

## ระบบบริหารจัดการลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)

ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) คือ การลงลายเซ็นในรูปแบบอิเล็กทรอนิกส์ โดยใช้ใบรับรอง (Certificate) กำกับในไฟล์เอกสาร ซึ่งทำให้สามารถระบุตัวบุคคลหรือองค์กรผู้เป็นเจ้าของลายเซ็น เพื่อแสดงว่าบุคคลหรือองค์กรดังกล่าวเป็นเจ้าของหรือ ยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น และสามารถตรวจสอบการเปลี่ยนแปลงของเอกสารย้อนหลังได้

การลงลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ด้วยการใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate) จะใช้เทคโนโลยีเข้ารหัสกุญแจสาธารณะ (Public Key Infrastructure : PKI) ทำให้การใช้ลายเซ็นอิเล็กทรอนิกส์ ไม่ใช่แค่การนำภาพลายเซ็นหรือสัญลักษณ์ไปประทับบนไฟล์เท่านั้น เพราะการใช้ลงลายเซ็นอิเล็กทรอนิกส์ จะมีการเข้ารหัสและถอดรหัส เป็นวิธีการที่ช่วยให้ผู้ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นๆ เชื่อมั่นได้ว่าผู้ที่ลงลายมือชื่ออิเล็กทรอนิกส์ เป็นผู้ทำธุรกรรมหรือยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์ดังกล่าวจริง อีกทั้งยังสามารถตรวจสอบได้ว่า ข้อมูลอิเล็กทรอนิกส์ดังกล่าวถูกแก้ไขหลังจากที่มีการลงลายเซ็นอิเล็กทรอนิกส์หรือไม่ ซึ่งสอดคล้องตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 9 และ 26 และ ระเบียบมหาวิทยาลัยเทคโนโลยีสุรนารี ว่าด้วยงานสารบรรณ พ.ศ. 2566

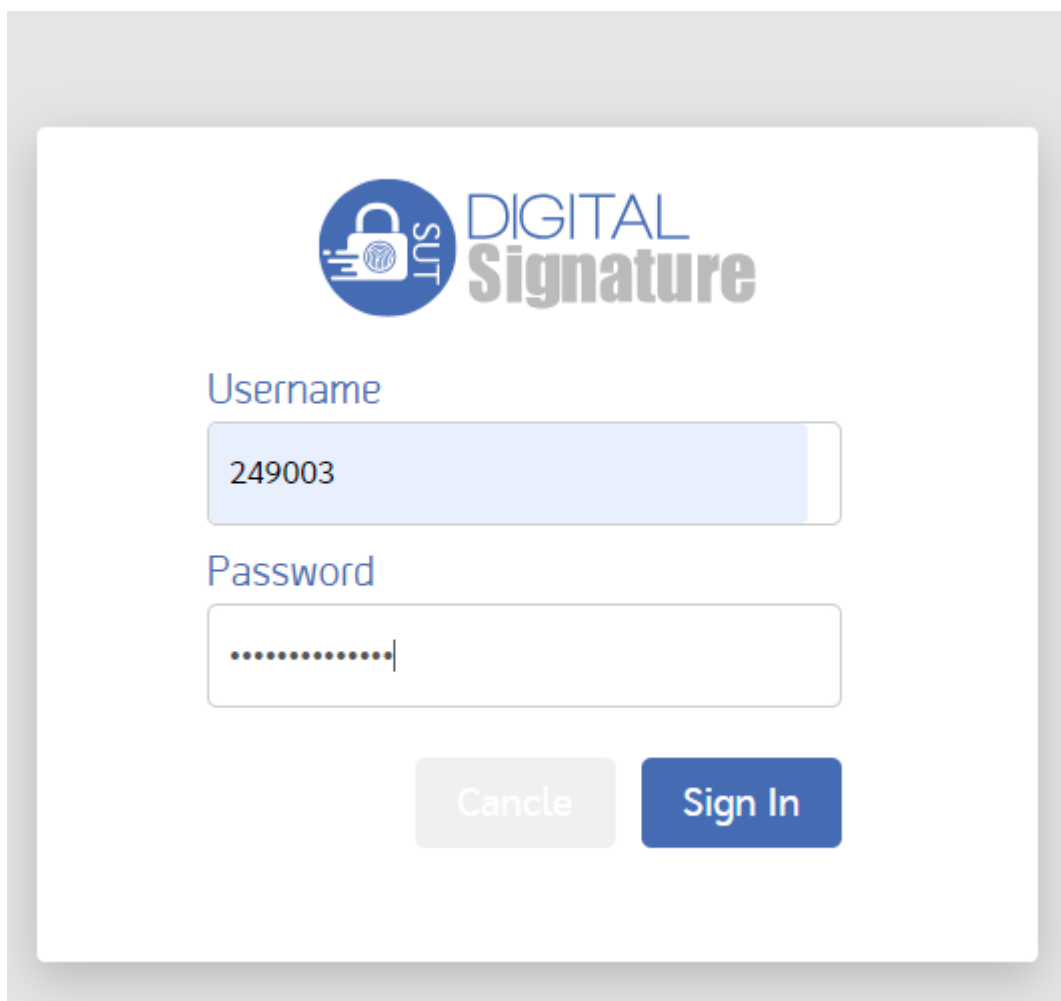


ศูนย์คอมพิวเตอร์ ได้พัฒนาระบบบริหารจัดการลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) สำหรับให้บริการใบรับรอง(Certificate) แก่ลายเซ็นอิเล็กทรอนิกส์ ซึ่งจะทำให้ผู้ใช้งานสามารถ

- สามารถบริหารจัดการใบรับรองลายเซ็นได้ด้วยตนเอง
- การกำหนด password ที่ใช้ควบคู่กับลายเซ็นได้ด้วยตนเอง
- ขอยกเลิก (Revoke) ลายเซ็นได้ โดยไม่ต้องรอเจ้าหน้าที่ดำเนินการ

## 1.การเข้าสู่ระบบบริหารจัดการลายเซ็นอิเล็กทรอนิกส์ (Digital Signature)

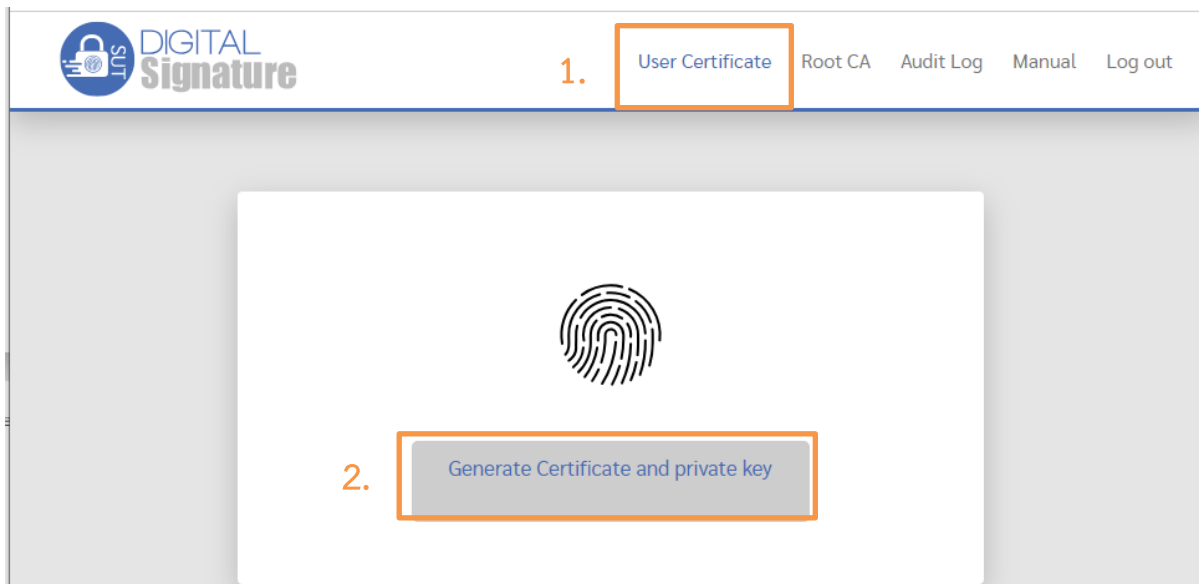
1.1 เข้าสู่ระบบบริหารจัดการลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ที่เว็บไซต์ <https://digital-cert.sut.ac.th> และ Login ด้วยรหัสพนักงาน – password เดียวกับระบบ SUTmail



The image shows a login form for the Digital Signature system. At the top, there is a logo consisting of a blue padlock icon with 'SUT' written inside it, followed by the text 'DIGITAL Signature'. Below the logo, there are two input fields. The first is labeled 'Username' and contains the text '249003'. The second is labeled 'Password' and contains a series of dots representing a masked password. At the bottom of the form, there are two buttons: a light gray 'Cancel' button and a blue 'Sign In' button.

## 2. การสร้างใบรับรองลายเซ็นอิเล็กทรอนิกส์ และการกำหนด private key

2.1 ที่เมนู “User Certificate” คลิก “Generate Certificate and private key” เพื่อสร้าง ใบรับรองลายเซ็นอิเล็กทรอนิกส์ และ สร้างรหัส private key



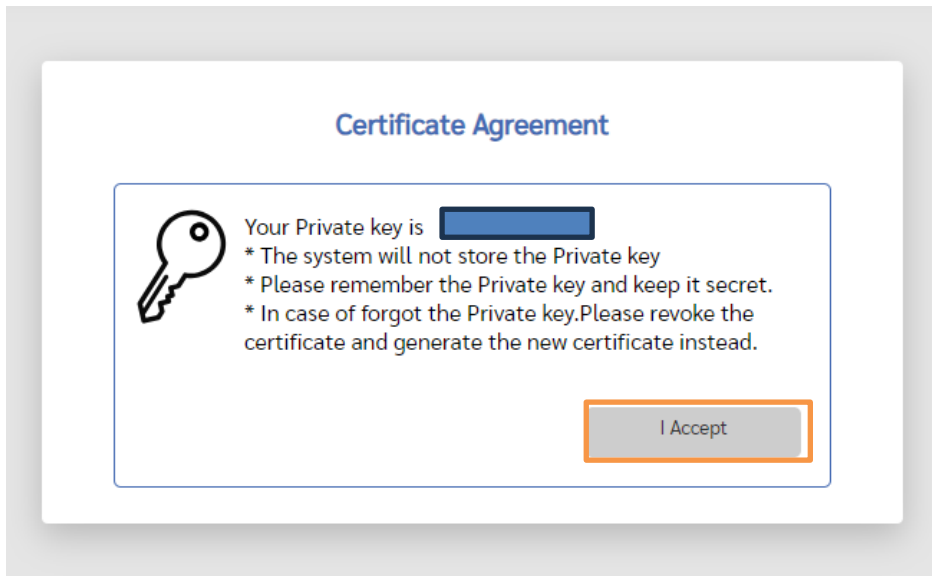
### 2.2 กำหนดรหัสผ่าน (private key)

- รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร
- รหัสผ่านต้องประกอบด้วยอักษรตัวพิมพ์ใหญ่, ตัวพิมพ์เล็ก, และตัวเลข

เมื่อสร้างรหัสผ่าน (private key) เรียบร้อยแล้ว กดปุ่ม submit

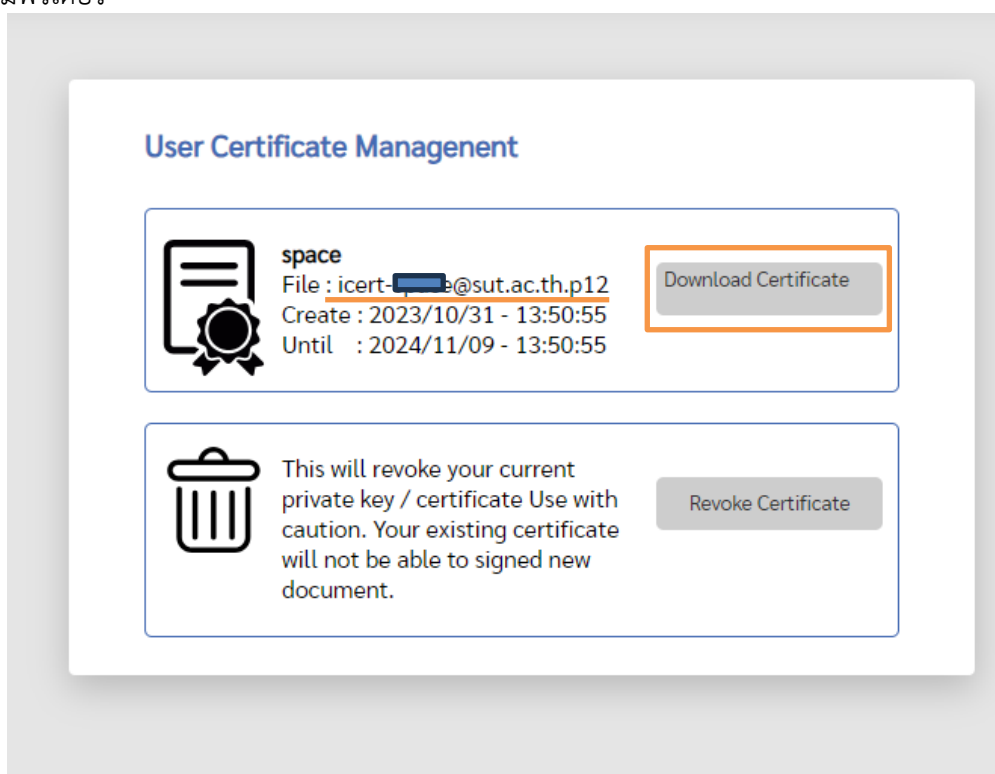
The screenshot shows a form titled 'Choose PKCS12 Encryption Password'. It includes the following elements: a fingerprint icon at the top; the title 'Choose PKCS12 Encryption Password' with sub-requirements: 'At least 8 characters', 'Contains uppercase and lowercase letters', and 'Contains numbers'; two input fields labeled 'Password' and 'Confirm-password', both containing masked characters (dots); and two buttons at the bottom: 'Cancel' and 'Submit', with the 'Submit' button highlighted by an orange box.

2.3 ระบบจะแสดง private key ที่ท่านได้ตั้งไว้ ให้กดปุ่ม I accept เพื่อยอมรับ



ทั้งนี้ระบบจะไม่เก็บ private key ของท่าน / กรณีที่ท่านไม่สามารถจำ private key ที่ใช้ควบคู่กับ certificate ได้ ให้ทำการ เพิกถอน (revoke) ใบรับรองลายเซ็นอิเล็กทรอนิกส์ (certificate) เดิม และสร้างใบรับรองลายเซ็นอิเล็กทรอนิกส์และกำหนด private key ใหม่อีกครั้ง

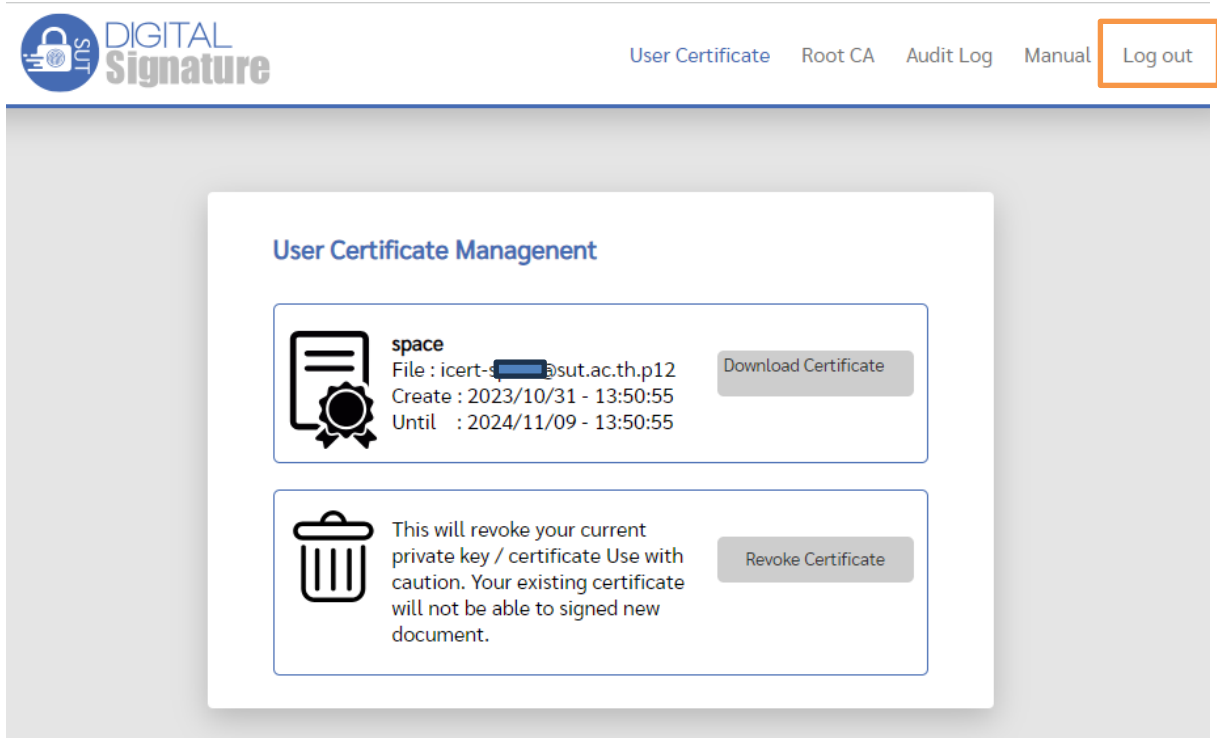
2.4 ระบบจะแสดง ใบรับรองลายเซ็นอิเล็กทรอนิกส์ (certificate) ของท่าน ให้ท่านทำการ download โดยคลิกที่ปุ่ม “Download Certificate” ระบบจะดาวน์โหลดไฟล์ “icert-email@sut.ac.th.p12” เก็บไว้ในเครื่องคอมพิวเตอร์



- ท่านจะได้รับใบรับรองอิเล็กทรอนิกส์ (ไฟล์นามสกุล .p12) ซึ่งใช้ควบคู่กับ private key ตามขั้นตอนที่ 2.3
- เมื่อดาวน์โหลดใบรับรองอิเล็กทรอนิกส์ (ไฟล์นามสกุล .p12) เรียบร้อยแล้ว ให้ดำเนินการติดตั้งตามคู่มือต่อไป
  - [คู่มือการติดตั้งเพื่อใช้งาน Digital Signature](#) (ด้วยโปรแกรม Acrobat Reader)
  - [คู่มือการติดตั้งเพื่อใช้งาน Digital Signature](#) (ด้วยโปรแกรม Foxit PDF Editor)

## 2.5 การ log out ออกจากระบบ

คลิกที่เมนู logout เพื่อออกจากระบบ



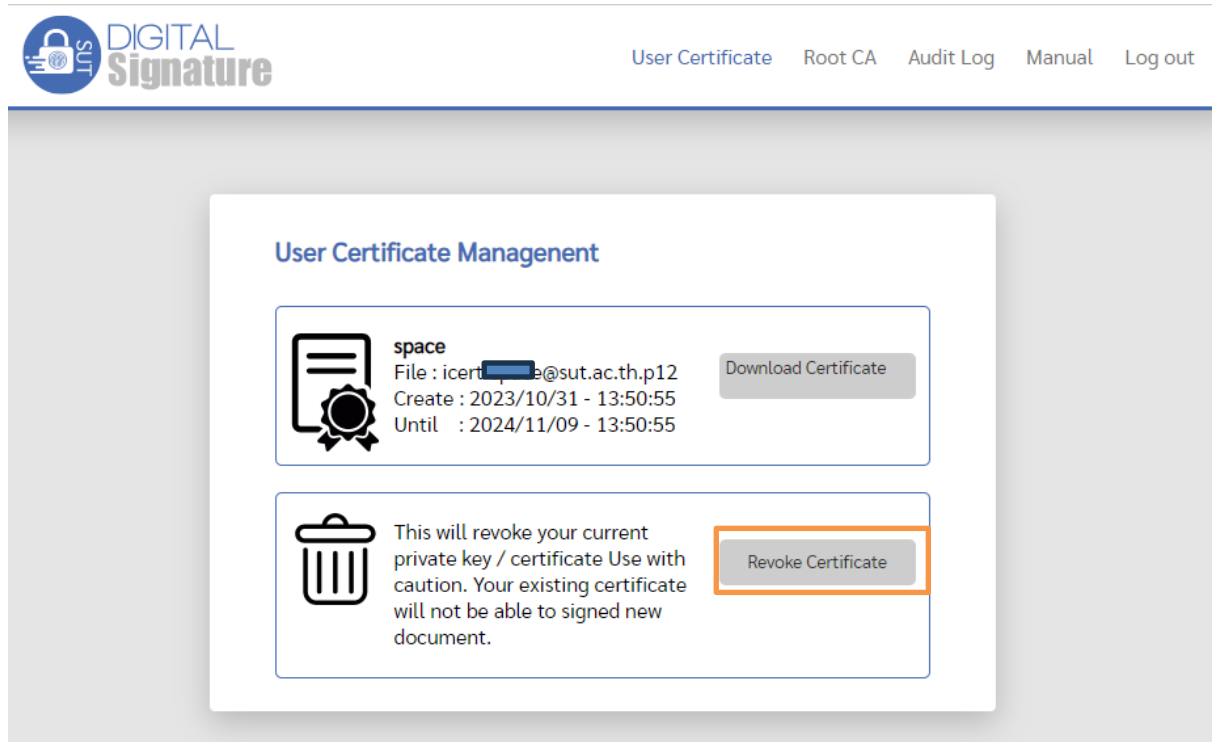
## 3. การเพิกถอนใบรับรองลายเซ็นอิเล็กทรอนิกส์ (revoke certificate)

ท่านสามารถเพิกถอนใบรับรองลายเซ็นอิเล็กทรอนิกส์ได้ในกรณีดังนี้

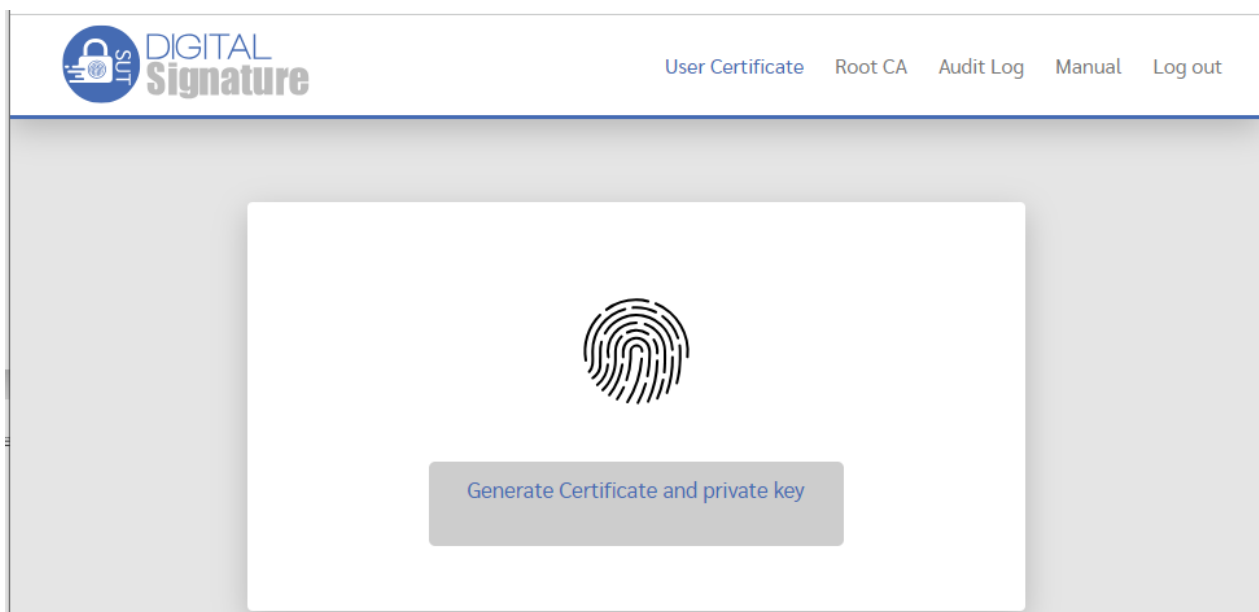
- กรณีที่ใบรับรองลายเซ็นอิเล็กทรอนิกส์หมดอายุการใช้งาน
- จำ private key ที่ใช้ควบคู่กับใบรับรองลายเซ็นอิเล็กทรอนิกส์ไม่ได้ ทำให้ไม่สามารถลงลายเซ็นอิเล็กทรอนิกส์ได้

- Private key รั่วไหล หรือไม่เป็นความลับ

ทั้งนี้ท่านสามารถเพิกถอนใบรับรองลายเซ็นอิเล็กทรอนิกส์ (revoke certificate) โดยการกดปุ่ม “Revoke Certificate”



จากนั้นจะปรากฏเมนูการสร้าง certificate ใหม่อีกครั้ง



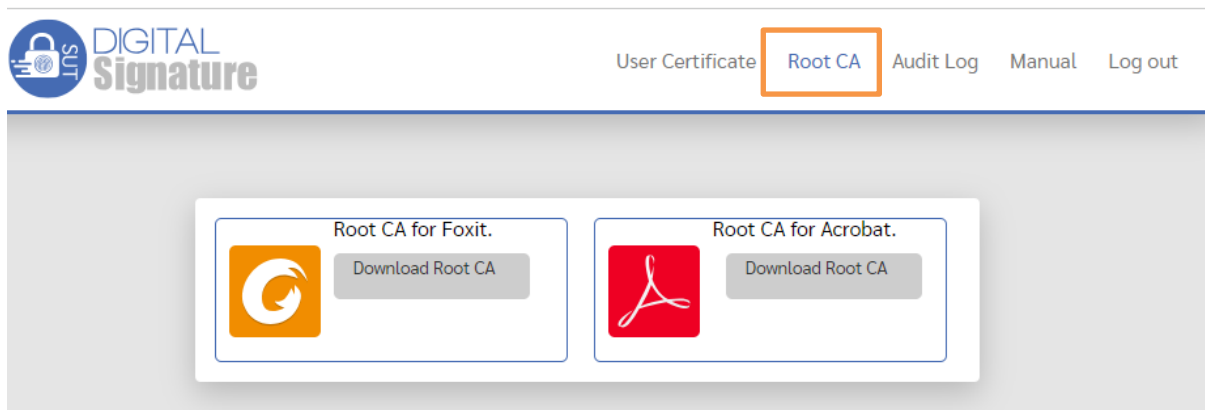
## 4. แนะนำการใช้งานเมนูอื่นๆ

### 4.1 เมนู Root CA

ใช้สำหรับการดาวน์โหลดไฟล์ Root CA ที่ได้จาก Thai University Consortium เพื่อติดตั้ง Thai University Consortium RootCA ลงบนเครื่องคอมพิวเตอร์ ทำให้เครื่องคอมพิวเตอร์เชื่อถือใบรับรองลายเซ็นอิเล็กทรอนิกส์ (trust certificate)

รายละเอียดดังปรากฏในคู่มือการติดตั้งใบรับรองลายเซ็นอิเล็กทรอนิกส์

- [คู่มือการติดตั้งเพื่อใช้งาน Digital Signature](#) (ด้วยโปรแกรม Acrobat Reader)
- [คู่มือการติดตั้งเพื่อใช้งาน Digital Signature](#) (ด้วยโปรแกรม Foxit PDF Editor)



### 4.2 เมนู Audit log

สำหรับการตรวจสอบรายการดำเนินการบนระบบ digital signature

