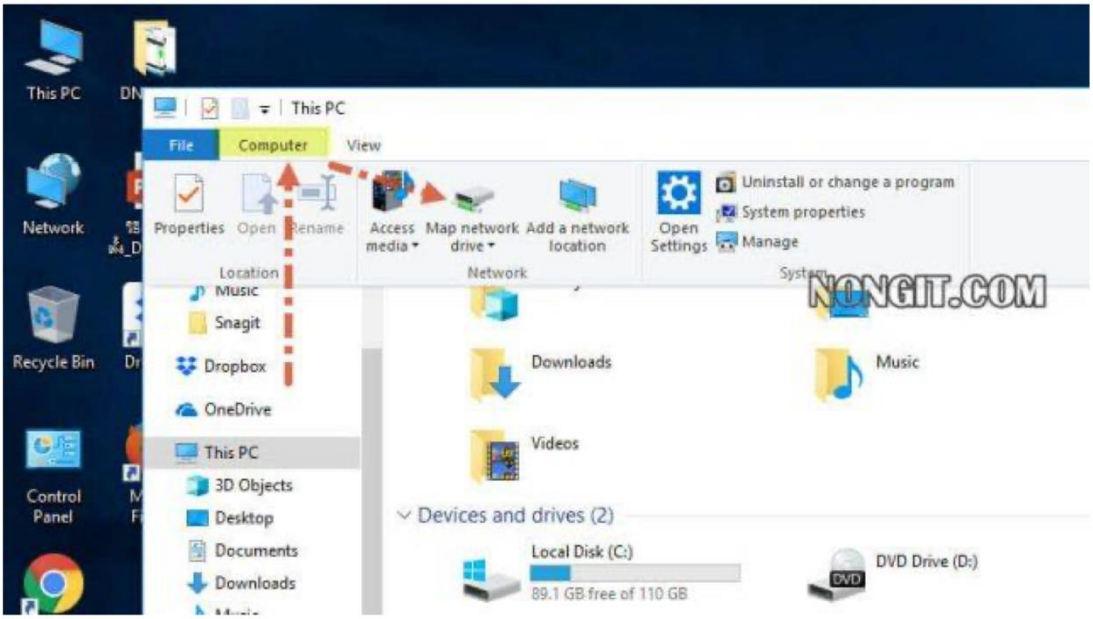
*ที่มา : คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550 โดย ไพบูลย์ อมรภิญโญเกียรติ
ในภาคผนวก ก. ประเภท ข. ข้อที่3

2. วิธีการ Map Drive สำหรับ File Sharing

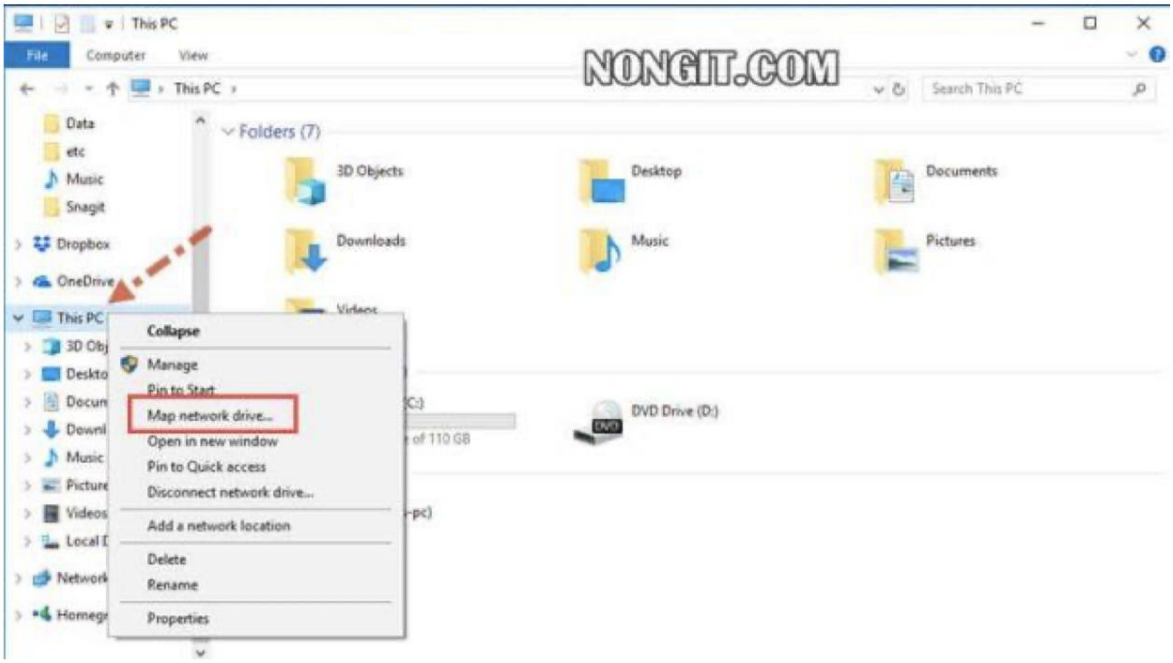
วิธี Map Drive ใน Windows 10

ตัวอย่างนี้จะเป็นขั้นตอนที่ทำใน Windows 10 แต่จะมีการอ้างอิงบางขั้นตอนที่เหมือน ๆ กัน โดยจะมีข้อมูลบอกสำหรับ Windows 8.1 และ Windows 7 ไว้ด้วย

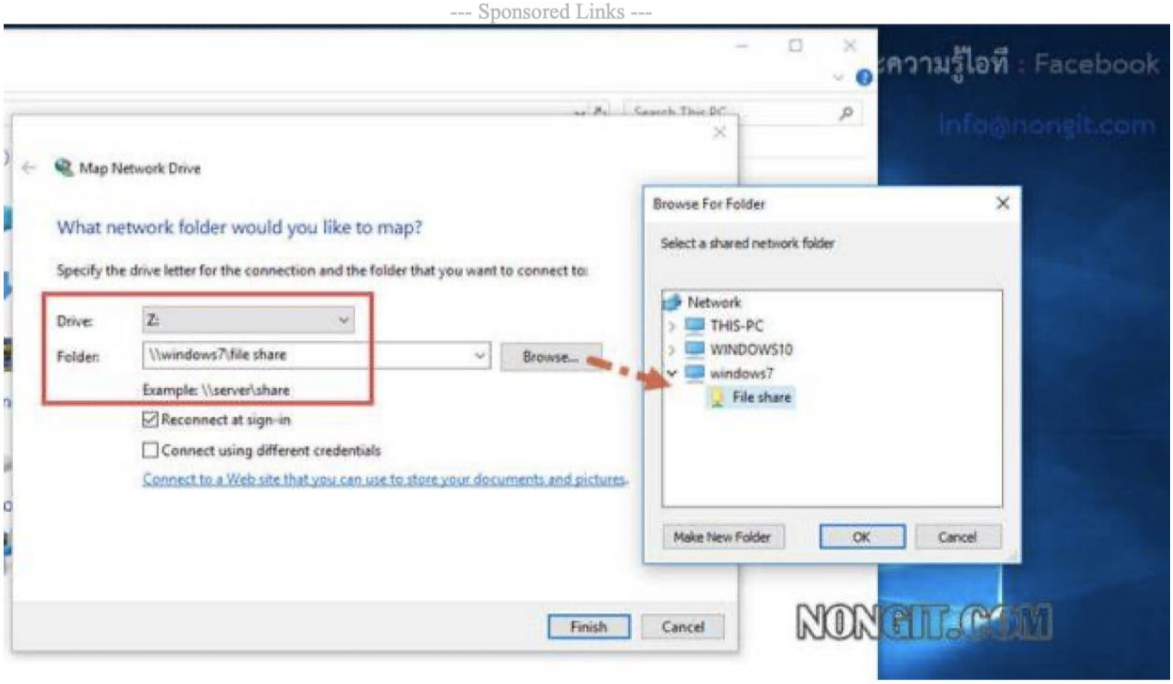
1. ที่หน้า Desktop ให้เปิด This PC จากนั้นที่หน้าต่างของ This PC ให้คลิกแถบ **Computer** แล้วให้คลิกเลือก **Map network drive**



2. และยังสามารถคลิกขวาที่ This PC แล้วเลือก **Map network drive** ได้อีกเช่นกัน (ปล. ขั้นตอนนี้จะใช้ได้ใน Windows 8.1 และ Windows 7 ด้วย)



3. จากนั้นจะแสดงหน้าต่าง "Map network drive" เลือก Drive: ได้ตามต้องการ และที่ช่อง Folder: ให้ทำการใส่ข้อมูลของเครื่องคอมฯหรือเซิฟเวอร์ที่แชร์ไฟล์ไว้แล้ว
    - กรณีที่เราทราบชื่อ Folder ก็ให้ระบุชื่อของ Folder นั้นไปด้วย ยกตัวอย่างเป็น "\\server name\folder หรือ "\\computer name\folder" แล้วคลิกปุ่ม **Finish**
    - และหากไม่ทราบชื่อหรือจำชื่อของ Folder ไม่ได้ ก็ให้ใส่เพียงชื่อเครื่อง ตัวอย่าง "\\Server name" หรือ "\\Computer name" แล้วคลิกปุ่ม **Browse…** แล้วเลือก Folder ที่ต้องการ ตามด้วยคลิก **Finish**

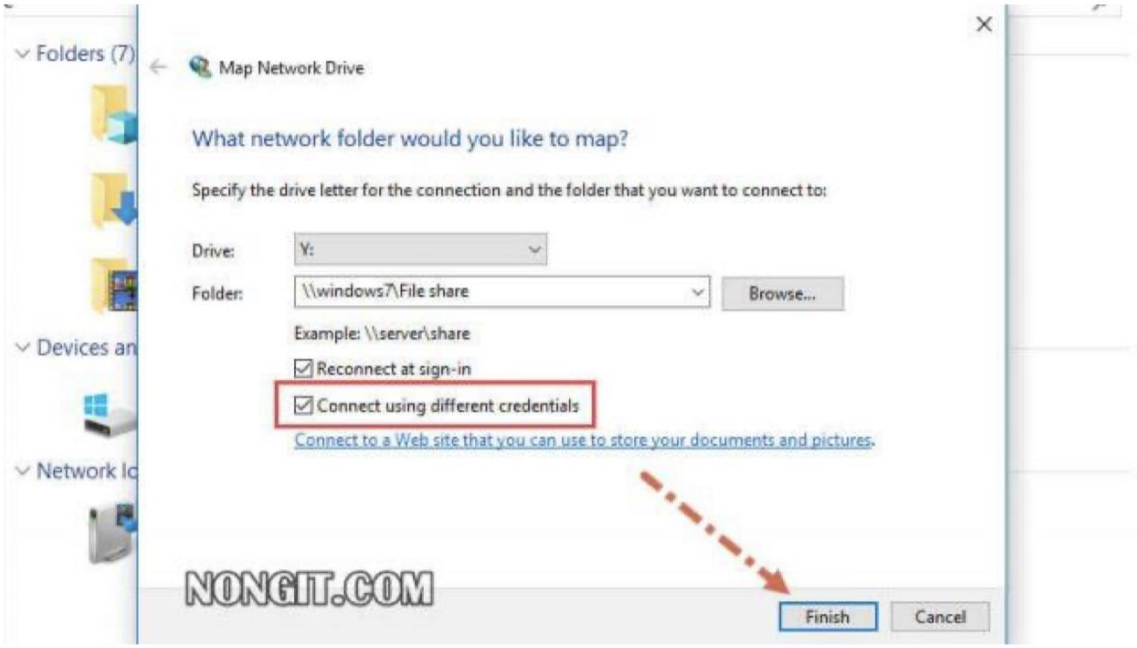


4. หลังจากนั้นไดร์ของ File share ก็จะแสดงในหน้า This PC แล้วครับ

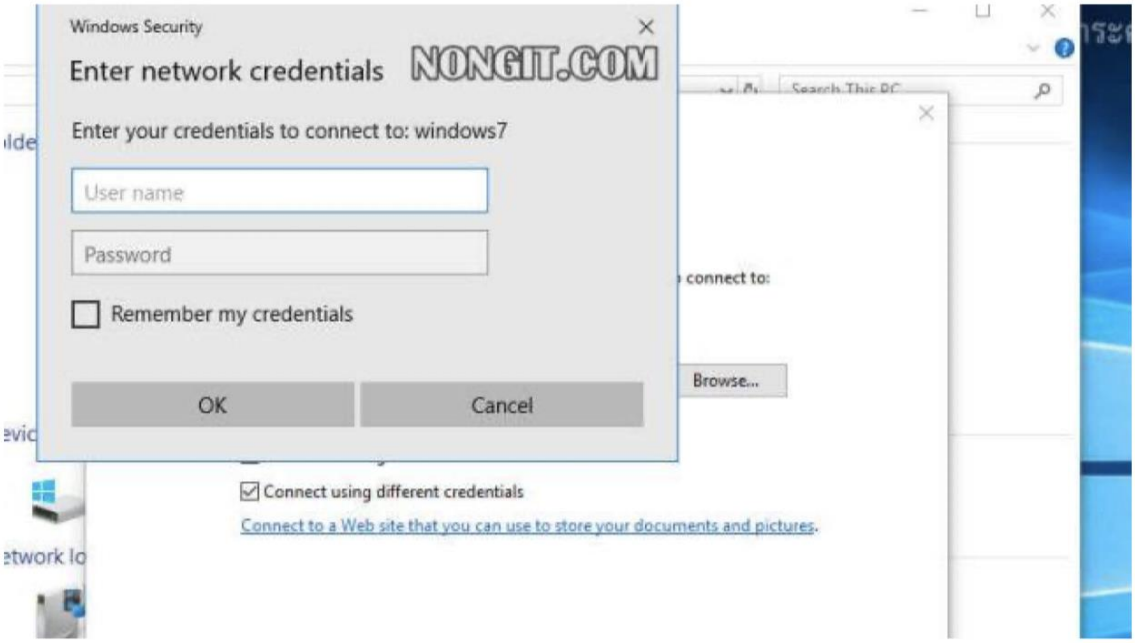
วิธี Map Drive กรณีที่มีการกำหนด User และ Password

โดยการกำหนดสำหรับการแชร์ไฟล์โดยกำหนดสิทธิ์การเข้าถึงข้อมูลไว้ นั้นคือตั้ง User และ Password ไว้ ซึ่งก่อนที่จะเข้าใช้ Folder ที่เปิดแชร์ไว้ได้นั้นก็ต้องมี user และ รหัส

5. โดยขั้นตอนนั้นก็ให้ทำเหมือนข้อ 1 ถึง 3 แต่ที่ข้อ 3 นั้นให้เลือกที่ช่อง (/) **Connect using different credentials**ด้วย แล้วก็คลิกปุ่ม **Finish**



6. จะแสดงหน้าต่างให้**ใส่ Username และ Password** ก็ให้ใส่ข้อมูลให้เรียบร้อย เมื่อเสร็จแล้วก็คลิก **Ok** เพียงเท่านี้ Map network drive ก็จะเพิ่มลงในส่วนของหน้า This PC หรือ Computer



ต่อไปนี้หากต้องการเข้าใช้งานข้อมูลผ่านการแชร์ไฟล์ก็ไม่ต้องไปค้นหา Server ก่อนอีกแล้ว เพราะเราสามารถเปิด This PC แล้วก็เข้าไดร์ Z: หรือ X: ตามที่ได้กำหนด Map network drive ไว้ ง่ายๆแสนง่าย

3. Certificate Authority (CA)

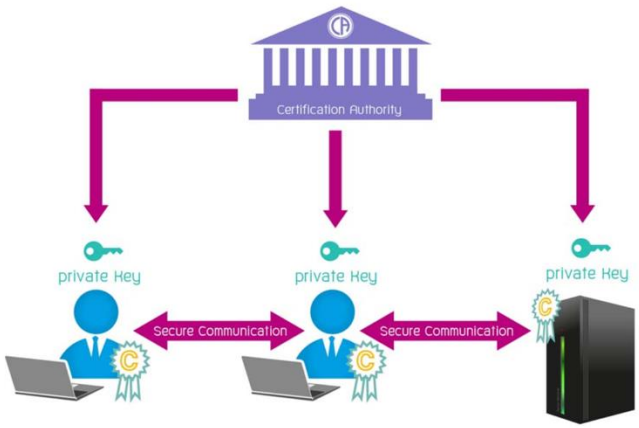
Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) คือชุดของข้อกำหนดที่อนุญาต (เหนือสิ่งอื่นใด) ในการสร้างลายเซ็นดิจิทัล ผ่าน PKI ธุรกรรมลายเซ็นดิจิทัลแต่ละรายการจะมีคีย์คู่หนึ่ง ได้แก่ คีย์ส่วนตัวและคีย์สาธารณะ คีย์ส่วนตัวตามชื่อจะไม่ถูกแชร์และจะใช้โดยผู้ลงนามในการเซ็นชื่อในเอกสารแบบอิเล็กทรอนิกส์เท่านั้น คีย์สาธารณะสามารถใช้ได้โดยเปิดเผยและใช้โดยผู้ที่ต้องการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ของผู้ลงนาม PKI บังคับใช้ข้อกำหนดเพิ่มเติมเช่น Certificate Authority (CA) ใบรับรองดิจิทัลสำหรับซอฟต์แวร์การลงทะเบียนของผู้ใช้ปลายทางและเครื่องมือในการจัดการต่ออายุและเพิกถอนคีย์และใบรับรอง

ส่วนประกอบของ Public Key Infrastructure (PKI)

Certificate Authority (CA)

หมายถึงองค์กรผู้ออกใบรับรอง ระบบลายเซ็นดิจิทัลต้องอาศัยคีย์สาธารณะ (Public Key) และส่วนตัว (Private Key) กุญแจเหล่านี้จะต้องได้รับการปกป้องเพื่อความปลอดภัยและเพื่อหลีกเลี่ยงการปลอมแปลงหรือการใช้งานที่เป็นอันตราย เมื่อส่งหรือลงนามในเอกสารต้องมั่นใจได้ว่าเอกสารและคีย์ถูกสร้างขึ้นอย่างปลอดภัยและใช้คีย์ที่ถูกต้อง Certificate Authority ซึ่งเป็นผู้ให้บริการด้านความน่าเชื่อถือประเภทหนึ่งเป็นองค์กรที่ได้รับการยอมรับและมีความน่าเชื่อถือในการรับรองความปลอดภัย และสามารถให้ใบรับรองดิจิทัล (Digital Certificate) ได้ รวมถึงจัดเก็บรวมทั้งมีระบบตรวจสอบยืนยันความถูกต้อง มีฐานข้อมูลใบรับรองที่ถูกยกเลิกไปให้สามารถสืบค้นและตรวจสอบได้

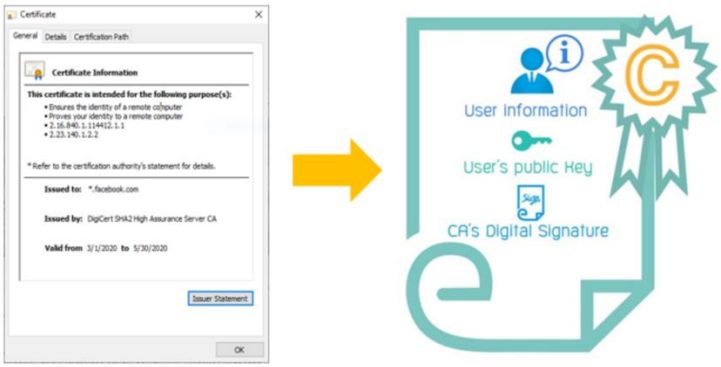


Digital Certificate

หมายถึงใบรับรองดิจิทัล เป็นเอกสารอิเล็กทรอนิกส์ที่ออกโดยองค์กรผู้ออกใบรับรอง (Certificate Authority หรือ CA) ประกอบด้วยคีย์สาธารณะสำหรับลายเซ็นดิจิทัลและระบุข้อมูลประจำตัวที่เกี่ยวข้องกับคีย์เช่นชื่อบุคคล ชื่อองค์กร เป็นใบรับรองใช้เพื่อยืนยันว่าคีย์สาธารณะเป็นขององค์กรที่ออกใบรับรอง CA ซึ่งทำหน้าที่เป็นผู้ค้ำประกันหรือรับรองความถูกต้องของบุคคลหรือองค์กร ใบรับรองดิจิทัลต้องออกโดยหน่วยงานที่เชื่อถือได้และใช้ได้ตามเวลาที่กำหนดเท่านั้น และจำเป็นต้องใช้เพื่อสร้างลายเซ็นดิจิทัล

Digital Certificate จะประกอบไปด้วยข้อมูลหลัก 3 ส่วน

- ข้อมูลของเจ้าของ Digital Certificate
- Public Key ของเจ้าของ Digital Certificate
- Digital Signature ของผู้ให้บริการออกใบรับรอง Digital Certificate



Digital Signature

หมายถึงลายเซ็นดิจิทัล เพื่อการลงนามเอกสารทั้งแบบออนไลน์และออฟไลน์ ประกอบด้วยลายมือชื่อที่ได้จากการนำเข้าภาพลายมือชื่อหรือสร้างลายมือชื่อขึ้นใหม่บนอุปกรณ์คอมพิวเตอร์ พร้อมทั้งทำการ sign แบบดิจิทัลด้วยใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ลงไปในเอกสาร ในการลงนามแบบออนไลน์จะมีอินเทอร์เฟซหรือหน้าจอสำหรับการส่งและลงนามเอกสารทางออนไลน์และทำงานร่วมกับผู้ออกใบรับรอง (CA) เพื่อมอบใบรับรองดิจิทัลที่เชื่อถือได้ และจะมีขั้นตอนการลงนาม การจัดเก็บ และส่งเอกสารเป็นระบบ ส่วนการลงนามแบบออฟไลน์ผู้ลงนามจะต้องมีซอฟต์แวร์ในการลงนามเอกสาร โดยตัวซอฟต์แวร์สามารถนำเข้าหรือสร้างใบรับรองดิจิทัลและสามารถตรวจสอบความถูกต้องของใบรับรองดิจิทัลได้

วัตถุประสงค์ในการลงนามด้วยลายเซ็นดิจิทัล

การลงนามด้วยลายเซ็นดิจิทัลมีวัตถุประสงค์เพื่อให้เอกสารที่ลงนามในระบบอิเล็กทรอนิกส์มีผลตามกฎหมาย โดยมีหลักวัตถุประสงค์หลัก ๆ ดังนี้

1) การยืนยันตัวบุคคล (Authentication)

สำหรับยืนยันตัวบุคคล โดยที่บุคคลที่ลงนามจะต้องมีข้อมูลระบุตัวตนอย่างชัดเจนในใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยองค์กรออกใบรับรอง (Certificate Authority) ที่เชื่อถือได้ (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 15,16)

2) ความครบถ้วนของข้อมูล (Data Integrity)

เพื่อยืนยันว่าเอกสารที่ส่งเป็นเอกสารที่ถูกต้อง ไม่มีการดัดแปลงแก้ไข หรือหากเอกสารถูกแก้ไขก็สามารถตรวจพบได้ และไม่ใช่เอกสารที่ส่งซ้ำ (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 17,18)

3) การห้ามปฏิเสธความรับผิด (Non-repudiation)

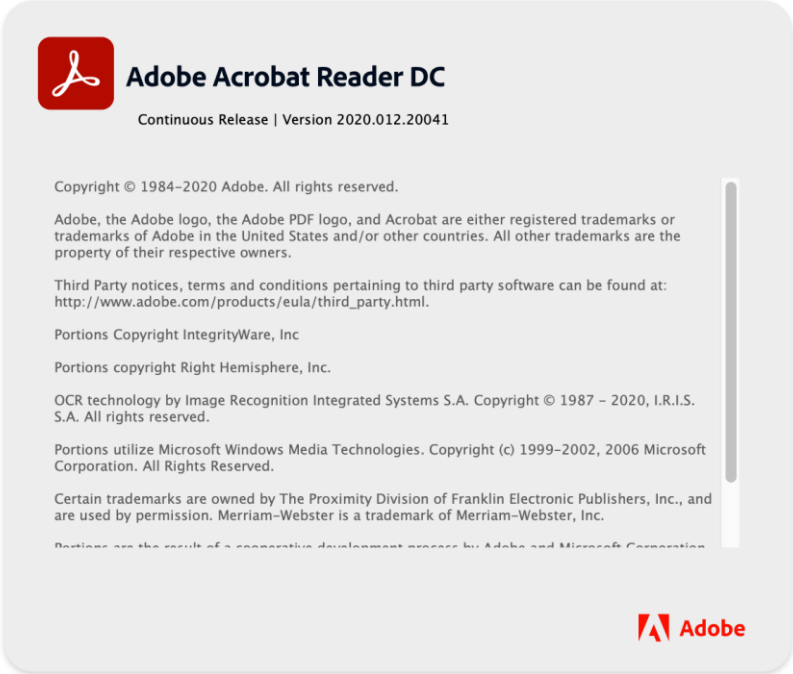
เป็นการป้องกันไม่ให้บุคคลผู้ส่งปฏิเสธว่าตนไม่ได้ส่งข้อมูลอิเล็กทรอนิกส์ โดยผู้ลงนามเอกสารโดยใช้ใบรับรองดิจิทัล (Digital Certificate) ที่ออกโดยองค์กรออกใบรับรอง (Certificate Authority) ที่เชื่อถือได้ จะไม่สามารถปฏิเสธความรับผิดชอบในเอกสารที่ตนลงนามได้ (พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา 19)

ขั้นตอนการลงนามในเอกสาร

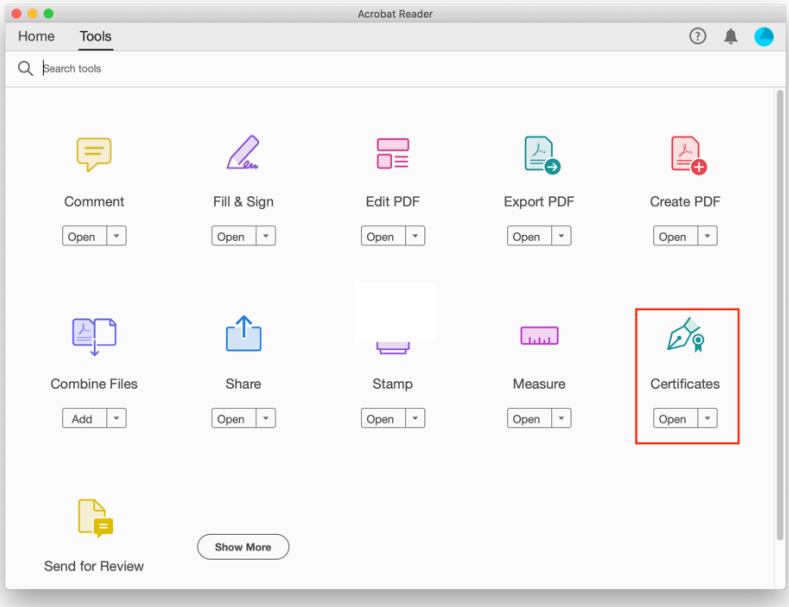
เมื่อได้ไฟล์ใบรับรองดิจิทัล (Digital Certificate) โดยปกติจะเป็นไฟล์แบบ pkcs12 (.p12) จะสามารถนำมาใช้ในการลงนามเอกสารได้

ขั้นตอนการลงนามแบบ Offline โดยเอกสาร PDF

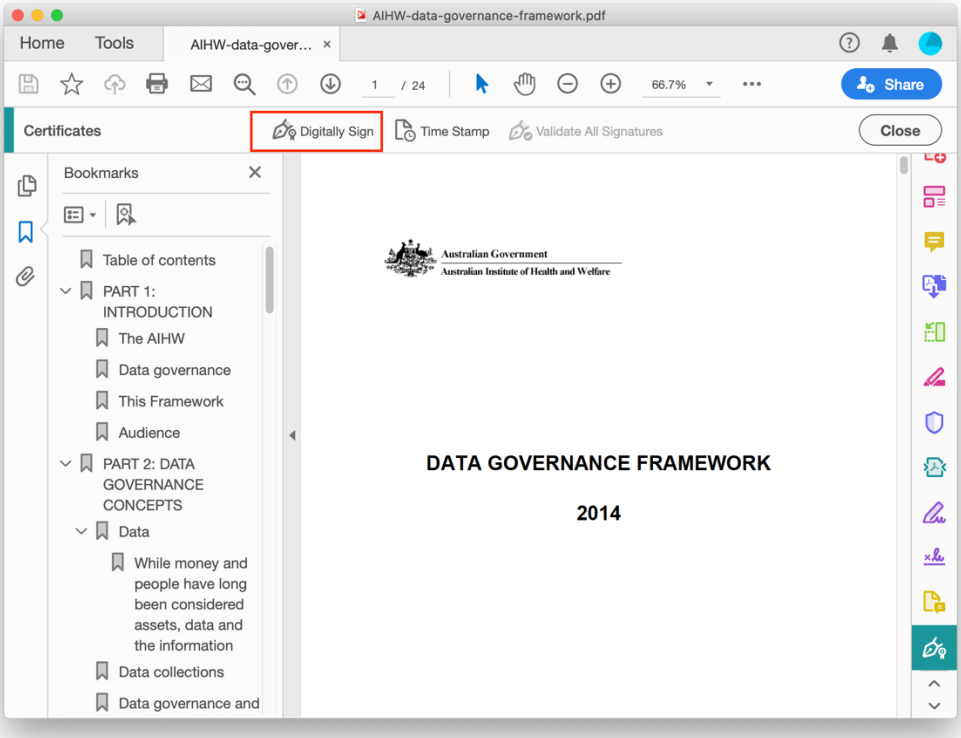
1. เรียกใช้ Adobe Acrobat Reader



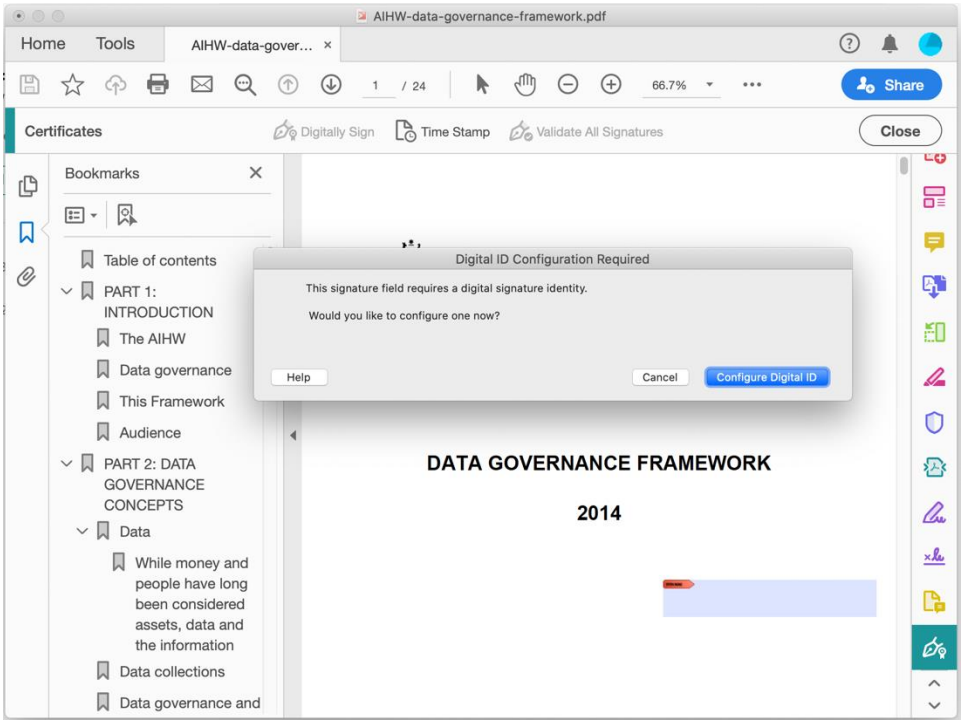
2. เลือกแท็บ Tools
3. คลิก Certificates



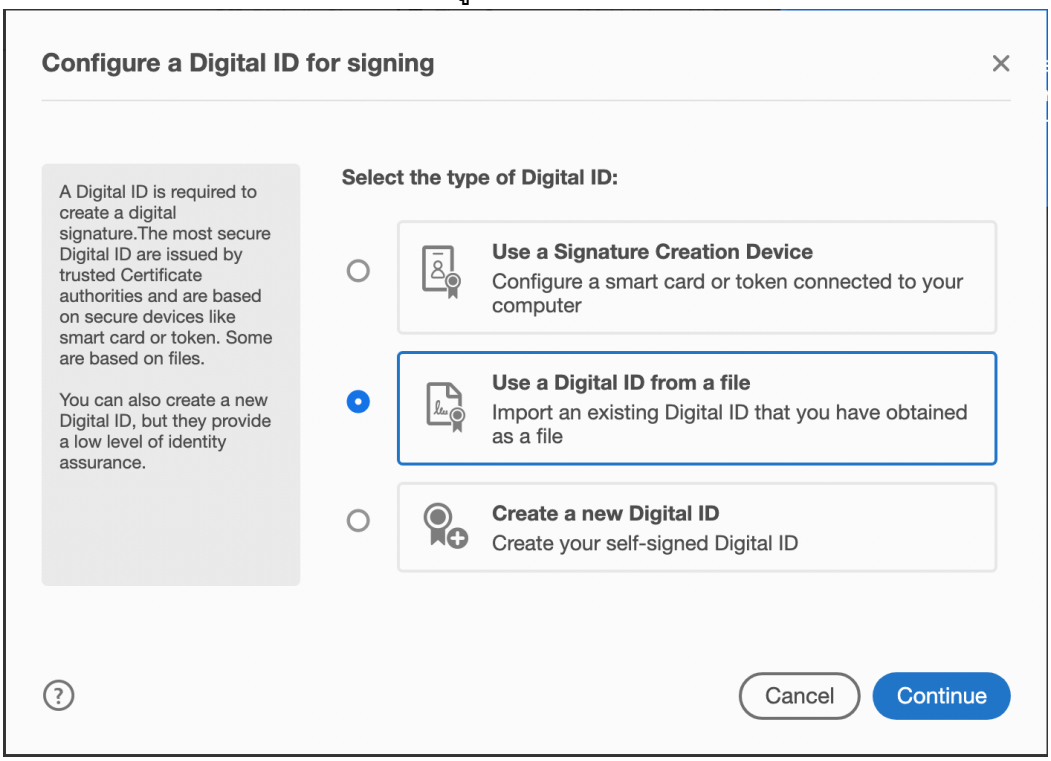
4. คลิก Digitally Sign เพื่อเซ็นเอกสาร



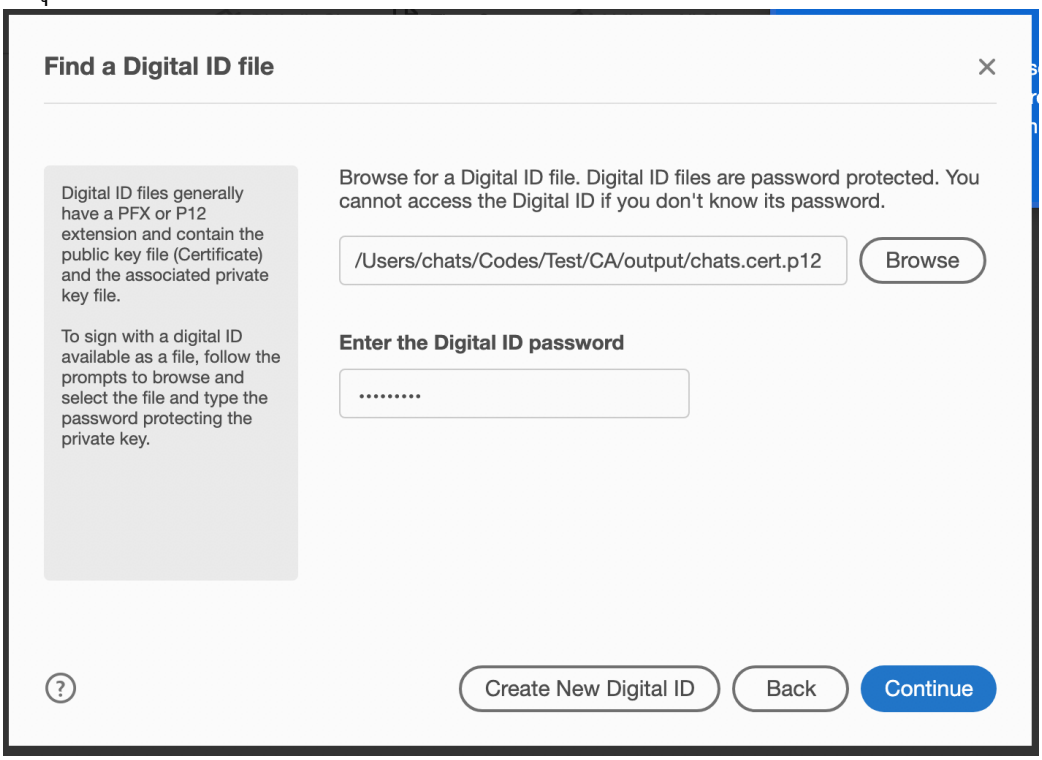
5. การเซ็นเอกสารต้องใช้ Digital Signature จึงต้องกำหนดค่า Digital ID ก่อน



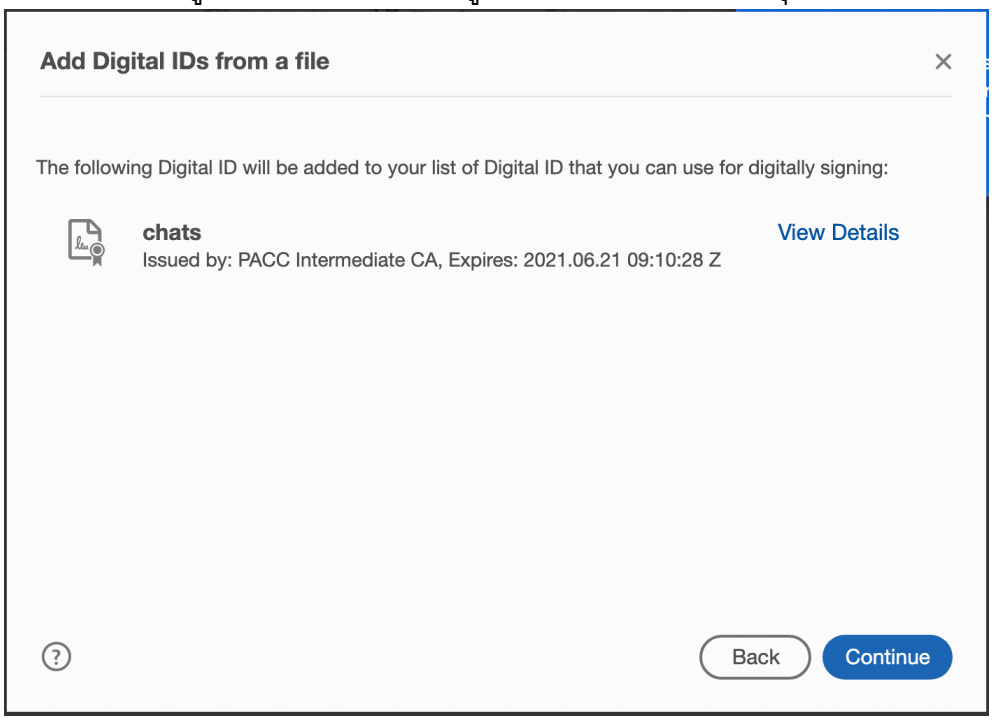
6. ใช้ Digital ID จากไฟล์ .p12 ที่ได้จากผู้ออกใบรับรอง (CA)



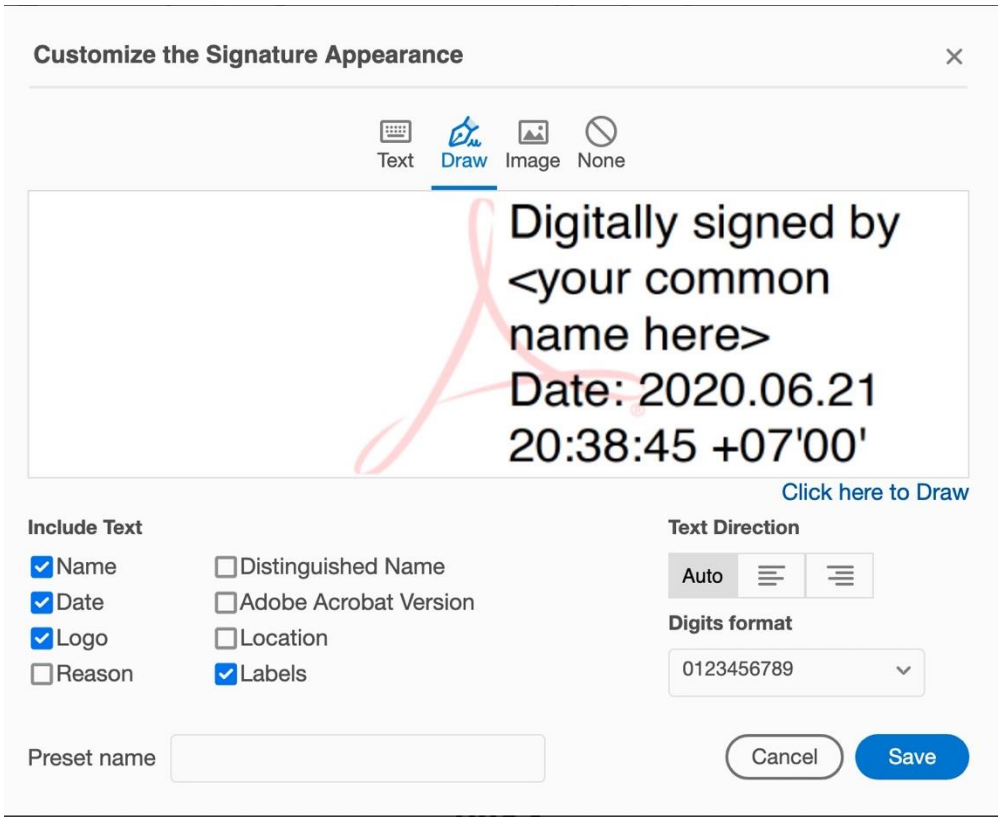
7. ระบุ Digital ID จากไฟล์ .p12 พร้อมกรอกรหัสผ่านของไฟล์ .p12



8. ตรวจสอบความถูกต้องของ Digital ID (ผู้ออกใบรับรอง วันหมดอายุ)

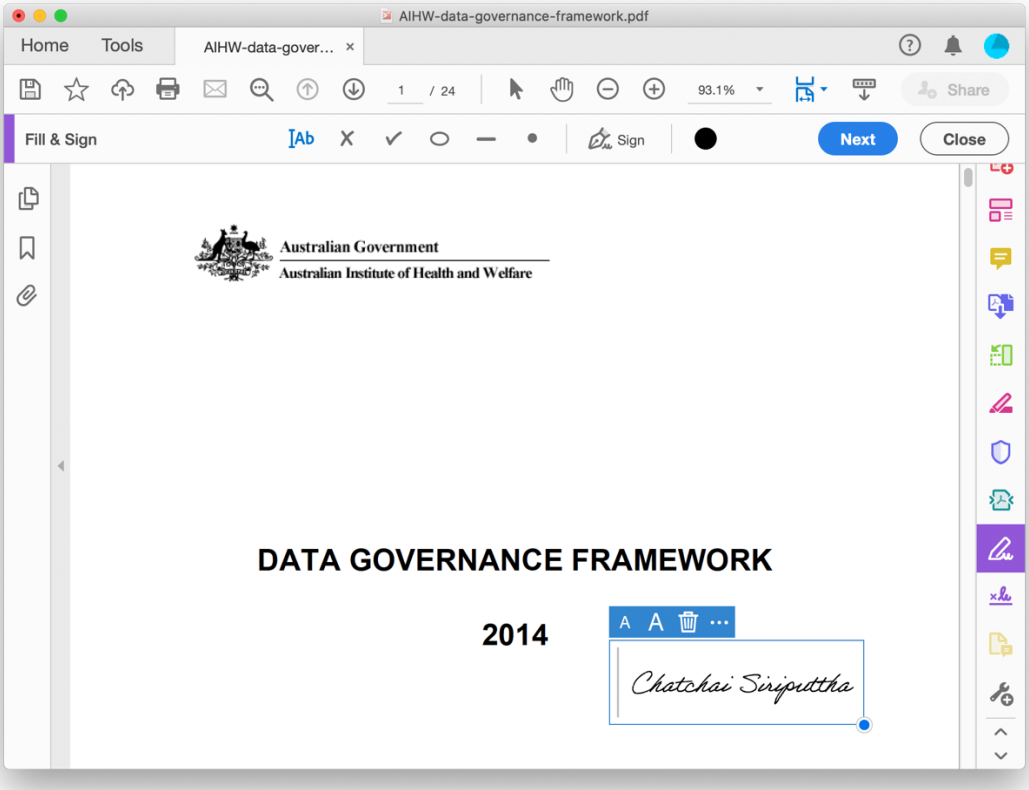


9. กำหนดค่า ลายเซ็นที่ต้องการให้ปรากฏในเอกสาร



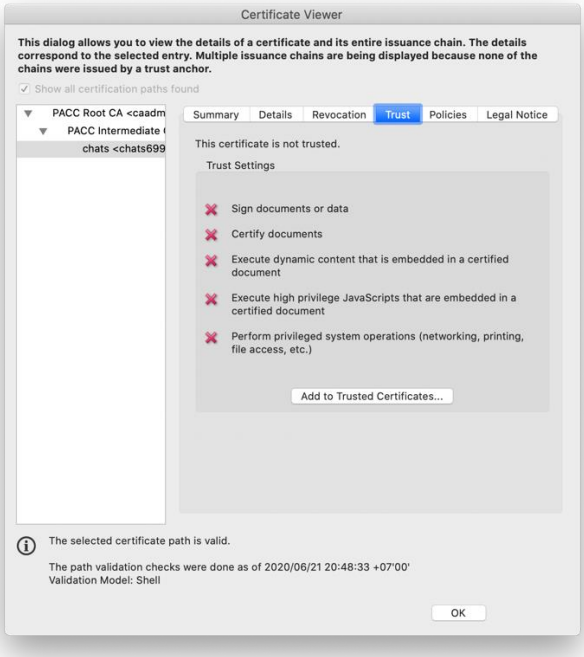
10. กำหนดค่า ลายเซ็นที่ต้องการให้ปรากฏในเอกสาร

11. กำหนดค่า ลายเซ็นที่ต้องการให้ปรากฏในเอกสาร จัดตำแหน่งตามต้องการ

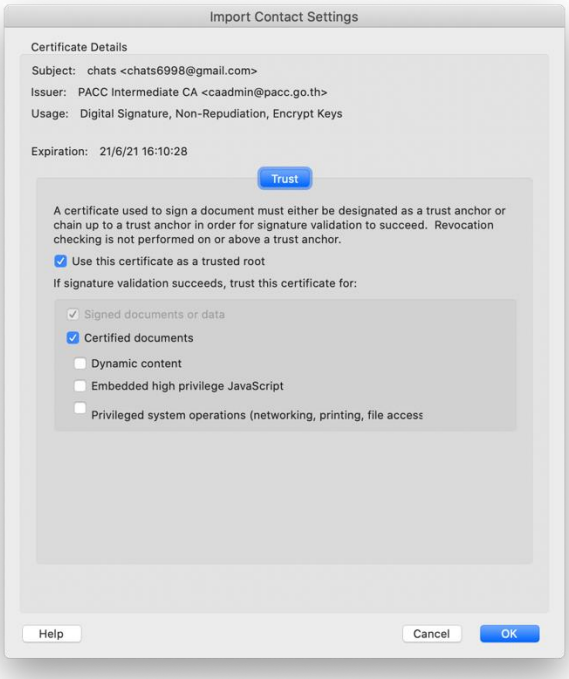


12. ตรวจสอบความถูกต้องของเอกสาร

- ลายเซ็นต้องประกอบด้วย Digital ID
- ภายใน Digital ID จะมีผู้ออก Certificate โดยเป็น CA ของ PACC
- ระบุชื่อ และ อีเมล์ของผู้เซ็นเอกสาร



13. ทำการ Trust Certificate โดย trust ที่ระดับบนสุด คือ PACC Root CA



14. ตรวจสอบเอกสารที่มีการลงนาม และตรวจสอบความถูกต้องของ Digital ID และ Trust Certificate