

Thai Digital ID Co., Ltd.

คู่มือการใช้งาน Token

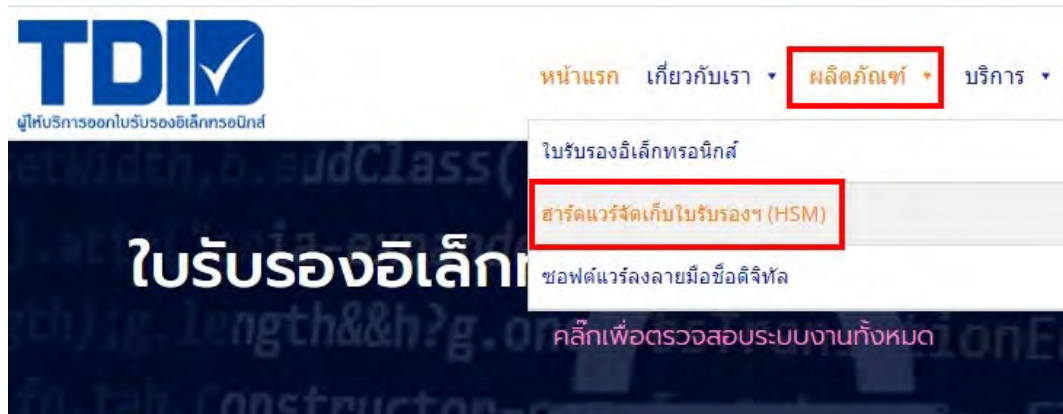
version 1.0

สารบัญ

สารบัญ.....	2
1. การติดตั้งโปรแกรม SafeNet Authentication Client 8.0 (SAC)	3
2. การ Initialization Token	7
3. การตรวจสอบข้อมูลใบรับรองฯ (Certificate)	9
4. การลบใบรับรองฯ (Certificate) ออกจาก Token	9
5. การ Import Certificate File เข้า Token	10
6. Token Lock หรือ Pin Lock.....	14
7. การเปลี่ยนแปลง Password.....	16
8. การ Setting Password Quality	17

1. การติดตั้งโปรแกรม SafeNet Authentication Client 8.0 (SAC)

1.1 เข้าที่หน้าเว็บไซต์ <https://www.thaidigitalid.com> และเลือกหัวข้อ “ผลิตภัณฑ์” > ฮาร์ดแวร์จัดเก็บใบรับรองฯ (HSM)



1.2 เลือก “ไดรเวอร์” จากนั้นให้ทำการดาวน์โหลดโปรแกรม SafeNet Authentication Client ตามรุ่นที่เหมาะสมกับ Windows ที่ใช้งาน เพื่อบันทึกตัวติดตั้งโปรแกรมลงเครื่องคอมพิวเตอร์



หรือสามารถ Click Link นี้ --> [SafeNet Authentication Client 32 Bit](#) , [SafeNet Authentication Client 64 Bit](#)

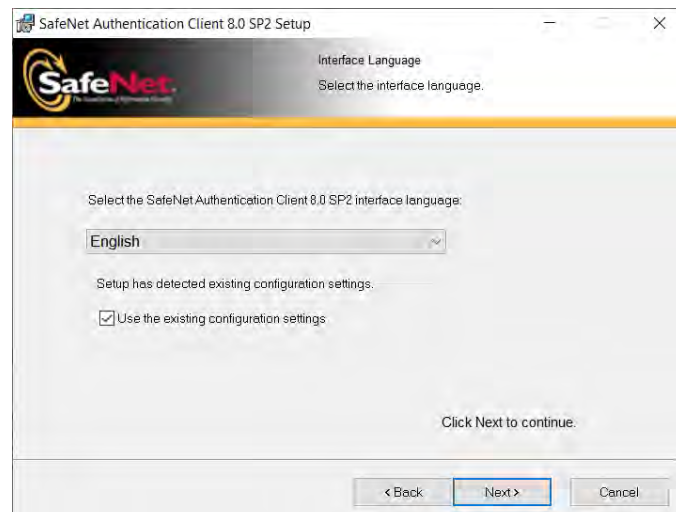
1.3 หลังจากบันทึกตัวติดตั้งโปรแกรมเรียบร้อยแล้ว Click ขวา ที่ไฟล์ “SAC-x64.msi” หรือ “SAC-x32.msi” ตามรุ่นของ Windows ที่ใช้งาน > เลือก Install



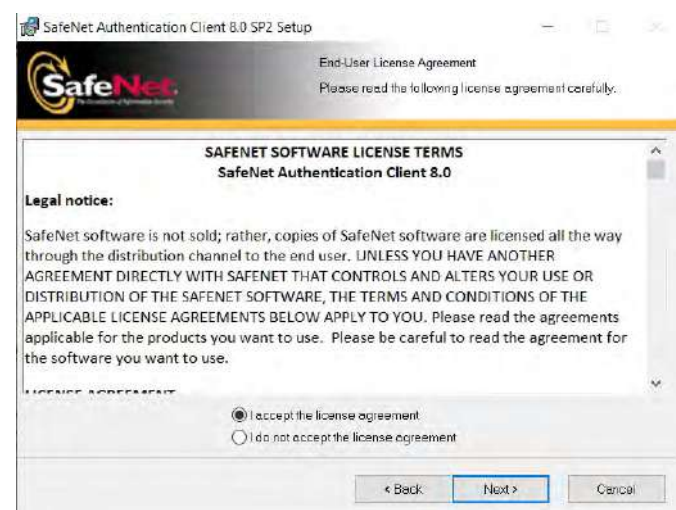
1.4 Click ปุ่ม “Next” เพื่อเริ่มติดตั้งโปรแกรม SafeNet Authentication Client 8.0



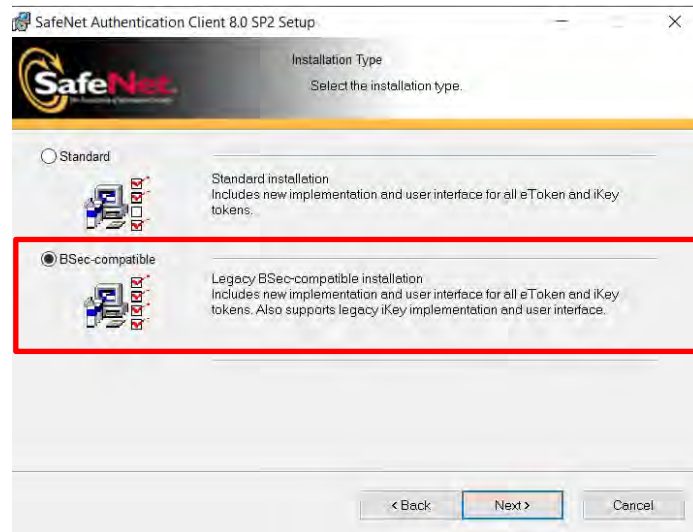
1.5 เลือกภาษาที่ใช้ติดตั้งโปรแกรม SafeNet Authentication Client 8.0 ในที่นี้เลือก “English” > กดปุ่ม Next



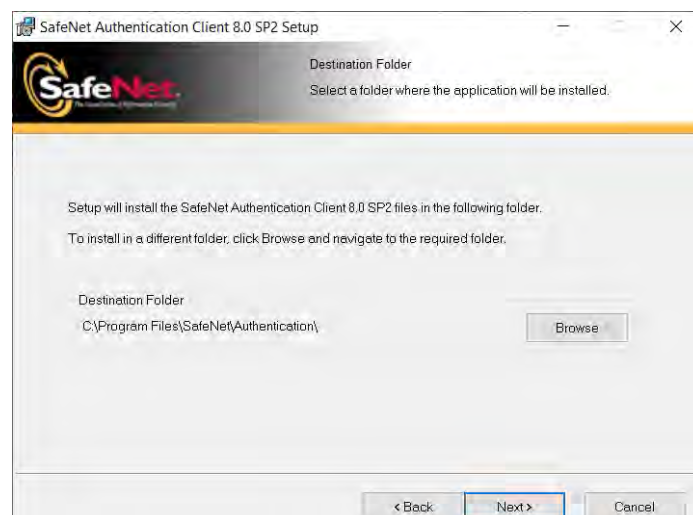
1.6 เลือก “I accept the license agreement” เพื่อยอมรับเงื่อนไขในการติดตั้งโปรแกรม SafeNet Authentication Client 8.0 และกดปุ่ม Next



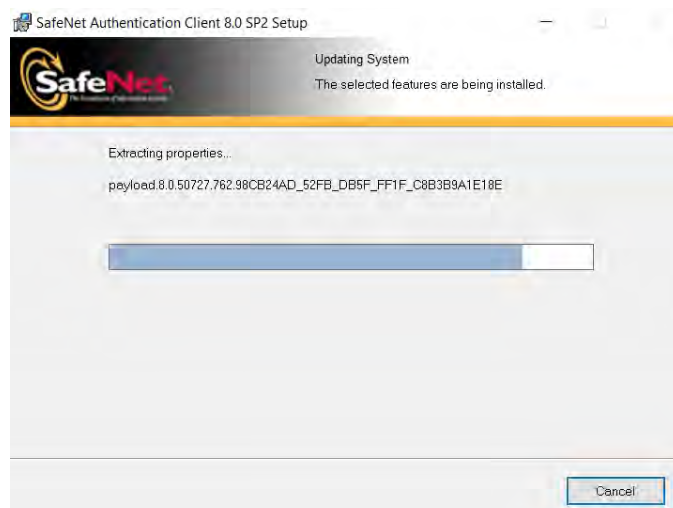
1.7 เลือกรูปแบบในการติดตั้งโปรแกรม SafeNet Authentication Client 8.0 โดยในที่นี่
ให้เลือก “BSecCompatible”



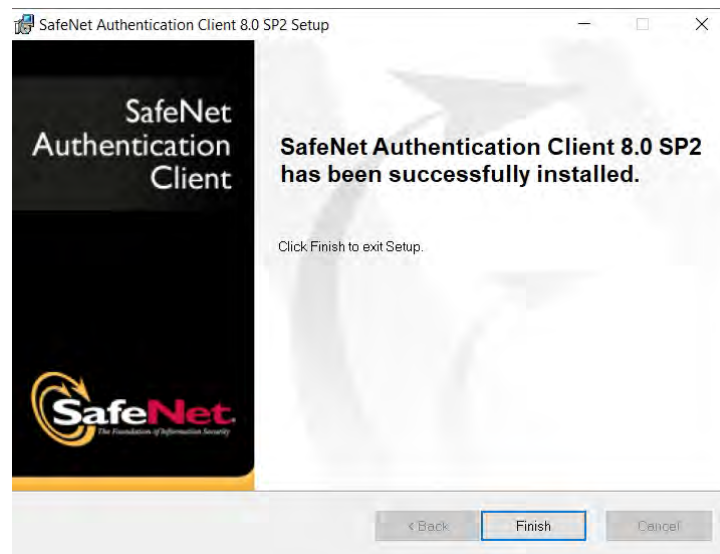
1.8 เลือกที่อยู่ในการติดตั้งโปรแกรม SafeNet Authentication Client 8.0 > กดปุ่ม Next



1.9 ระบบจะแสดงหน้าจอโปรแกรม SafeNet Authentication Client 8.0 ที่กำลังติดตั้ง



1.10 หน้าจอแสดงการติดตั้งโปรแกรม SafeNet Authentication Client 8.0 สำเร็จ > กดปุ่ม Finish



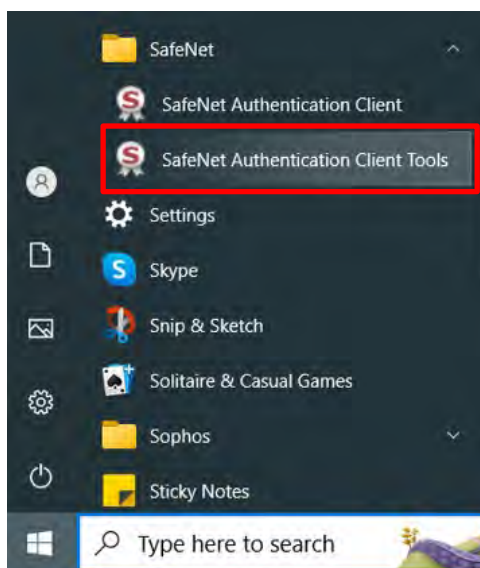
2. การ Initialization Token

สำหรับ Initial Token เป็นวิธีการ format Token เพื่อตั้งค่า Token ในส่วนของ Token Name, รหัส User, รหัส Admin และอื่นๆ โดยหลังจาก Initial Token แล้ว ข้อมูลใน Token จะหายไปทั้งหมด ดังนั้นผู้ใช้งานควรตรวจสอบข้อมูลใน Token ว่ายังมีการใช้งานอยู่หรือไม่ ก่อนทำการ Initial Token

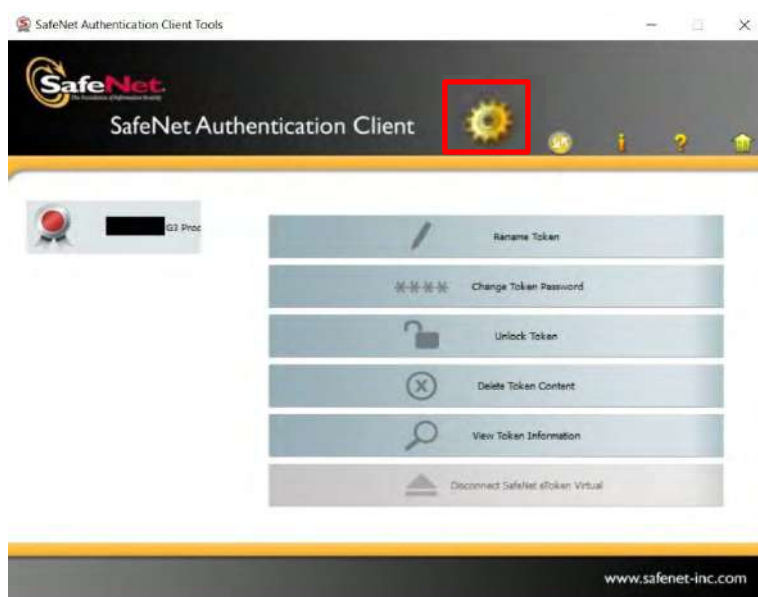
ขั้นตอนการตั้งค่าเริ่มต้น (Initialization) ให้กับ Token

2.1 ดาวน์โหลดและติดตั้งโปรแกรม SafeNet Authentication Client 8.0 (SAC) *(ตามขั้นตอนในข้อที่ 1)*

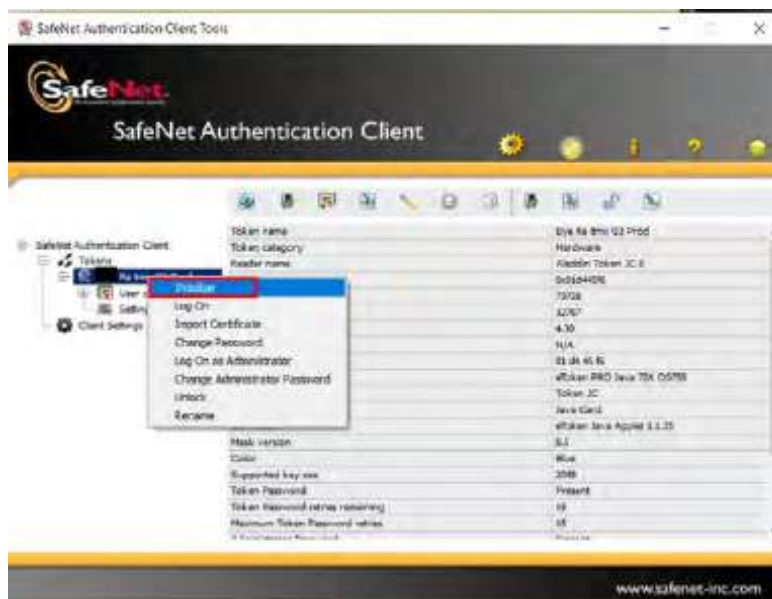
2.2 เสียบ Token กับคอมพิวเตอร์และเปิดโปรแกรม SafeNet Authentication Client 8.0 (SAC) โดยไปที่ปุ่ม Start
> Safenet > SafeNet Authentication Client Tool



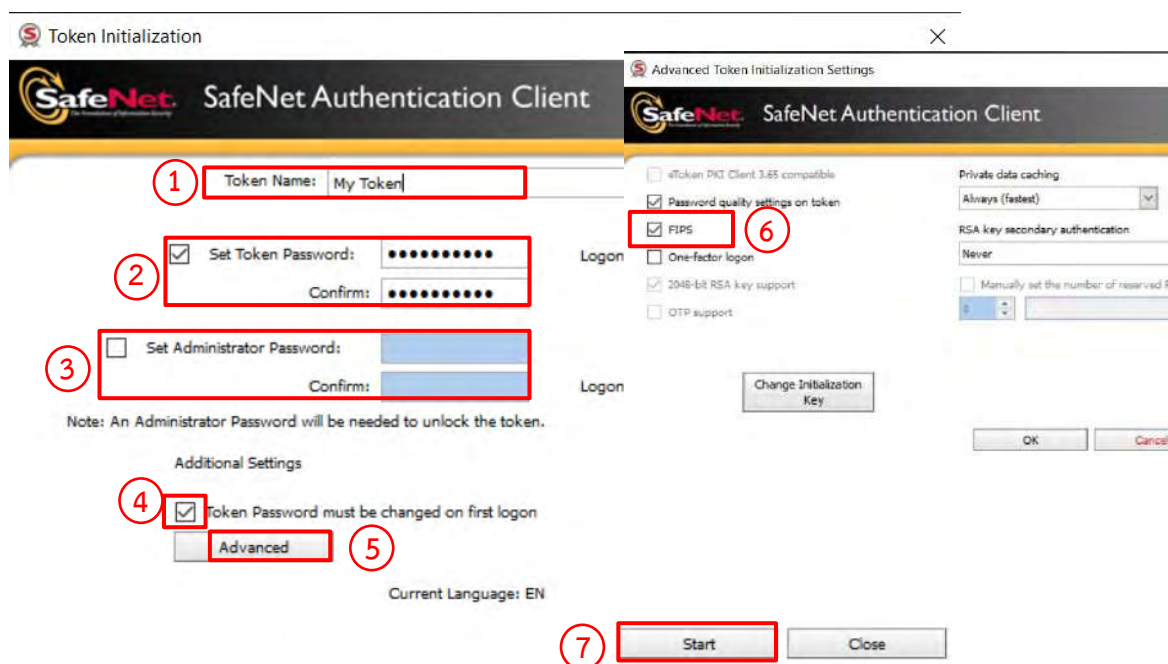
2.3 Click ที่รูปเฟือง (Advance View) หน้าแรกของโปรแกรม SafeNet Authentication Client 8.0 (SAC)



2.4 Click ขวาที่ชื่อ Token > เลือก “Initialize”



2.5 ทำการตั้งค่า Token



2.5.1 ใส่ชื่อ Token

2.5.2 กำหนด User Password

2.5.3 กำหนด Administrator Password เพื่อใช้ในการปลดล็อค เมื่อ Token ถูกล็อค **ผู้ใช้งานจำเป็นต้องตั้งรหัส Admin

2.5.4 เลือก ลบเครื่องหมายถูกออก

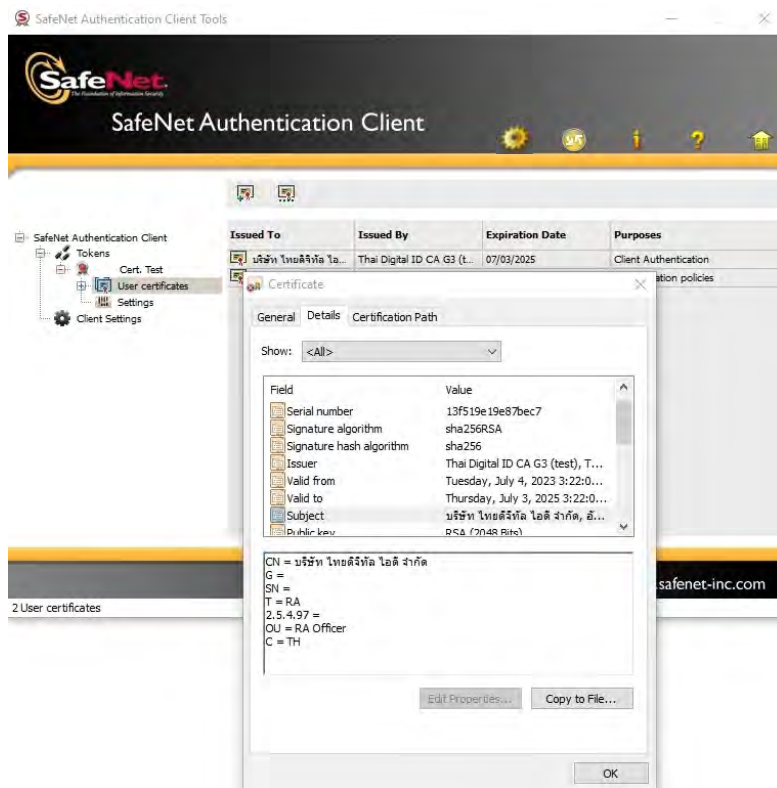
2.5.5 Click ที่ปุ่ม Advanced

2.5.6 เลือก “FIPS” > กดปุ่ม OK

2.5.7 Click ที่ปุ่ม Start > กดปุ่ม OK เพื่อยืนยันการทำ Initial

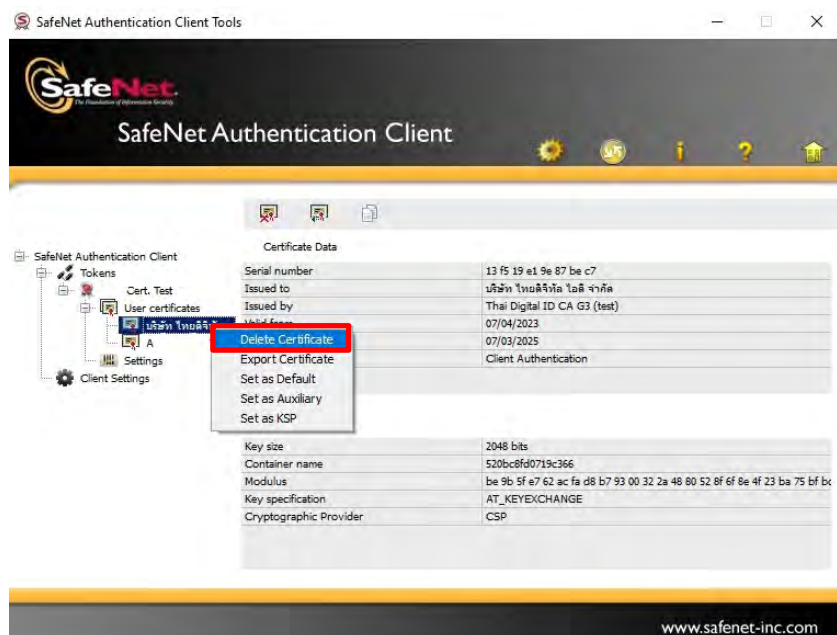
3. การตรวจสอบข้อมูลใบรับรองฯ (Certificate)

เลือกชื่อ Token > Click “User certificate” > Double Click ใบรับรองฯ ที่ต้องการตรวจสอบด้านขวา > เลือกหัวข้อ Detail ระบบจะแสดงข้อมูลใบรับรองฯ ขึ้นมา



4. การลบใบรับรองฯ (Certificate) ออกจาก Token

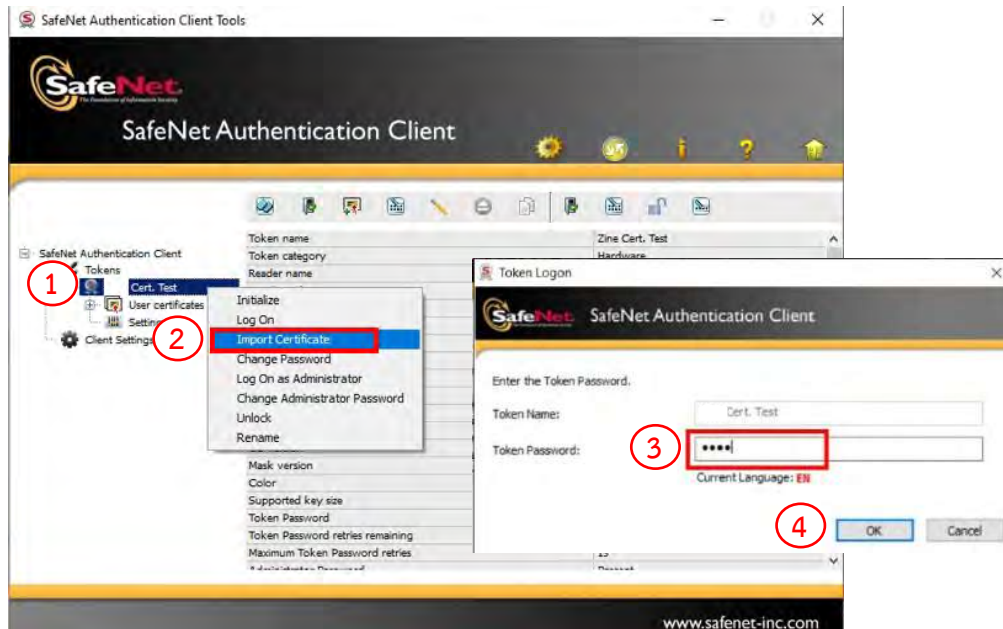
Double Click ที่ User Certificate โปรแกรมจะแสดงใบรับรองฯ ที่มีอยู่ใน Token ทั้งหมดด้านล่าง > Click ขวา ที่ใบรับรองฯ ที่ต้องการลบ > เลือก Delete Certificate



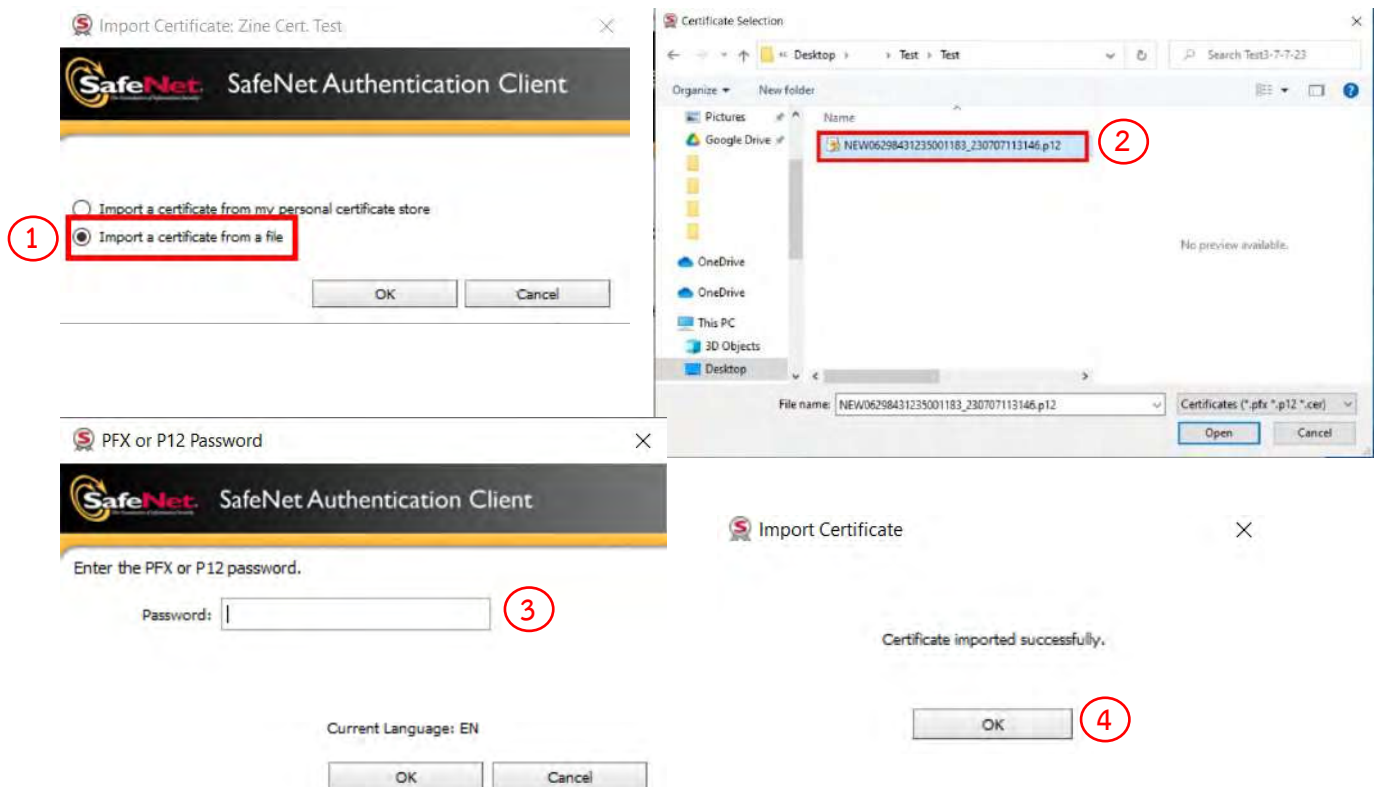
5. การ Import Certificate File เข้า Token

5.1 Import ใบรับรองฯ (Certificate) รูปแบบ PKCS12 (นามสกุลไฟล์ .p12)

5.1.1 Click ขวาที่ชื่อ Token > เลือก “Import Certificate” > ใส่ Password Token

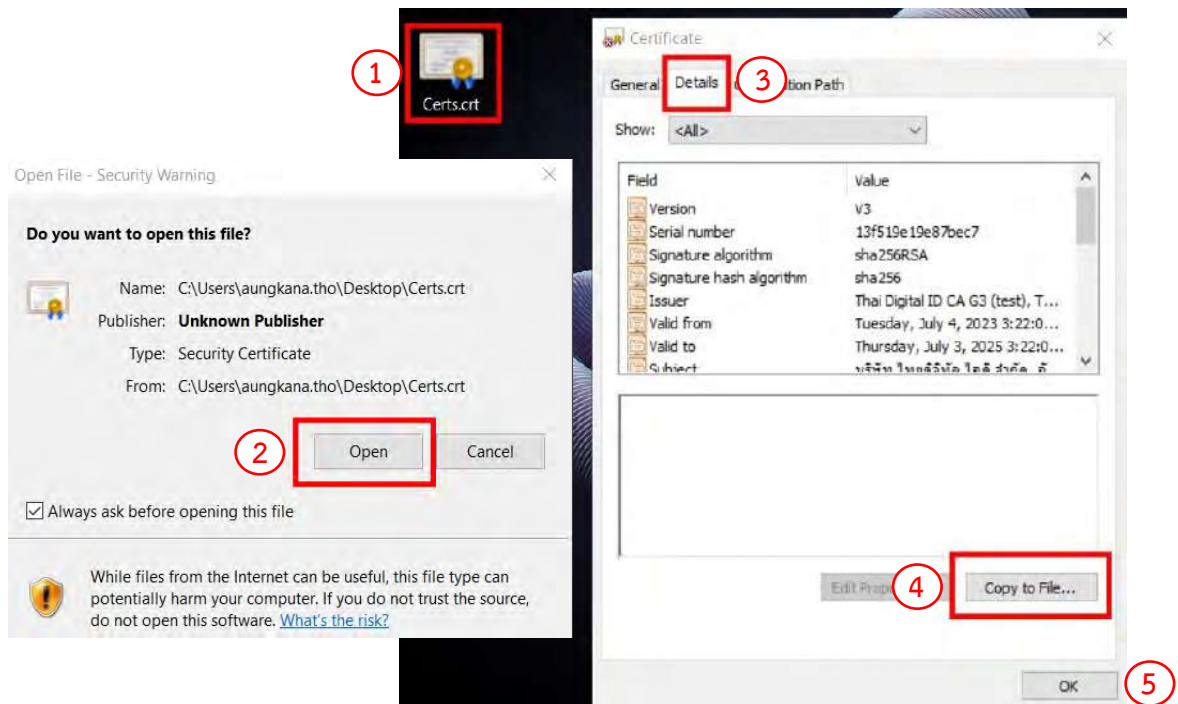


5.1.2 เลือก “Import a certificate from a file” > กดปุ่ม OK > เลือกไฟล์ใบรับรองฯ ที่ต้องการ Import > ใส่ Password Certificate File (.p12) > กดปุ่ม OK > หน้าจอแสดงการ Import certificate สำเร็จ

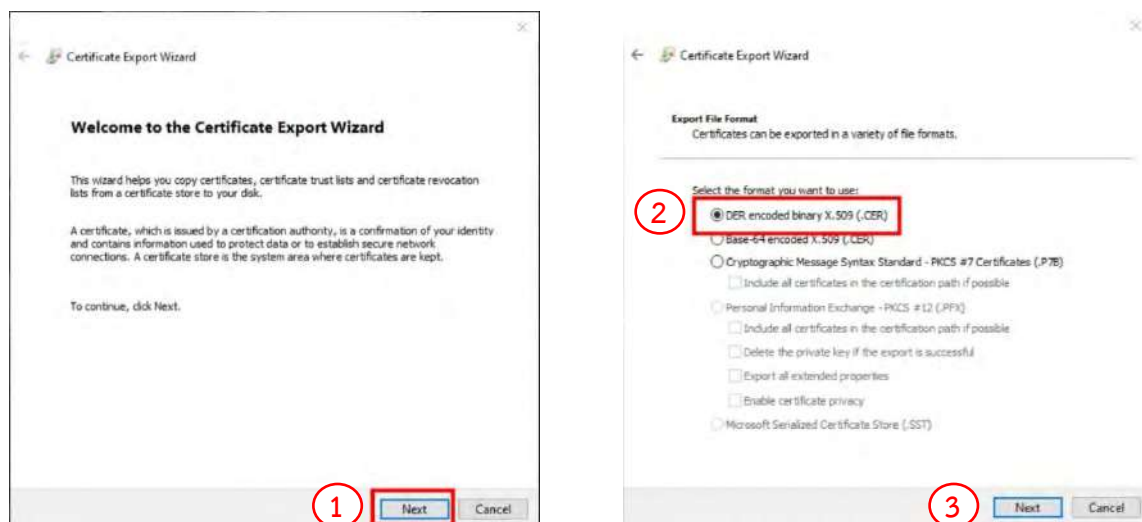


5.2 Import ใบรับรองฯ (Certificate) รูปแบบ PKCS11 (นามสกุลไฟล์ .cer)

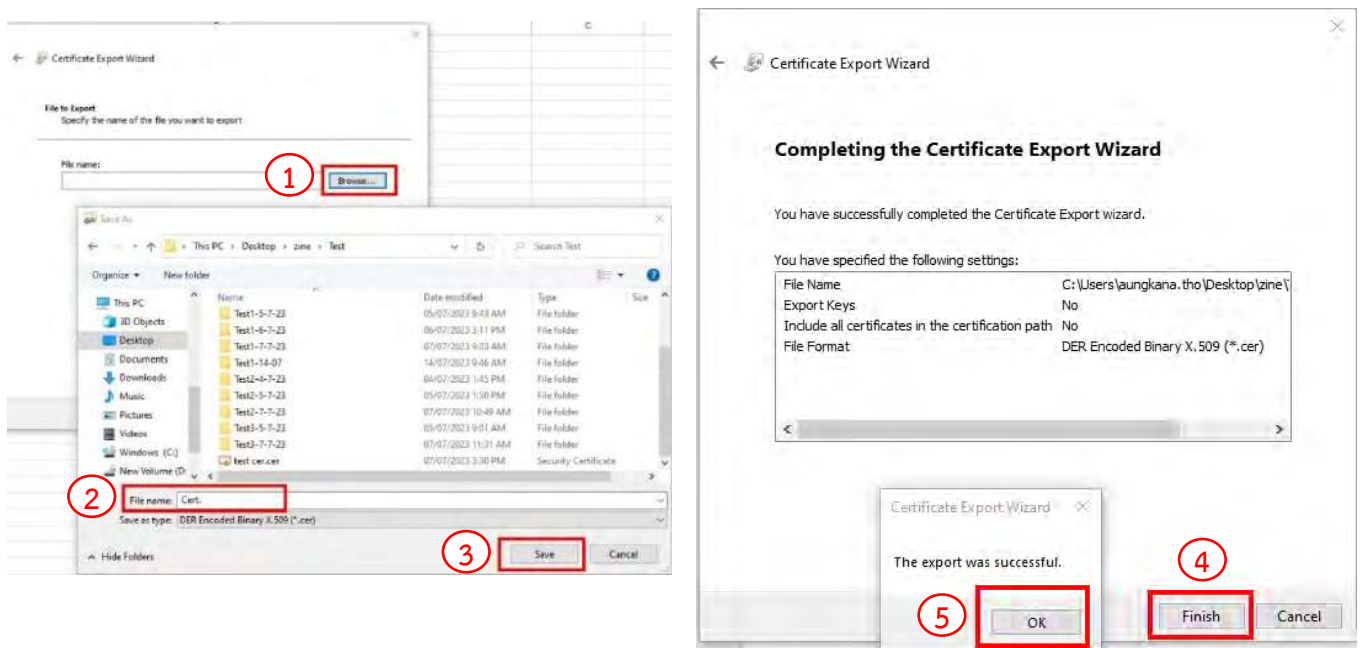
5.2.1 Double Click ที่ไฟล์ใบรับรองฯ (นามสกุลไฟล์ .cer) > Open > Detail > Copy to File



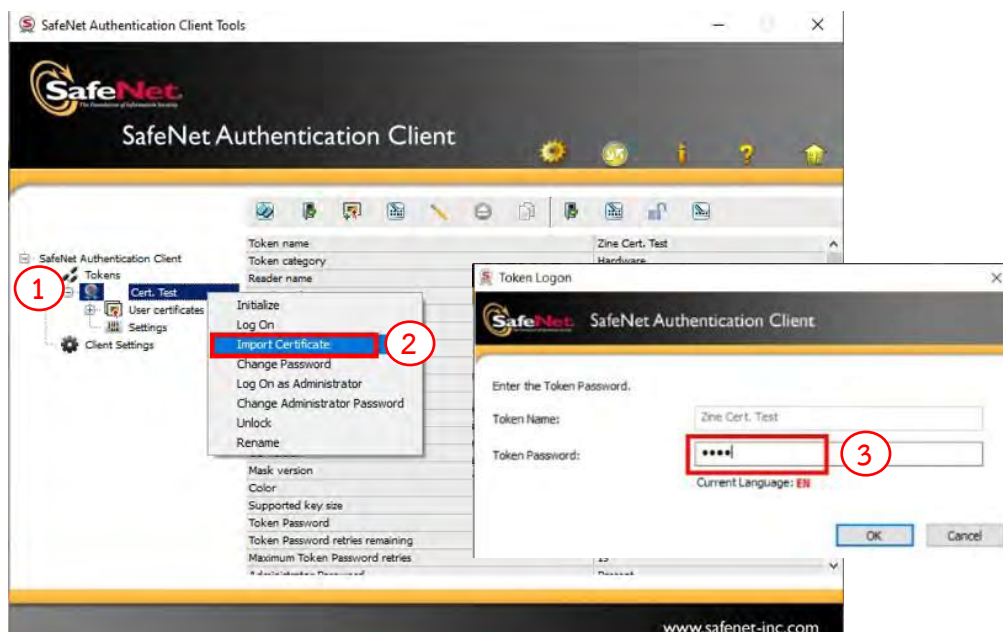
5.2.2 จะมี pop-up ขึ้นมา > กดปุ่ม Next > เลือก DER Encoded binary X.509 (.CER) > กดปุ่ม Next อีกครั้ง



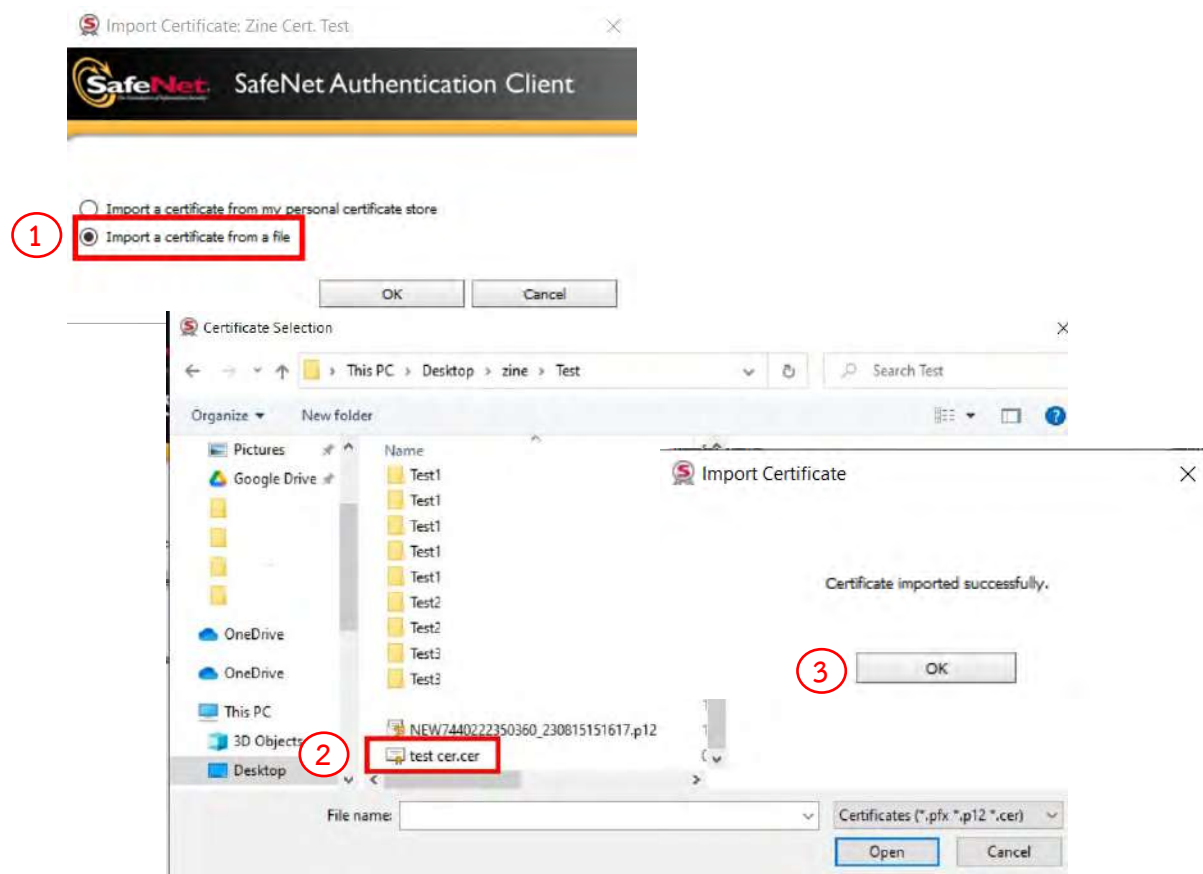
5.2.3 กดปุ่ม Browse > เลือกโฟลเดอร์จัดเก็บไฟล์และตั้งชื่อไฟล์ใบรับรองฯ > Save > Next > Finish
> กดปุ่ม OK จากนั้นผู้ใช้งานจะได้ไฟล์นามสกุล .cer บันทึกลงบนเครื่องคอมพิวเตอร์



5.2.4 เข้าโปรแกรม SafeNet Authentication Client Tool > Click ขวาที่ชื่อ Token > เลือก “Import Certificate” > ใส่ Password Token



5.2.5 เลือก “Import a certificate from a file” > กดปุ่ม OK > เลือกไฟล์ใบรับรองฯ ที่ต้องการ Import
> หน้าจอแสดงการ Import certificate สำเร็จ



**กรณีใบรับรองฯ (Certificate) รูปแบบ PKCS11 ที่ได้ติดตั้งอยู่ใน Token แล้ว ผู้ใช้งานสามารถ Export หรือนำออกจาก Token ได้ แต่จะไม่สามารถนำใบรับรองฯ ไปใช้งานได้ เนื่องจาก Private Key ใน Token จะไม่สามารถดึงออกมาได้ทุกกรณี

6. Token Lock หรือ Pin Lock

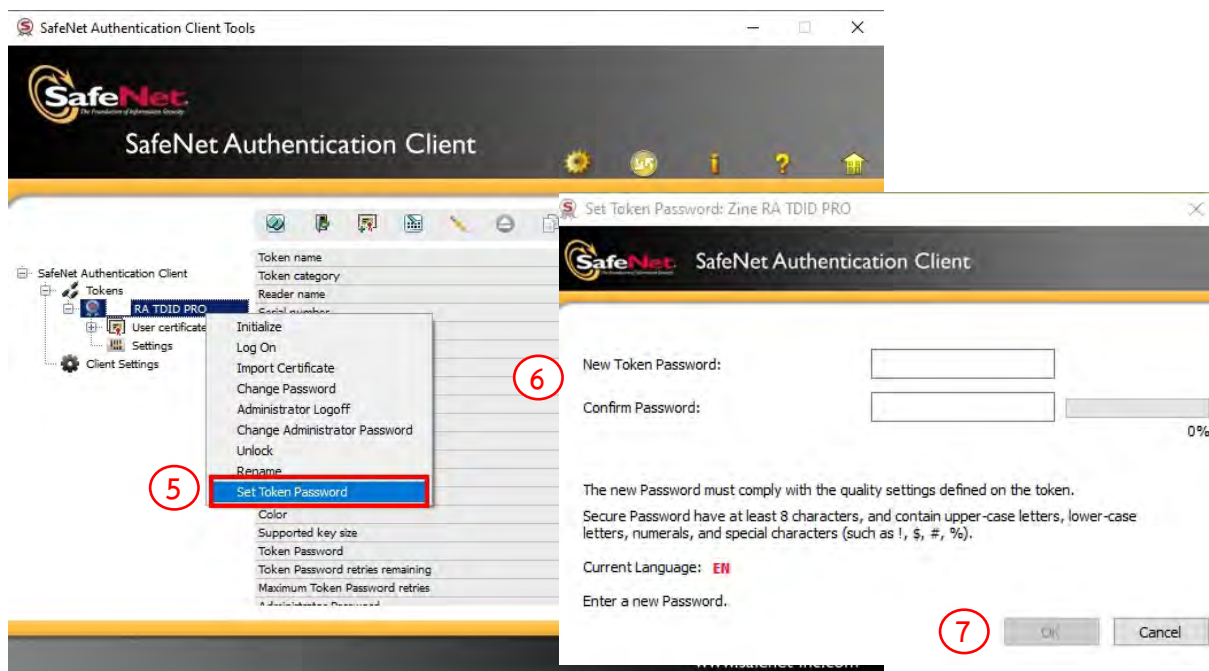
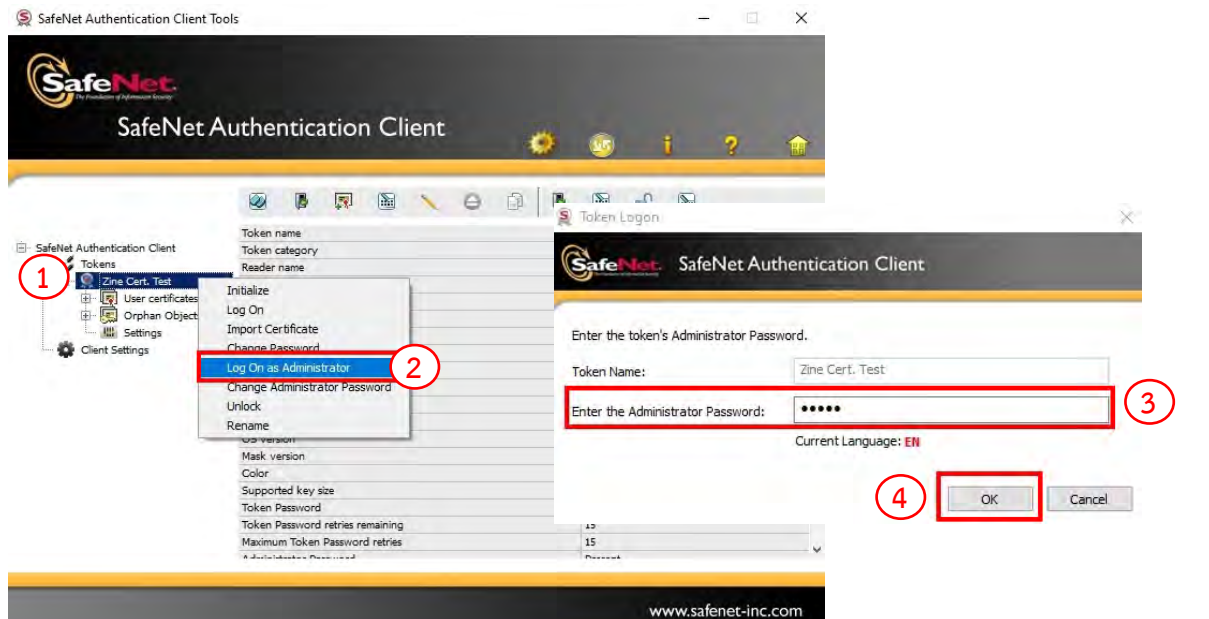
คือการใส่รหัสผิจนครบจำนวนครั้งที่ตามที Token กำหนดไว้ ซึ่งจะแบ่งออกเป็น 2 กรณี ดังนี้

6.1 กรณี User Password Lock หากมีการตั้งค่ารหัส Administrator ไว้ สามารถทำการแก้ไขได้ดังนี้

6.1.1 Click ขวาที่ชื่อ Token แล้วเลือก Log On as Administrator

6.1.2 โปรแกรมจะให้ใส่รหัส Admin แล้วกดปุ่ม OK

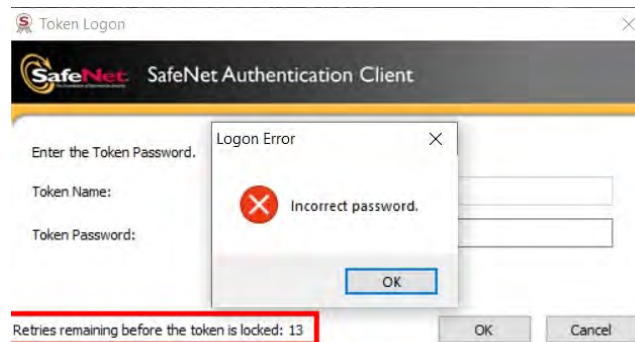
6.1.3 Click ขวาที่ชื่อ Token อีกครั้ง แล้วเลือก Set Token Password เพื่อตั้ง User Password ใหม่



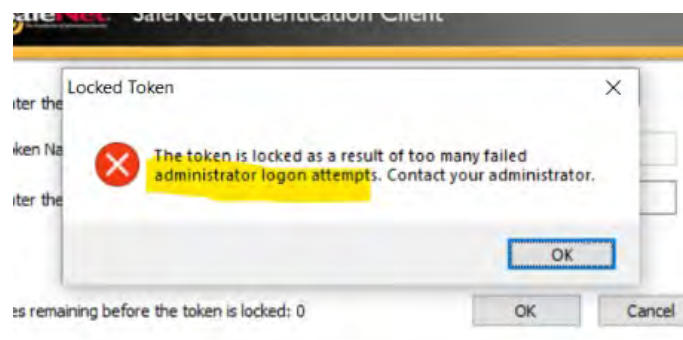
6.2 กรณี Admin Password Lock

6.2.1 Click คลิกขวาที่ชื่อ Token > เลือก Log on as Administrator ถ้าโปรแกรมแสดง pop-up ให้ใส่รหัสผ่าน แสดงว่า Token ยังไม่ Lock

- ถ้าจำรหัส Admin ได้ และระบบยังสามารถให้ใส่รหัส Admin ก็จะสามารถเข้าใช้งาน Token ได้ ทั้งนี้ให้สังเกตข้อความด้านล่างจะแสดงข้อความแจ้งจำนวนครั้งที่เหลือในการใส่รหัส

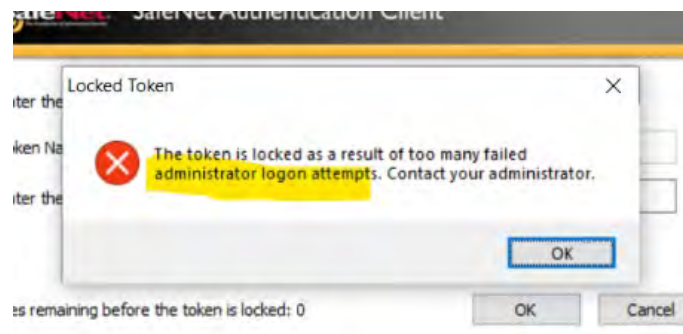


หากใส่รหัสครบตามที่โปรแกรมกำหนดไว้ Token จะ Lock ทันที ดังภาพด้านล่าง



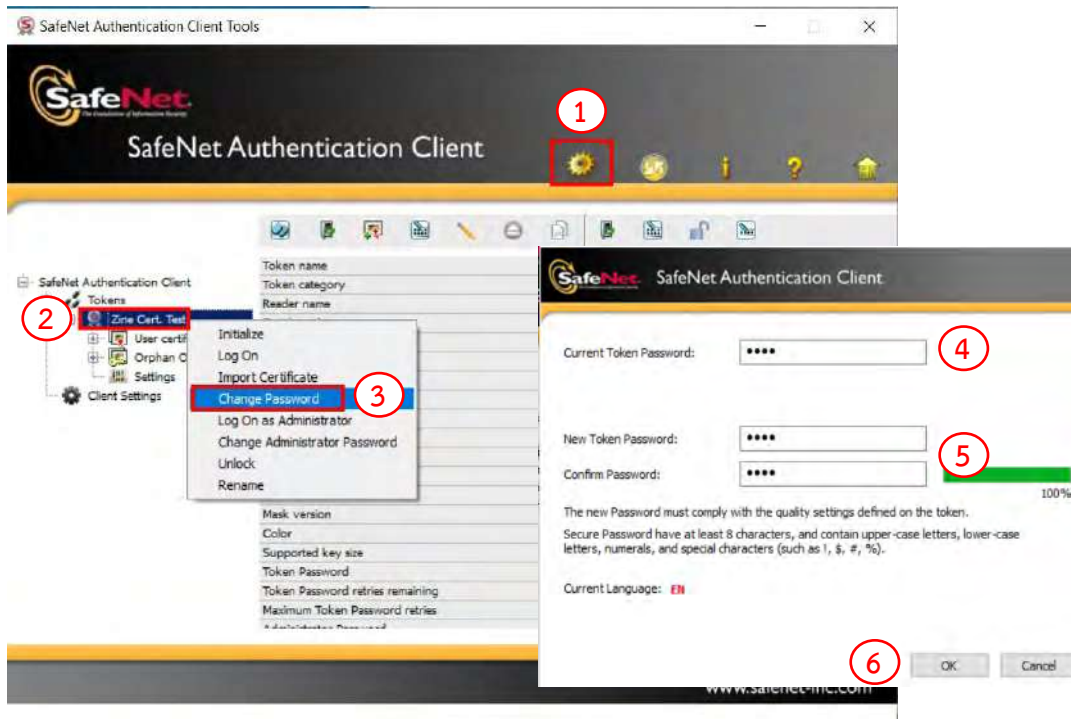
- ถ้าจำรหัส Admin ไม่ได้ แนะนำให้ Initial Token ซึ่งใบรับรองฯ ที่อยู่ใน Token จะหายไปทั้งหมด

6.2.2 กรณี Click ขวาที่ชื่อ Token > เลือก Log on แล้วโปรแกรมขึ้น Error ตามรูป แสดงว่า Token Lock กรณีนี้จะไม่สามารถแก้ไขได้ทุกกรณี ผู้ใช้งานต้องซื้อ Token + ใบรับรองฯ ใหม่เท่านั้น

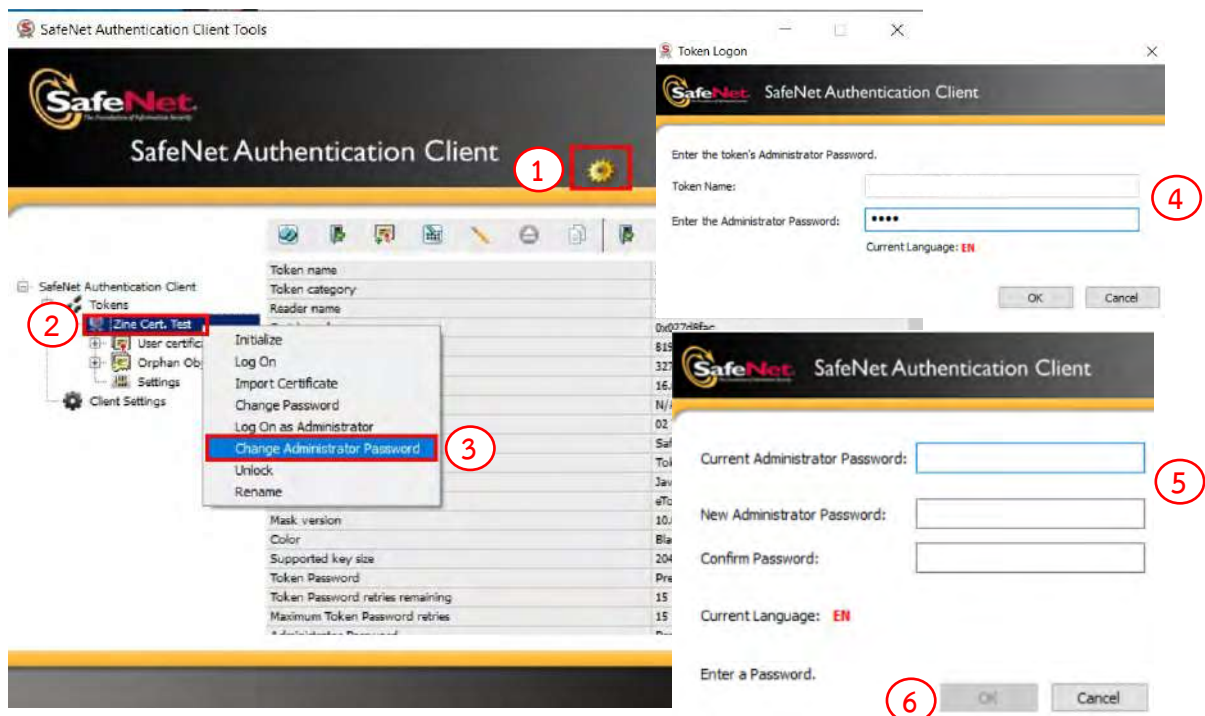


7. การเปลี่ยนแปลง Password

7.1 เปลี่ยน User Password กดที่รูปเฟือง (Advance View) > Click ขวาที่ชื่อ Token > เลือก “Chang Password”
> ใส่รหัสปัจจุบัน 1 ครั้ง และใส่รหัสใหม่ 2 ครั้ง > กดปุ่ม OK



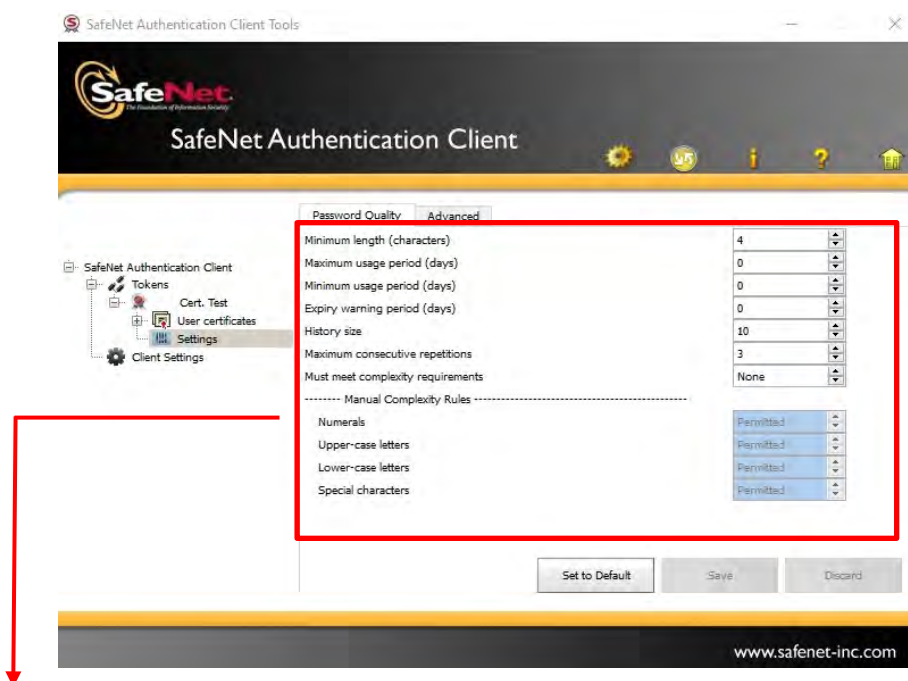
7.2 เปลี่ยน Administrator Password กดที่รูปเฟือง (Advance View) > Click ขวาที่ชื่อ Token
> เลือก “Chang Administrator Password” > ใส่รหัสปัจจุบัน 1 ครั้ง > กดปุ่ม OK > ใส่รหัส Admin ปัจจุบัน 1 ครั้ง
และใส่รหัสใหม่ 2 ครั้ง > กดปุ่ม OK



8. การ Setting Password Quality

คือการตั้งค่าเงื่อนไขของ Password ให้มีความปลอดภัยมากยิ่งขึ้น โดยเข้าที่โปรแกรม SafeNet > กดที่รูปเฟือง

(Advance View) > Setting > Password Quality



เงื่อนไข	ความหมาย
Minimum length (characters)	กำหนดจำนวนตัวอักษรขั้นต่ำของรหัส Token ทั้ง User และ Admin
Maximum usage period (days)	กำหนดให้รหัส User ได้สูงสุดกี่วัน
Minimum usage period (days)	กำหนดให้รหัส User ได้ต่ำสุดกี่วัน
Expiry warning period (days)	กำหนดวันแจ้งเตือนรหัส User หมดอายุล่วงหน้า - เมื่อมีการแจ้งเตือน โปรแกรมจะให้เปลี่ยนรหัส User ใหม่ทันที แต่สามารถยกเลิกได้ หากยังไม่ต้องการจะเปลี่ยนรหัสใหม่
History size	กำหนดจำนวนรหัสผ่านก่อนหน้านี้ที่ต้องไม่ตั้งค่าซ้ำอีก
Maximum consecutive repetitions	กำหนดจำนวนครั้งของรหัส User เดิมที่ใช้ ซ้ำกันได้กี่ครั้ง
Must meet complexity requirements	กำหนดเงื่อนไขการตั้งรหัส - None : ไม่กำหนด จะใส่ตัวอักษรเป็นอะไรก็ได้ - At least 2 types : ต้องมีอย่างน้อย 2 ประเภท - At least 3 types : ต้องมีอย่างน้อย 3 ประเภท - Manual : สามารถกำหนดได้เองว่าจะให้มีตัวอักษรประเภทไหนบ้าง
Manual Complexity Rules	กำหนดเงื่อนไขประเภทตัวอักษร - Numerals : ตัวเลข - Upper-case letters : ตัวอักษรพิมพ์ใหญ่ - Lower-case letters : ตัวอักษรพิมพ์เล็ก - Special characters : อักขระพิเศษ