



คู่มือการจัดการใบรับรองอิเล็กทรอนิกส์
สำหรับผู้ดูแลระบบสารสนเทศอิเล็กทรอนิกส์

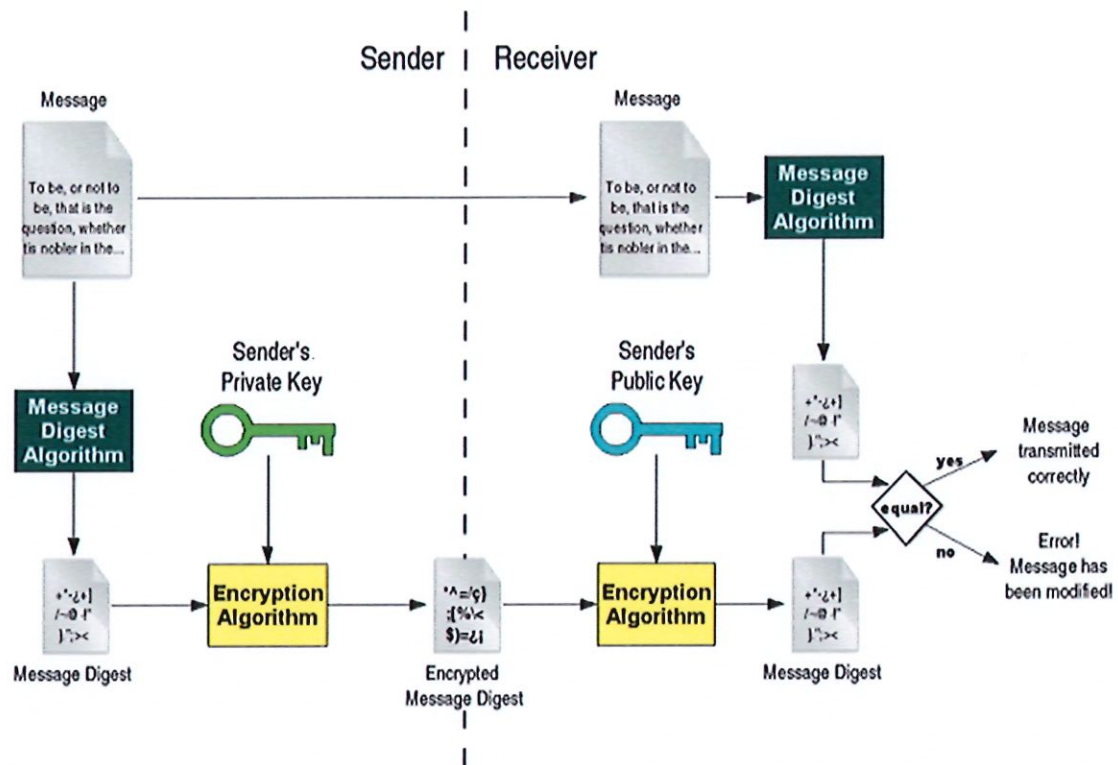
จัดทำโดย
บริษัท วิชั่นเน็ต จำกัด

คู่มือการจัดการใบรับรองอิเล็กทรอนิกส์

สารบัญ

คู่มือการจัดการใบรับรองอิเล็กทรอนิกส์	1
การลงนามอิเล็กทรอนิกส์ (Digital Signature)	2
ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)	3
การรองรับมาตรฐานใบรับรองอิเล็กทรอนิกส์	3
โปรแกรมสร้างใบรับรองอิเล็กทรอนิกส์ด้วยตนเอง	4
ออกใบรับรองอิเล็กทรอนิกส์	4
จัดส่งใบรับรองอิเล็กทรอนิกส์	4
การลงทะเบียนใบรับรองอิเล็กทรอนิกส์	5
ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยระบุบุคคล	5
ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยการนำเข้า	6
การนำเข้าใบรับรองอิเล็กทรอนิกส์	7
การเพิ่มใบรับรองอิเล็กทรอนิกส์สู่บุคคล	7
ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยการสร้างเป็นชุด	8
สาเหตุที่ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ไม่สำเร็จ	9
การจัดการใบรับรองอิเล็กทรอนิกส์	9
การกำหนดใบรับรองอิเล็กทรอนิกส์หลัก	9
ระงับใบรับรองอิเล็กทรอนิกส์	10
ลบใบรับรองอิเล็กทรอนิกส์	10

การลงนามอิเล็กทรอนิกส์ (Digital Signature)



กระบวนการลงนามอิเล็กทรอนิกส์นั้น จะใช้หลักการของการเข้ารหัสแบบอสมมาตร ใช้ Private key ในการเข้ารหัสเท่านั้น และ Public Key ในการถอดรหัสเท่านั้น ดังนั้นผู้ที่มี Private Key (กุญแจส่วนตัว) จะไม่สามารถถอดรหัสได้ และผู้ที่มี Public Key (กุญแจสาธารณะ) จะไม่สามารถเข้ารหัสได้

จากหลักการที่กล่าวมาข้างต้นจึงนำมาใช้การลงนามอิเล็กทรอนิกส์ โดยกระบวนการลงนามอิเล็กทรอนิกส์มีขั้นตอนโดยย่อต่อไปนี้

1. นำข้อมูลอิเล็กทรอนิกส์ที่ต้องการลงนามผ่านกระบวนการ hash เพื่อให้ได้ค่าตัวแทนของข้อมูลอิเล็กทรอนิกส์นั้นๆ
2. นำ Private Key เข้ารหัสค่าตัวแทนของข้อมูล เพื่อให้ได้ลายเซ็นอิเล็กทรอนิกส์

และกระบวนการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ที่ผ่านการลงนามมีขั้นตอนโดยย่อต่อไปนี้

1. นำ Public Key ถอดรหัสลายเซ็นอิเล็กทรอนิกส์ เพื่อให้ได้ค่าตัวแทนของข้อมูลของผู้ลงนาม
2. นำข้อมูลอิเล็กทรอนิกส์ที่ต้องการตรวจสอบผ่านกระบวนการ hash ที่เป็นกระบวนการเดียวกันกับการลงนาม เพื่อให้ได้ค่าตัวแทนของข้อมูลอิเล็กทรอนิกส์นั้นๆ
3. นำค่าตัวแทนของข้อมูลที่ได้จากการถอดรหัสและผ่านกระบวนการ hash มาเปรียบเทียบว่าตรงกันหรือไม่
4. กรณีทั้งสองค่าตรงกัน คือการลงนามถูกต้อง หรือไม่มีการแก้ไขข้อมูลหลังการลงนาม

5. กรณีทั้งสองค่าไม่ตรงกัน คือลายเซ็นอิเล็กทรอนิกส์ไม่ใช่ของผู้ลงนาม หรือมีการแก้ไขข้อมูลหลังการลงนาม

เพื่อให้เกิดความน่าเชื่อถือของการลงนามอิเล็กทรอนิกส์ ผู้ลงนามอิเล็กทรอนิกส์จะต้องเป็นเพียงผู้เดียวที่ครอบครองและใช้ Private Key ได้ ส่วน Public Key จะทำการแจกจ่ายให้กับผู้ที่ต้องการตรวจสอบการลงนาม

ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

ในการลงนามอิเล็กทรอนิกส์จำเป็นต้องใช้ชุดกุญแจที่ประกอบด้วย Private Key (กุญแจส่วนตัว) และ Public Key (กุญแจสาธารณะ) ซึ่งชุดกุญแจดังกล่าวเป็นส่วนหนึ่งใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ใบรับรองอิเล็กทรอนิกส์ที่ระบบนี้ใช้จะอยู่ในมาตรฐาน PKCS#12 ที่จัดเก็บในรูปแบบไฟล์ PFX (Personal Information Exchange) ซึ่งสามารถกำหนดรหัสผ่านการใช้งานเพื่อเพิ่มความปลอดภัยและป้องกันไม่ให้บุคคลอื่นนำไปลงนาม

ใบรับรองอิเล็กทรอนิกส์สามารถจัดหาได้จาก ผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ ออกใบรับรองจากเครื่องแม่ข่ายใบรับรองอิเล็กทรอนิกส์ หรือ ออกใบรับรองจากโปรแกรมสร้างใบรับรองอิเล็กทรอนิกส์ด้วยตนเอง

การใช้งานใบรับรองอิเล็กทรอนิกส์ของระบบฯ หลังจากจัดหาหรือสร้างไฟล์ใบรับรองอิเล็กทรอนิกส์แล้ว จะต้องทำการลงทะเบียนใบรับรองเข้าสู่ระบบ การลงทะเบียนใบรับรองจะเป็นการบันทึกเฉพาะ Public Key (กุญแจสาธารณะ) ที่อยู่ในไฟล์ใบรับรองอิเล็กทรอนิกส์เข้าสู่ระบบเท่านั้น สำหรับใช้ในการตรวจทานการลงนามและใช้ในการตรวจสอบการลงนามในภายหลัง โดยระบบฯ จะไม่บันทึกหรือ Private Key (กุญแจส่วนตัว) ด้วยมาตรการรักษาความปลอดภัยดังกล่าว กรณีที่เจ้าของใบรับรองอิเล็กทรอนิกส์ลืมรหัสผ่านหรือทำใบรับรองหาย ระบบจะไม่สามารถกู้คืนใบรับรองนั้นได้ จำเป็นต้องระงับใบรับรองอิเล็กทรอนิกส์นั้นและจัดหาใบรับรองอิเล็กทรอนิกส์ใหม่ทดแทนเท่านั้น

การรองรับมาตรฐานใบรับรองอิเล็กทรอนิกส์

ระบบงานเข้าถึงข้อมูลหรือใช้งานใบรับรองอิเล็กทรอนิกส์โดยการขอใช้บริการจากระบบปฏิบัติการ ดังนั้นการที่ระบบงานจะสามารถเข้าถึงข้อมูลหรือใช้งานใบรับรองอิเล็กทรอนิกส์ในมาตรฐานต่าง ๆ ได้นั้น ขึ้นอยู่กับการรองรับมาตรฐานต่าง ๆ ของระบบปฏิบัติ

ตัวอย่างเช่น ใบรับรองอิเล็กทรอนิกส์ที่ใช้มาตรฐานอัลกอริทึมในการสร้างลายมือชื่อ (Signature algorithm) แบบ SHA256 RSA สามารถใช้งานได้บนระบบปฏิบัติการ Microsoft Windows Server 2019 หรือใหม่กว่า แต่ใบรับรองอิเล็กทรอนิกส์เดียวกันจะไม่สามารถใช้งานได้ในระบบปฏิบัติการ Microsoft Windows Server 2016 ซึ่งไม่รองรับมาตรฐานดังกล่าว

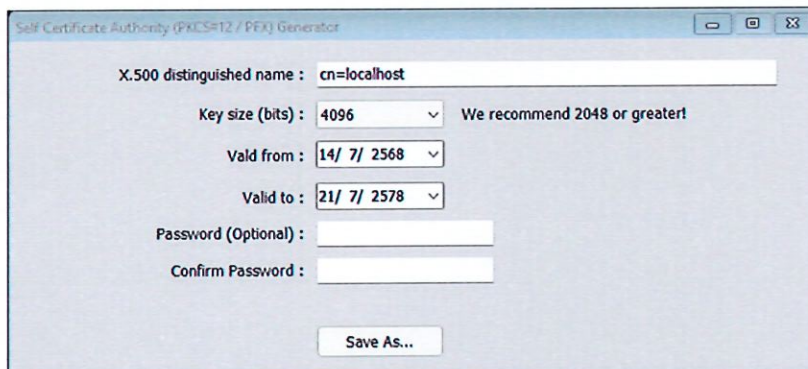
ดังนั้นถ้าต้องการใช้งานใบรับรองอิเล็กทรอนิกส์ตามมาตรฐานใด ต้องปรับปรุงระบบปฏิบัติการให้รองรับมาตรฐานของใบรับรองอิเล็กทรอนิกส์ที่ต้องการใช้งานนั้น

โปรแกรมสร้างใบรับรองอิเล็กทรอนิกส์ด้วยตนเอง

ในกรณีที่ต้องการออกใบรับรองอิเล็กทรอนิกส์เองโดยไม่จัดหาจากผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ หรือออกใบรับรองจากบริการออกใบรับรองอิเล็กทรอนิกส์ ระบบฯ ได้เตรียมโปรแกรมสร้างใบรับรองอิเล็กทรอนิกส์ด้วยตนเอง โดยใช้มาตรฐานอัลกอริทึมในการสร้างลายมือชื่อ (Signature algorithm) แบบ SHA1 RSA

ออกใบรับรองอิเล็กทรอนิกส์

1. เข้าใช้งานจากเมนู “เครื่องมือ”, “Administrative Tools”, “Digital Signature” และ “Self-certificate Authority (PFX) generator” ตามลำดับ
2. กรอกชื่อของ certificate ในรูปแบบ distinguished name ในช่อง “X.500 distinguished name”



3. ระบุขนาดการสร้างในช่อง “Key size (bits)”
4. กรอกรวันเริ่มต้นและหมดอายุในช่อง “Valid from” และ “Valid to”
5. ระบุรหัสผ่านในช่อง “Password” และ “Confirm Password”
6. กดปุ่ม “Save As” เพื่อสร้างไฟล์ใบรับรองอิเล็กทรอนิกส์ (Digital certificate)

โปรแกรมนี้อนุญาตให้ไม่ต้องกำหนดรหัสผ่านการใช้งานใบรับรองอิเล็กทรอนิกส์ แต่เพื่อความปลอดภัยต้องระบุรหัสผ่านการใช้งาน

จัดส่งใบรับรองอิเล็กทรอนิกส์

เมื่อได้ไฟล์ใบรับรองอิเล็กทรอนิกส์แล้ว สามารถส่งเป็นไฟล์โดยตรงให้กับเจ้าของใบรับรองอิเล็กทรอนิกส์ผ่านช่องทางสื่อสารข้อมูลต่างๆ หรือเพื่อความสะดวกในการลงนามในอนาคต สามารถ

บันทึกในอุปกรณ์บันทึกข้อมูลที่ถอดได้ (Removable storage) โดยนำไฟล์ใบรับรองอิเล็กทรอนิกส์ตั้งชื่อเป็น “edocument.pfx” และวางไว้ที่โฟลเดอร์แรก (Root folder) ของอุปกรณ์

และเมื่อเจ้าของใบรับรองอิเล็กทรอนิกส์ได้รับไฟล์แล้ว เพื่อความปลอดภัยให้ทำการเปลี่ยนรหัสผ่านการใช้งานใบรับรองอิเล็กทรอนิกส์ที่ได้รับ โดยเจ้าของใบรับรองสามารถศึกษาการเปลี่ยนรหัสผ่านได้จากคู่มือการลงนามอิเล็กทรอนิกส์

การลงทะเบียนใบรับรองอิเล็กทรอนิกส์

เมื่อต้องการให้ใบรับรองอิเล็กทรอนิกส์สามารถใช้งานในระบบได้ จำเป็นต้องลงทะเบียนเข้าสู่ระบบฯ ซึ่งจะใช้น้ำจอจัดการผู้ใช้งานในการลงทะเบียน

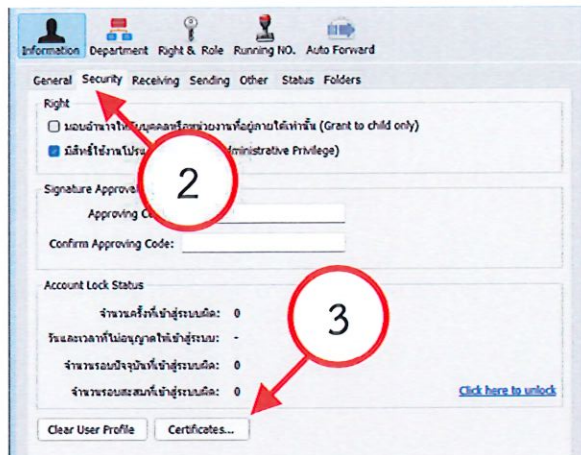
Issuer	Default	Not After	Import date/time
Enabled			
CN=dev	Default	18/1/2575	18/1/2565 16:22
CN=ผู้พัฒนาระบบ		11/1/2575	11/1/2565 10:12
CN=ผู้พัฒนาระบบ 1		10/1/2575	10/1/2565 17:30
CN=ผู้พัฒนาระบบ 1		17/12/2574	17/12/2564 16:21
Disabled			
CN=ผู้พัฒนาระบบ Vision Net		19/11/2574	27/11/2564 9:43
CN=ผู้พัฒนาระบบ Vision Net		19/11/2574	19/11/2564 11:33
CN=VisionNet		10/9/2574	26/10/2564 16:19

รายการใบรับรองที่นำเข้า ในหน้าจอมีคอลัมน์ดังนี้

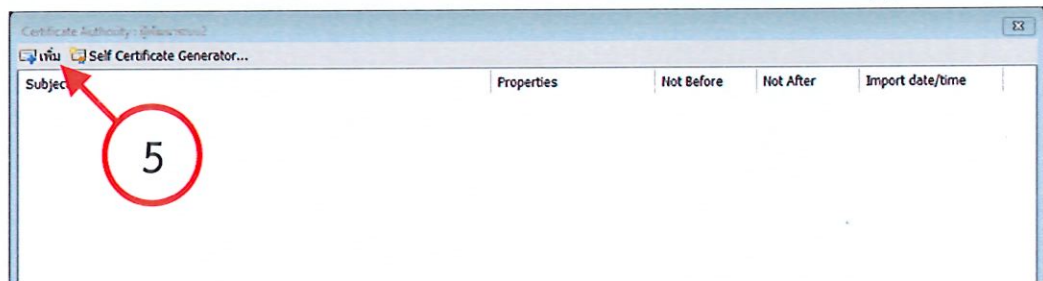
1. Issuer: แสดงชื่อของผู้ถือใบรับรองอิเล็กทรอนิกส์ หรือชื่อของใบรับรองอิเล็กทรอนิกส์ ในรูปแบบ X.500 distinguished name
2. Default: เป็นใบรับรองปริยายหรือไม่ ใช้ในกรณีที่ผู้ลงนามใช้ใบรับรองอิเล็กทรอนิกส์ที่ไม่ส่งรหัสประจำใบรับรอง (Thumbprint) เข้าสู่กระบวนการลงนาม ระบบทำการตรวจทานจากใบรับรองทั้งหมดของผู้ลงนามผู้นี้ โดยจะให้ใบรับรองปริยายเป็นใบรับรองใบแรกที่ตรวจทานก่อน
3. Not After: แสดงวันที่สิ้นสุดหรือหมดอายุของใบรับรองอิเล็กทรอนิกส์
4. Import date/time: วันที่ลงทะเบียนหรือนำเข้าใบรับรองอิเล็กทรอนิกส์

ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยระบุบุคคล

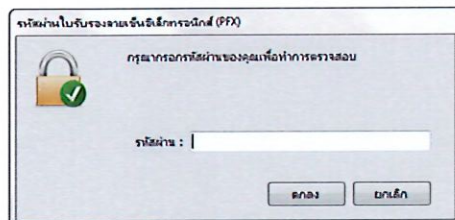
1. เข้าใช้งานจากเมนู “เครื่องมือ” , “สมุดรายชื่อ” กรอกรหัสผ่านเพื่อเข้าสู่ความสามารถของผู้ดูแลระบบ ตามลำดับ
2. จากนั้นให้ทำการเปิดหน้าจอของบุคคลที่ต้องการลงทะเบียน ไปยังหน้า “Security”



3. กดปุ่ม “Certificates” ที่อยู่มุมล่างขวา
4. โปรแกรมจะเปิดหน้าจอสำหรับลงทะเบียนหรือเพิ่มใบรับรองอิเล็กทรอนิกส์เข้าสู่ผู้ใช้งาน



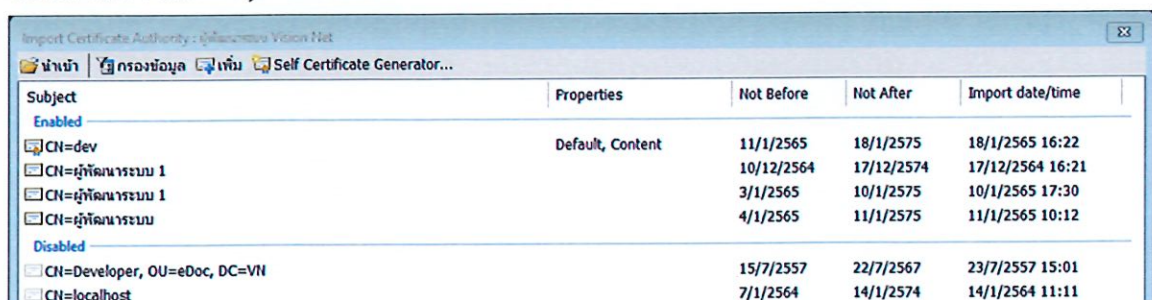
5. ปุ่ม “เพิ่ม” เพื่อเรียกหน้าจอเลือกไฟล์
6. เลือกไฟล์ใบรับรองอิเล็กทรอนิกส์ที่ต้องการลงทะเบียน
7. กรอกรหัสผ่านเพื่ออนุญาตให้โปรแกรมเข้าถึงข้อมูล public key ของใบรับรองอิเล็กทรอนิกส์



8. การนำเข้าเสร็จสิ้น

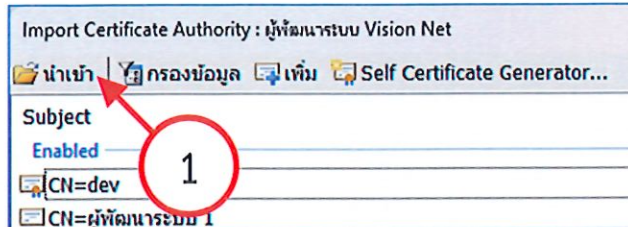
ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยการนำเข้า

เข้าใช้งานจากเมนู “เครื่องมือ”, “Administrative Tools”, “Digital Signature” และ “Import Certificate Authority” ตามลำดับ

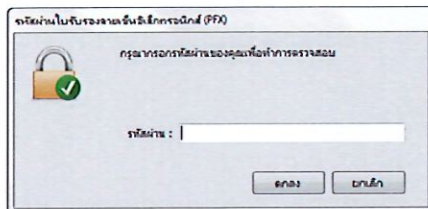


การนำเข้าใบรับรองอิเล็กทรอนิกส์

1. ปุ่ม “นำเข้า”



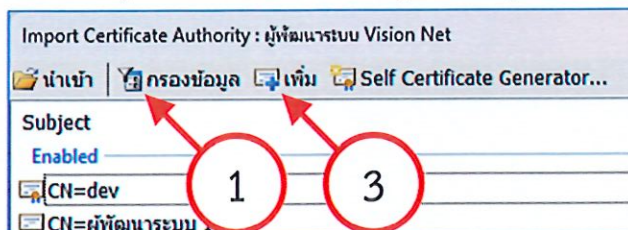
2. โปรแกรมจะเปิดหน้าจอสมุดรายชื่อ เพื่อให้เลือกบุคคลที่ต้องการรับการลงทะเบียน
3. โปรแกรมจะเปิดหน้าจอ เพื่อเลือกไฟล์ใบรับรองอิเล็กทรอนิกส์ที่ต้องการลงทะเบียน
4. กรอกรหัสผ่านเพื่ออนุญาตให้โปรแกรมเข้าถึงข้อมูล public key ของใบรับรองอิเล็กทรอนิกส์



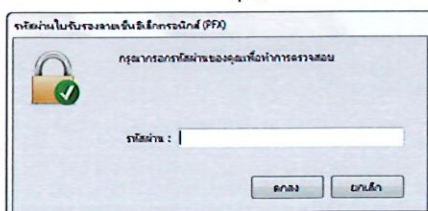
5. การนำเข้าเสร็จสิ้น

การเพิ่มใบรับรองอิเล็กทรอนิกส์สู่บุคคล

1. กรณีที่ชื่อบุคคลที่แสดงบนหน้าจอไม่ตรงกับบุคคลที่ต้องการเพิ่มใบรับรองอิเล็กทรอนิกส์ ให้ปุ่ม “กรองข้อมูล” เพื่อให้เลือกกรองข้อมูลเฉพาะบุคคลที่ต้องการ



2. โปรแกรมจะเปิดหน้าจอสมุดรายชื่อ เพื่อให้เลือกบุคคล
3. กดปุ่ม “เพิ่ม” โปรแกรมจะเปิดหน้าจอ เพื่อเลือกไฟล์ใบรับรองอิเล็กทรอนิกส์ที่ต้องการลงทะเบียน
4. กรอกรหัสผ่านเพื่ออนุญาตให้โปรแกรมเข้าถึงข้อมูล public key ของใบรับรองอิเล็กทรอนิกส์

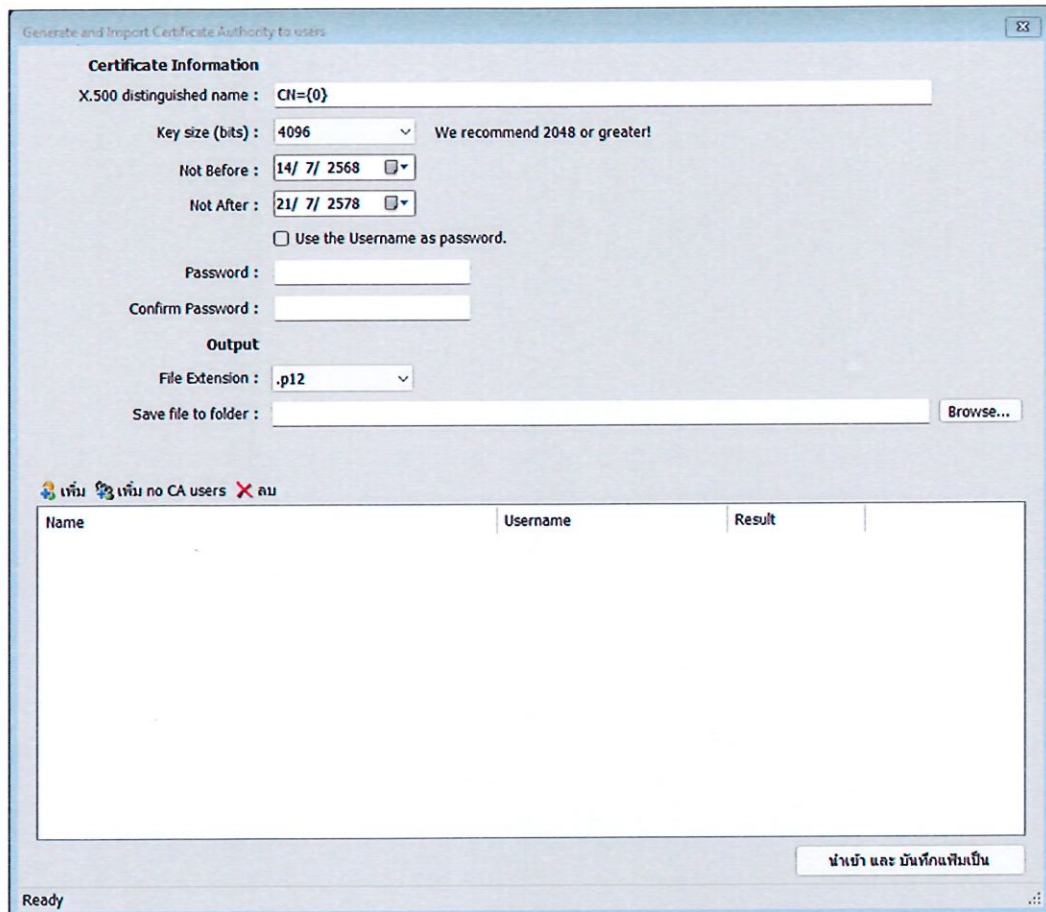


5. การเพิ่มเสร็จสิ้น

ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ โดยการสร้างเป็นชุด

เป็นการสร้างใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้งานที่ระบุ ลงทะเบียนเข้าผู้ใช้งาน และส่งออกเป็นไฟล์สำหรับส่งมอบให้กับผู้ใช้งาน

1. เข้าใช้งานจากเมนู “เครื่องมือ”, “Administrative Tools”, “Digital Signature” และ “Generate and import Certificate Authority to users” ตามลำดับ



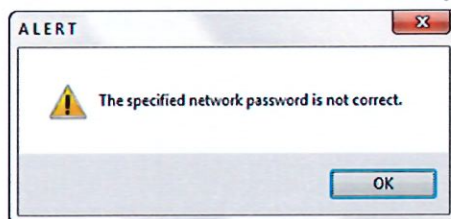
2. กรอกชื่อของ certificate ในรูปแบบ distinguished name ในช่อง “X.500 distinguished name” โดยข้อความ “{0}” แทน ชื่อ-นามสกุล ของผู้ใช้งาน
3. ระบุขนาดการสร้างในช่อง “Key size (bits)”
4. กรอกวันเริ่มต้นและหมดอายุในช่อง “Valid from” และ “Valid to”
5. กรณีที่ต้องการกำหนดให้รหัสผ่านเป็นชื่อผู้ใช้งาน ให้ทำเครื่องหมายถูกที่ “Use the Username as password”
6. กรณีไม่กำหนดให้รหัสผ่านเป็นชื่อผู้ใช้งาน ให้ระบุรหัสผ่านในช่อง “Password” และ “Confirm Password”
7. ระบุข้อมูลการส่งออก “Output” โดยเลือกนามสกุลของไฟล์ที่ “File Extension”

8. ระบุโฟลเดอร์ที่ต้องการส่งออกไฟล์ใบรับรองอิเล็กทรอนิกส์ที่ “Save file to folder” โดยการกรอกที่อยู่ของโฟลเดอร์ หรือกดปุ่ม “Browse” เพื่อเลือกที่อยู่ของโฟลเดอร์
9. เพิ่มผู้ใช้งานที่ต้องการสร้างใบรับรองอิเล็กทรอนิกส์
 - a. เพิ่มรายบุคคล โดยการกดปุ่ม “เพิ่ม”
 - b. เพิ่มผู้ใช้งานที่ยังไม่เคยมีใบรับรองอิเล็กทรอนิกส์ โดยการกดปุ่ม “เพิ่ม no CA users”
 - c. สามารถลบรายชื่อผู้ใช้งาน โดยการเลือกรานชื่อ จากนั้นกดปุ่ม “ลบ”
10. กดปุ่ม “นำเข้า และ บันทึกแฟ้มเป็น” เพื่อสร้างไฟล์ใบรับรองอิเล็กทรอนิกส์ นำเข้าสู่ผู้ใช้งาน และบันทึกใบรับรองอิเล็กทรอนิกส์ไปยังโฟลเดอร์ที่กำหนด

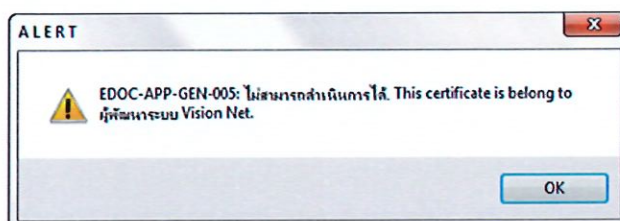
สาเหตุที่ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ไม่สำเร็จ

สาเหตุที่ลงทะเบียนใบรับรองอิเล็กทรอนิกส์ไม่สำเร็จ อาจเกิดจาก

1. ไฟล์ผิดประเภท
2. มาตรฐานของใบรับรองอิเล็กทรอนิกส์ไม่ตรงกับมาตรฐาน PKCS#12
3. รหัสผ่านของใบรับรองอิเล็กทรอนิกส์ไม่ถูกต้อง



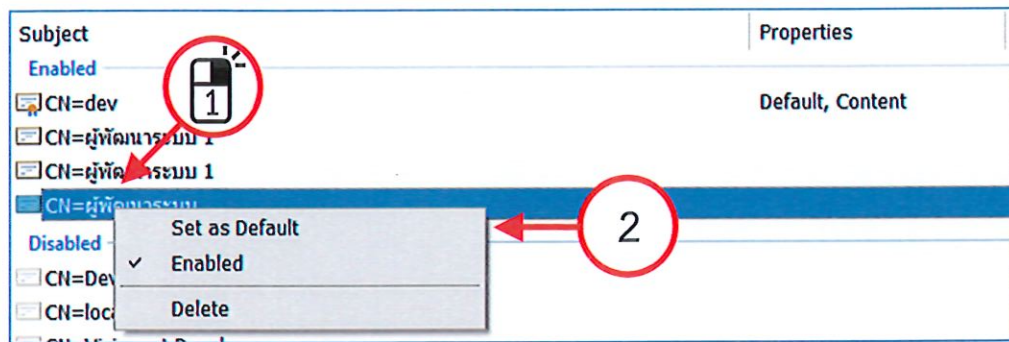
4. ทะเบียนใบรับรองอิเล็กทรอนิกส์ซ้ำซ้อน หรือใบรับรองอิเล็กทรอนิกส์นี้ได้เคยลงทะเบียนกับระบบแล้ว



การจัดการใบรับรองอิเล็กทรอนิกส์

การกำหนดใบรับรองอิเล็กทรอนิกส์หลัก

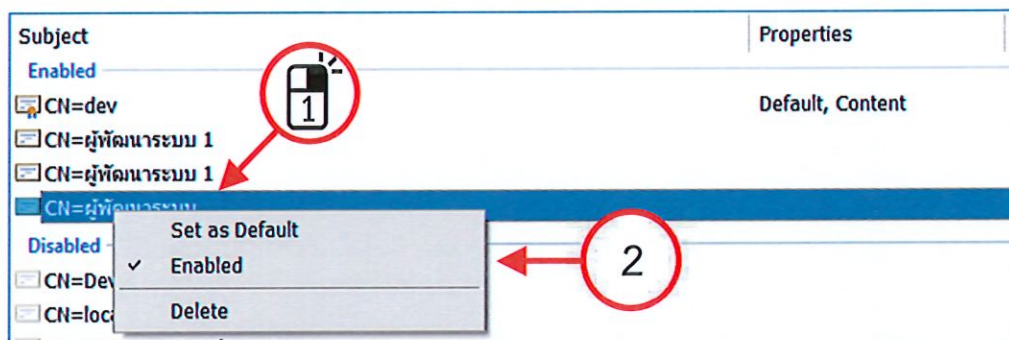
ระบบสามารถให้แต่ละบุคคลมีใบรับรองอิเล็กทรอนิกส์มากกว่าหนึ่งใบ ดังนั้นเพื่อให้เกิดประสิทธิภาพในการตรวจทานลายเซ็นอิเล็กทรอนิกส์จากใบรับรองอิเล็กทรอนิกส์หลายใบ จะต้องกำหนดใบรับรองปริยาย ซึ่งการกำหนดใบรับรองปริยายทำได้โดย



1. คลิกขวาที่ใบรับรองที่ต้องการ
2. เลือกเมนู "Set as Default"
3. หลังจากเสร็จสิ้น จะขึ้นคำว่า "Default" ที่คอลัมน์ "Default"

ระงับใบรับรองอิเล็กทรอนิกส์

ในกรณีที่มียามากกว่าหนึ่งใบรับรองต้องการที่จะยกเลิกใบรับรองที่ไม่ใช้งาน หรือต้องการระงับใบรับรองที่เจ้าของสิทธิ์ผ่านหรือทำหายทำได้โดย

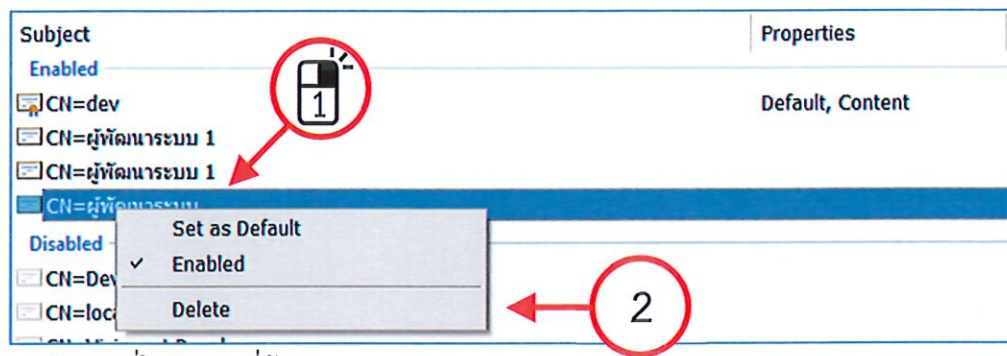


1. คลิกขวาที่ใบรับรองที่ต้องการ
2. เลือกเมนู "Enabled"
3. หลังจากเสร็จสิ้น ใบรับรองแสดงสัญลักษณ์เป็นสีจาง จะเข้าไปอยู่ในกลุ่ม "Disabled"

โดยเมื่อระงับหรือยกเลิกใบรับรองอิเล็กทรอนิกส์แล้ว ระบบจะไม่อนุญาตให้ลงนามด้วยใบรับรองนั้น แต่ยังคงใช้ในการตรวจสอบลายเซ็นที่ลงนามด้วยใบรับรองนี้

ลบใบรับรองอิเล็กทรอนิกส์

ในกรณีที่ต้องการใบรับรองอิเล็กทรอนิกส์ที่ยังไม่ผ่านการใช้งานทำได้โดย



1. คลิกขวาที่ใบรับรองที่ต้องการ
2. เลือกเมนู "Delete"
3. กรณีที่ลบไม่สำเร็จ อาจเกิดจากใบรับรองอิเล็กทรอนิกส์ได้ผ่านการใช้งานแล้ว

