



สำนักคอมพิวเตอร์

คู่มือ KMUTT Digital Document (ฉบับปรับปรุง)

คณะทำงานระบบเอกสารดิจิทัล มจร.

กัลยา ทังวงศ์เจริญ (ผู้จัดทำคู่มือ)
20/7/2564

คำนำ

การจัดทำคู่มือการจัดการกับลายเซ็นดิจิทัลด้วยโปรแกรม Adobe Acrobat Pro DC นี้ เป็นฉบับปรับปรุงพัฒนาในหัวข้อเนื้อหาที่ผู้ใช้งานต้องการเพิ่มเติม อันเป็นส่วนหนึ่งในระบบ KMUTT DMS (Document Management System) หรือ KMUTT Digital Document ของมหาวิทยาลัย สำหรับการบริหารจัดการเอกสารที่มีการนำลายเซ็นดิจิทัลเข้ามาใช้งาน และเพื่อใช้ประกอบโครงการ “การอบรมเชิงปฏิบัติการการใช้โปรแกรม Adobe Acrobat Pro DC จัดการไฟล์เอกสาร PDF ประกอบระบบ Digital Document” แก่บุคลากรของหน่วยงานภายใน มจร. ได้เรียนรู้ สามารถเข้าใจ และใช้งานระบบ KMUTT Digital Document ที่จะเกิดขึ้นต่อไป

กัลยา ทั้งวงศ์เจริญ (ผู้เขียนคู่มือฯ)

ฝ่ายอบรม สำนักคอมพิวเตอร์

กรกฎาคม 2564

สารบัญ

คู่มือการดาวน์โหลดและติดตั้งโปรแกรม Acrobat Pro DC ของ มจร.....	4
คู่มือการดาวน์โหลดและติดตั้ง Certificate User กับ Root CA	6
วิธีการเข้าไปรับการยืนยันตัวตนสำหรับบุคลากร มจร.....	7
วิธีติดตั้งชุดยืนยันตัวตนในโปรแกรม Adobe Acrobat Pro DC	11
การติดตั้ง Root CA ไฟล์.crt	11
วิธีติดตั้งผู้ให้ลายเซ็นดิจิทัล (Certificate User) ไฟล์ “PKCS#12.p12”	15
วิธีการเซ็นเอกสารด้วยลายเซ็นดิจิทัล.....	17
คู่มือการเซ็นและการส่งต่อเอกสารด้วยลายเซ็นดิจิทัล	20
การเซ็นแบบมี 1 ลายเซ็น	20
การเซ็นแบบมีการเซ็นต่อกันหลายคน.....	20
การเพิ่มความคิดเห็น (Annotations) ในเอกสารประกอบการเซ็นต่อกันหลายคน.....	26
การเพิกถอนลายเซ็นดิจิทัล (Revoke Digital Signature)	29
การสร้างภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัล.....	32
การสร้างภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัลด้วยการ “Draw”	33
การนำเข้าและสร้างไฟล์ภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัลด้วยการ “Image”	35
การสร้างไฟล์ภาพลายเซ็นข้อความให้เข้ากับหน้าเอกสารในไฟล์เอกสาร .pdf.....	37

คู่มือ KMUTT Digital Document

ระบบ KMUTT Digital Document คือ ระบบจัดการเอกสาร เช่น บันทึกข้อความ หรือ หนังสือที่ใช้ในการปฏิบัติงานให้อยู่ในรูปแบบของเอกสารดิจิทัล รวมไปถึงการเซ็นเอกสารด้วยลายเซ็นดิจิทัล และเวียนเอกสารเพื่อส่งต่อหรือย้อนกลับบนระบบเครือข่ายคอมพิวเตอร์ ที่สามารถยืนยันตัวตนของเจ้าของลายเซ็น ความน่าเชื่อถือของเอกสาร และความปลอดภัยของระบบ เพื่อประหยัดทรัพยากรกระดาษและเข้ากับสถานการณ์ COVID-19 ด้วยการ Work From Home มีวิธีการและการจัดเตรียมระบบสำหรับระดับ User ดังนี้

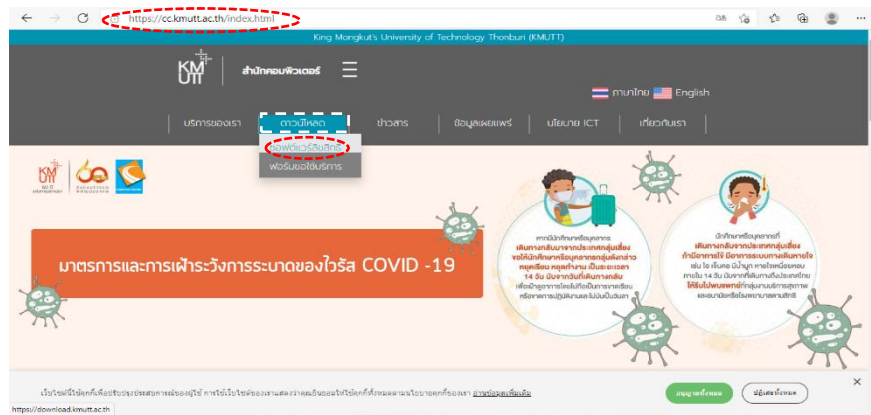
1. Network ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ เช่น การสร้างและแชร์ไฟล์เตอร์ , อินเทอร์เน็ต , อีเมล สำหรับการเวียนเอกสาร เพื่อส่งต่อหรือย้อนกลับเอกสารดิจิทัล ขึ้นกับความเหมาะสมและนโยบายของผู้บริหารของแต่ละหน่วยงาน
2. Digital Signature ได้แก่ Root CA / Intermediate CA Certificate และ User Certificate เป็นส่วนที่สำนักคอมพิวเตอร์ ดำเนินการบริหารจัดการให้แก่ มจร. และบุคลากร โดยเข้ารับบริการได้ที่เว็บ Url: mysign.kmutt.ac.th
3. Hardware ได้แก่ เครื่องคอมพิวเตอร์ PC และ Notebook ที่ควรมี Spec. ไม่น้อยกว่า ดังนี้
 - หน่วยประมวลผล (CPU) : Core i5 ขึ้นไป , หน่วยความจำ (RAM) : 4 GB. ขึ้นไป , ฮาร์ดดิสก์ (HDD) : ควรเป็นแบบ SSD , และ ระบบปฏิบัติการ (OS) : Windows 8 ขึ้นไป
4. Software ได้แก่ โปรแกรม Adobe Acrobat Pro DC สำหรับสร้างหรือปรับแต่ง-แก้ไขเอกสารให้อยู่ในรูปแบบ “เอกสารดิจิทัล” และสามารถนำเข้า-ใช้งานลายเซ็นดิจิทัลที่ยืนยันตัวตนจริงได้

สำหรับระบบ KMUTT Digital Document นี้ ระดับผู้ใช้งาน (User) ในบทบาทผู้สร้าง-ใช้งานเอกสารดิจิทัล , เซ็นเอกสารดิจิทัลนี้ด้วยลายเซ็นดิจิทัล , และเวียนติดตามเอกสารที่อาจมีการส่งต่อให้ผู้บริหารระดับต่างๆ และผู้ที่เกี่ยวข้องลงนามด้วยลายเซ็นดิจิทัลเช่นกัน ควรมีความรู้ดังนี้

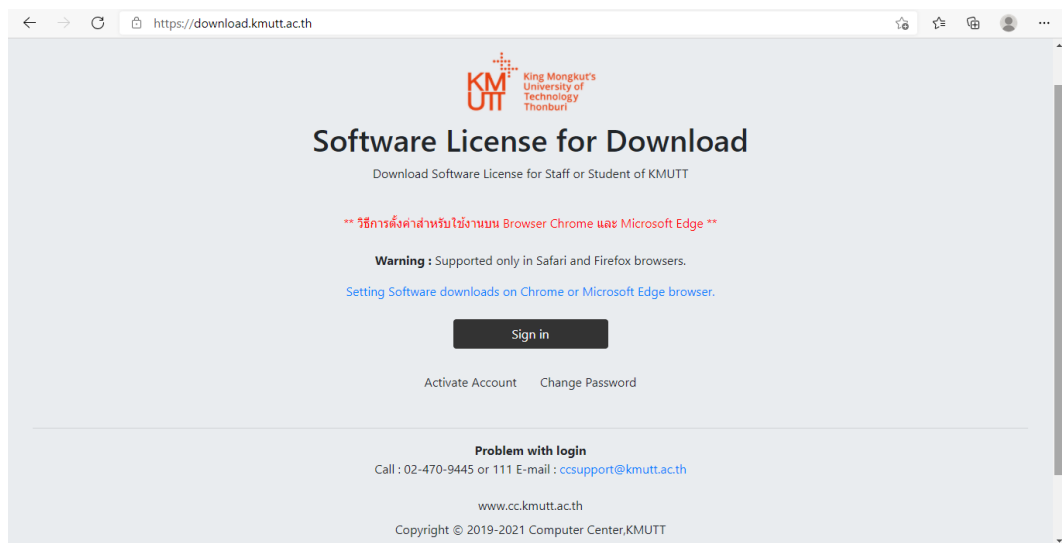
คู่มือการดาวน์โหลดและติดตั้งโปรแกรม Acrobat Pro DC ของ มจร.

ในเครื่องและอุปกรณ์คอมพิวเตอร์ที่จะใช้ระบบ KMUTT Digital Document ควรมีการติดตั้งโปรแกรม Adobe Acrobat Pro DC ดังนี้

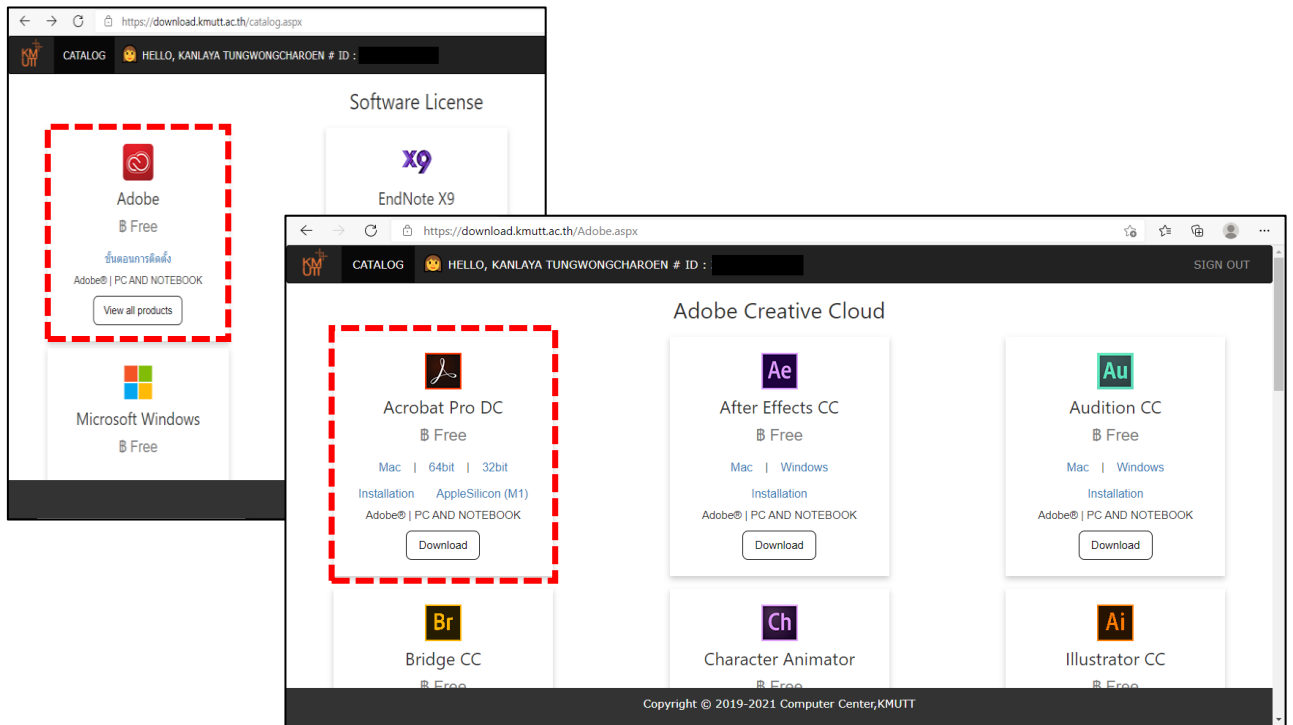
1. เข้าเว็บ Url: <https://cc.kmutt.ac.th> ที่แท้ับ “ดาวน์โหลด” คลิกเลือก “ซอฟต์แวร์ลิขสิทธิ์”



2. ให้ปฏิบัติตามหน้าเว็บ (ถ้าปรากฏกรณียังไม่เคยตั้งค่าสำหรับโปรแกรม Browser บางยี่ห้อ) คลิกปุ่ม “Sign in” > พิมพ์ชื่อ e-Mail และ Password



3. เข้าสู่หน้า “CATALOG” ของชุดซอฟต์แวร์ลิขสิทธิ์ “Software License” > (กรอกลี้นประ) ชุด “Adobe” > คลิกลิงค์ “ขั้นตอนการติดตั้ง” เพื่อศึกษาวิธีการติดตั้งโปรแกรม > คลิกปุ่ม “View all products” เพื่อเข้าไปเลือกโปรแกรม “Acrobat Pro DC” โดยเลือกให้ตรงกับ Windows System Type: “64bit” หรือ “32bit” หรือ เครื่องระบบ “Mac”



4. หลังจากเลือกได้แล้ว > เข้าไปคลิกไฟล์ติดตั้งของโปรแกรม และให้ดำเนินการติดตั้งตาม “ขั้นตอนการติดตั้ง (Installation)” > ได้โปรแกรม (ไอคอน) แสดงที่ Desktop พร้อมใช้งาน



คู่มือการดาวน์โหลดและติดตั้ง Certificate User กับ Root CA

ระบบ KMUTT Digital Document มีความจำเป็นที่ต้องการให้บุคลากรของ มจร. มีลายเซ็นดิจิทัล แทนของการเซ็นเอกสารด้วยปากกาบนกระดาษเอกสารในระบบเดิม ควรมีความรู้และเข้าใจใน เรื่องลายเซ็นดิจิทัล ดังนี้

โดยปกติแล้ว “ลายเซ็น (Signature)” เป็นรูปแบบในการระบุตัวตนวิธีหนึ่ง เพื่อใช้ยืนยันตัวบุคคล โดยได้รับการรับรองตามกฎหมาย หากมีการปลอมลายเซ็นจะมีวิธีการตรวจสอบโดยผู้ชำนาญการทางพิสูจน์หลักฐานที่ได้รับการแต่งตั้งจากศาลว่าเป็นผู้ชำนาญการ ส่วน “ลายเซ็นดิจิทัล (Digital Signature)” ไม่ได้หมายถึงการเอาภาพ “ลายเซ็น” (image) ไปแปะไว้ที่ไฟล์เอกสารที่ต้องการลงนาม เพราะปลอมกันได้ง่าย จึงต้องมีวิธีการจัดการในการระบุตัวตนในระบบดิจิทัลเพื่อความปลอดภัย โดยใช้สิ่งที่ยืนยันว่าเป็นบุคคลนั้นได้จริงๆ คือ คีย์ส่วนตัว (Private Key) ของแต่ละบุคคลในการลงนามทางดิจิทัลนั้น หลักการของลายเซ็นอิเล็กทรอนิกส์ คือ ลายเซ็นดิจิทัลที่ลงในไฟล์เอกสารแต่ละไฟล์อาจไม่เหมือนกัน แต่จะมีตัวบ่งชี้เพื่อยืนยันว่าเป็นของเจ้าของลายเซ็นคนเดียวกัน คือ ผู้ใช้ใบรับรองดิจิทัล (Certificate User) ซึ่งออกโดย “ผู้ให้บริการออกใบรับรอง (Certification Authority : CA)” ทำให้มั่นใจได้ว่าเจ้าของลายเซ็นดิจิทัลนี้มีตัวตนจริง โดยอาศัยเทคโนโลยีที่เรียกว่า PKI (Public Key Infrastructure) สำหรับการเข้ารหัสและถอดรหัสลายเซ็นดิจิทัล (Digital Signature)

ดังนั้น บุคลากร มจร. ต้องเข้าดำเนินการยืนยันตัวตน โดยเริ่มที่การดาวน์โหลดไฟล์ในเว็บ <https://mysign.kmutt.ac.th> เพื่อรับชุดการยืนยันตัวตน อันประกอบด้วย 2 ส่วน สำหรับติดตั้ง (Setup) ในโปรแกรม Adobe Acrobat Pro DC และเซ็นลงในไฟล์เอกสารในระบบ KMUTT Digital Document ได้ ดังนี้

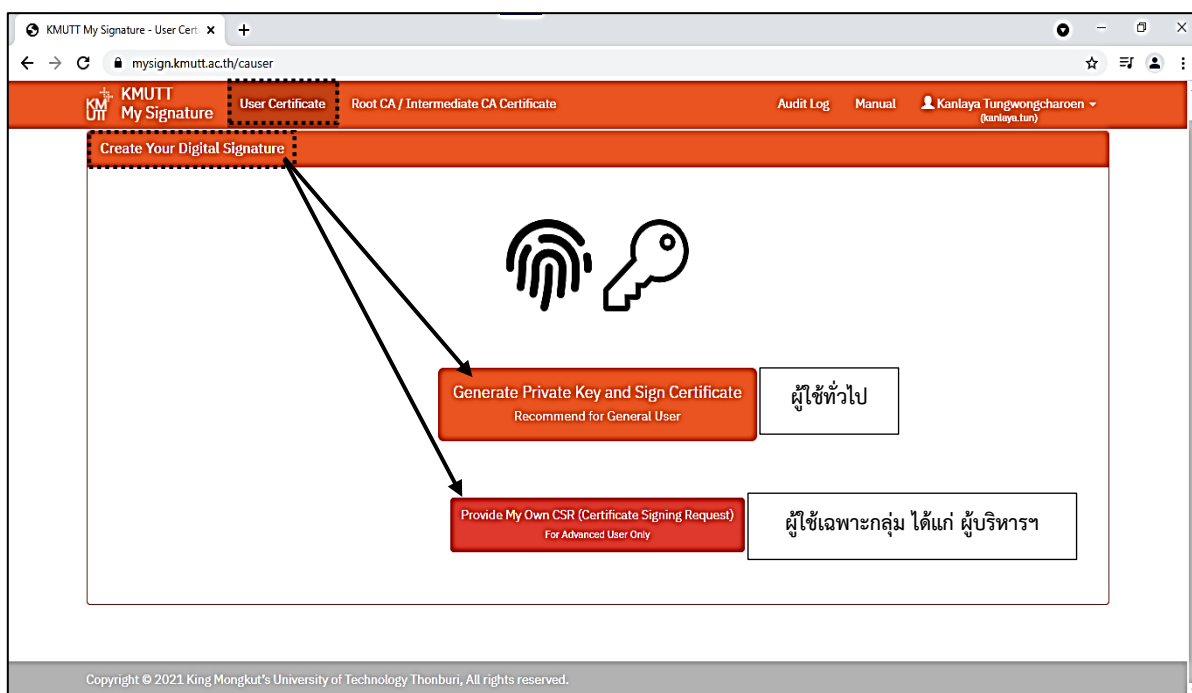
- ส่วน “Root CA” คือ Thai University Consortium Certification Authority ได้ออกใบรับรองให้แก่ มจร. ได้รับการลงทะเบียนยืนยันตัวตน เข้าร่วมอยู่ในกลุ่มมหาวิทยาลัยในประเทศไทยโดยผ่านความเห็นชอบโดยกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม (อว.) แล้ว โดยบุคลากร มจร. ต้องไป Download รับไฟล์ชื่อ “CA.crt” และต้องติดตั้งลงในโปรแกรม Adobe Acrobat Pro DC ครั้งแรกครั้งเดียว เพื่อ โปรแกรมจะทำการตรวจสอบ ยืนยัน และยอมรับความถูกต้องในการใช้งานจาก มจร.
- ส่วน “Certificate User” คือ ผู้ใช้ใบรับรองดิจิทัล ที่จะได้รับการสร้างคีย์ส่วนตัว (Private Key) ในรูปแบบไฟล์ “PKCS#12.p12” (บุคลากร มจร. จะได้เป็น “ชื่อ Login.p12” เช่น “kalya.tub.p12”) เป็น ลายเซ็นดิจิทัล (Digital Signature) ที่ต้องนำไปติดตั้งลงในโปรแกรม Adobe Acrobat Pro DC สำหรับเซ็นลงในไฟล์เอกสาร

เมื่อบุคลากร มจร. ได้ดำเนินการรับทั้ง 2 ส่วนนี้แล้ว จักต้องเก็บลงในเครื่องอุปกรณ์คอมพิวเตอร์ และค้นคืนเพื่อใช้ติดตั้งในโปรแกรม Acrobat Pro DC ทุกเครื่องอุปกรณ์คอมพิวเตอร์ที่จะใช้ระบบ KMUTT Digital Document การเก็บรักษาต้องเก็บในส่วนที่ปลอดภัยและเป็นความลับไม่ควรเปิดเผย เพื่อป้องกันการถูกขโมยไปใช้งานแทน ซึ่งทางสำนักคอมพิวเตอร์จะไม่รับผิดชอบหากพบความบกพร่องจากกรณีนี้

วิธีการเข้าไปรับการยืนยันตัวตนสำหรับบุคลากร มจร.

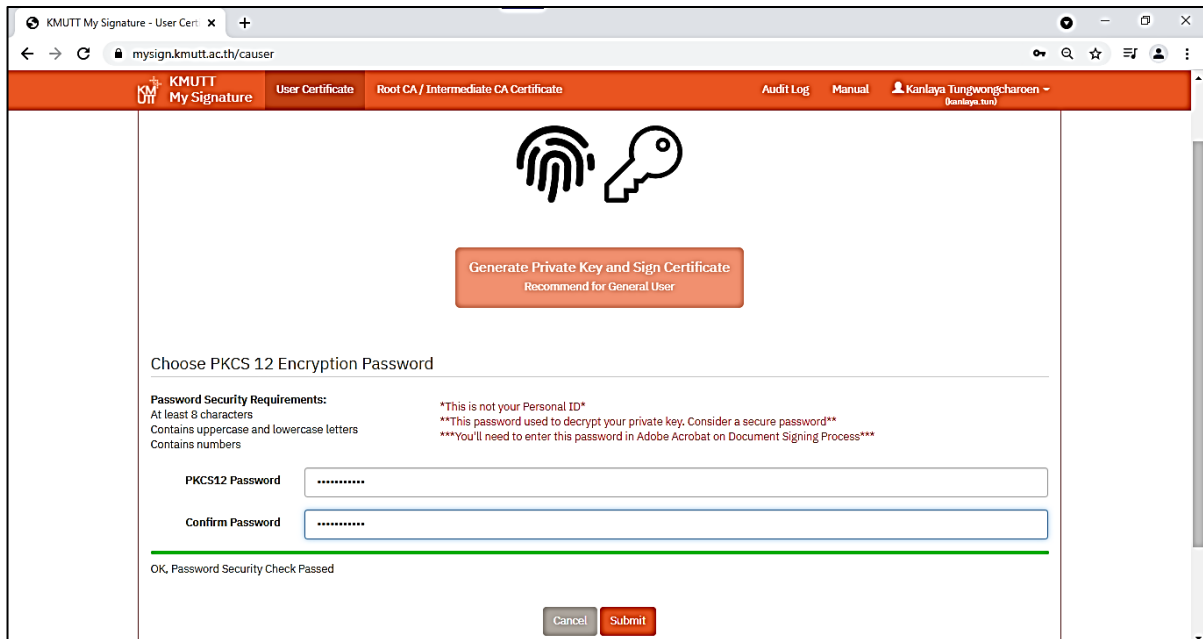
บุคลากร มจร. ต้องเข้าไปรับการยืนยันตัวตน เพื่อดาวน์โหลดชุดรับชุดยืนยันตัวตน 2 ส่วน โดยสิ่งที่ต้องเตรียม คือ “เลขที่บัตรประชาชน (Personal ID)” และดำเนินการตามขั้นตอน ดังนี้

1. เข้าเว็บ Url: <https://mysign.kmutt.ac.th> > พิมพ์ชื่อ e-Mail และ Password เพื่อ Login เข้าสู่ระบบ
2. **สร้างคีย์ส่วนตัวและเป็นผู้ใช้ใบรับรองลายเซ็นดิจิทัล** (Generate Private Key and Sign Certificate User) เพื่อให้ได้ไฟล์ “PKCS#12.p12” สามารถสร้างได้ 2 วิธี คือ
 - 2.1. **Generate Private Key and Sign Certificate** (Recommend for General User) สำหรับผู้ใช้ทั่วไป ที่ระบบจะดำเนินการสร้างให้โดยอัตโนมัติ
 - 2.2. **Provide My Own CSR** (For Advanced User Only) สำหรับผู้ใช้เฉพาะกลุ่ม ได้แก่ ผู้บริหารองค์กร ที่จำเป็นต้องดำเนินการสร้างด้วยตัวเอง เพื่อเสริมความปลอดภัยแก่ลายเซ็นของผู้บริหาร
3. ทั้ง 2 วิธี เริ่มที่แท็บ “User Certificate” ในหน้าต่าง “Create Your Digital Signature”



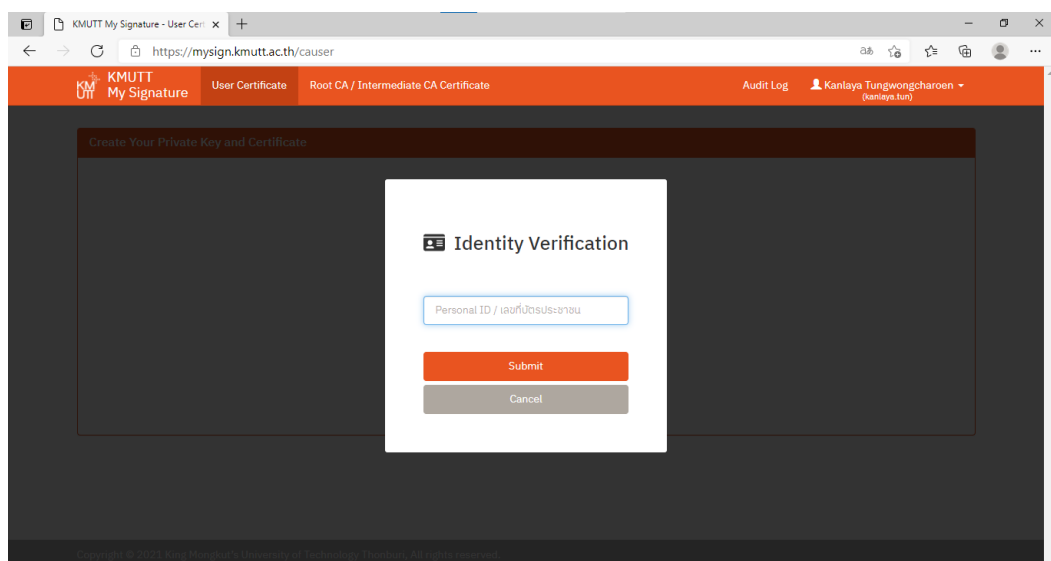
- 3.1. สำหรับผู้ใช้ทั่วไป (Recommend for General User) > คลิกปุ่ม “Generate Private Key and Sign Certificate” > แล้วดำเนินการต่อใน ข้อ 4.
- 3.2. สำหรับผู้ใช้เฉพาะกลุ่ม ได้แก่ ผู้บริหารองค์กร (For Advanced User Only) > คลิกปุ่ม “Provide My Own CSR (Certificate Signing Request)” > แล้วปฏิบัติเองตามวิธี (ถ้าพบปัญหาโปรดติดต่อเบอร์ 111 สำนักคอมพิวเตอร์)

4. สำหรับผู้ใช้ทั่วไป (Recommend for General User) > คลิกปุ่ม “Generate Private Key and Sign Certificate” > พิมพ์ในช่อง “PKCS12 Password และ Confirm Password” เพื่อตั้งและยืนยันรหัสผ่านให้แกไฟล์ PKCS12 > คลิกปุ่ม “Submit”

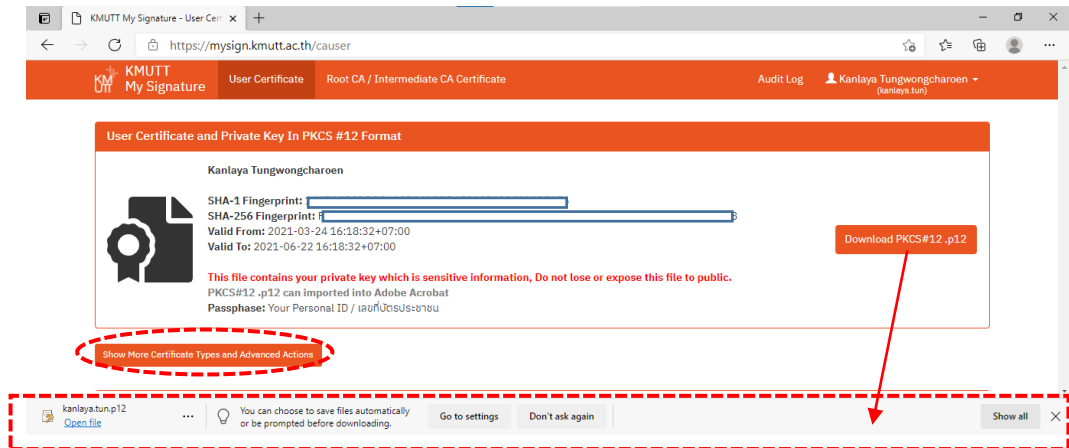


Password Security Requirements: (ข้อกำหนดด้านความปลอดภัยของรหัสผ่าน) : อย่างน้อย 8 อักขระ ประกอบด้วยอักขรตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, และตัวเลข โปรดจดจำจะนำไปใช้ติดตั้งใน Acrobat Pro DC

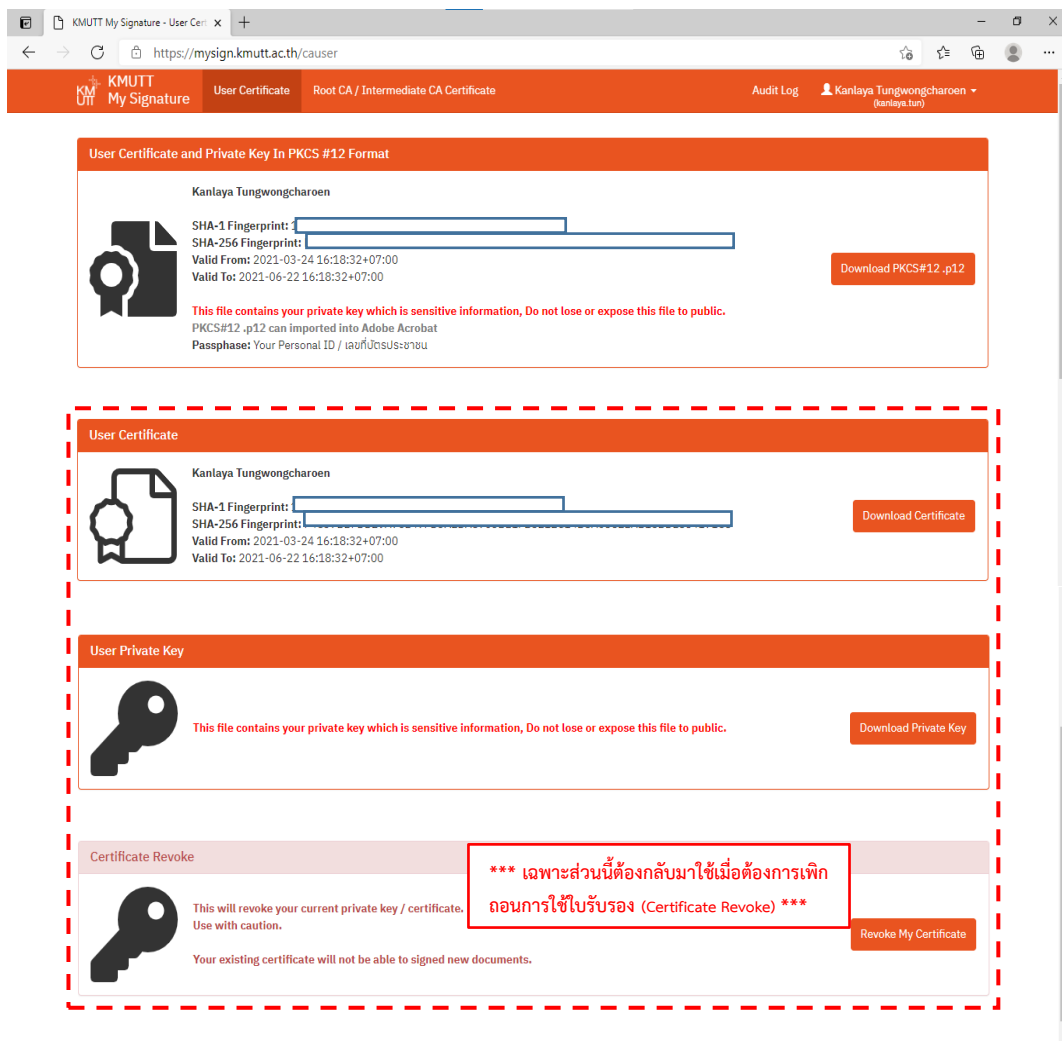
5. ปรากฏหน้าต่าง “Identity Verification” > ในช่อง “Personal ID / เลขที่บัตรประชาชน” พิมพ์เลขที่บัตรประชาชน > คลิกปุ่ม “Submit”



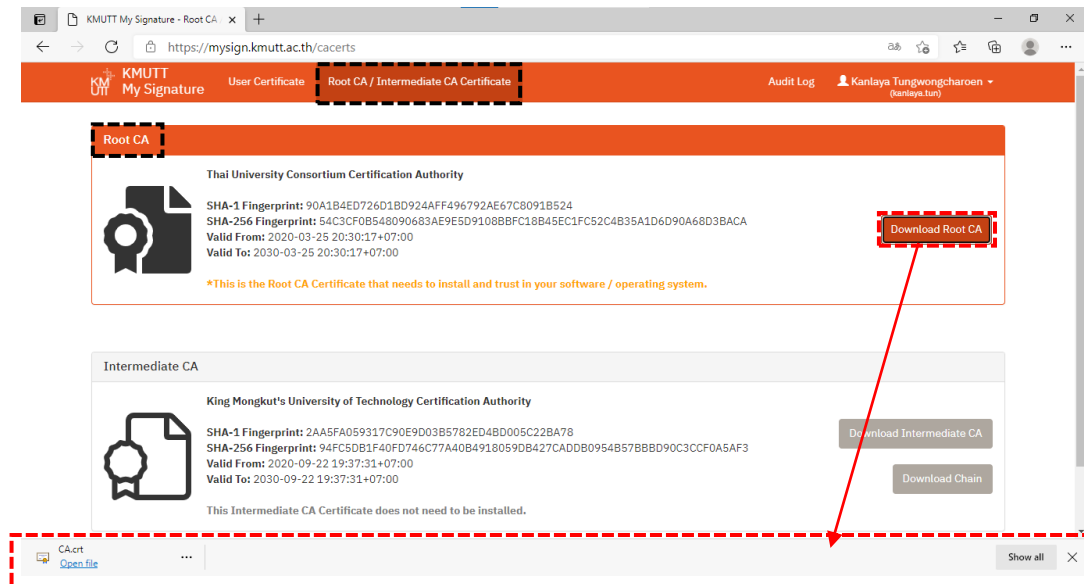
6. ปรากฏหน้าต่าง “User Certificate and Private Key In PKCS #12 Format” > คลิกปุ่ม “Download PKCS#12.p12” > ปรากฏหน้าต่าง “Identity Verification Download PKSC#12 .p12” พิมพ์เลขที่บัตรประชาชน (Personal ID) > คลิกปุ่ม “Submit” อีกครั้ง > ระบบจะดาวน์โหลดไฟล์ “ชื่อ Login.p12” เก็บไว้ในเครื่องอุปกรณ์คอมพิวเตอร์



7. ถ้าต้องการดูรายละเอียดไฟล์เพิ่ม > คลิกปุ่ม “Show More Certificate Types and Advanced Actions” > ปรากฏดังรายการไฟล์ในเส้นประ (ไม่ควร Download มีรวมอยู่ในไฟล์ PKCS#12.p12 แล้ว)

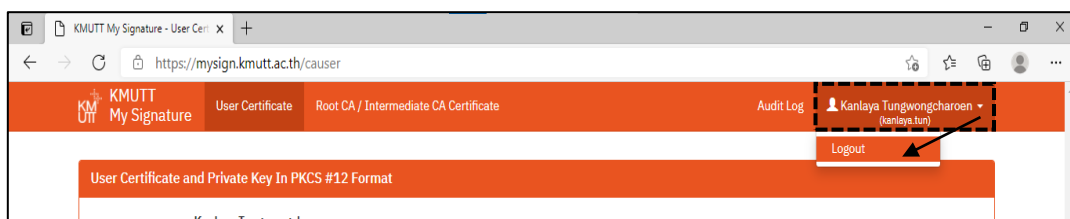


8. **Download Root CA** เพื่อให้ได้ไฟล์ “CA.crt” > คลิกแท็บ “Root CA/Intermediate CA Certificate” ในหน้าต่าง “Root CA” > คลิกปุ่ม “Download Root CA” และจัดเก็บไฟล์ “CA.crt” ไว้ในเครื่องอุปกรณ์คอมพิวเตอร์ (ควรจัดเก็บที่เดียวกับไฟล์ “ชื่อ Login.p12”)



ไฟล์ “CA.crt” สำหรับนำไปติดตั้งใน Adobe Acrobat Pro DC ในครั้งแรกครั้งเดียวที่จะเริ่มใช้ลายเซ็นดิจิทัล

9. เมื่อดำเนินการเสร็จ Logout ออกจากระบบ “KMUTT My Signature” > คลิก ▼ ข้างชื่อ-สกุล ผู้ใช้ระบบ > คลิก “Logout”



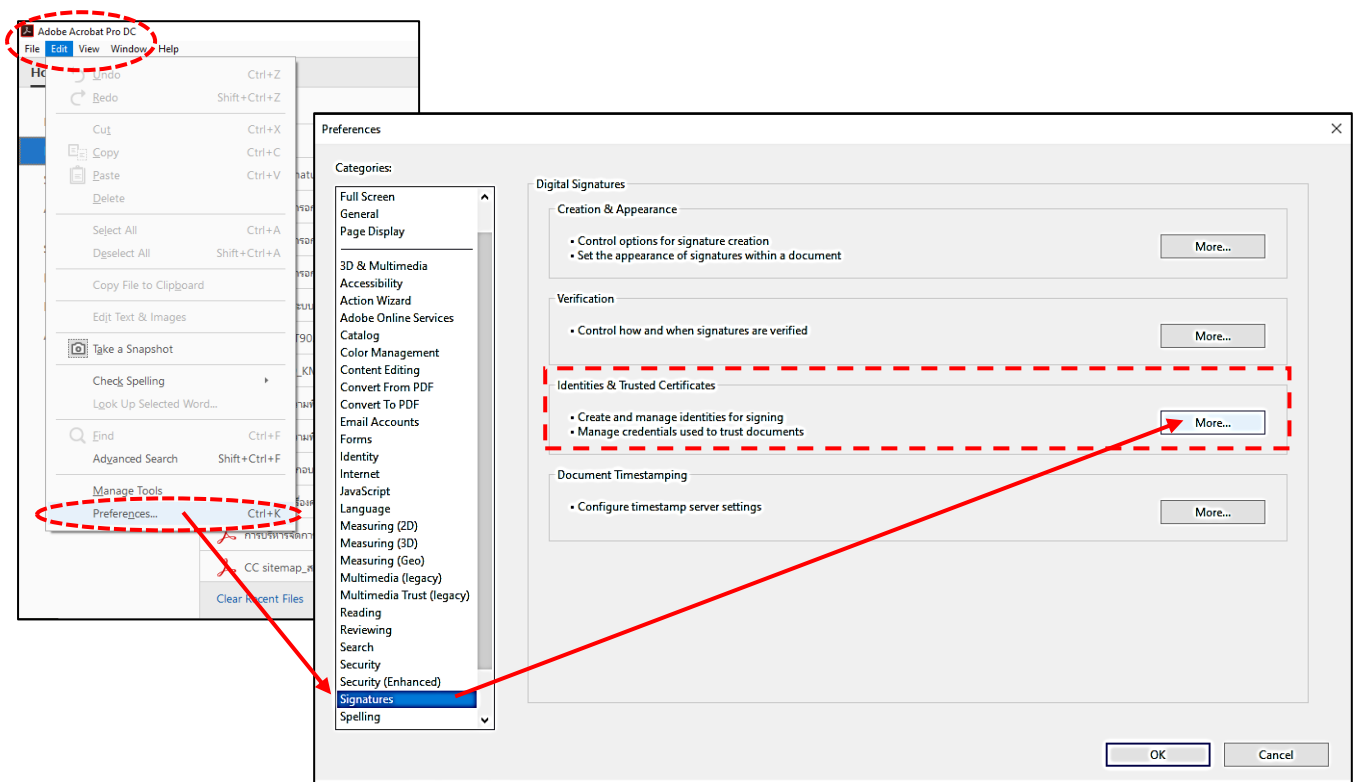
วิธีติดตั้งชุดยืนยันตัวตนในโปรแกรม Adobe Acrobat Pro DC

เมื่อได้รับชุดยืนยันตัวตนทั้ง 2 ส่วน (ไฟล์ “ชื่อ Login.p12” และไฟล์ “CA.crt”) นำไปติดตั้งลงในโปรแกรม Adobe Acrobat Pro DC ให้รู้จัก ยอมรับ และตรวจสอบลายเซ็นดิจิทัลของแต่ละบุคคลได้ ดังนี้

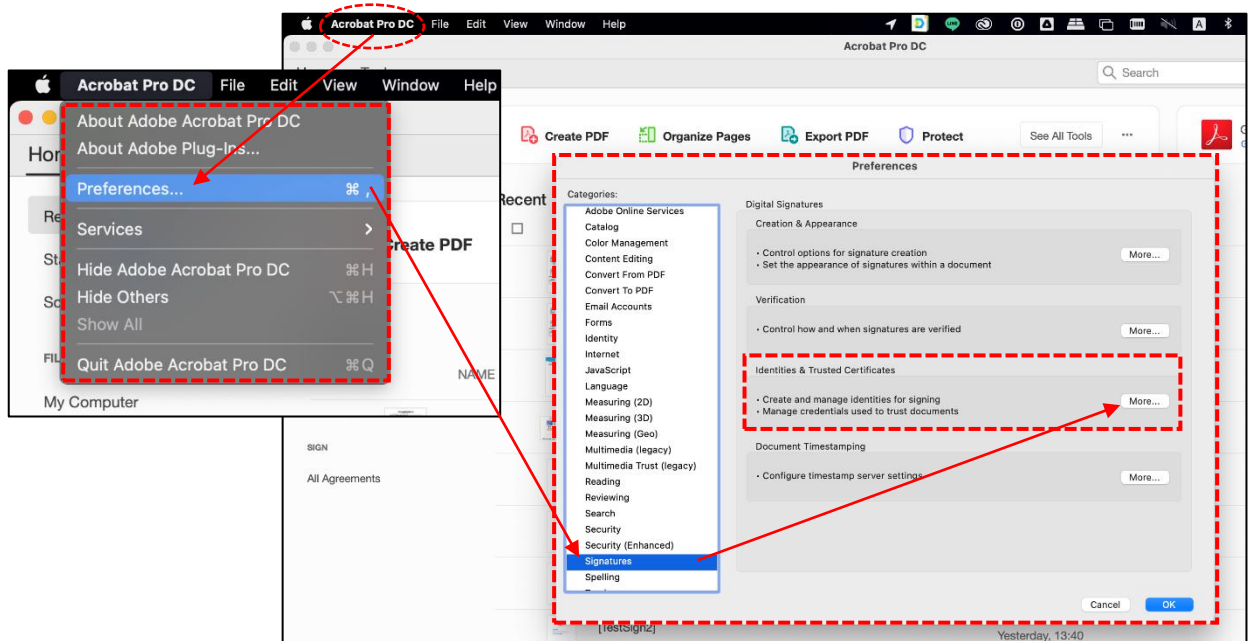
การติดตั้ง Root CA ไฟล์.crt

1. (เริ่มที่) ต้องติดตั้ง Root CA ก่อน ด้วยไฟล์ “CA.crt”

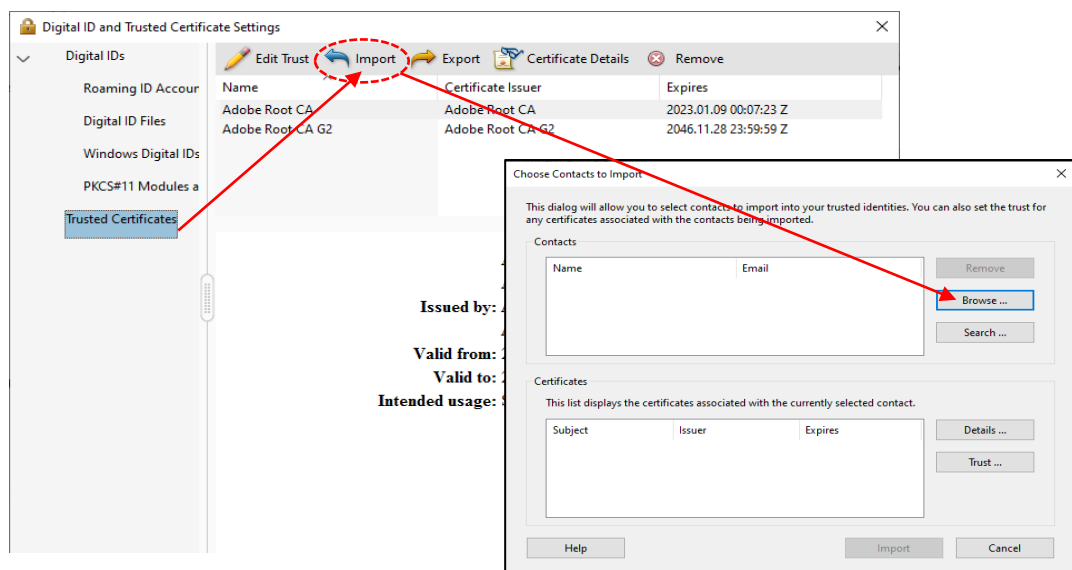
1.1. สำหรับเครื่องคอมพิวเตอร์ที่ใช้ Windows โดยเปิดโปรแกรม Acrobat Pro DC > เมนู “Edit” คลิกคำสั่ง “Preferences...” > ปรากฏหน้าต่าง “Preferences” ด้านซ้าย “Categories:” > เลือกคลิกคำสั่ง “Signatures” > ด้านขวาช่อง “Digital Signatures” > ส่วน “Identities & Trusted Certificates” คลิกที่ปุ่ม “More”



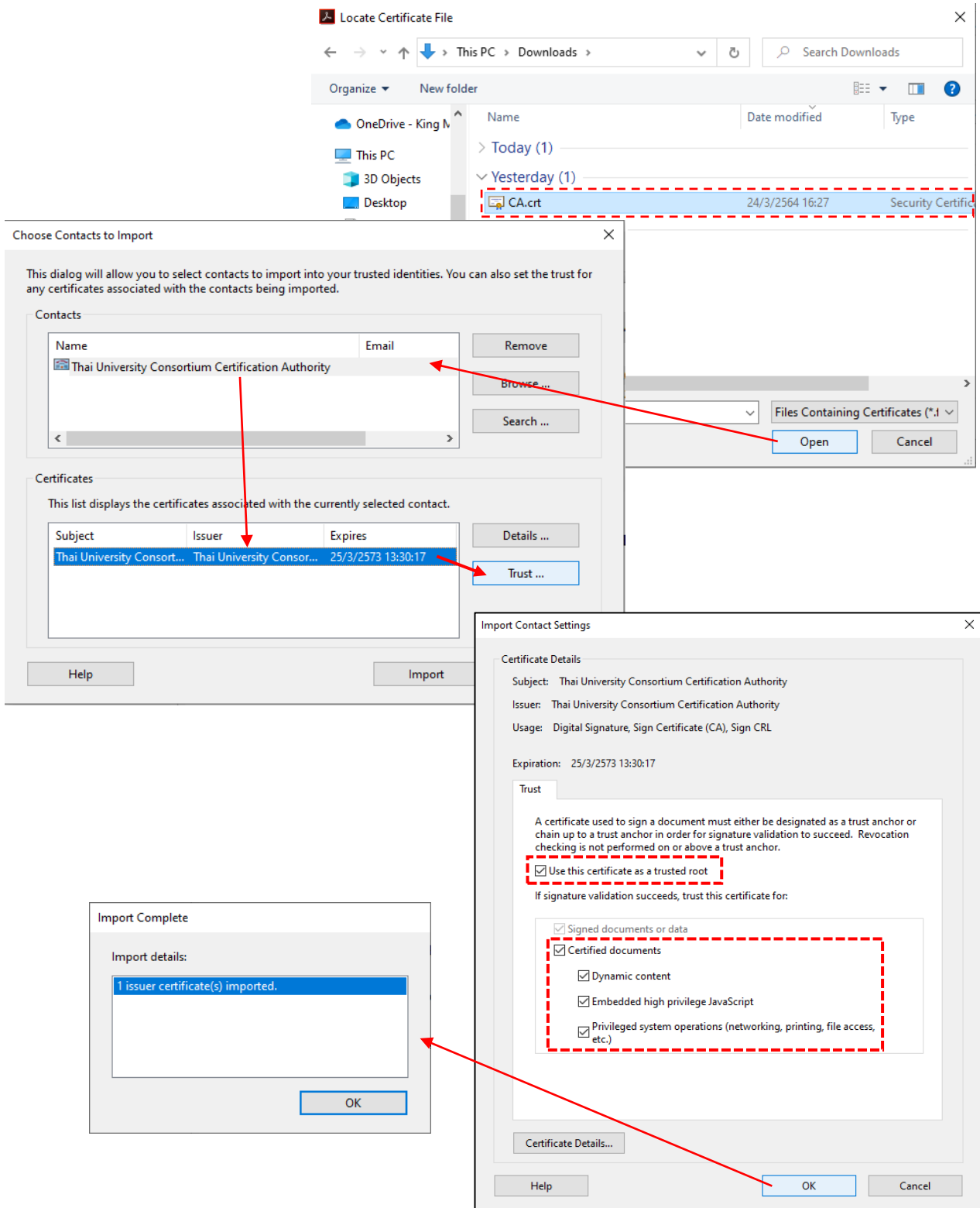
- 1.2. การเข้าหน้าต่าง Preferences ใน Mac Book สำหรับเครื่องคอมพิวเตอร์ที่ใช้ Mac OS โดยเปิดโปรแกรม Acrobat Pro DC > เมนู “Acrobat Pro DC” คลิกคำสั่ง “Preferences...” > ปรากฏหน้าต่าง “Preferences” ด้านซ้าย “Categories:” > เลือกคลิกคำสั่ง “Signatures” > ด้านขวาช่อง “Digital Signatures” > ส่วน “Identities & Trusted Certificates” คลิกที่ปุ่ม “More”



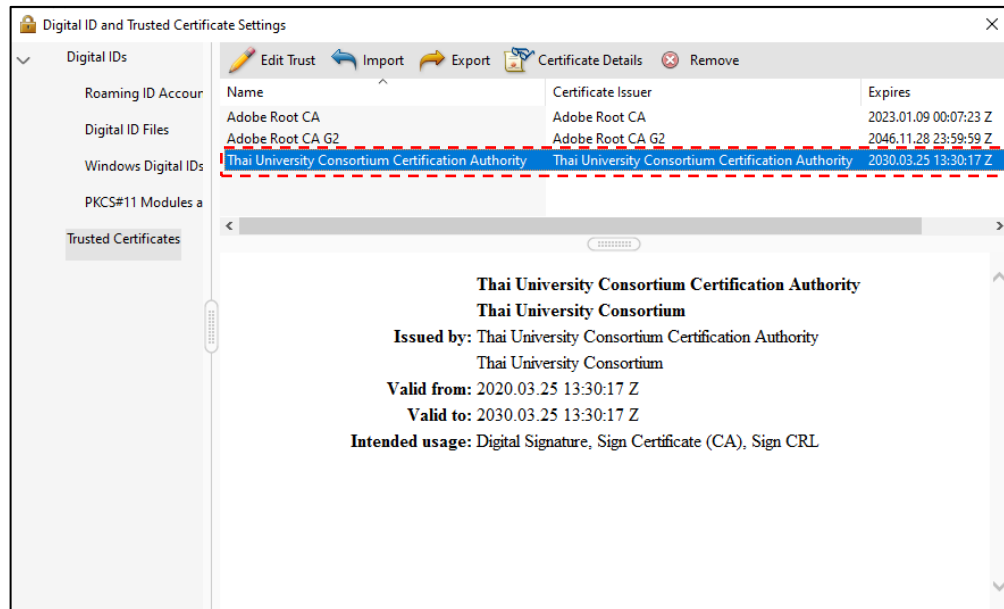
2. ปรากฏหน้าต่าง “Digital ID and Trusted Certificate Setting” ด้านซ้าย “Digital IDs” คลิก คำสั่ง “Trusted Certificates” > ด้านขวา คลิก คำสั่ง “Import” > ปรากฏหน้าต่าง “Choose Contacts to Import” > ด้านบน “Contacts” คลิกปุ่ม “Browse...”



- เลือกไฟล์เตอร์ที่เก็บ และคลิกไฟล์ “CA.crt” > คลิกปุ่ม “Open” > กลับมาที่ “Contacts” จะปรากฏรายละเอียดของไฟล์ คลิกชื่อ “Thai University Consortium Certificate Authority” > ดำเนินการต่อด้านล่าง “Certificates” ก็จะมีปรากฏและให้คลิกเลือกรายการเดียวกัน > คลิกปุ่ม “Trust ...” > ปรากฏหน้าต่าง “Import Contact Settings” > คลิก ในทุกช่องที่ยอมรับ > คลิกปุ่ม “OK” > ปรากฏหน้าต่าง “Import Complete” คลิกปุ่ม “OK”

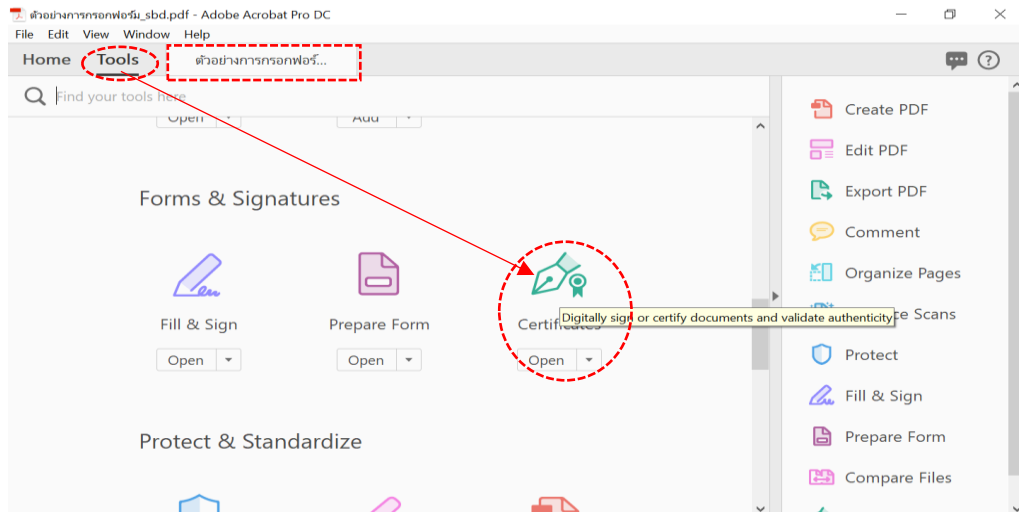


4. กลับมาที่หน้าต่าง “Digital ID and Trusted Certificate Settings” ปรากฏรายละเอียด Root CA จากไฟล์ “CA.crt” แสดงว่าเครื่องอุปกรณ์คอมพิวเตอร์และโปรแกรม Acrobat Pro DC ในเครื่องนี้รู้จักและยอมรับลายเซ็นดิจิทัลจาก มจร. ที่ผ่านการรับรองจาก “Thai University Consortium Certification Authority” แล้ว > คลิกปิดหน้าต่างและออกจากส่วนนี้ (จบเสร็จ ในส่วนของ Root CA)

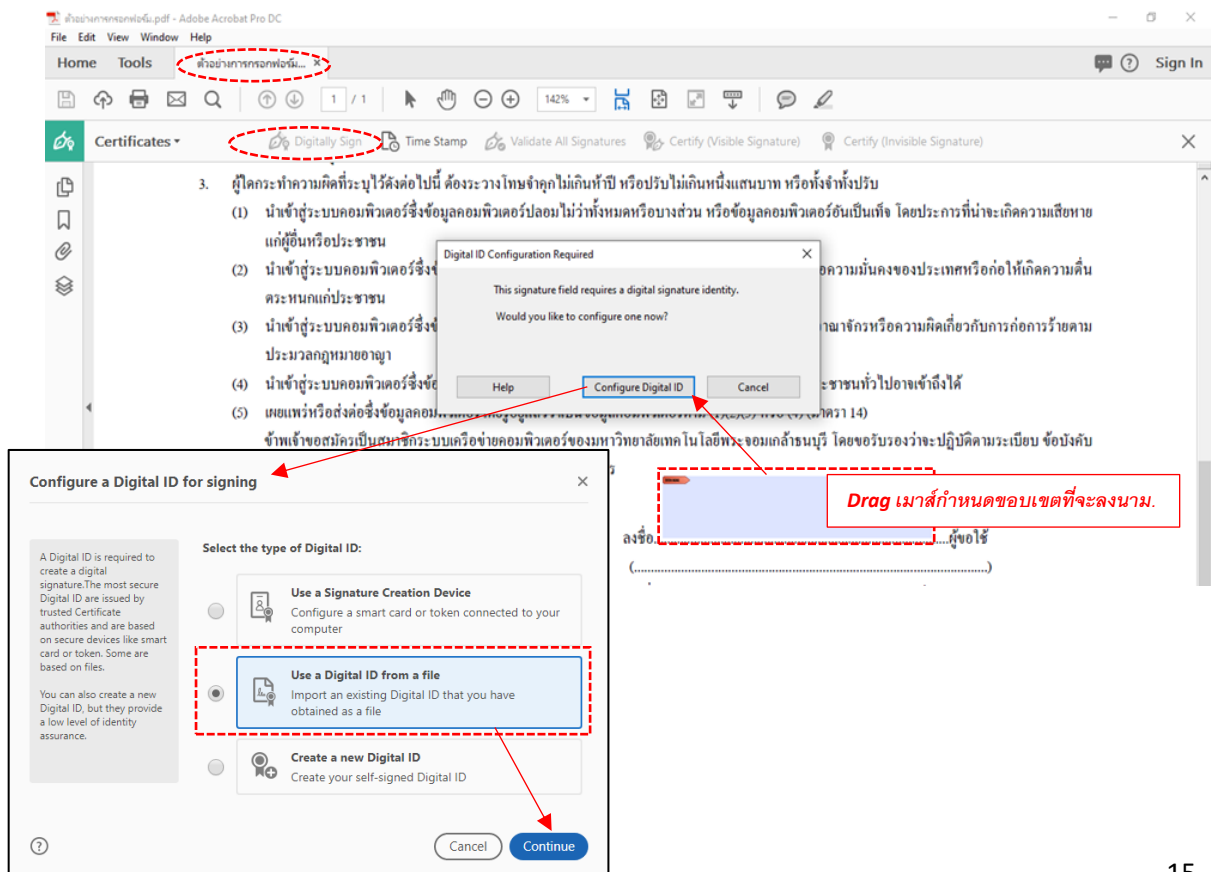


วิธีติดตั้งผู้ใช้งานเซ็นดิจิทัล (Certificate User) ไฟล์ “PKCS#12.p12”

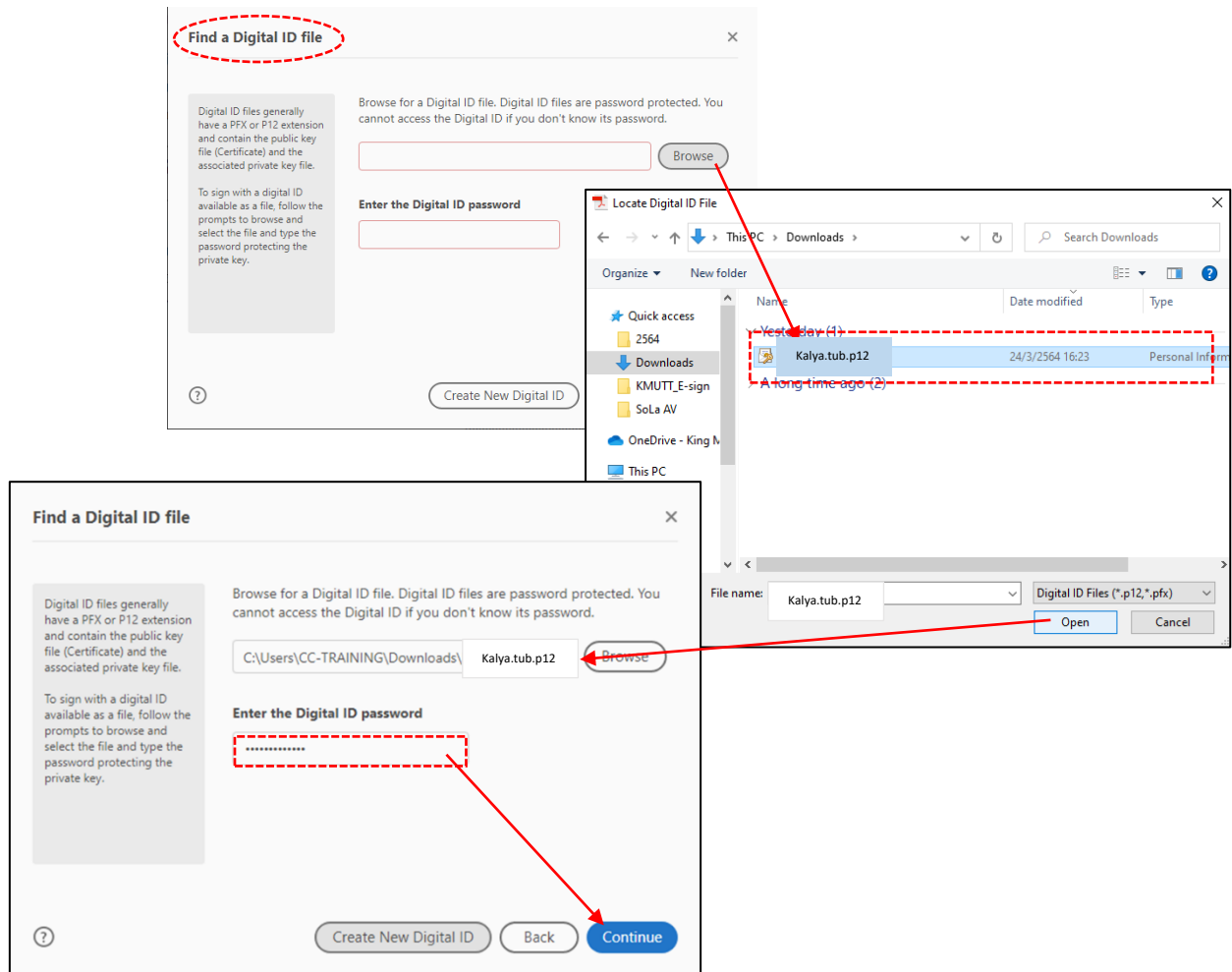
1. [ต่อกด้วย] การติดตั้ง“ผู้ใช้ใบรับรองดิจิทัล (User Certificate: PKCS#12.p12)” ด้วยไฟล์ “ชื่อLogin.p12” โดยตั้งแต่ครั้งแรก ให้เปิดไฟล์เอกสาร (.pdf) ที่ต้องการลงนาม ด้วยโปรแกรม Acrobat Pro DC > ที่แท็บ “Tools” กลุ่ม “Forms & Signatures” คลิกคำสั่ง “Certificates”



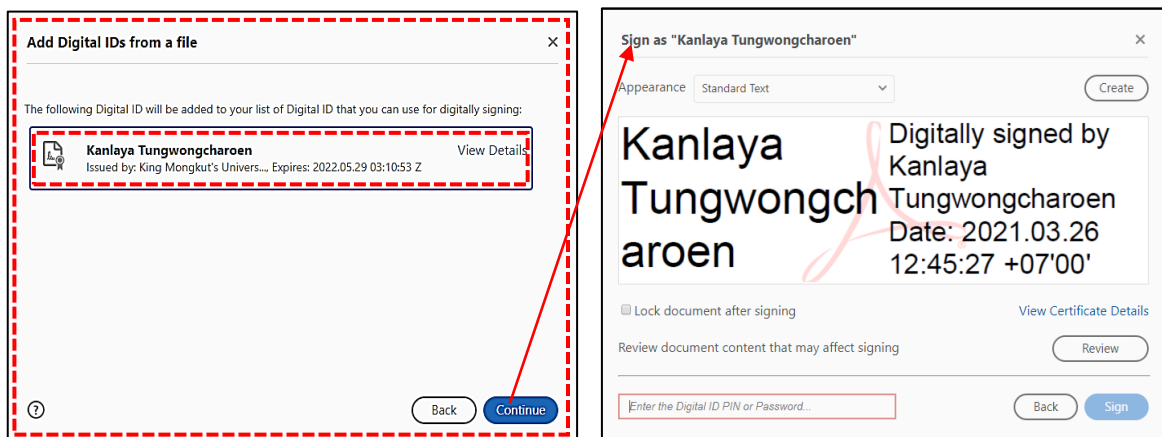
2. กลับเข้าหน้าไฟล์เอกสาร ปรากฏแถบเครื่องมือ “Certificates” คลิกคำสั่ง “Digitally Sign” > ไปตำแหน่งที่จะลงนาม โดยการ Drag เม้าส์กำหนดขอบเขต และจะปรากฏหน้าต่าง “Digital ID Configuration Required” คลิกปุ่ม “Configure Digital ID” > ปรากฏหน้าต่าง “Configure a Digital ID for signing” > คลิกเลือก “ Use a Digital ID from a file” > คลิกปุ่ม “Continue”



3. ปรากฏหน้าต่าง “Find a Digital ID file” คลิกปุ่ม “Browse” > เลือกไฟล์เดอร์ตที่เก็บ และคลิกไฟล์ “ชื่อLogin.p12” > คลิกปุ่ม “Open” > กลับมาที่หน้าต่าง “Find a Digital ID file” > ในช่อง “Enter the Digital ID password” พิมพ์ “PKCS12 Password” ที่ตั้ง/ยืนยันไว้ตอน Download ในระบบเว็บ mysign.kmutt.ac.th > คลิกปุ่ม “Continue”




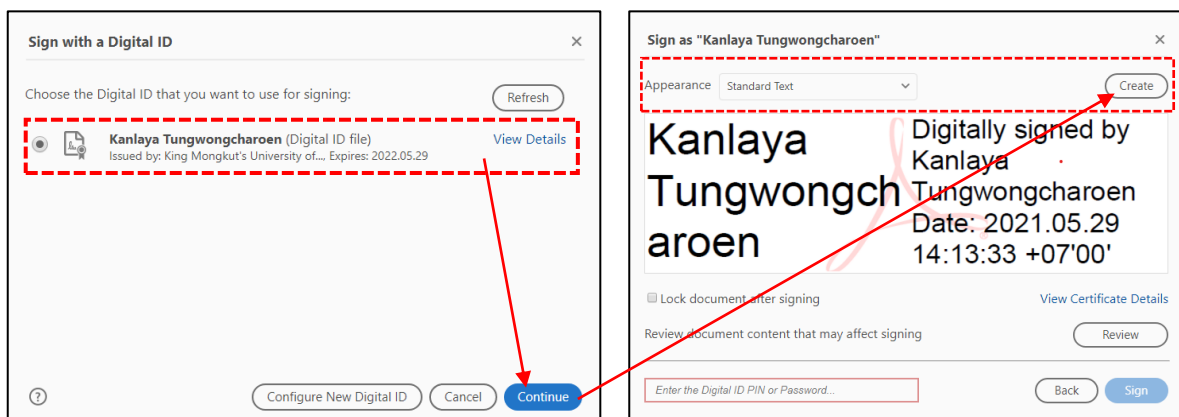
4. ปรากฏหน้าต่าง “Add Digital IDs from a file” คลิกเลือก “ชื่อ-นามสกุลของตนเอง” > คลิกปุ่ม “Continue” > ปรากฏหน้าต่าง “Sign as ชื่อ-นามสกุล เจ้าของไฟล์ (ชื่อLogin.p12)” [จบเสร็จ ในส่วนของ การติดตั้งไฟล์ “PKCS#12.p12” (ชื่อLogin.p12)]



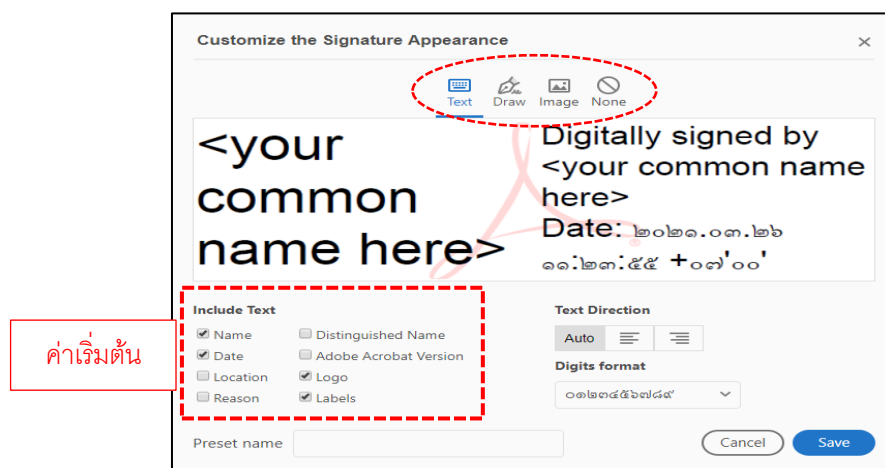
วิธีการเซ็นเอกสารด้วยลายเซ็นดิจิทัล

เมื่อติดตั้งชุดยืนยันตัวตนทั้ง 2 ส่วนแล้ว (ไฟล์ “ชื่อ Login.p12” และไฟล์ “CA.crt” ข้างต้น) สามารถทำการเซ็นไฟล์เอกสารด้วยลายเซ็นดิจิทัล ด้วยโปรแกรม Adobe Acrobat Pro DC ดังนี้

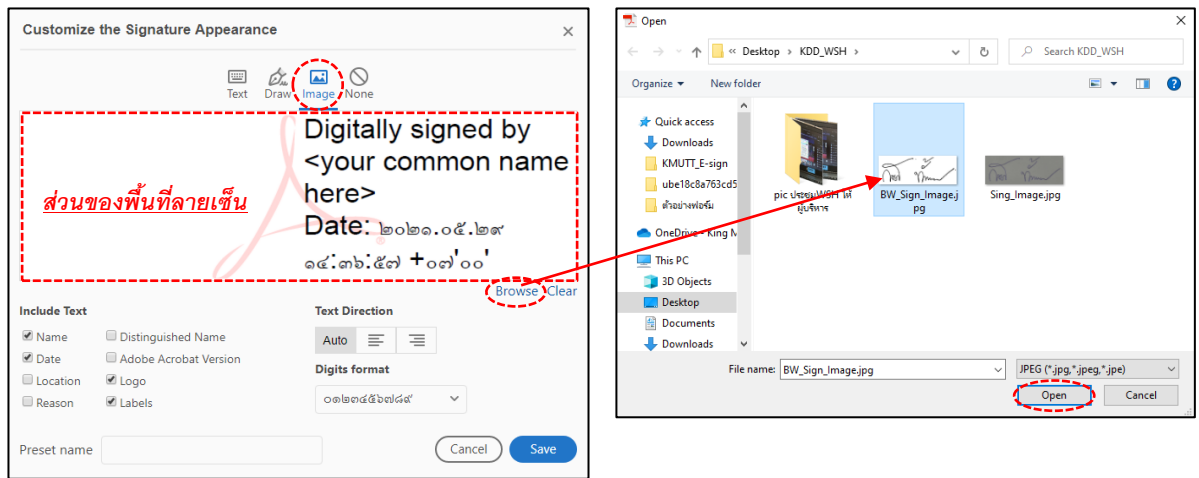
1. เปิดไฟล์เอกสาร คลิกเลือกแท็บ “Tools” กลุ่ม “Forms & Signatures” คลิกปุ่มคำสั่ง  > ปรากฏแถบเครื่องมือ “Certificates” ในหน้าเอกสาร > คลิกคำสั่ง “Digitally Sign” > ไปตำแหน่งที่จะลงนาม โดยการ Drag เมาส์กำหนดขอบเขต และจะปรากฏหน้าต่าง “Sign with a Digital ID” คลิกเลือก “ชื่อ-นามสกุล (Digital ID file)” แล้วคลิกปุ่ม “Continue” > ปรากฏหน้าต่าง “Sign as “ชื่อ-นามสกุล (Digital ID file)”” > ที่ช่อง “Appearance” แสดงชื่อ “Standard Text” (แสดงว่ายังไม่เคยใช้ลายเซ็นดิจิทัล) คลิกปุ่ม “Create”



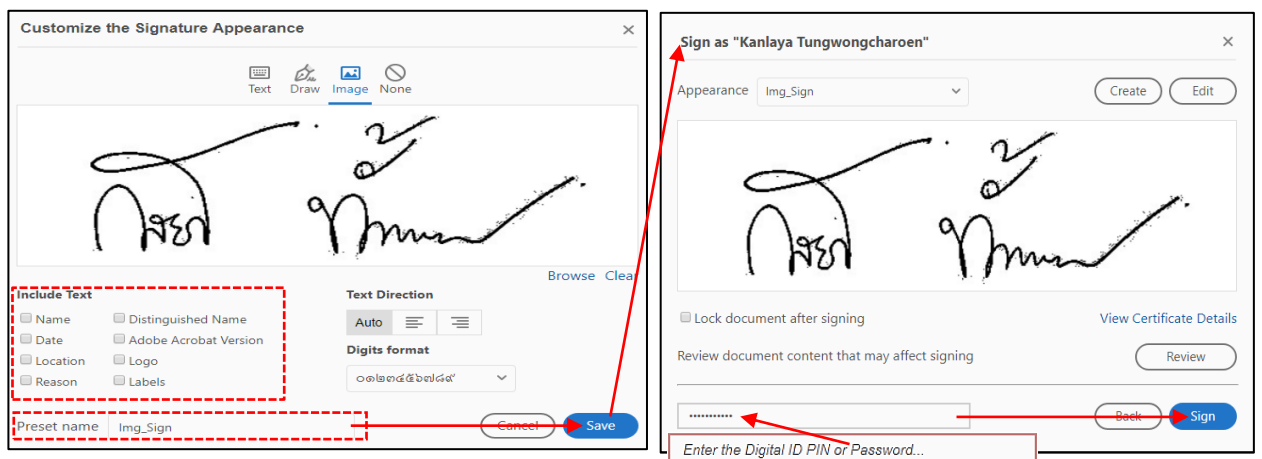
2. ปรากฏหน้าต่าง “Customize the Signature Appearance” รูปแบบของลายเซ็นดิจิทัล และค่าเริ่มต้นในส่วนของ “Include Text”



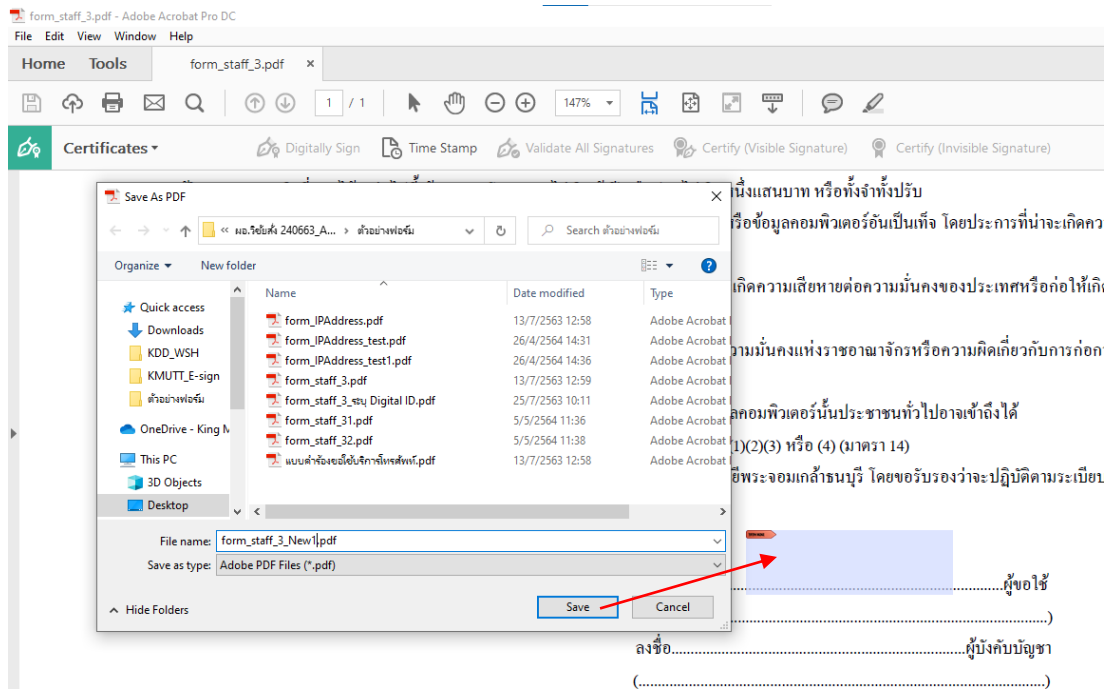
3. ในคู่มือฯ นี้ เลือกตัวอย่าง “Image” > คลิกปุ่ม “Browse” ปรากฏหน้าต่างที่เก็บและคลิก “ไฟล์ภาพลายเซ็น.jpg” > คลิกปุ่ม “Open” แล้ว “ภาพลายเซ็น” จะแสดงใน “ส่วนของพื้นที่ลายเซ็น”




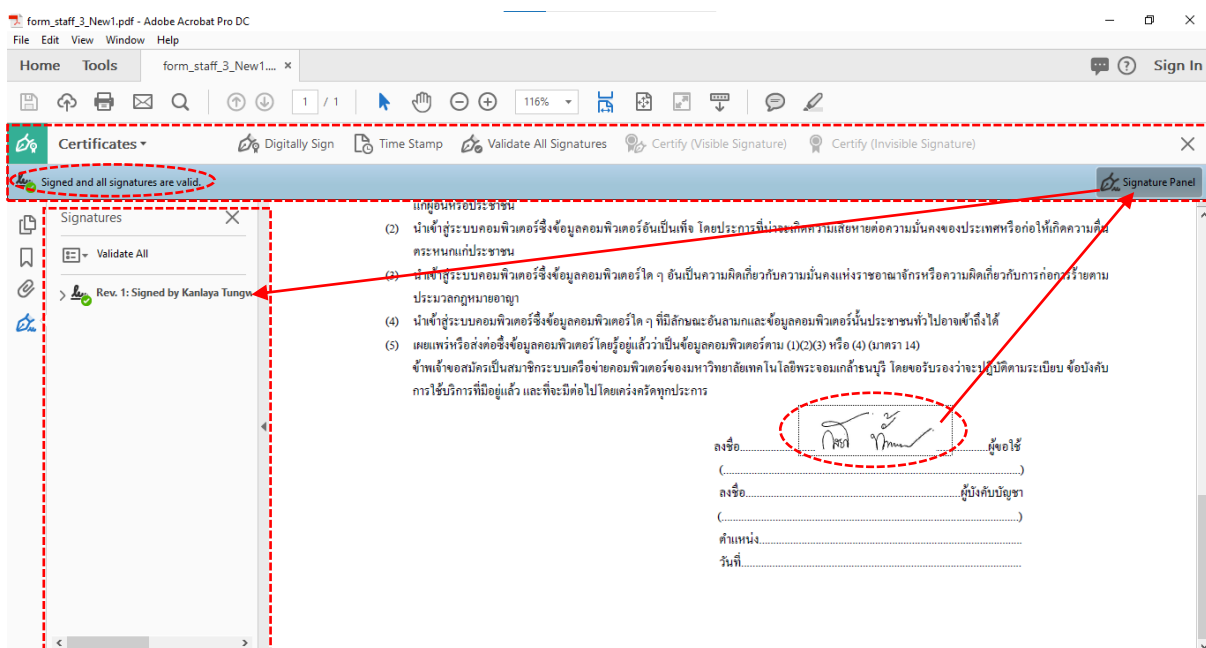
4. “Include Text” เป็นส่วนประกอบของพื้นที่เซ็น จะมีการกำหนดค่าเริ่มต้น ซึ่งถ้าต้องการให้มีเฉพาะลายเซ็น ให้คลิกเป็น (Clear ✓ ออกหมด) > “Preset name” สามารถเก็บลักษณะลายเซ็นที่สร้างด้วยรูปแบบต่าง ๆ โดยตั้งชื่อลงในช่อง เช่น ตัวอย่างนี้ตั้งชื่อว่า “Img_Sign” สำหรับค้นคืนกลับมาใช้ใหม่ได้ (ในส่วนเริ่มต้นลงลายเซ็นดิจิทัลที่ช่อง “Appearance”) > คลิกปุ่ม “Save”
5. กลับมาที่หน้าต่าง “Sign as “ชื่อ-นามสกุล (Digital ID file)” ที่แสดงลักษณะลายเซ็นที่จะใส่ลงในพื้นที่เซ็น > ในช่อง “Enter the Digital ID PIN or Password...” ให้คลิกเข้าไปในช่องและพิมพ์ “PKCS12 Password” ที่ตั้ง/ยืนยันไว้ตอน Download ในระบบเว็บ mysign.kmutt.ac.th > คลิกปุ่ม “Sign”



- กลับมาที่ไฟล์เอกสารที่กำหนดพื้นที่ลงลายเซ็น และปรากฏหน้าต่าง “Save As PDF” ให้พิมพ์ตั้งชื่อไฟล์เอกสารใหม่เพื่อป้องกันการแก้ไขเอกสารที่มีการลงลายเซ็นดิจิทัลแล้ว > คลิกปุ่ม “Save”



- ปรากฏลายเซ็นดิจิทัล (Digital Signature) ในพื้นที่ลงลายเซ็น และแถบเครื่องมือ “Certificates” > คลิกปุ่ม “Signature Panel” เพื่อแสดงรายการลงลายเซ็นดิจิทัลที่ถูกต้อง (ยืนยันตัวตนจริง) และสามารถ
ใช้ตรวจสอบความถูกต้องได้ต้องโดยสังเกตสัญลักษณ์  Signed and all signatures are valid. (ถ้าพบเป็นสัญลักษณ์อื่นต้องรีบตรวจสอบกลับทันที)



คู่มือการเซ็นและการส่งต่อเอกสารด้วยลายเซ็นดิจิทัล

ระบบ KMUTT Digital Document เป็นการปรับระบบรูปแบบการบริหารจัดการกับเอกสาร **จากเดิม**เอกสารรูปแบบกระดาษส่งต่อถึงผู้ที่เกี่ยวข้องโดยการใช้บุคคลเดินส่งต่อเอกสารและลงลายเซ็นด้วยมือ **ปรับเปลี่ยน**ให้อยู่ในรูปแบบไฟล์เอกสาร (ชื่อไฟล์.pdf) ส่งต่อไฟล์เอกสารนั้นในระบบเครือข่าย (Network) ถึงผู้ที่เกี่ยวข้องและลงลายเซ็นด้วยลายเซ็นดิจิทัล ซึ่งจะช่วยลดการใช้กระดาษ เข้ากับสถานการณ์การแพร่ระบาดของ COVID-19 ด้วยการทำงานแบบ Work From Home แต่ยังคงประสานติดต่อกันเอกสารไม่ต้องหยุดทั้งยังคงความปลอดภัย ความเชื่อมั่นถูกต้อง และการตรวจสอบกลับในไฟล์เอกสารได้ ดังตัวอย่างการดำเนินงานหลังจากได้เตรียมระบบตามวิธีการข้างต้นทั้งหมดแล้ว ดังนี้

การเซ็นแบบมี 1 ลายเซ็น

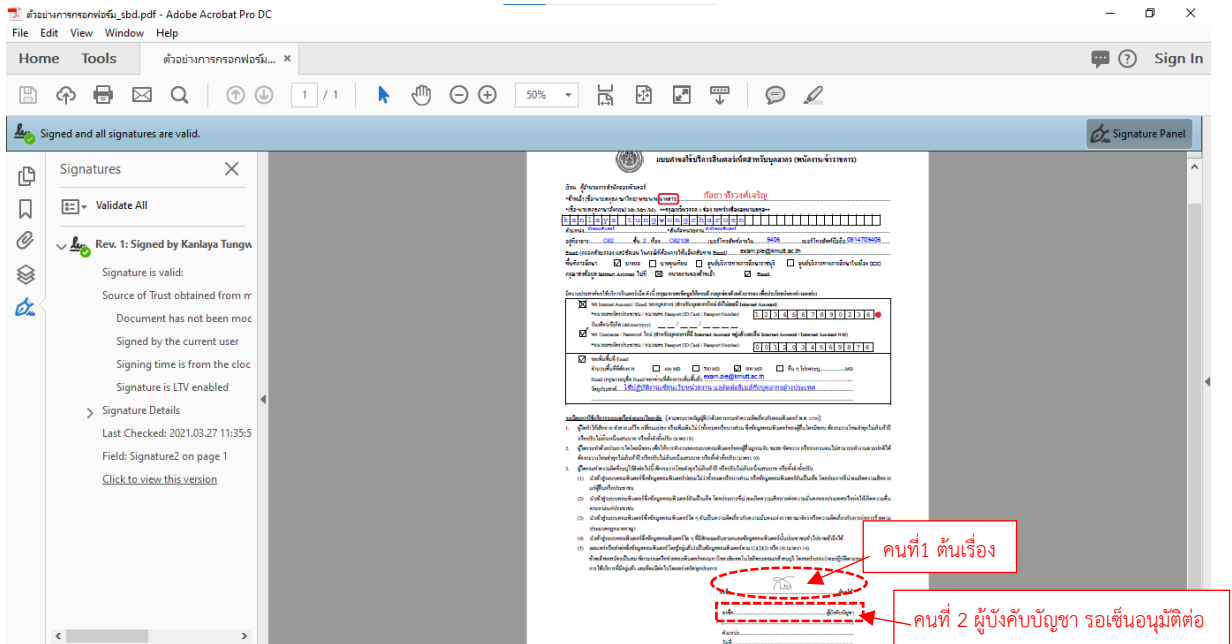
สามารถศึกษาการเซ็นแบบมี 1 ลายเซ็น ได้ที่หัวข้อ [“วิธีการเซ็นเอกสารด้วยลายเซ็นดิจิทัล”](#) ที่ [\(หน้า 17\)](#)

การเซ็นแบบมีการเซ็นต่อกันหลายคน

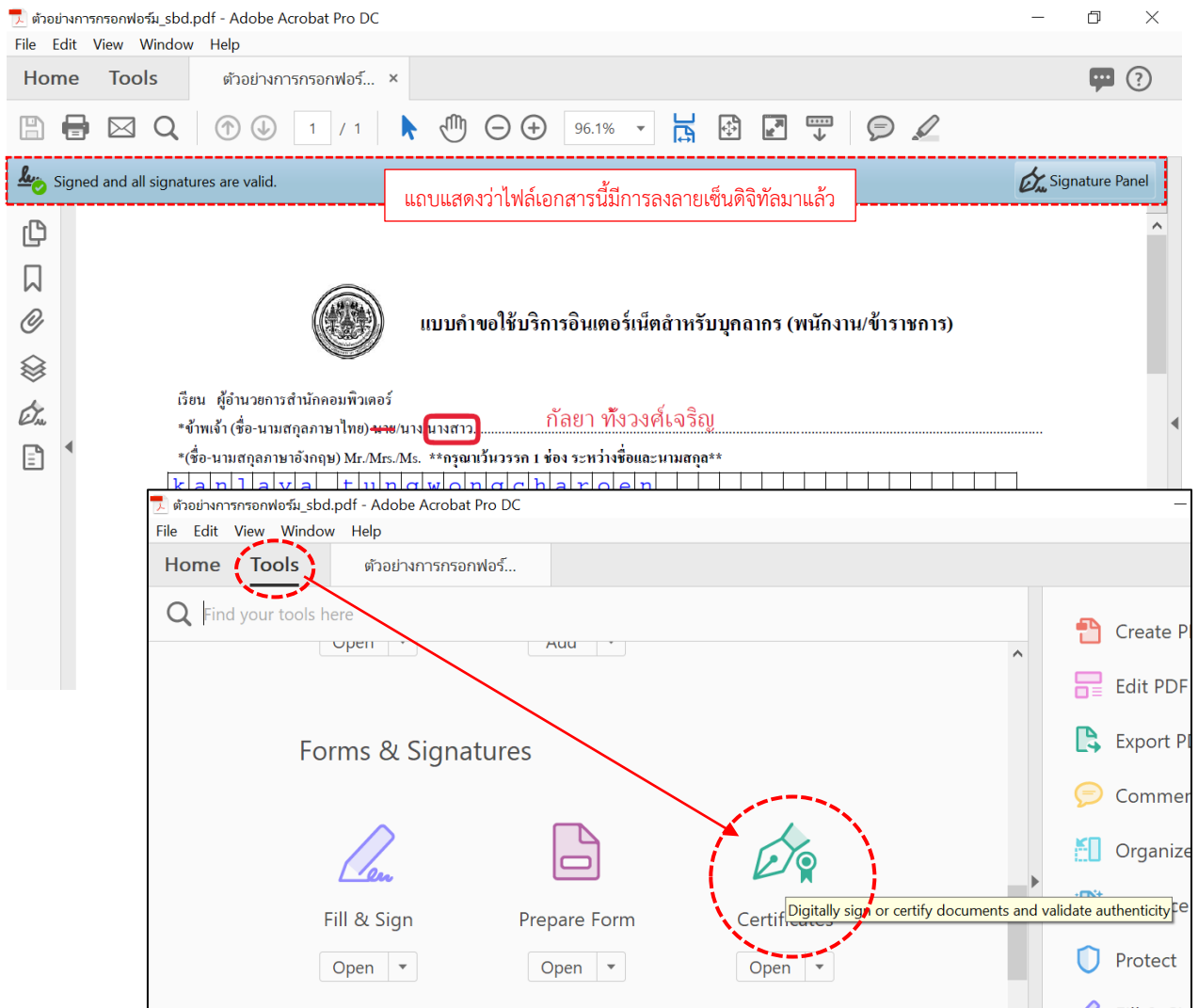
การลงนามในไฟล์เอกสารแบบมีการเซ็นต่อกันหลายคน (ภาษาราชการ เรียกว่า การเขียนหนังสือราชการ) สามารถใช้การลงนามด้วยลายเซ็นดิจิทัลได้เช่นกัน แต่มี **ข้อควรทราบ** ไว้ก่อน คือ ถ้าคนที่ 1 มีการลงลายเซ็นด้วยลายเซ็นดิจิทัล (Digital Signature) แล้ว คนรอเซ็นลำดับต่อไป จะไม่สามารถใช้วิธีการปะภาพลายเซ็นต่อได้ด้วย Tools > Forms & Signatures > Fill & Sign ดังนั้นคนต่อไป จะใช้ได้แต่การลงความคิดเห็นด้วย Tools > Review & Approve > Comment และลายเซ็นดิจิทัล (Digital Signature) เท่านั้น

วิธีการลงนามในไฟล์เอกสารแบบมีการเซ็นต่อกันหลายคน ทำดังนี้

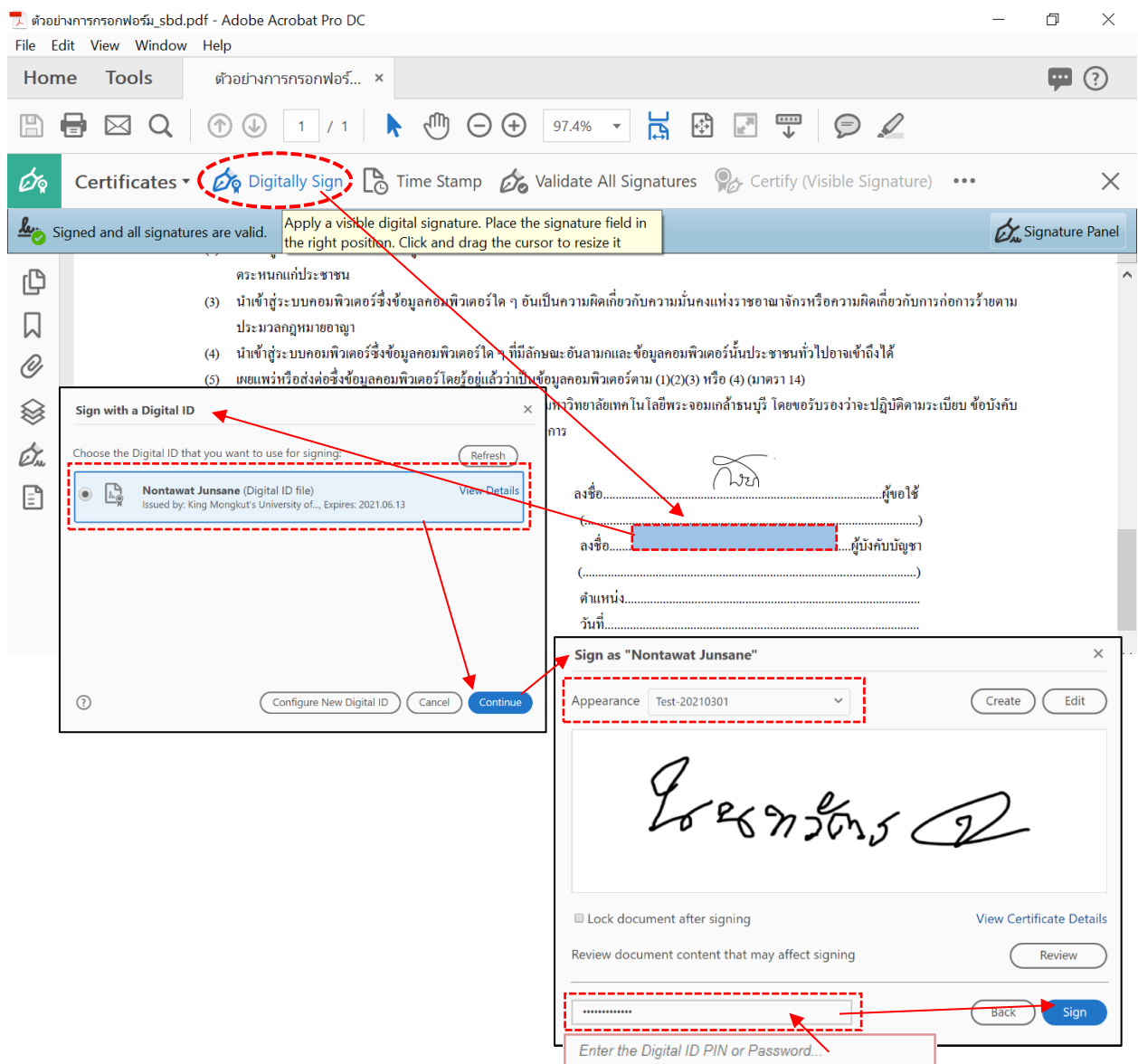
1. ไฟล์เอกสารที่ได้ลงลายเซ็นดิจิทัลจากผู้ร้องขอใช้บริการฯ (คนที่1 ต้นเรื่อง) ลงนามด้วยลายเซ็นดิจิทัลที่ได้รับการรับรองแล้ว > นำส่งต่อถึงผู้ที่เกี่ยวข้อง เช่น ต้องการให้ผู้บังคับบัญชาลงนามต่อ ก็นำไฟล์เอกสารนี้ นำส่งผ่านระบบเครือข่าย (Network) เช่น e-Mail , หรือการแชร์ไฟล์เตอร์ , ฯลฯ (ตามแต่ละหน่วยงานตกลงภายในโดยผู้บริหารสูงสุดของหน่วยงานเห็นชอบ)



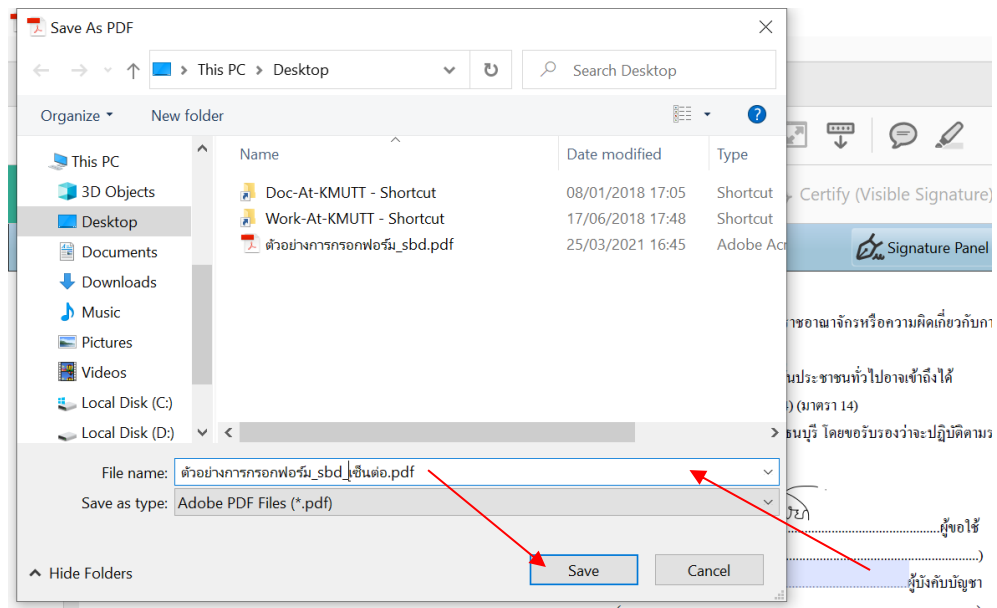
2. เมื่อผู้บังคับบัญชาได้รับและเปิดไฟล์เอกสาร จะพบว่ามีการลงนามด้วยลายเซ็นดิจิทัลมาแล้ว > เลื่อนไปยังช่วงท้ายไฟล์เอกสารหาจุดที่ผู้บังคับบัญชาต้องลงนามต่อ (คนที่ 2 หรือคนต่อไป ผู้มีสิทธิอนุมัติเบื้องต้นและระดับต่อไป) > ดำเนินการลงนามต่อด้วยลายเซ็นดิจิทัล คลิกที่แท็บ “Tools” กลุ่ม “Forms & Signatures” คลิกคำสั่ง “Certificates”



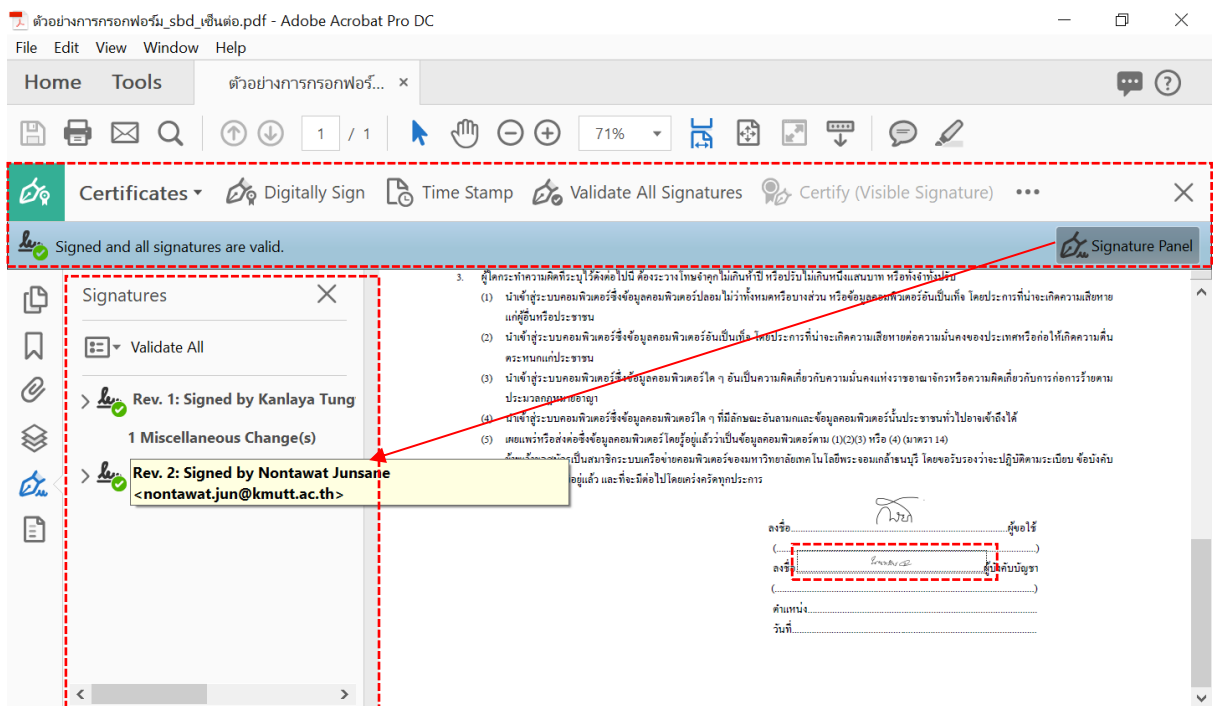
- กลับเข้าหน้าไฟล์เอกสาร ปรากฏแถบเครื่องมือของคำสั่ง “Certificates” > คลิกคำสั่ง “Digitally Sign” > Drag เม้าส์กำหนดพื้นที่ที่จะลงลายเซ็น > ปรากฏหน้าต่าง “Sign with a Digital ID” คลิกเลือก Digital ID file ที่ได้จากการติดตั้งไฟล์ยืนยันตัวตนผู้ใช้ไว้รับรอง > คลิกปุ่ม “Continue” > ปรากฏหน้าต่าง “Sign as “ชื่อ นามสกุล”” (ของผู้เซ็นที่ต้องผ่านการยืนยันเช่นข้างต้นมาก่อนแล้ว) > คลิกเลือกใช้และดูตัวอย่างรูปแบบลายเซ็นในช่อง “Appearance” > และในช่อง “Enter the Digital ID PIN or Password...” ให้คลิกเข้าไปในช่องและพิมพ์ “PKCS12 Password” ที่ตั้ง/ยืนยันไว้ตอน Download ในระบบเว็บ mysign.kmutt.ac.th > คลิกปุ่ม “Sign”



4. กลับมาที่ไฟล์เอกสารที่กำหนดพื้นที่ลงลายเซ็น และปรากฏหน้าต่าง “Save As PDF” ให้พิมพ์ตั้งชื่อไฟล์เอกสารใหม่เพื่อป้องกันการแก้ไขเอกสารที่มีการลงลายเซ็นดิจิทัลแล้ว > คลิกปุ่ม “Save”

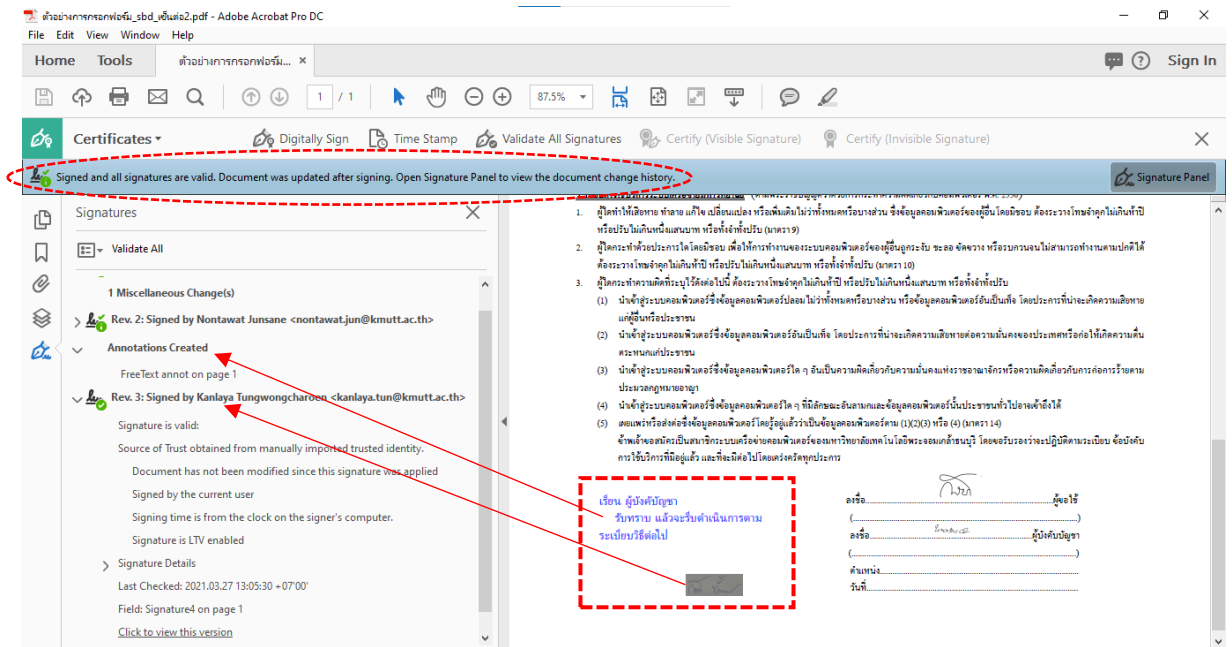


5. ปรากฏลายเซ็นดิจิทัล (Digital Signature) ในพื้นที่ลงลายเซ็น และแถบเครื่องมือ “Certificates” > คลิกปุ่ม “Signature Panel” เพื่อแสดงรายการลงลายเซ็นดิจิทัลที่ถูกต้อง (ยืนยันตัวตนจริง) และสามารถใช้ตรวจสอบความถูกต้องได้โดยสังเกตสัญลักษณ์ (ถ้าพบเป็นสัญลักษณ์อื่นต้องรีบตรวจสอบกลับทันที)

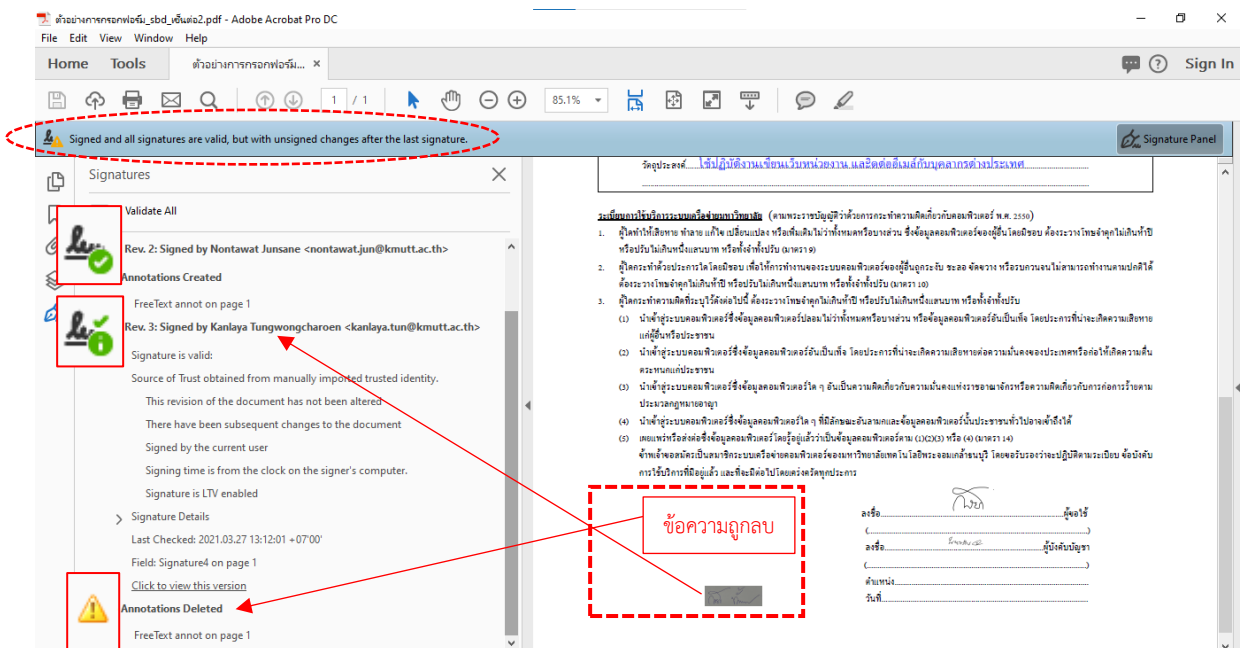


6. ตัวอย่างไฟล์เอกสารที่มีการลงลายเซ็นดิจิทัลแบบมีการเซ็นต่อกันหลายหลายคน และมีการเขียนหนังสือที่ผิดพลาด จะสามารถตรวจสอบกลับได้ที่ “Signature Panel” จะพบสัญลักษณ์ และการแจ้งข้อความเตือน ดังนี้

- ฉบับปกติ



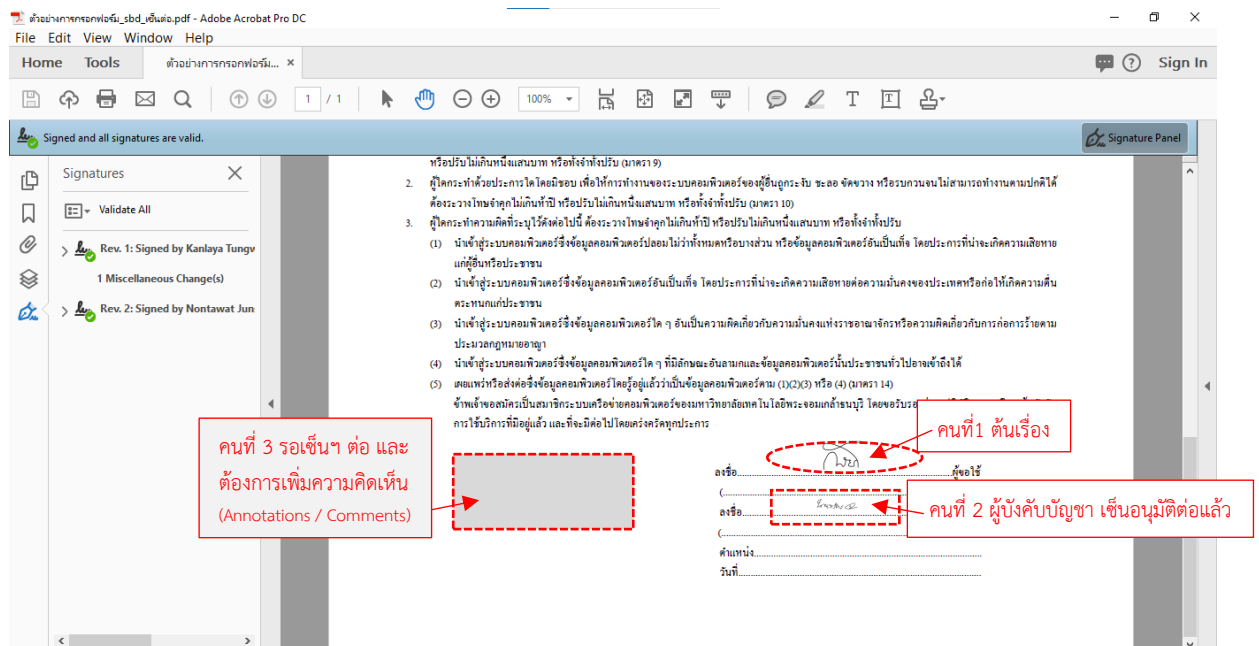
- ฉบับมีการเปลี่ยนแปลงที่ผิดพลาด ตรวจสอบกลับทันที



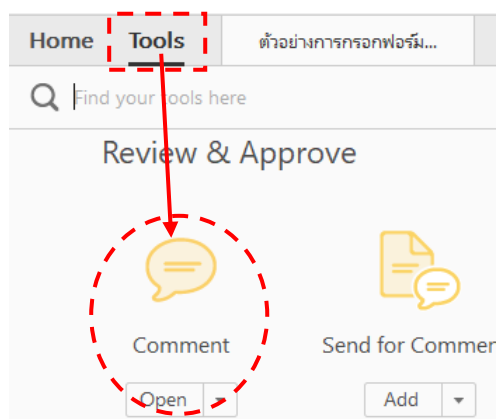
การเพิ่มความคิดเห็น (Annotations) ในเอกสารประกอบการยื่นต่อกันหลายคน

นอกจากการลงลายเซ็นดิจิทัลประกอบในไฟล์เอกสารแล้ว ยังอาจมีกรณีที่ผู้เซ็นเอกสารต่อนั้น ต้องการเพิ่มความคิดเห็น (Annotations) ลงในไฟล์เอกสาร สามารถทำได้เช่นตัวอย่าง ดังนี้

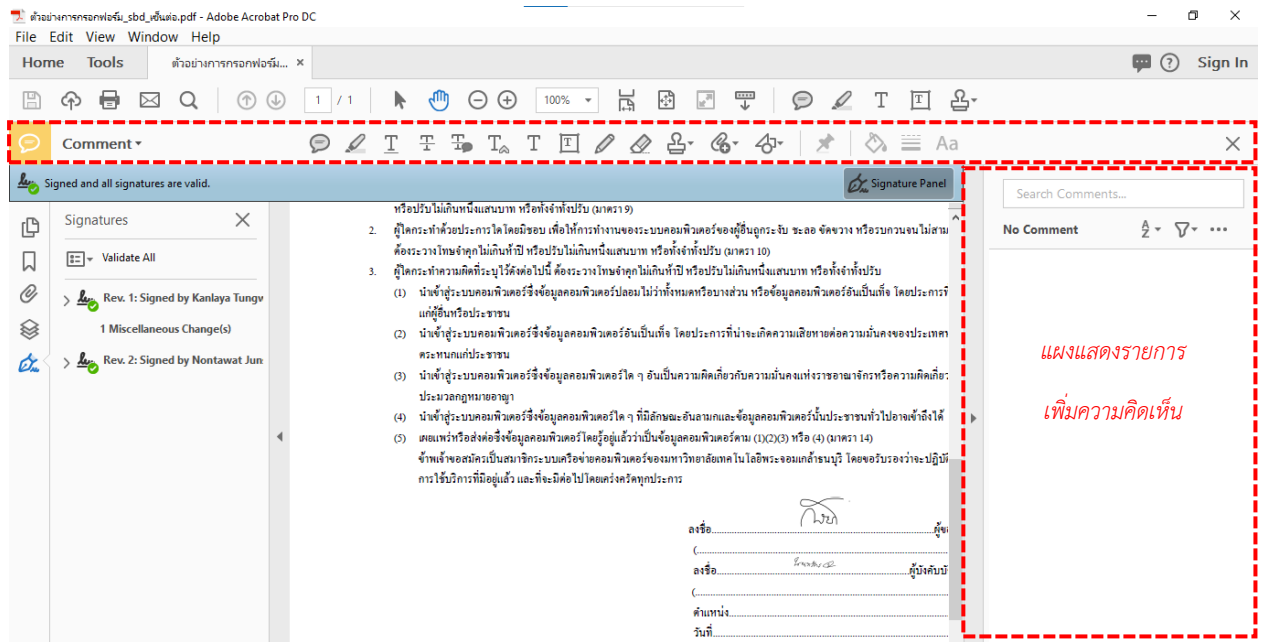
1. ไฟล์เอกสารที่ได้ลงลายเซ็นดิจิทัลจากคนที่ 1 (ต้นเรื่อง: ผู้ขอใช้) ลงนามด้วยลายเซ็นดิจิทัลที่ได้รับการรับรองแล้ว > นำส่งต่อถึงผู้ที่เกี่ยวข้อง เช่น ต้องการให้ผู้บังคับบัญชาลงนามต่อ ก็นำไฟล์เอกสารนี้ นำส่งผ่านระบบเครือข่าย (Network) เช่น e-Mail , หรือการแชร์ไฟล์เตอร์ , ฯลฯ (ตามแต่ละหน่วยงานตกลงภายในโดยผู้บริหารสูงสุดของหน่วยงานเห็นชอบ) และได้ผ่านการลงนามจากคนที่ 2 (ผู้ยื่นต่อ: ผู้บังคับบัญชา) แล้ว





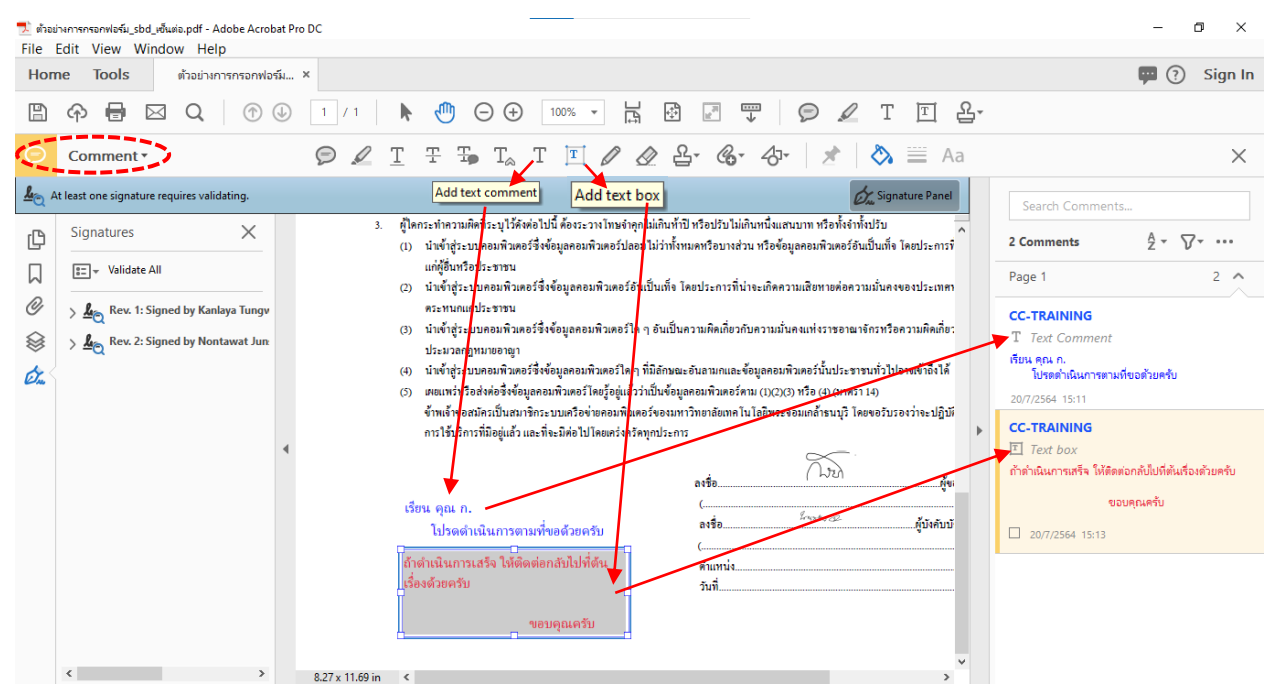
2. ถ้ายังต้องมีคนที่ 3 เซ็นฯ ต่อ และต้องการเพิ่มความคิดเห็น (Annotations) ด้วย ให้ไปที่แท็บ “Tools” > กลุ่ม “Review & Approve” > คลิกคำสั่ง “Comment”



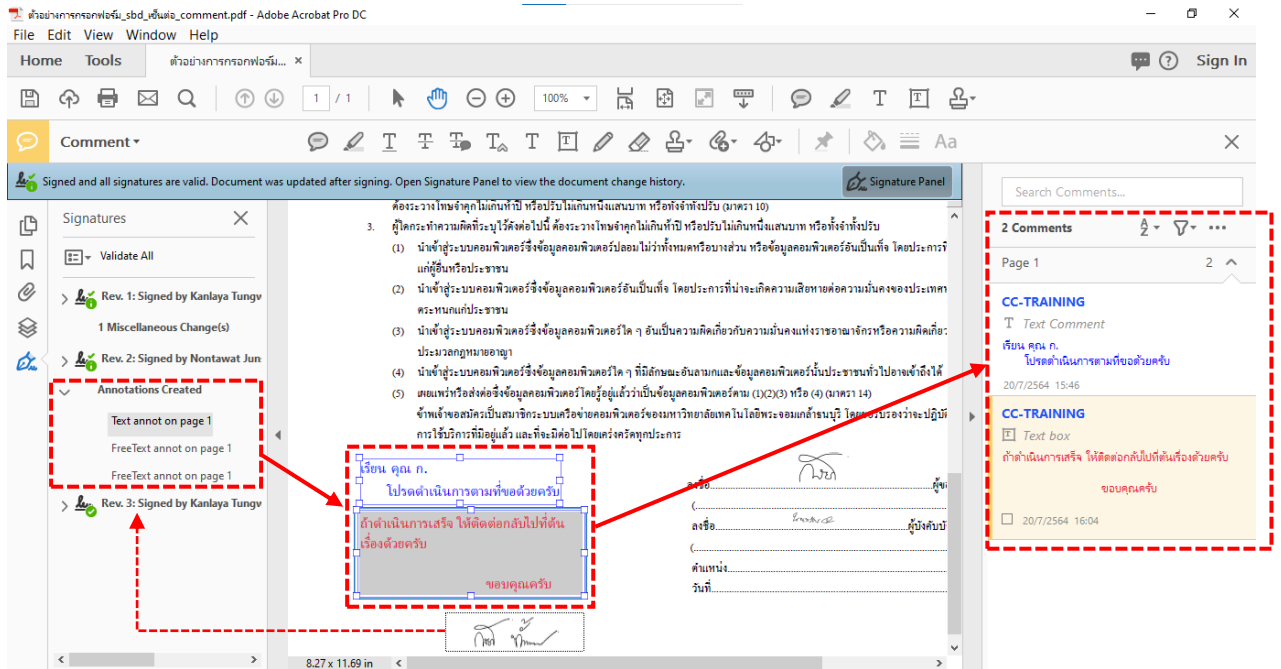
3. กลับมาที่หน้าไฟล์เอกสาร > พร้อมแถบเครื่องมือ “Comment” และแผงแสดงรายการ เพิ่มความคิดเห็น > สำหรับการเพิ่มความคิดเห็น (Annotations)



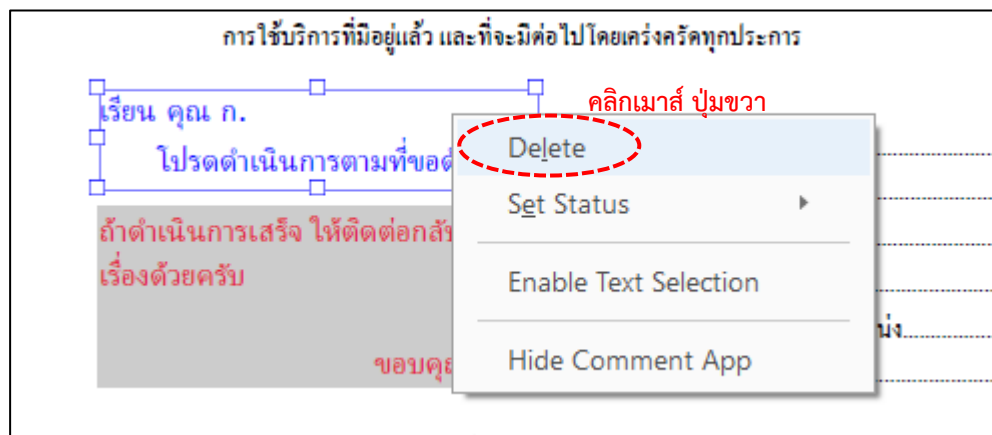
4. ที่แถบเครื่องมือ “Comment” > เลือกคลิกคำสั่ง “Add text comment  ” หรือ “Add text box  ” > คลิกกำหนดจุดตำแหน่งที่พิมพ์ข้อความ > พิมพ์ข้อความ “ความคิดเห็น” ที่ต้องการ



5. เมื่อพิมพ์ข้อความตรงจุดกำหนดตำแหน่งแล้ว > ยังปรากฏที่ “แผงแสดงรายการ เพิ่มความคิดเห็น” > และจึงดำเนินการเซ็นเอกสารด้วย “ลายเซ็นดิจิทัล” ต่อไป (ในส่วนของ แผงลายเซ็นดิจิทัล ก็แสดงลักษณะของ “ความคิดเห็น (Annotations)” ของเจ้าของลายเซ็นเช่นกัน)



6. ถ้าต้องการลบ “ความคิดเห็น” ออก > คลิกเลือก “ขอบเขตของข้อความ” หรือ “กล่องข้อความ” > กดปุ่มแป้นพิมพ์ “Delete” (หรือคลิกเมาส์ปุ่มขวา > คลิกคำสั่ง “Delete”)



การเพิกถอนลายเซ็นดิจิทัล (Revoke Digital Signature)

เมื่อต้องการยกเลิกลายเซ็นดิจิทัลที่เคยใช้ หรือมีการเปลี่ยนเครื่องคอมพิวเตอร์ จะต้องทำการยกเลิก Revoke (การเพิกถอน) ออกจากระบบ เพื่อความปลอดภัยและป้องกันการขโมยใช้งานโดยคนอื่น โดยทำ 3 ขั้นตอนหลัก ดังนี้

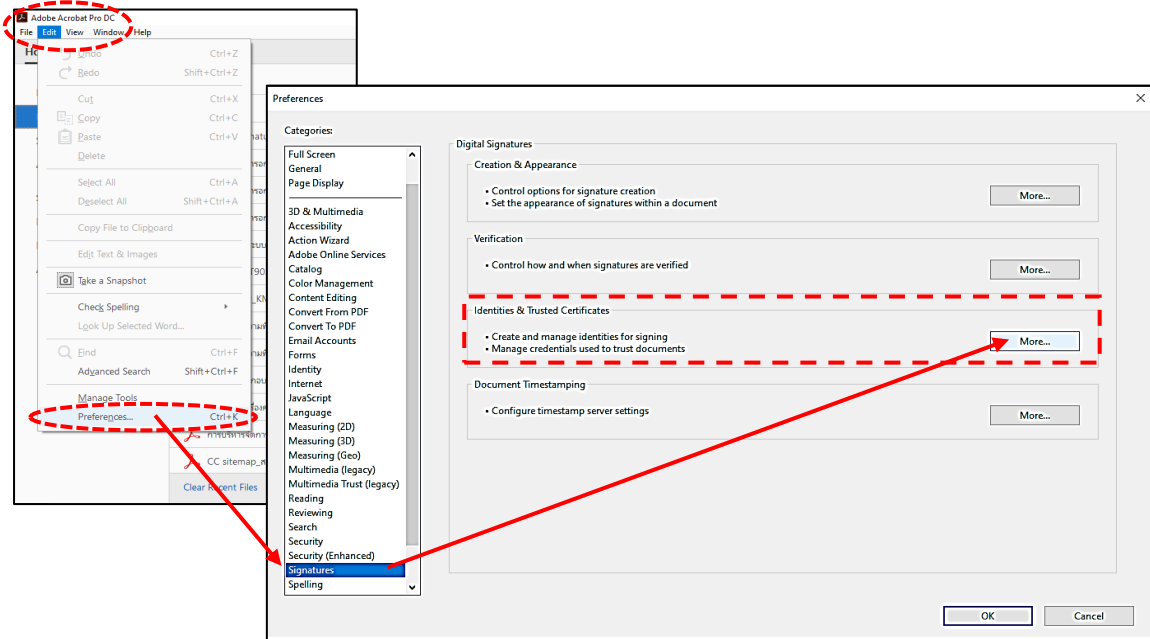
ขั้นตอนหลักที่ 1 ทำที่เว็บ Url: mysign.kmutt.ac.th

1. เข้าเว็บ Url: <https://mysign.kmutt.ac.th> > ที่แท็บ “User Certificate” คลิกปุ่ม “Show More Certificate Types and Advanced Actions” > ปรากฏรายการเพิ่ม ทำที่ “Certificate Revoke” > คลิกปุ่ม “Revoke My Certificate” > เสร็จขั้นตอนหลักที่ 1

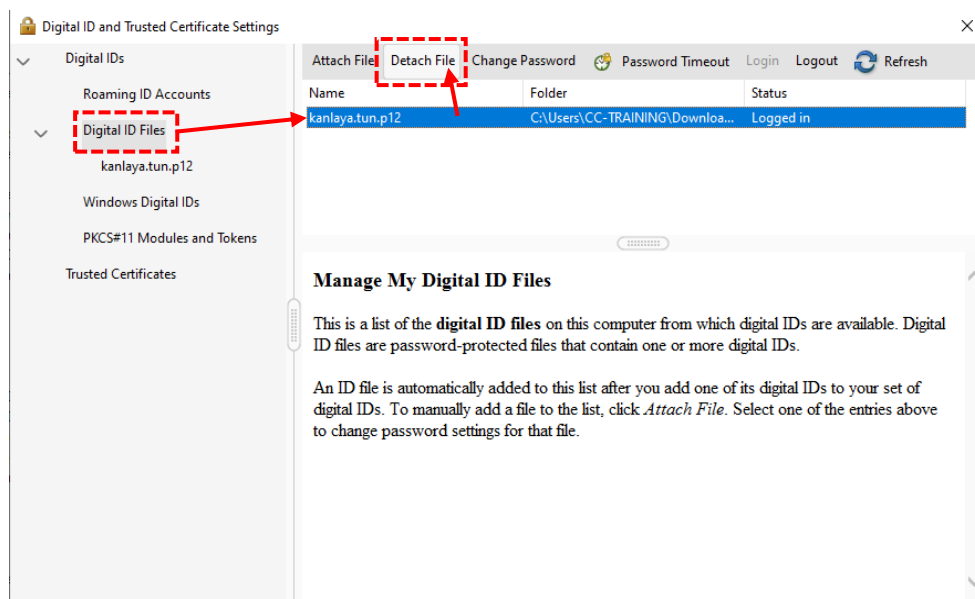
The screenshot shows the 'User Certificate and Private Key In PKCS #12 Format' section of the KMUTT My Signature website. The user is Kanlaya Tungwongcharoen. The interface includes a 'Show More Certificate Types and Advanced Actions' button, which is highlighted with a red dashed box. Below this, there are three main sections: 'User Certificate', 'User Private Key', and 'Certificate Revoke'. The 'User Certificate' section shows the user's name, SHA-1 and SHA-256 fingerprints, and validity dates, with a 'Download Certificate' button. The 'User Private Key' section contains a warning: 'This file contains your private key which is sensitive information, Do not lose or expose this file to public.' and a 'Download Private Key' button. The 'Certificate Revoke' section, also highlighted with a red dashed box, contains a warning: 'This will revoke your current private key / certificate. Use with caution. Your existing certificate will not be able to signed new documents.' and a 'Revoke My Certificate' button, which is circled in red.

ขั้นตอนหลักที่ 2 ทำที่โปรแกรม Adobe Acrobat Pro DC

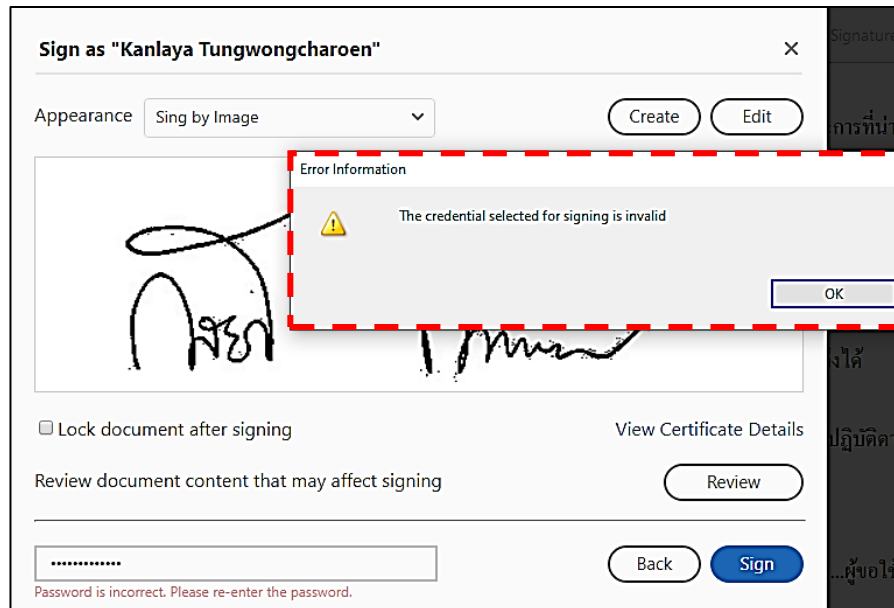
1. เปิดโปรแกรม Adobe Acrobat Pro DC > เมนู “Edit” คลิกคำสั่ง “Preferences...” > ปรากฏหน้าต่าง “Preferences” ด้านซ้าย “Categories:” > เลือกคลิกคำสั่ง “Signatures” > ด้านขวาช่อง “Digital Signatures” > ส่วน “Identities & Trusted Certificates” คลิกที่ปุ่ม “More”



2. ปรากฏหน้าต่าง “Digital ID and Trusted Certificate Setting” ด้านซ้าย “Digital IDs” คลิกคำสั่ง “Digital ID Files” > ย้ายไปด้านขวา คลิกเลือกไฟล์ “Login.p12” > คลิกคำสั่ง “Detach File” > ไฟล์ “Login.p12” จะถูกลบหายไป

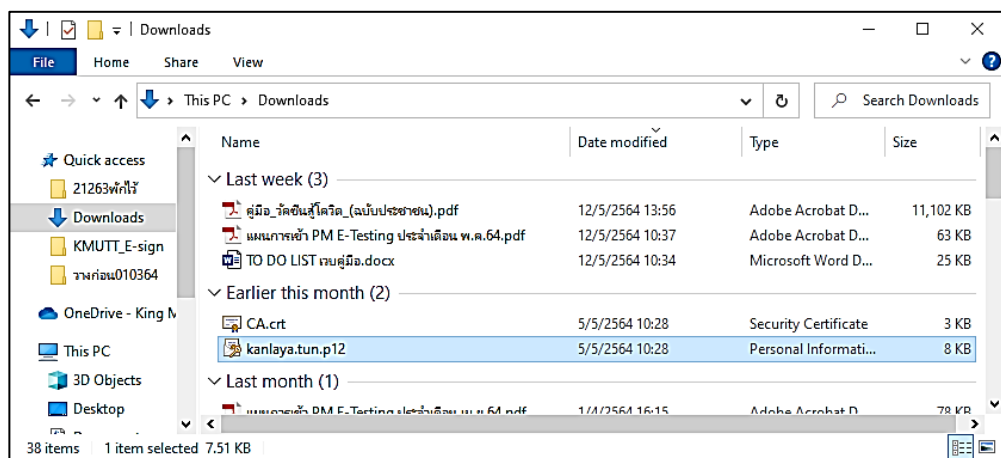


- เมื่อจะมีการลงลายเซ็นดิจิทัล ผลที่ได้หลัง Revoke ลายเซ็นดิจิทัล > ปรากฏหน้าต่าง “Error Information”



ขั้นตอนหลักที่ 3 ทำที่โฟลเดอร์จัดเก็บไฟล์ “Login.p12”

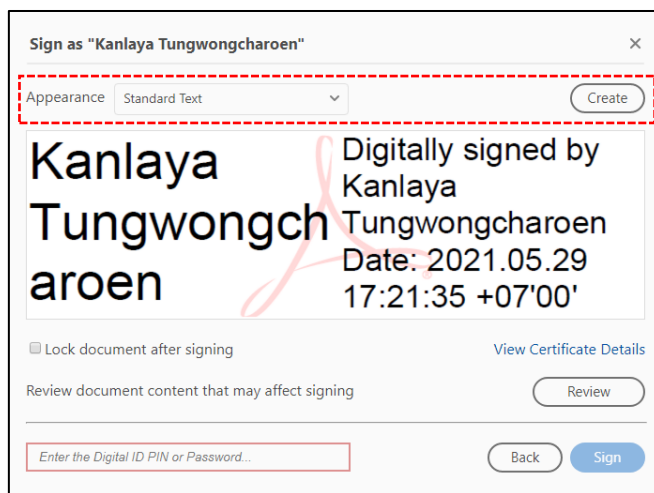
- เปิดโฟลเดอร์ที่จัดเก็บ คลิกไฟล์ “Login.p12” > กดแป้นพิมพ์ “Delete” ลบไฟล์ (เพื่อป้องกันการลบส่น ถ้ามีการสร้างคีย์ส่วนตัว (Private Key) ไฟล์ “PKCS#12.p12” ขึ้นใหม่ ส่วนไฟล์ CA.crt จะลบออกหรือไม่ก็ได้ แนะนำว่าควรลบออก)



- ข้อควรทราบ ลายเซ็นดิจิทัล กับรูปลักษณะลายเซ็นต่างๆ ที่สร้างไว้ใน Adobe Acrobat Pro DC คือ คนละเรื่องกัน นั่นคือ เมื่อลบไฟล์ “ไฟล์ชื่อ.p12” รูปลักษณะลายเซ็นยังอยู่และนำกลับมาใช้ได้ แต่จะไม่ได้รับการรองรับ เมื่อมีการใช้ลายเซ็นดิจิทัลจะเกิด Error

การสร้างภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัล

การสร้างลายเซ็นที่ใช้เป็นลายเซ็นดิจิทัล ด้วยโปรแกรม Adobe Acrobat Pro DC ทำในขั้นตอนหลังจากเปิดไฟล์เอกสารแล้ว เลือกใช้ Tools > Forms & Signatures > Certificates และใช้คำสั่ง “Digitally Sign” พร้อม Drag เม้าส์กำหนดพื้นที่ลงลายเซ็น ปรากฏหน้าต่าง “Sign as “ชื่อ-นามสกุล(Digital ID file)” > ที่ช่อง “Appearance” แสดงชื่อ “Standard Text” (แสดงว่ายังไม่เคยใช้ลายเซ็นดิจิทัล หรือชื่ออื่นที่เคยเปิดใช้ไว้ก่อนหน้าแล้ว) คลิกปุ่ม “Create” คือ ส่วนออกแบบหรือเลือกใช้รูปแบบของลายเซ็น ที่บุคลากร มจร. จะเลือกใช้เป็นลายเซ็นดิจิทัล (Digital Signature) ดังนี้



1. คลิกปุ่ม “Create” > ปรากฏหน้าต่าง “Customize the Signature Appearance” รูปแบบของลายเซ็นดิจิทัล สามารถเลือกสร้างได้ 3 แบบ ได้แก่
 - a. Text คือ ลายเซ็นแบบตัวอักษรพิมพ์ โดยนำข้อมูลชื่อ นามสกุล จากไฟล์ (ชื่อLogin.p12) มาแสดงเป็นค่า Default ที่ปรากฏเมื่อยังไม่เคยมีการเรียกใช้ลายเซ็นแบบอื่นมาก่อน
 - b. Draw คือ การใช้เมาส์หรืออุปกรณ์เขียน (Stylus pens) วาดลายเซ็น เหมือนการเซ็นเอกสารสดอย่างที่เคยปฏิบัติ
 - c. Image คือ การนำเข้าลายเซ็น ที่เกิดจากถ่ายภาพหรือสแกนเก็บเป็นไฟล์รูปภาพไว้
 - d. None คือ ระบบจะจัดการลงข้อมูล ขึ้นคำว่า “Digitally signed by <your common name here>”



ขออธิบายการสร้างภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัล 2 วิธี คือ การ Draw และการ Image ดังนี้

การสร้างภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัลด้วยการ “Draw”

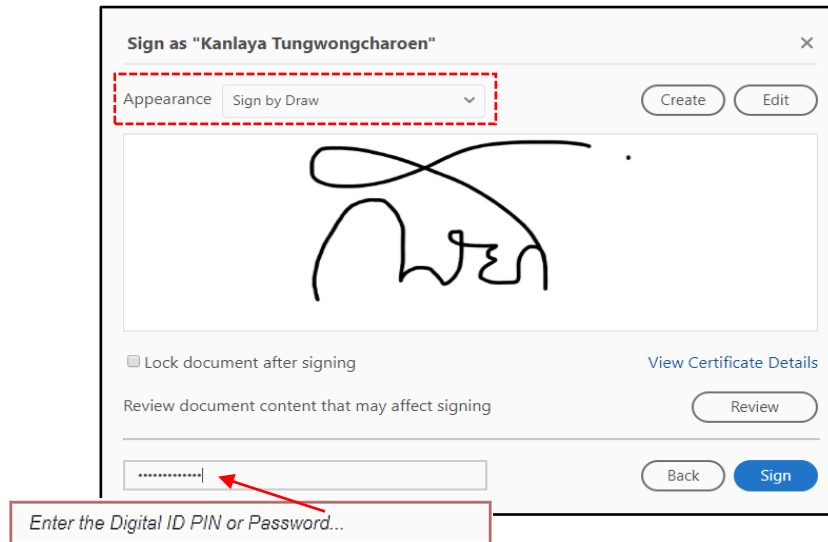
1. ที่หน้าต่าง “Customize the Signature Appearance” เลือกคลิก “Draw” > คลิกคำสั่ง “Click here to Draw” ปรากฏหน้าต่างพื้นที่วาดลายเซ็น > ใช้เมาส์หรืออุปกรณ์เขียน (Stylus pens) วาดลายเซ็นเหมือนการเซ็นเอกสารสต่ออย่างที่เคยปฏิบัติ > คลิกปุ่ม “Apply” (ถ้าวาดแล้วไม่ถูกใจ สามารถลบได้โดยคลิกปุ่ม “Clear” แล้ววาดใหม่)



2. รูปวาดลายเซ็นจะปรากฏพื้นที่แสดงลายเซ็น > ถัดมา ในส่วนประกอบของพื้นที่เซ็น “Include Text” จะมีค่าที่กำหนดเป็นค่าเริ่มต้นไว้ ซึ่งถ้าต้องการให้มีเฉพาะลายเซ็นที่เป็นชื่อที่วาด ให้คลิกเป็น (Clear ✓ ออกหมด) > ส่วนในช่อง “Preset name” สำหรับเก็บลักษณะลายเซ็นนี้ไว้สำหรับค้นคืนกลับมาใช้ใหม่ได้ เช่น ตัวอย่างนี้ตั้งชื่อเป็น “Sign by Draw” > คลิกปุ่ม “Save”

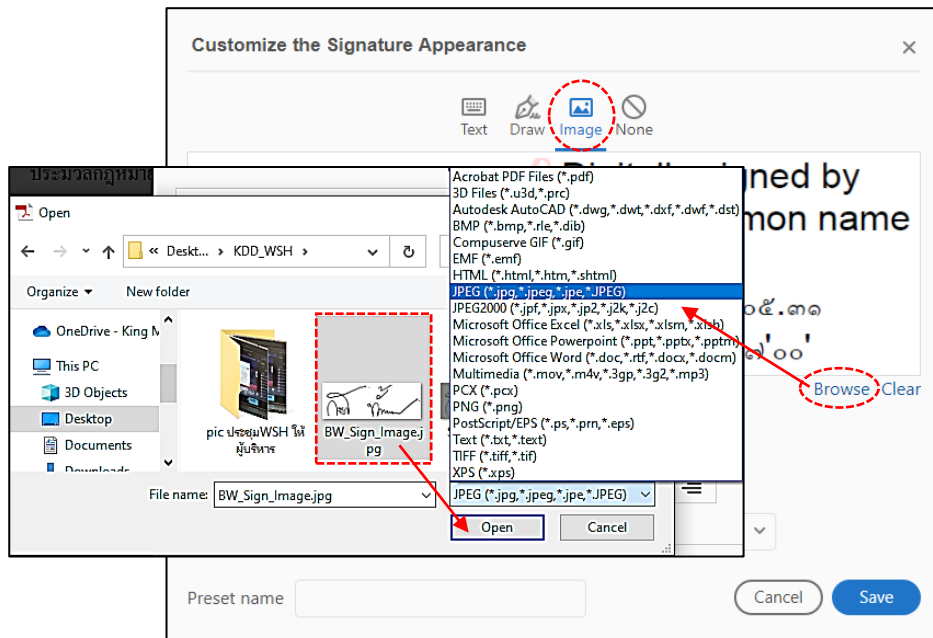


3. กลับมาหน้าต่าง “Sign as “ชื่อ-นามสกุล(Digital ID file)”” > ที่ช่อง “Appearance” แสดงชื่อตั้งไว้เอง “Sign by Draw” และแสดงลักษณะลายเซ็นที่จะใส่ลงในพื้นที่เซ็น > ในส่วน “Enter the Digital ID PIN or Password...” ให้คลิกเข้าไปในช่องและพิมพ์ “PKCS12 Password” ที่ตั้ง/ยืนยันไว้ตอน Download ในระบบเว็บ mysign.kmutt.ac.th > คลิกปุ่ม “Sign” ลายเซ็นก็จะถูกนำไปแสดงในหน้าไฟล์เอกสารพร้อมให้ Save as เป็นไฟล์ใหม่

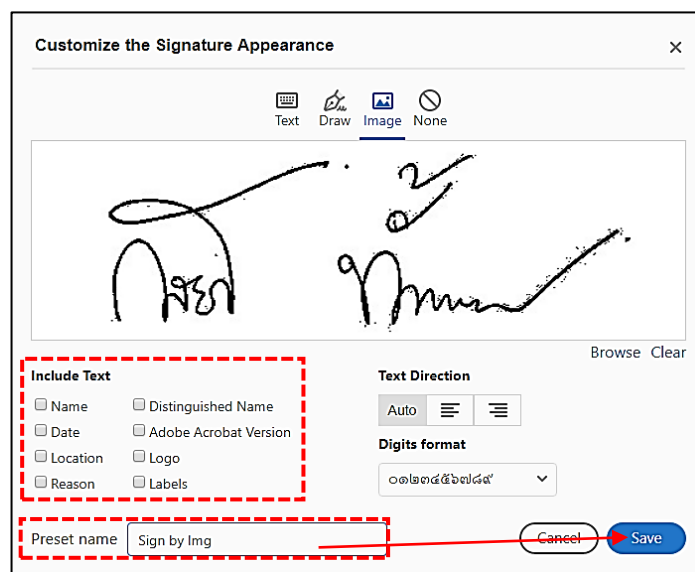


การนำเข้าและสร้างไฟล์ภาพลายเซ็นเก็บไว้เรียกใช้เป็นลายเซ็นดิจิทัลด้วยการ “Image”

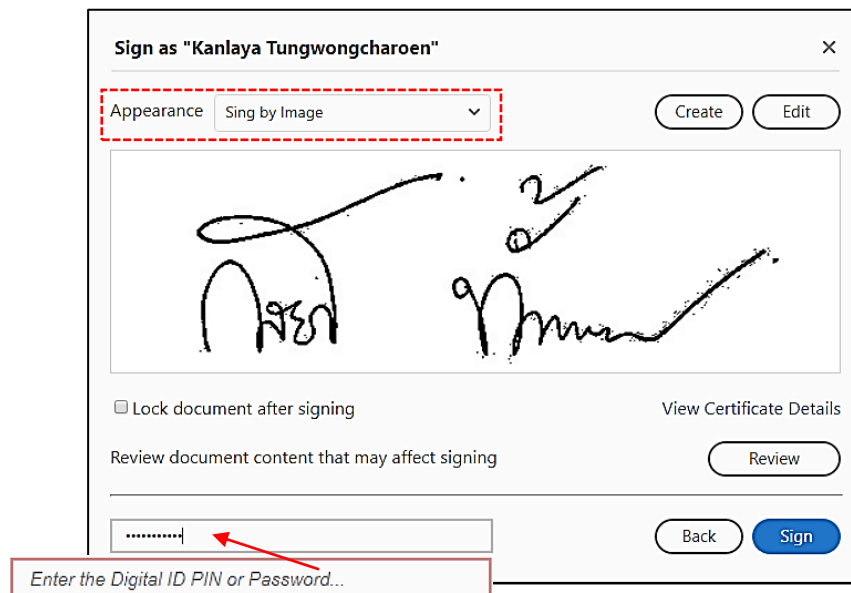
1. ที่หน้าต่าง “Customize the Signature Appearance” เลือกคลิก “Image” > คลิกคำสั่ง “Browse” ปรากฏหน้าต่างไฟล์เดสก์ทอปที่เก็บไฟล์ภาพลายเซ็น > คลิกเลือกไฟล์ภาพลายเซ็น > คลิกปุ่ม “Open” (ถ้าไฟล์ภาพแสดงแล้วไม่ถูกใจ สามารถลบได้โดย คลิกปุ่ม “Clear” แล้วเปิดเลือกไฟล์ภาพใหม่)



2. ไฟล์รูปภาพลายเซ็นจะปรากฏพื้นที่แสดงลายเซ็น > ถัดมา ในส่วนประกอบของพื้นที่เซ็น “Include Text” จะมีค่าที่กำหนดเป็นค่าเริ่มต้นไว้ ซึ่งถ้าต้องการให้มีเฉพาะลายเซ็นที่มาจากไฟล์รูปภาพ ให้คลิกเป็น (Clear ✓ ออกหมด) > ส่วนในช่อง “Preset name” สำหรับเก็บลักษณะลายเซ็นนี้ไว้สำหรับค้นคืนกลับมาใช้ใหม่ได้ เช่น ตัวอย่างนี้ตั้งชื่อเป็น “Sign by lmg” > คลิกปุ่ม “Save”



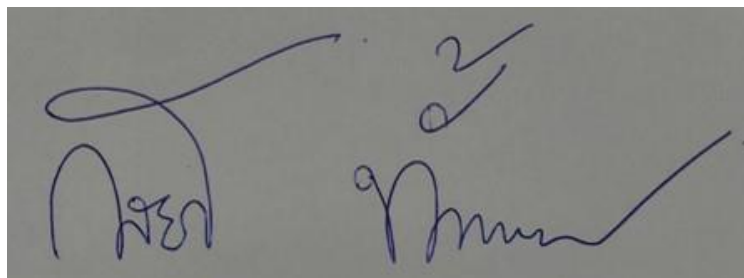
3. กลับมาหน้าต่าง “Sign as “ชื่อ-นามสกุล(Digital ID file)”” > ที่ช่อง “Appearance” แสดงชื่อตั้งไว้เอง “Sign by Image” และแสดงลักษณะลายเซ็นที่จะใส่ลงในพื้นที่เซ็น > ในส่วน “Enter the Digital ID PIN or Password...” ให้คลิกเข้าไปในช่องและพิมพ์ “PKCS12 Password” ที่ตั้ง/ยืนยันไว้ตอน Download ในระบบเว็บ mysign.kmutt.ac.th > คลิกปุ่ม “Sign” ลายเซ็นก็จะถูกนำไปแสดงในหน้าไฟล์เอกสารพร้อมให้ Save as เป็นไฟล์ใหม่



(จากตัวอย่างที่ หน้า 18)

การสร้างไฟล์ภาพลายเซ็นขาวดำให้เข้ากับหน้าเอกสารในไฟล์เอกสาร .pdf

1. จรดปากกาเขียนลายเซ็นขนาดปกติ-ใหญ่กว่าเล็กน้อย ในกระดาษเปล่าสีขาว > ใช้กล้องถ่ายภาพลายเซ็นนี้ให้ชัดเจน หรือ สแกน-ตัดภาพลายเซ็นเก็บเป็นไฟล์ > โหลดเข้าเก็บในเครื่องคอมพิวเตอร์ ตัวอย่าง เป็นการถ่ายด้วยกล้องสมาร์ทโฟนปกติ ได้เป็นไฟล์ .jpg พบว่าลายเซ็นปากกาหมึกสีน้ำเงิน และพื้นกระดาษสีขาวจะเพี้ยนเป็นสีเทาที่บ



Tip: ไฟล์รูปภาพลายเซ็นที่สร้างด้วยวิธีการต่างๆ สามารถนำมาปรับด้วยโปรแกรมตกแต่งภาพได้ เพื่อให้ได้ไฟล์ที่นำไปใช้แล้วไม่เกิดปัญหารอยภาพแตก ไม่คมชัด โดยควรปรับค่าที่เกี่ยวข้องให้มีค่าไม่น้อยกว่าดังนี้

ขนาดของภาพ กว้าง (Width) X สูง (Height) : 500 pixels X 500 pixels

หน่วยเป็น “เซนติเมตร” ประมาณ : 13.23 cm. X 13.23 cm.

หน่วยเป็น “นิ้ว” ประมาณ : 5.21 inch. X 5.21 inch.

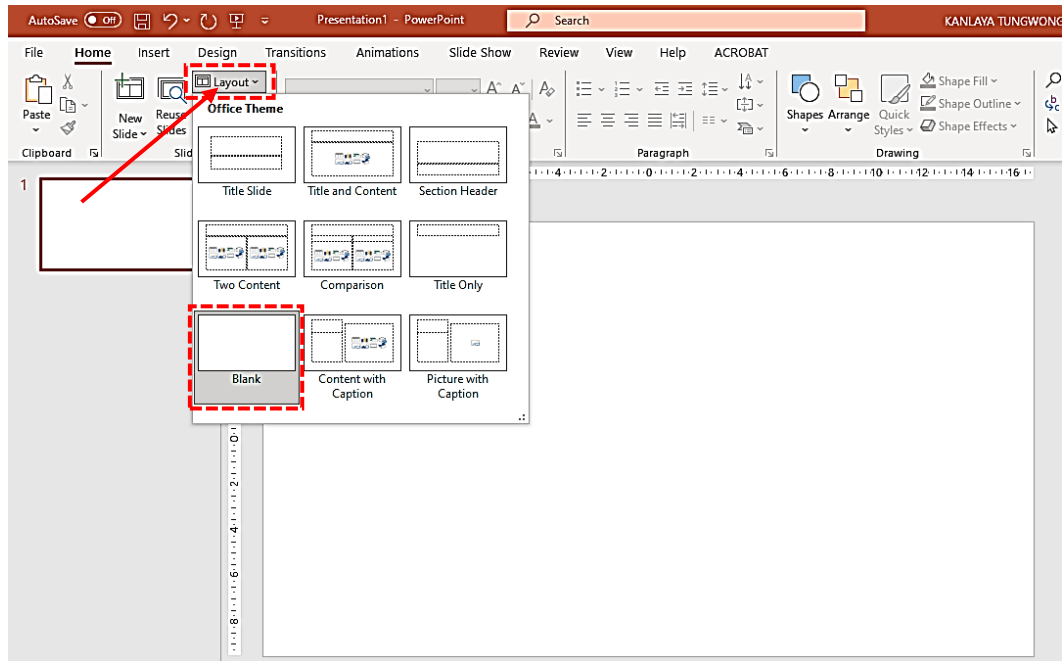
ความละเอียด (Resolution) : 72 ppi. (Pixels/Inch)

พื้นหลัง (Background) : โปร่งใส (Transparent)

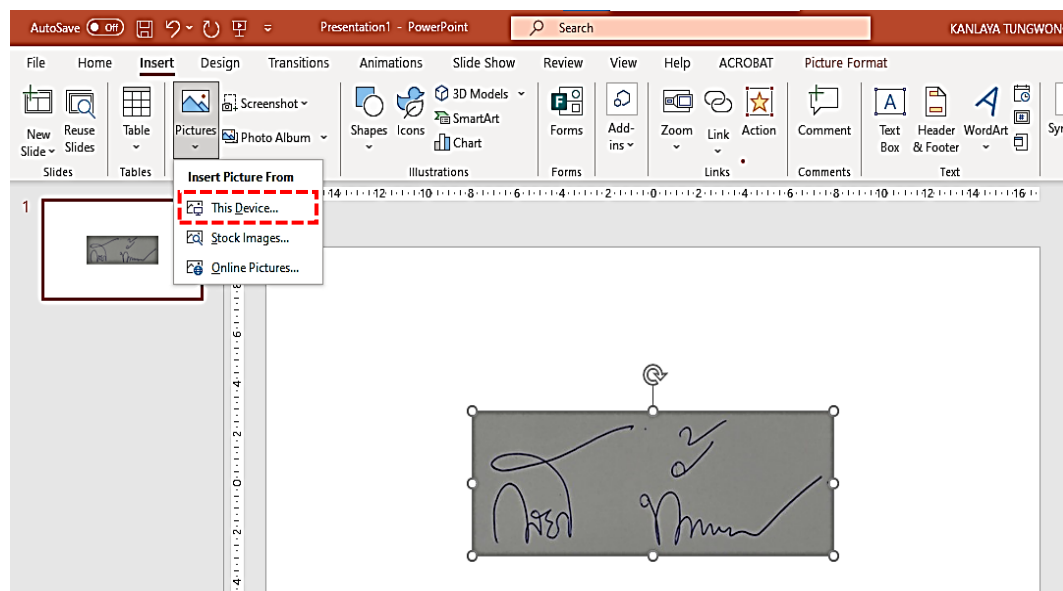
ประเภทของไฟล์ที่จัดเก็บ (Filetype) : .png หรือ .jpg

(นิยม .png เนื่องจาก จะสามารถใช้การตัดพื้นหลังออกจากภาพได้ และเหมาะสมกับ digital file มากกว่า .jpg ที่มีพื้นหลัง)

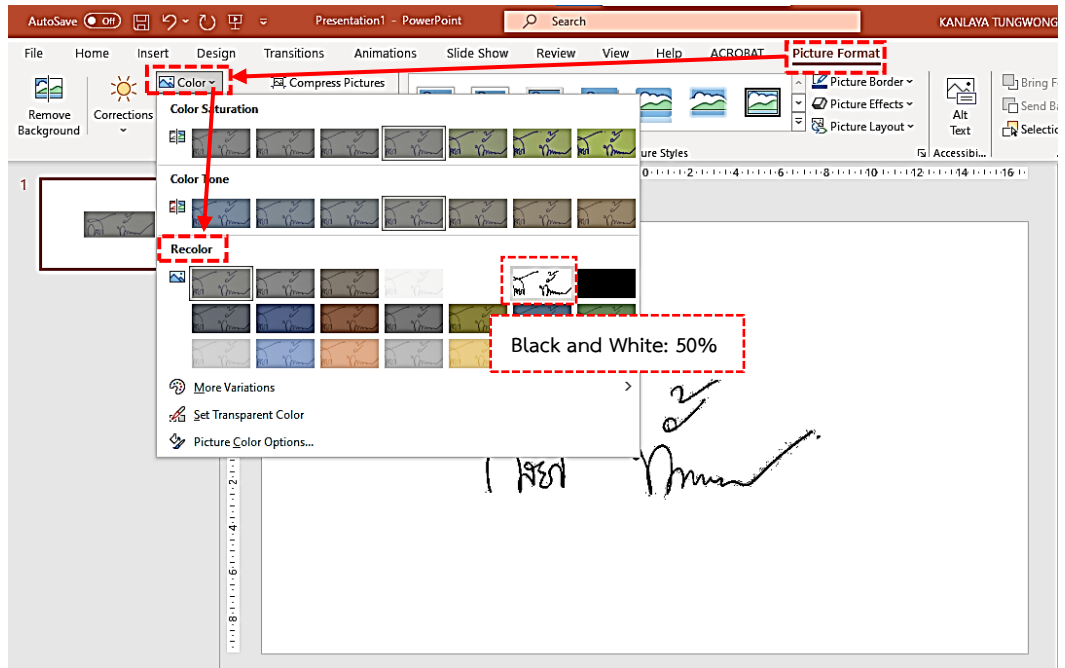
2. จะนำมาปรับแก้ไขภาพต้นแบบนี้เป็นลายเซ็นสีดำ และพื้นกระดาษเป็นสีขาว ในตัวอย่างใช้โปรแกรม Microsoft Office PowerPoint ดังนี้
 - 2.1. เปิดโปรแกรม PowerPoint เลือก “Blank Presentation Template” > ปรับเค้าโครง Slide / Layout เป็นแบบ “Blank”



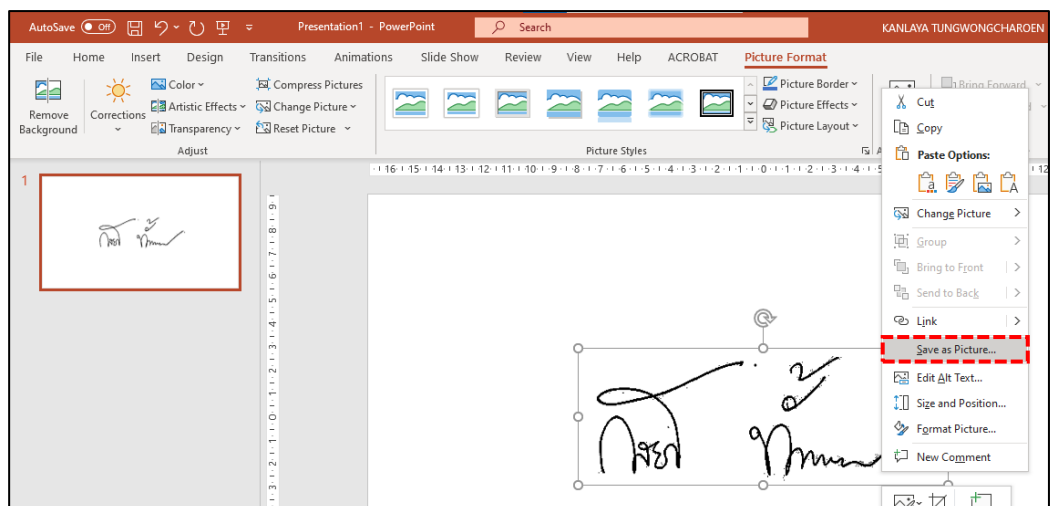
- 2.2. แทรกไฟล์ภาพลายเซ็น ที่โหลดจากสมาร์ทโฟนเข้ามาในเครื่องคอมพิวเตอร์แล้ว > ไฟล์ที่ถูกสั่งเปิดจะเป็นวัตถุ “รูปภาพจากไฟล์ภาพในเครื่องคอมพิวเตอร์” แสดงบน Slide



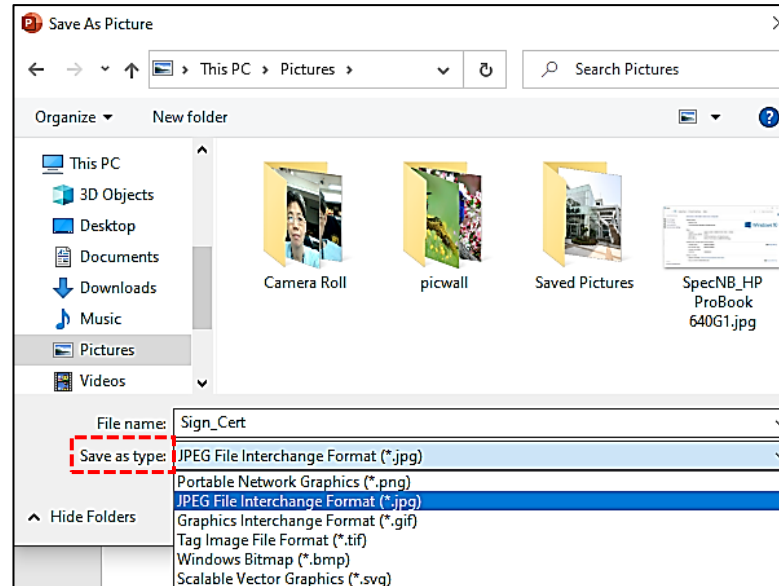
- 2.3. ทำการคลิกเลือกวัตถุรูปภาพลายเซ็น > ที่เมนู “Picture Format” กลุ่มคำสั่ง “Adjust” > คลิก
 ▼ ข้างคำสั่ง “Color” > ส่วน “Recolor” เลือกคลิก “Black and White: 50%” > วัตถุไฟล์
 รูปภาพจะถูกปรับเปลี่ยนสีพื้นเป็นสีขาว



- 2.4. ทำการ Save เป็นไฟล์รูปภาพใหม่โดย คลิกเลือกวัตถุรูปภาพลายเซ็นที่เปลี่ยนเป็นรูปขาวดำแล้ว >
 คลิกเมาส์ปุ่มขวา แสดงรายการเมนูย่อย > เลือกคลิกคำสั่ง “Save as Picture...”



2.5. ปราบกฏหน้าต่าง “Save As Picture” > ทำการเลือกไฟล์เตอร์จัดเก็บ , ตั้งชื่อที่ช่อง “File name:” , และเลือกชนิดของไฟล์รูปภาพ ที่ช่อง “Save as type:” แนะนำ ควรเป็น .jpg หรือ .png ที่นิยม เป็นไฟล์ภาพ > คลิกปุ่ม “Save” > ปิดโปรแกรม PowerPoint โดยไม่ต้องบันทึกไฟล์



ได้ไฟล์ภาพลายเส้นขาวดำที่ไม่หลอกตาแลดูสวยงามเข้ากับหน้าไฟล์เอกสาร .pdf สำหรับนำไปใช้ในหัวข้อ การนำเข้าและสร้างไฟล์ภาพลายเส้นเก็บไว้เรียกใช้เป็นลายเส้นดิจิทัลด้วยการ “Image”