Sixcape IDcentral

7.0.0.0

Integration Guide

CryptoServer HSM

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-07-28
Status	PUBLISHED
Document No.	IG-2026-0081

Table of Contents

1 Introduction 5
1.1 About This Guide 5
1.2 Target Audience for This Guide 5
1.3 Document Conventions 5
1.4 Abbreviations 6
2 Overview 9
2.1 IDcentral 9
2.2 Utimaco u.trust Identify 9
3 Integration Requirements and Prerequisites 10
3.1 Tested Versions 10
3.2 Software Requirements 10
3.3 Prerequisites 10
4 Utimaco u.trust Identify Configuration 12
4.1 Creating CMP Client Certificate Profile for Issuing Client Certificate used for Authentication 12
4.2 Creating Smartcard Certificate Profile for Certificate that Client Can Request 16
5 IDcentral Smartcard License Configuration 23
5.1 Hardware Token License Activation 23
5.2 Creating a User for License Allotment 26
5.3 Hardware Token License Allotment to User 32
5.4 Removal of Hardware Token License Allotment 34
6 Integrating IDcentral with Utimaco u.trust Identify 36
6.1 Generate a Client Certificate to Authenticate to u.trust Identify PKI 36
6.1.1 Generate CSR for Client 36
6.1.2 Upload CSR file to CMS for Creating Client Certificate 49
6.1.3 Install and Export Client Certificate 50
6.2 u.trust Identify CA Configuration on IDcentral 63
6.2.1 CA Configuration 63
6.2.2 Certificate Profile Creation 67
6.2.3 Certificate Profile Assignment 71
6.2.4 Removal of User or Group from Certificate Profile 74
6.3 Device Provisioning 75

6.4 Device License Allotment to User ... 76
6.5 Removal of Device License Allotment ... 78
7 Secure Authentication Suite Smartcard Certificate Enrollment ... 79
7.1 Secure Authentication Suite Installation ... 79
7.2 (Optional) Enabling Virtual smart card ... 86
7.3 Smartcard Certificate Enrollment ... 88
7.4 Verify Smartcard Certificate from CMS Web ... 99
8 Troubleshooting ... 100
9 Further Information ... 103
10 Contact and Support Information ... 104

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco u.trust Identify product can be found in the document directory of the Utimaco u.trust Identify product bundle.

All Utimaco u.trust Identify product documentation is available from Utimaco's website at *https://utimaco.com/*.

1.1 About This Guide

This guide provides an integration guide explaining how to integrate an IDcentral with u.trust Identify.

1.2 Target Audience for This Guide

This guide is intended for administrators of IDcentral Administrator and of Utimaco u.trust Identify.

1.3 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 1: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AD	Active Directory
API	Application Programming Interface
CA	Certificate Authority
CMS	Cryptographic Message Syntax
CMPv2	Certificate Management Protocol version 2
CSAR	Cloud Service Architecture
CSR	Certificate Signing Request

Abbreviation	Meaning
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HSM	Hardware Security Module
ID	Identity
IP	Internet Protocol
IRP	Identity Registration Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MMC	Microsoft Management Console
MS SQL	Microsoft Structured Query Language
PCIe	PCI Express Interface
PFX	Personal Information Exchange
PIN	Personal Identification number
PKCS#11	Public-Key Cryptography Standard #11

Abbreviation	Meaning
PKI	Public Key Infrastructure
SRV	Service
SMIME	Secure Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
TPM	Trusted Platform Module
URL	Uniform Resource Locator
XML	Extensible Markup Language

Table 2: List of abbreviations

2 Overview

2.1 IDcentral

The IDcentral platform is the core digital identity and authentication infrastructure behind Sixscape's portfolio of products. The IDcentral on-prem offering provides X.509 digital certificate services in the form of certificate request, retrieval, deployment, and ongoing management including lifecycle management. The automation delivered ultimately shortens time to deployment and decreases total cost of ownership while ensuring you achieve your SLA and compliance obligations.

2.2 Utimaco u.trust Identify

u.trust Identify is the flexible and scalable all-in-one solution to deploy and operate a PKI, providing all core components that are needed for setting up and running a PKI and the secure and reliable generation, issuance, renewal, and revocation of certificates. Certificate Authority (CA), Certificate Management System (CMS) which also acts as a Registration Authority (RA), Validation Service (VS) including Online Certificate Status Protocol (OCSP) Responder and Proxy, as well as CRL support, and support for Active Directory Certificate Service (ADCS) integration. The flexible design allows for easy adaption of requirements from different industries, applications and use cases with minimal configuration effort. Whether it is smart metering, eHealth, wearables, eID, document signing, S/MIME, TLS, or a combination of all these use cases – u.trust Identify is the perfect fit.

3 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco u.trust Identify with IDcentral.

Operating System	IDcentral IRP Version	Utimaco u.trust Identify
Windows Server 2016	7.0.0.0	Release 2023.1

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
IDcentral Identity Registration	7.0.0.0
Secure Authentication Suite	1.1.1.0

Table 4: List of software requirements

Set up an account on the Utimaco support portal and request download access.

3.3 Prerequisites

This section lists the pre-requisites for integrating IDcentral with u.trust Identify.

- Sixscape IDcentral software should be installed as listed in Tested Versions.
- u.trust Identify must be deployed as listed in *Tested Versions*.

- The Sixscape's IDcentral Identity Registration Service, communicates with u.trust Identify PKI through the CMPv2 Protocol interface. Conforming deployments must enable and set up the CMPv2 interface in u.trust Identify PKI prior to configuring the connection in IDcentral. Refer u.trust Identify - CMS Installation and Administration Guide for more details.
- Outbound firewall rule should be enabled in IDcentral server for the CMPv2 service port of u.trust Identify PKI.
- A domain joined client computer running Windows 10 or above with an installed and fully functional TPM (version 1.2 or version 2.0) to issue smartcard certificate.
- Acquire the following licenses from IDcentral. The installation of license is demonstrated in the next chapter.
    - Hardware Token License Device License.
    - Device License.

4 Utimaco u.trust Identify Configuration

This section describes the process of configuring the u.trust Identify to work with IDcentral. The deployment of u.trust Identify PKI is out of scope of this documentation, you can refer to the manual *u.trust Identify - PKI Installation and Administration Guide* for deployment guide.

There are two types of certificate profile you will need to have installed on u.trust Identify CMS. First is the CMP ClientCertificate Profile which client will use to authenticate to u.trust Identify and will request certificate from the CA. This CMP Client Certificate Profile is preinstalled as part of u.trust Identify deployment. Second is the Smartcard Certificate profile that Client will use to request smartcard certificate from CA for their end users.

4.1 Creating CMP Client Certificate Profile for Issuing Client Certificate used for Authentication

1. Log in into Certificate Management System as tenant administrator.
2. Verify that you have a certificate profile for CMP client. If not, then you can create a certificate profile `CMP_CMS_USER_DEMOPKI-INFRA-CA_utimaco` as shown below and upload under certificate profile management.

CMP_CMS_USER_DEMOPKI-INFRA-CA.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<X509Profile xmlns="http://exceet-secure-solutions.de/xml/ns/pki/profile/v1">
 <appInfo>
 <myDescriptor>
 <project>example-pki</project>
 <category>End Entity Certificate</category>
 <title>Server Certificates</title>
 <details>C.EXAMPLE.CMP</details>
 </myDescriptor>
 </appInfo>
 <!-- for a End-Entity Certificate, it must be false -->
 <ca>false</ca>
 <!-- the validity of certificate in days -->
 <validity>1826</validity> <!-- 5 Jahre -->
 <!-- either current to use the current time or midnight to use the next
mid-night time -->
 <notBeforeTime>current</notBeforeTime>
 <!-- whether a new certificate with duplicated key is permitted -->
 <duplicateKey>false</duplicateKey>
 <!-- whether a new certificate with duplicated subject is permitted -->
 <duplicateSubject>true</duplicateSubject>
 - whether the request can contain the subject attribute serialNumber --
>
 <serialNumberInReq>true</serialNumberInReq>
 <!-- permitted public keys. If absent, then all public keys are permitted
-->
 <keyAlgorithms>
 <algorithm>
 <algorithm description="RSA">1.2.840.113549.1.1.1</algorithm>
 <parameters>
 <RSAParameters>
 <modulusLength>
 <range min="2048" max="2048"/>
<range min="3072" max="3072"/>
<range min="4096" max="4096"/>
 </modulusLength>
 </RSAParameters>
 </parameters>
 </algorithm>
 <algorithm>
 <algorithm description="EC">1.2.840.10045.2.1</algorithm>
 <parameters>
 <ECParameters>
 <curves>
 <curve
description="prime256v1">1.2.840.10045.3.1.7</curve>
 <curve description="secp384r1">1.3.132.0.34</curve>
<curve description="secp521r1">1.3.132.0.35</curve>
```

CMP_CMS_USER_DEMOPKI-INFRA-CA.xml

```
<curve
description="brainpoolp256r1">1.3.36.3.3.2.8.1.1.7</curve>
 <curve
description="brainpoolp384r1">1.3.36.3.3.2.8.1.1.11</curve>
 <curve
description="brainpoolp512r1">1.3.36.3.3.2.8.1.1.13</curve>
 </curves>
 <pointEncodings>
 <pointEncoding>4</pointEncoding>
 </pointEncodings>
 </ECParameters>
 </parameters>
 </algorithm>
 </keyAlgorithms>
 <subject>
 <dnBackwards>false</dnBackwards>
 rialNumber>false</incSerialNumber>
 <rdn minOccurs="1" maxOccurs="1">
 <type description="cn">2.5.4.3</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="serialNumber">2.5.4.5</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 <regex>[-'()=+,.:?/ a-zA-Z0-9]*</regex>
 </rdn>
 <rdn minOccurs="0" maxOccurs="9">
 <type description="ou">2.5.4.11</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 <rdn minOccurs="1" maxOccurs="1">
 <type description="o">2.5.4.10</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="l">2.5.4.7</type>
 <minLen>1</minLen>
 <maxLen>128</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="st">2.5.4.8</type>
 <minLen>1</minLen>
 <maxLen>128</maxLen>
 </rdn>
 <rdn minOccurs="1" maxOccurs="1">
 <type description="c">2.5.4.6</type>
```

CMP_CMS_USER_DEMOPKI-INFRA-CA.xml

```
 <minLen>1</minLen>
 <maxLen>2</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="dc">0.9.2342.19200300.100.1.25</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 ubject>
 <extensions>
 <extension required="true" permittedInRequest="false">
 <type description="subjectKeyIdentifier">2.5.29.14</type>
 <critical>false</critical>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="authorityKeyIdentifier">2.5.29.35</type>
 <critical>false</critical>
 <value>
 <authorityKeyIdentifier>
 <includeIssuerAndSerial>true</includeIssuerAndSerial>
 </authorityKeyIdentifier>
 </value>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="keyUsage">2.5.29.15</type>
 <critical>true</critical>
 <value>
 <keyUsage>
 <!-- valid values are digitalSignature, contentCommitment,
keyEncipherment, dataEncipherment,
 keyAgreement, keyCertSign, cRLSign, encipherOnly,
decipherOnly -->
 <usage required="true">digitalSignature</usage>
 <usage required="true">keyEncipherment</usage>
 <usage required="true">keyAgreement</usage>
 </keyUsage>
 </value>
 </extension>
 <extension required="false" permittedInRequest="true">
 <type description="subjectAltNames">2.5.29.17</type>
 <critical>false</critical>
 <!--
 <value>
 <subjectAltName>
 <rfc822Name/>
 </subjectAltName>
 </value>

 </extension>
 <extension required="true" permittedInRequest="false">
```

CMP_CMS_USER_DEMOPKI-INFRA-CA.xml

```
 <type description="basicConstraints">2.5.29.19</type>
 <critical>true</critical>
 <value>
 <basicConstraints>
 <pathLen>0</pathLen>
 </basicConstraints>
 </value>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="certificatePolicies">2.5.29.32</type>
 <critical>false</critical>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="cRLDistributionPoints">2.5.29.31</type>
 <critical>false</critical>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="authorityInfoAccess">1.3.6.1.5.5.7.1.1</type>
 <critical>false</critical>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="extendedKeyUsage">2.5.29.37</type>
 <critical>false</critical>
 <value>
 <extendedKeyUsage>
 <usage required="true" description="ip-kp
serverAuth">1.3.6.1.5.5.7.3.1</usage>
 <usage required="true" description="ip-kp
clientAuth">1.3.6.1.5.5.7.3.2</usage>
 </extendedKeyUsage>
 </value>
 </extension>
 </extensions>
</X509Profile>
```

4.2 Creating Smartcard Certificate Profile for Certificate that Client Can Request

1. Log in to CMS web as tenant administrator.
2. Navigate to **Certificate Profile Management**.
3. Create a Smartcard certificate profile so that clients can request a smartcard logon certificate. You can also download the existing certificate profile from CMS Web for example TLS profile and edit with smartcard entries as shown below:

ScardUPN.xml

```
# <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<X509Profile xmlns="http://exceet-secure-solutions.de/xml/ns/pki/profile/v1">
 <appInfo>
 <myDescriptor>
 <project>example-pki</project>
 <category>End Entity Certificate</category>
 <title>smartcard Certificates</title>
 <details>C.smartcard.TLS</details>
 </myDescriptor>
 </appInfo>
 <!-- for a End-Entity Certificate, it must be false -->
 <ca>false</ca>
 <!-- the validity of certificate in days -->
 <validity>1826</validity> <!-- 5 Jahre -->
 <!-- either current to use the current time or midnight to use the next
mid-night time -->
 <notBeforeTime>current</notBeforeTime>
 <!-- whether a new certificate with duplicated key is permitted -->
 <duplicateKey>false</duplicateKey>
 <!-- whether a new certificate with duplicated subject is permitted -->
 <duplicateSubject>true</duplicateSubject>
 <!-- whether the request can contain the subject attribute serialNumber --
>
 <serialNumberInReq>true</serialNumberInReq>
 <!-- permitted public keys. If absent, then all public keys are permitted
-->
 <keyAlgorithms>
 <algorithm>
 <algorithm description="RSA">1.2.840.113549.1.1.1</algorithm>
 <parameters>
 <RSAParameters>
 <modulusLength>
 048" max="2048"/>
<range min="3072" max="3072"/>
<range min="4096" max="4096"/>
 </modulusLength>
 </RSAParameters>
 </parameters>
 </algorithm>
 <algorithm>
 <algorithm description="EC">1.2.840.10045.2.1</algorithm>
 <parameters>
 <ECParameters>
 <curves>
 <curve
description="prime256v1">1.2.840.10045.3.1.7</curve>
 <curve description="secp384r1">1.3.132.0.34</curve>
<curve description="secp521r1">1.3.132.0.35</curve>
```

ScardUPN.xml

```
<curve
description="brainpoolp256r1">1.3.36.3.3.2.8.1.1.7</curve>
 <curve
description="brainpoolp384r1">1.3.36.3.3.2.8.1.1.11</curve>
 <curve
description="brainpoolp512r1">1.3.36.3.3.2.8.1.1.13</curve>
 </curves>
 <pointEncodings>
 <pointEncoding>4</pointEncoding>
 </pointEncodings>
 </ECParameters>
 </parameters>
 </algorithm>
 </keyAlgorithms>
 <subject>
 <dnBackwards>false</dnBackwards>
 <incSerialNumber>false</incSerialNumber>
<rdn minOccurs="0" maxOccurs="1">
 <type description="emailAddress">1.2.840.113549.1.9.1</type>
 <minLen>1</minLen>
 <maxLen>255</maxLen>
 <regex>^\S+@\S+$</regex>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="uid">0.9.2342.19200300.100.1.1</type>
 <minLen>0</minLen>
 Len>255</maxLen>
 <regex>^\S+@\S+$</regex>
 </rdn>
 <rdn minOccurs="1" maxOccurs="1">
 <type description="cn">2.5.4.3</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="serialNumber">2.5.4.5</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 <regex>[-'()=+,.:?/ a-zA-Z0-9]*</regex>
 </rdn>
 <rdn minOccurs="0" maxOccurs="9">
 <type description="ou">2.5.4.11</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="o">2.5.4.10</type>
 <minLen>1</minLen>
 <maxLen>64</maxLen>
 </rdn>
```

ScardUPN.xml

```
 <rdn minOccurs="0" maxOccurs="1">
 <type description="l">2.5.4.7</type>
 <minLen>1</minLen>
 <maxLen>128</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="st">2.5.4.8</type>
 <minLen>1</minLen>
 <maxLen>128</maxLen>
 </rdn>
 <rdn minOccurs="0" maxOccurs="1">
 <type description="c">2.5.4.6</type>
 <minLen>1</minLen>
 <maxLen>2</maxLen>
 </rdn>
 </subject>
 <extensions>
 sion required="true" permittedInRequest="false">
 <type description="subjectKeyIdentifier">2.5.29.14</type>
 <critical>false</critical>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="authorityKeyIdentifier">2.5.29.35</type>
 <critical>false</critical>
 <value>
 <authorityKeyIdentifier>
 <includeIssuerAndSerial>true</includeIssuerAndSerial>
 </authorityKeyIdentifier>
 </value>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="keyUsage">2.5.29.15</type>
 <critical>true</critical>
 <value>
 <keyUsage>
 <!-- valid values are digitalSignature, contentCommitment,
keyEncipherment, dataEncipherment,
 keyAgreement, keyCertSign, cRLSign, encipherOnly,
decipherOnly -->
 <usage required="true">digitalSignature</usage>
 <usage required="true">keyEncipherment</usage>
 <usage required="true">keyAgreement</usage>
 </keyUsage>
 </value>
 </extension>
 <extension required="false" permittedInRequest="true">
 <type description="subjectAltNames">2.5.29.17</type>
 <critical>false</critical>
 <!--
 <value>
```

ScardUPN.xml

```
 <subjectAltName>
 <rfc822Name/>
 </subjectAltName>
 </value>
 -->
 </extension>
 sion required="true" permittedInRequest="false">
 <type description="basicConstraints">2.5.29.19</type>
 <critical>true</critical>
 <value>
 <basicConstraints>
 <pathLen>0</pathLen>
 </basicConstraints>
 </value>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="certificatePolicies">2.5.29.32</type>
 <critical>false</critical>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="cRLDistributionPoints">2.5.29.31</type>
 <critical>false</critical>
 </extension>
 <extension required="false" permittedInRequest="false">
 <type description="authorityInfoAccess">1.3.6.1.5.5.7.1.1</type>
 <critical>false</critical>
 </extension>
 <extension required="true" permittedInRequest="false">
 <type description="extendedKeyUsage">2.5.29.37</type>
 <critical>false</critical>
 <value>
 <extendedKeyUsage>
 <usage required="true" description="ip-kp
smartCard">1.3.6.1.4.1.311.20.2.2</usage>
<usage required="true" description="ip-kp
clientAuth">1.3.6.1.5.5.7.3.2</usage>
 </extendedKeyUsage>
 </value>
 </extension>
 </extensions>
</X509Profile>
```

You can modify the certificate profile according to your requirements.

4. Save the file as `ScardUPN.xml`.

5. On CMS Web click on **Upload** and choose the necessary xml profile for smartcard certificate profile and fill in the below details as shown.

    a. Certificate Profile Name: Provide name for the smartcard certificate profile.

    b. CA: Choose the issuing CA from the list for issuing smartcard certificates.

6. Certificate Type: Provide a suitable name for certificate type. Please note that this name will be used while configuring the connection in IDcentral. Verify the contents and click **Upload.**

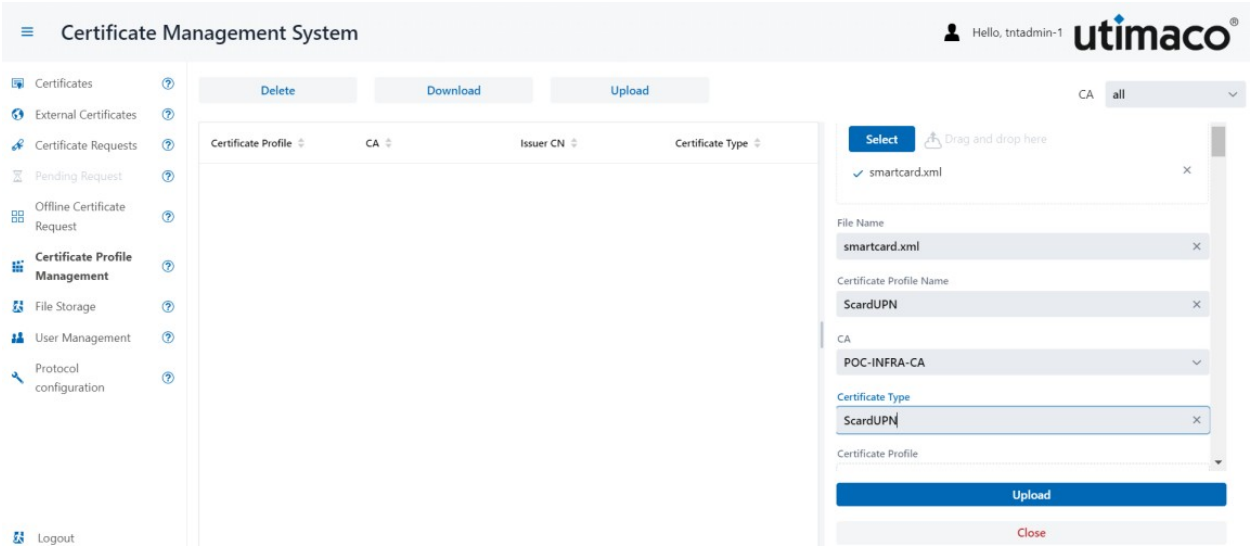


Figure 1 : Certificate Management System

7. Once uploaded successfully, the certificate profile will be listed under **Certificate Profile Management**.

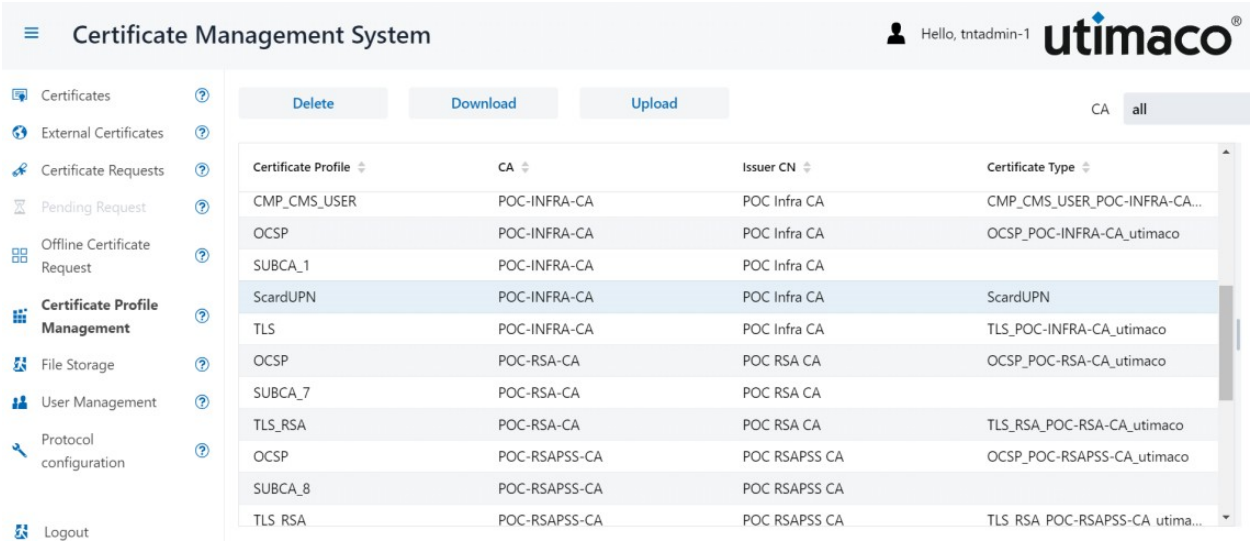


Figure 2 : Certificate Profile Management

8. Select the **User Management** option from CMS, then select the user with the admin privileges. For demonstration we have selected admin user **tntadmin-1** available in the test environment. Select the permission View, Enroll and Revoke for certificate type ScardUPN.

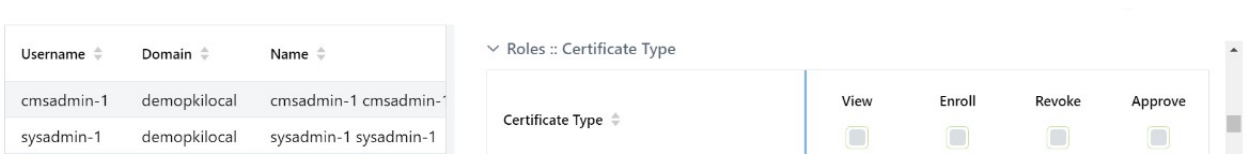


Figure 3 : User Management

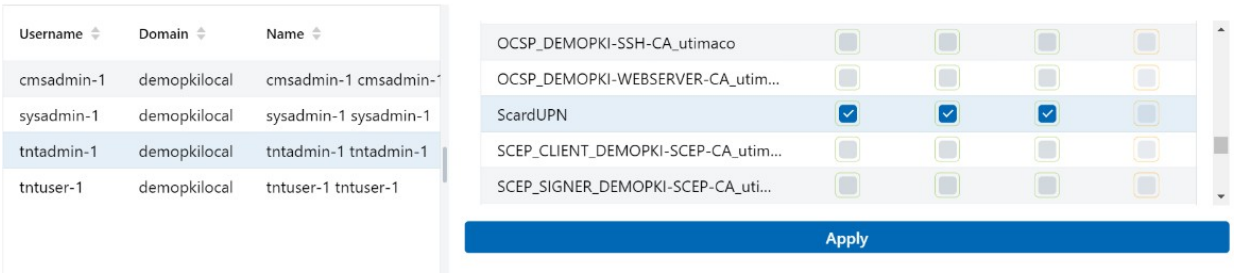


Figure 4 : User Management

9. Click on **Apply**.

5 IDcentral Smartcard License Configuration

To provision a certificate for a smartcard device Hardware Token, license must be activated in IDcentral Identity Registration platform. This section describes in detail the entity license assignment steps.

5.1 Hardware Token License Activation

1. Navigate to **Licenses** view from the left panel options.
2. Click on **Activate License.**

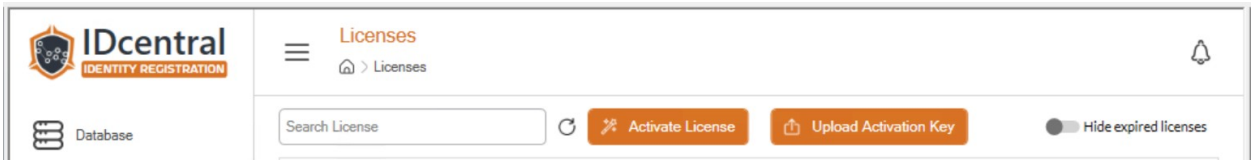


Figure 5 : Activate License on IDcentral

3. Enter the **Account Name** and **License Key** provided by Sixscape. Click on **Add License.**

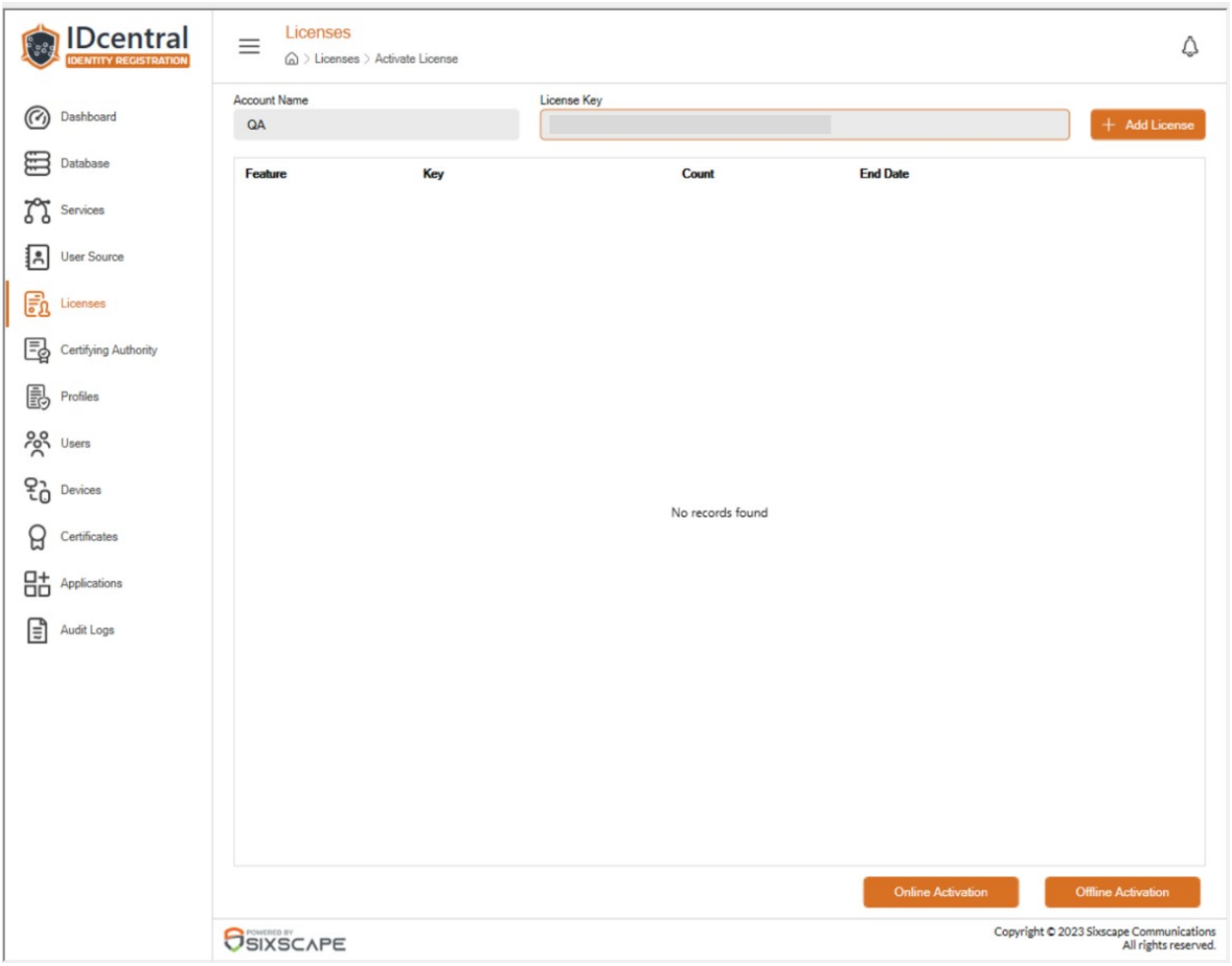


Figure 6 : Add License window

4. The hardware token license with the relevant information is displayed. Select the license in the center panel and click on **Offline Activation** to generate the license request file for the selected license. Alternatively, the administrator can also try clicking **Online Activation**.

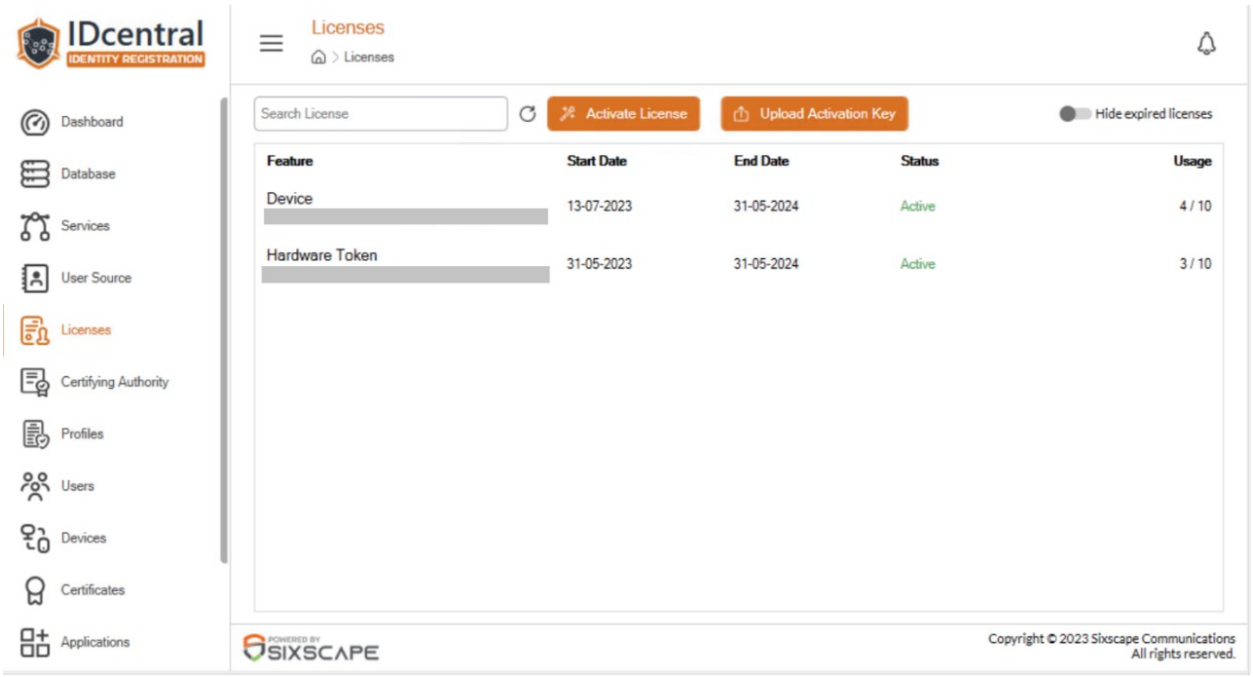


Figure 7 : Offline Activation window

5. If you have chosen **Offline Activation**, the license request file will be generated in `C:\Users\Public\SixscapeCertManager\OfflineLicenses`. Send the license request file to Sixscape for license activation.
6. After receiving the license activation file from Sixscape, go back to the IDcentral console. Under **Licenses**, select **Upload Activation Key**.

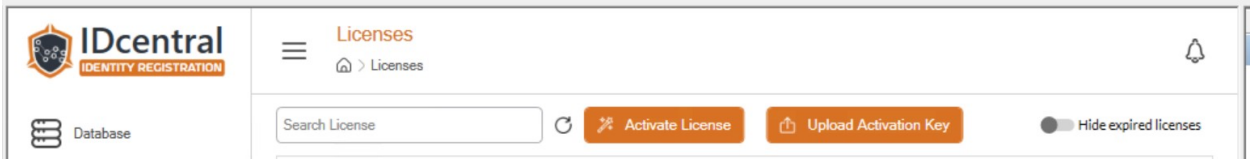


Figure 8 : Upload Activation Key in Licenses window

7. Browse to the license activation file from Sixscape.
8. After the license is activated, the license details will appear in the IDcentral management console.

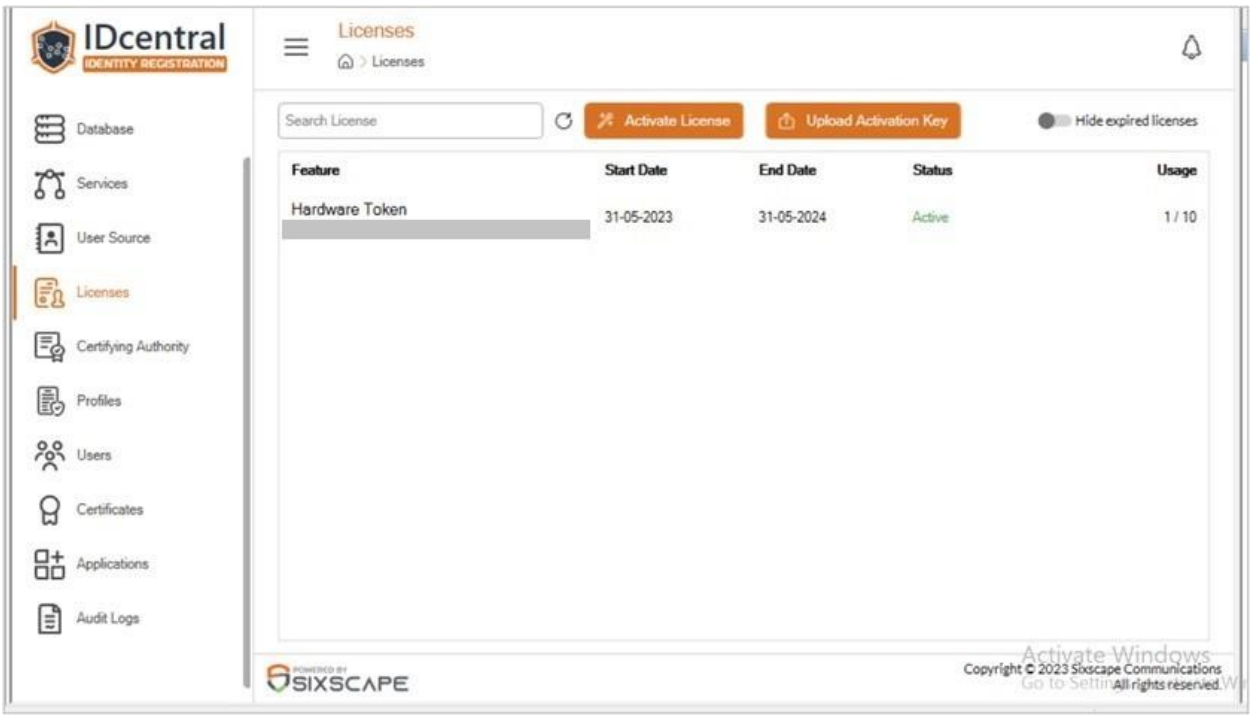


Figure 9 : Verifying Activated License

5.2 Creating a User for License Allotment

After license is activated, you can allot users to it who can request the smartcard certificate. For demonstration, a test user is being created in the AD. To create AD domain users on the domain controller:

1. Log in to the Windows AD domain server. Choose **Start** > **Administrative Tools** > **Active Directory Users and Computers**. The Active Directory Users and Computers page is displayed.
2. In the Active Directory Users and Computers dialog box, right-click **Users**.
3. Choose **New** > **User**.
4. Provide the user details and click **Next**.

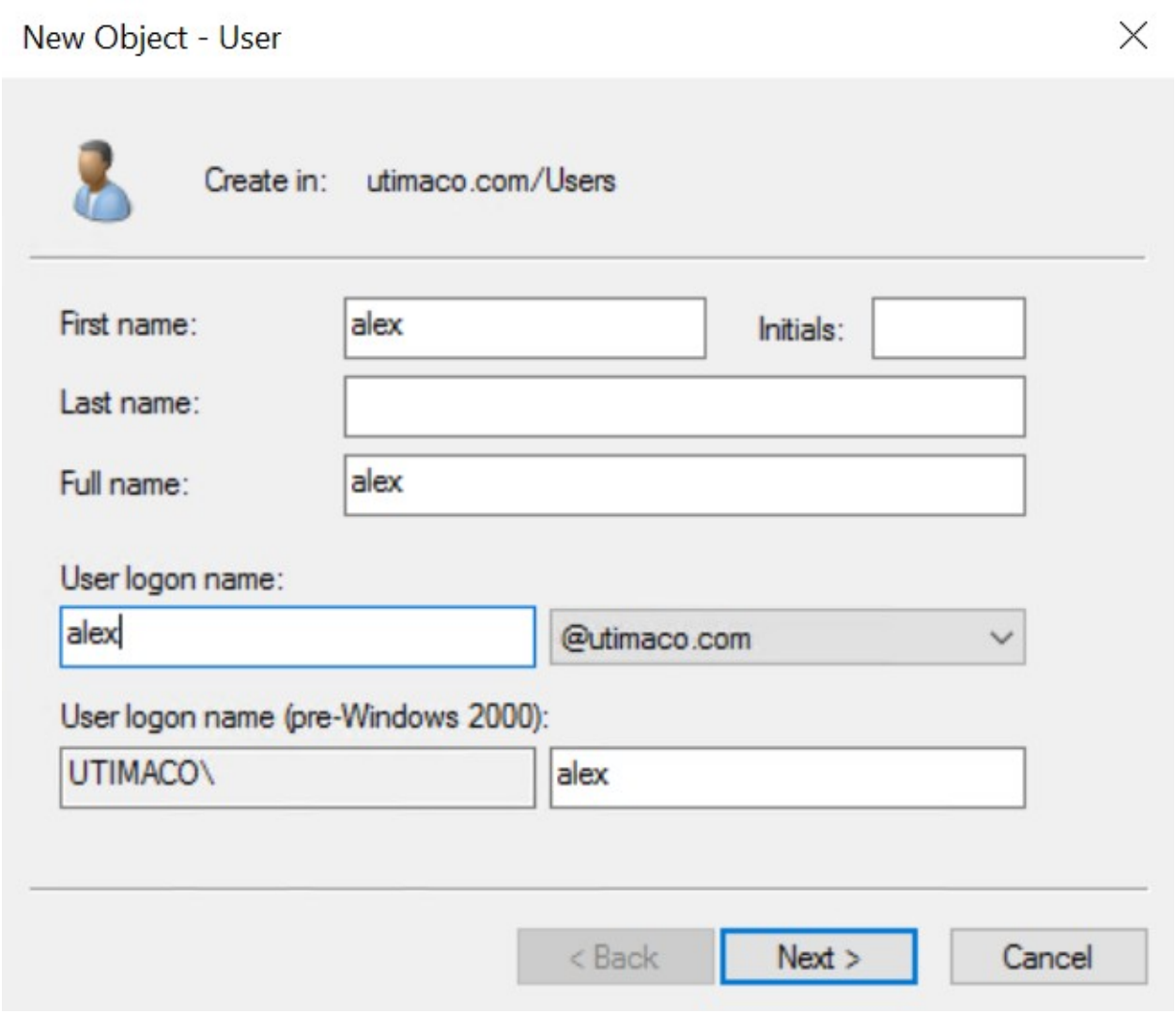


Figure 10 : Creating a domain user

5. Click **Next**.
6. Enter a new password and enter it again to confirm.
7. Select any other option according to your need. Click **Next**.

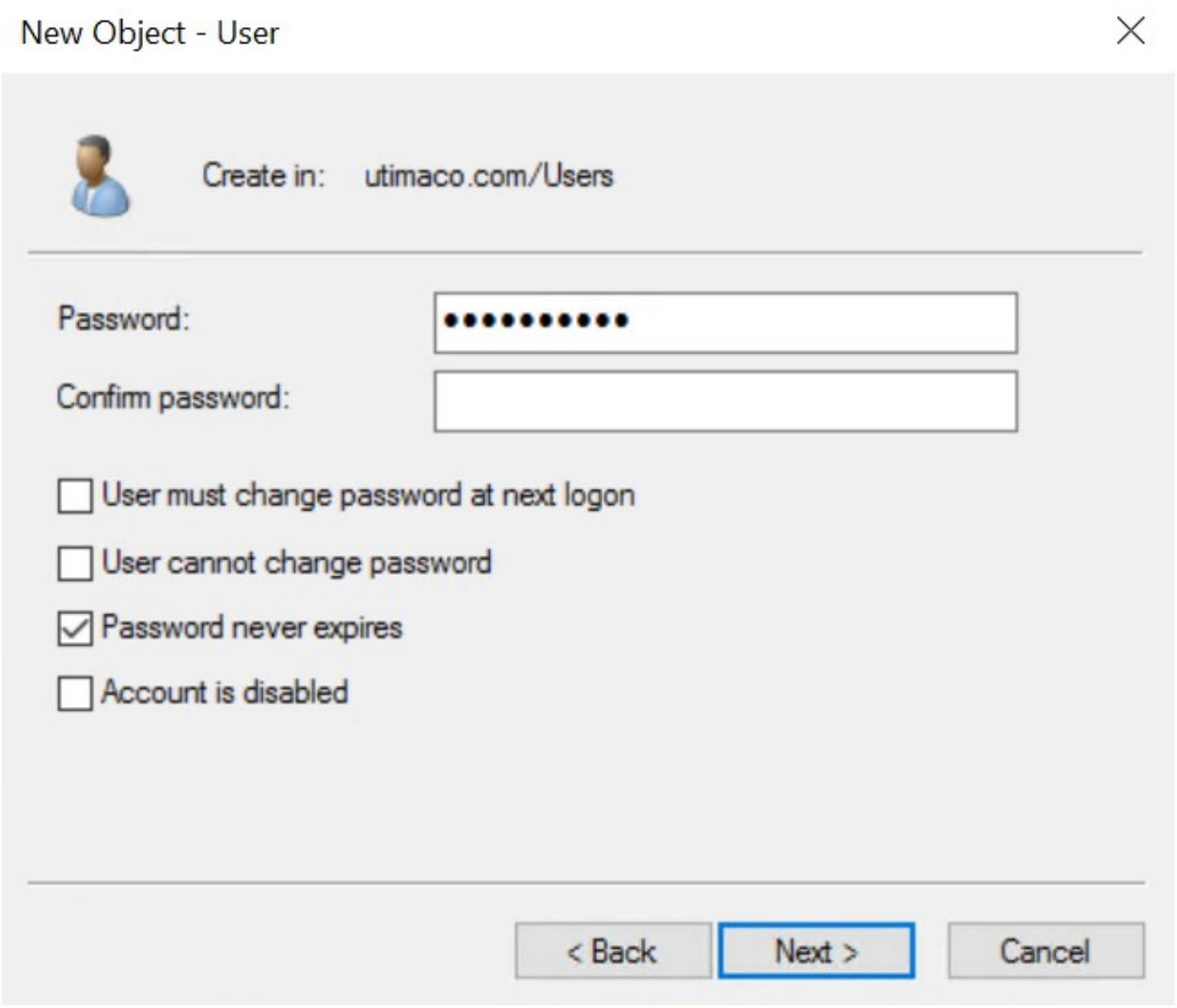


Figure 11 : User password settings

This completes the steps on how to create a user account in Active Directory.

8. Once user is created, add the user email address in User properties.

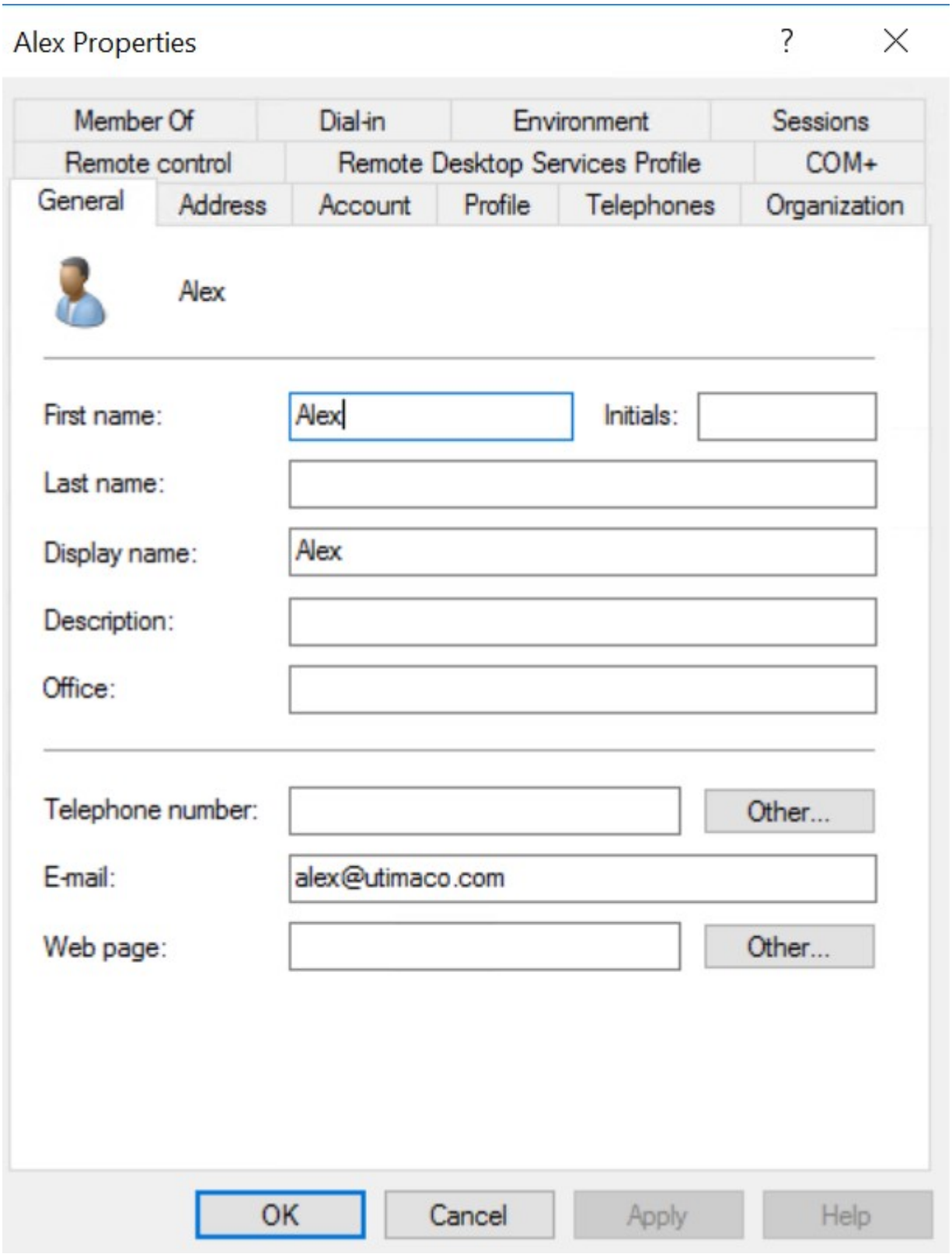


Figure 12 : Adding email address

9. Add the user to a group if required. Click **OK**.

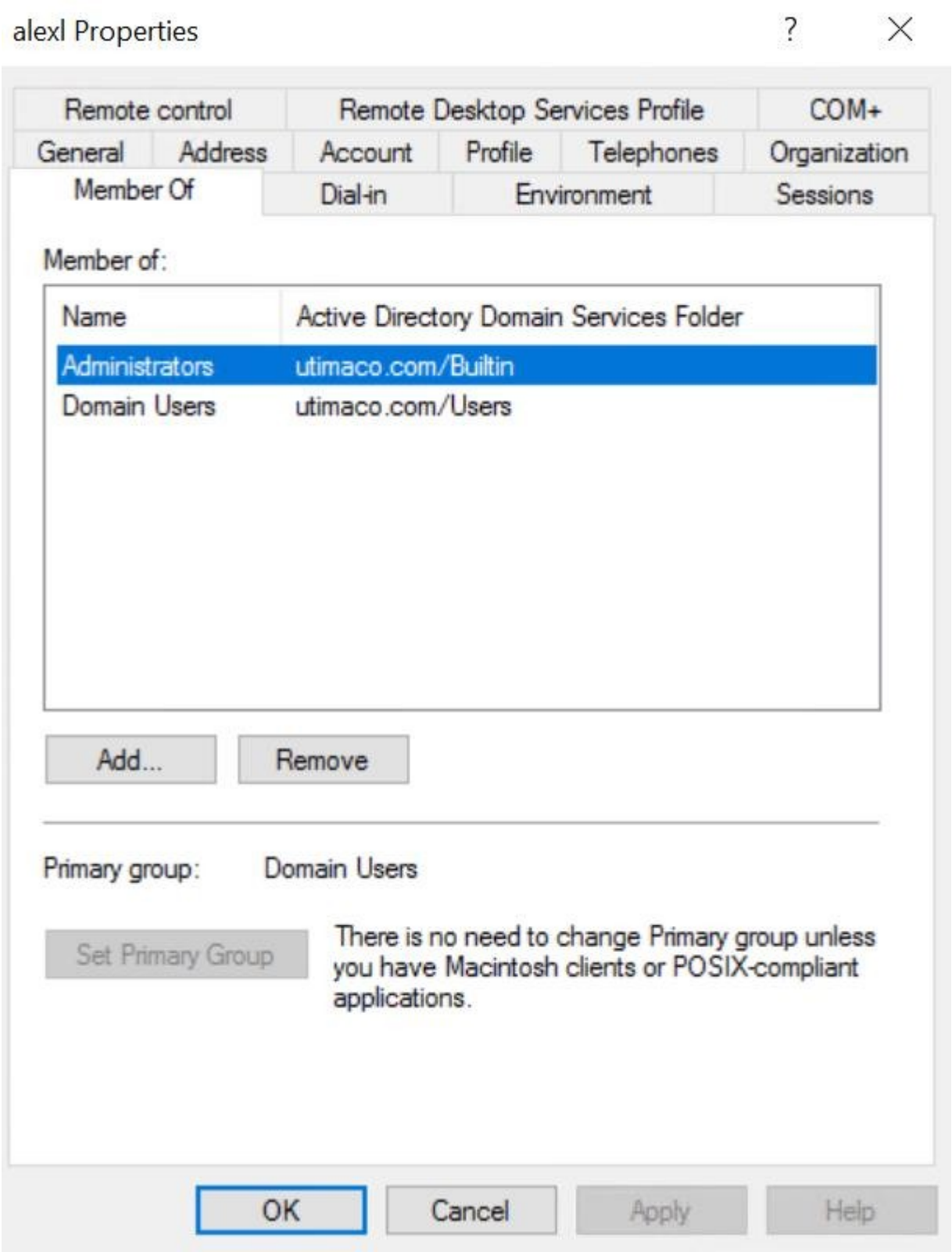


Figure 13 : Adding group to user

5.3 Hardware Token License Allotment to User

1. Navigate to **Licenses** view from the left panel options.
2. Click on **Hardware Token** license entry.
3. Click on **New Allotment.**

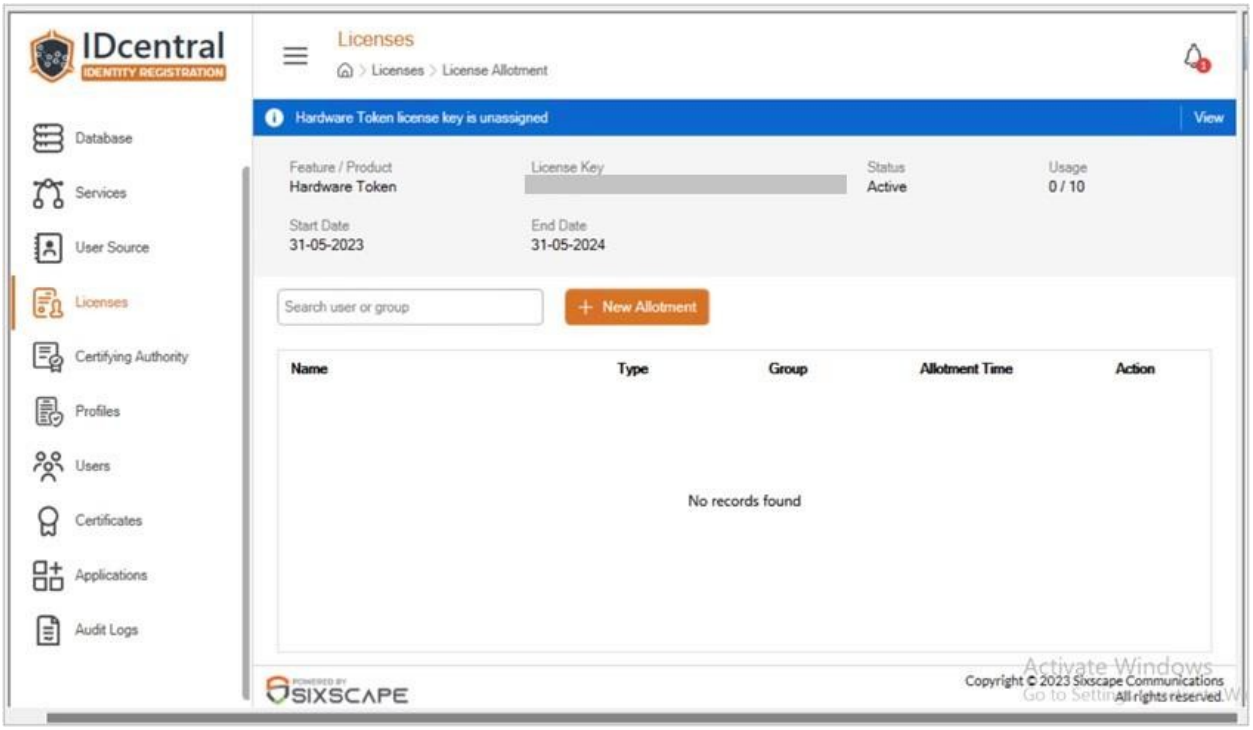


Figure 14 : License Allotment window

4. Directory Selection panel will be displayed on the right side. Search for a user or group in the search box.
5. Search for the required user/group and choose the same to move it to the **Selected Records**.
6. After selecting all the required users/groups, click on **Select.**

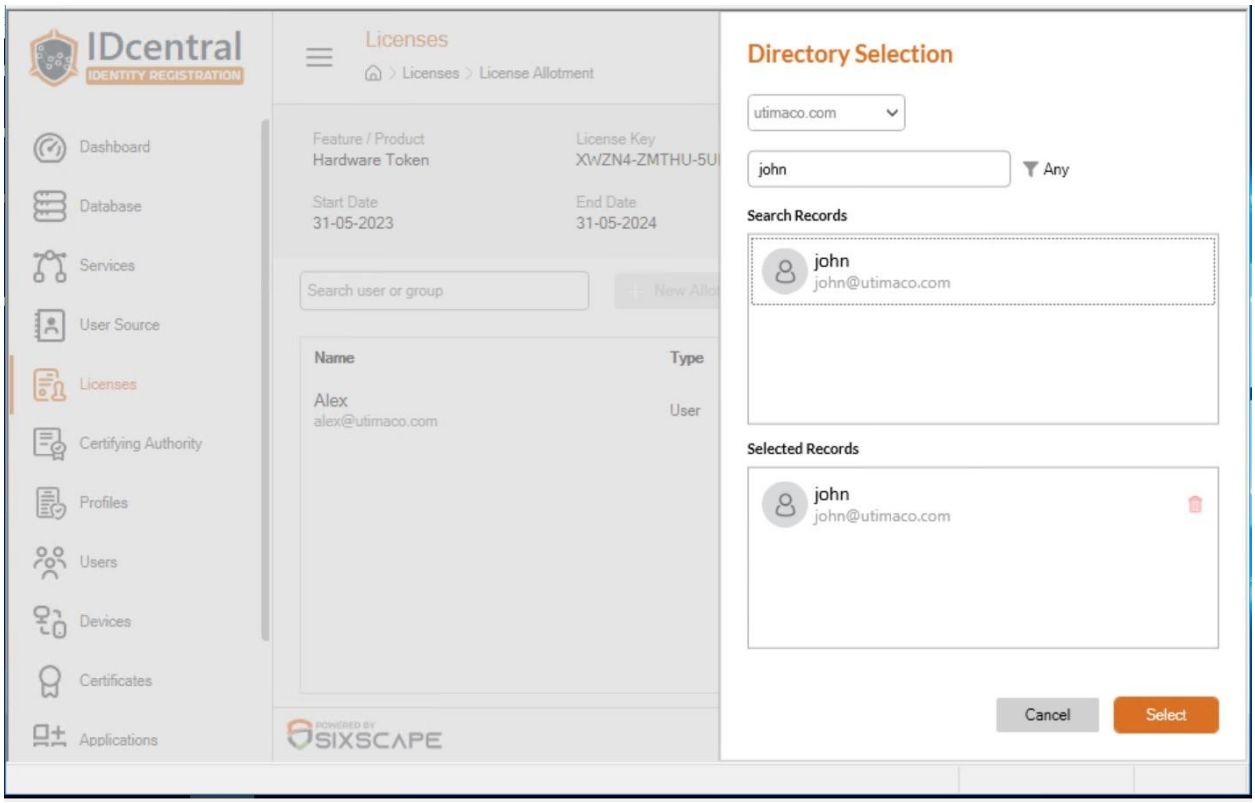


Figure 15 : Selection of user/group

7. On successful entity license allotment, the entity information will be listed in the view.

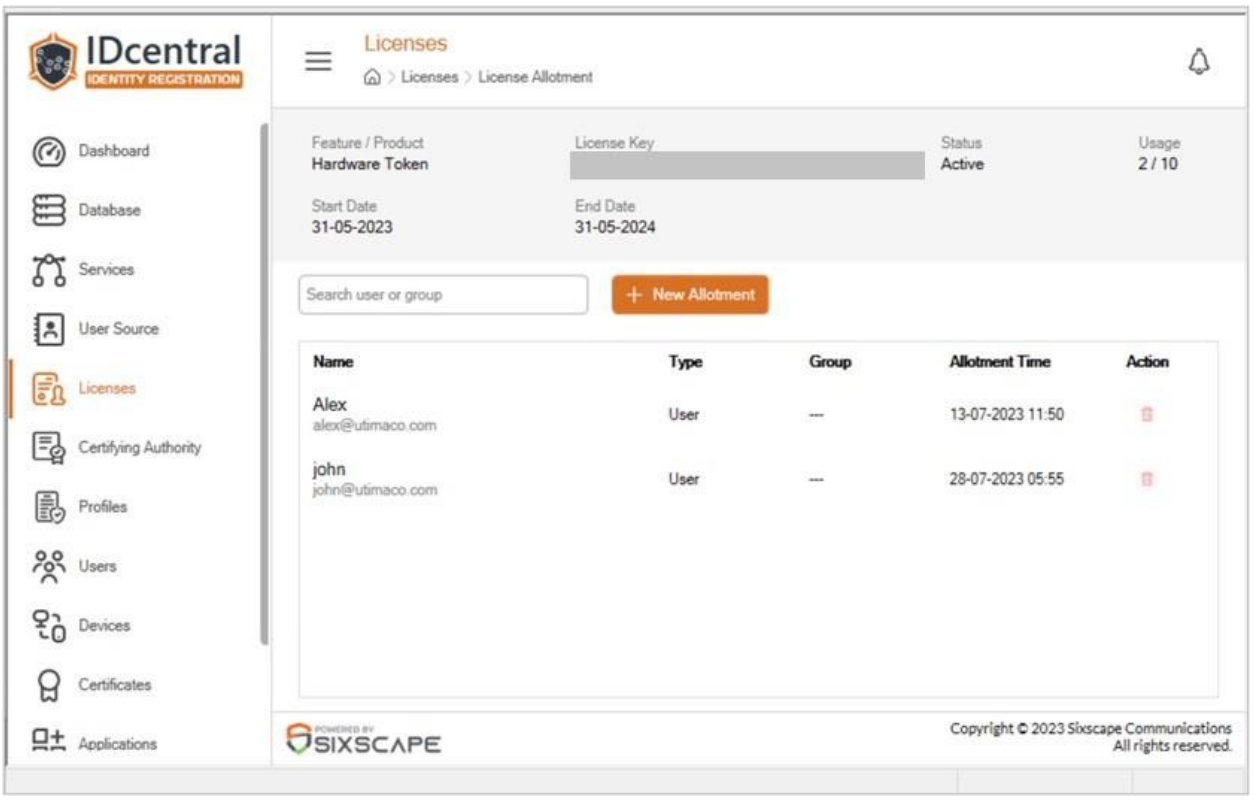


Figure 16 : License Allotment window

5.4 Removal of Hardware Token License Allotment

This section describes the steps to unassign license allotment for any user/group.

1. To unassign the entity, click on the delete icon (right side).
2. Click on **Delete** in the displayed confirmation dialog to delete entity allotment.

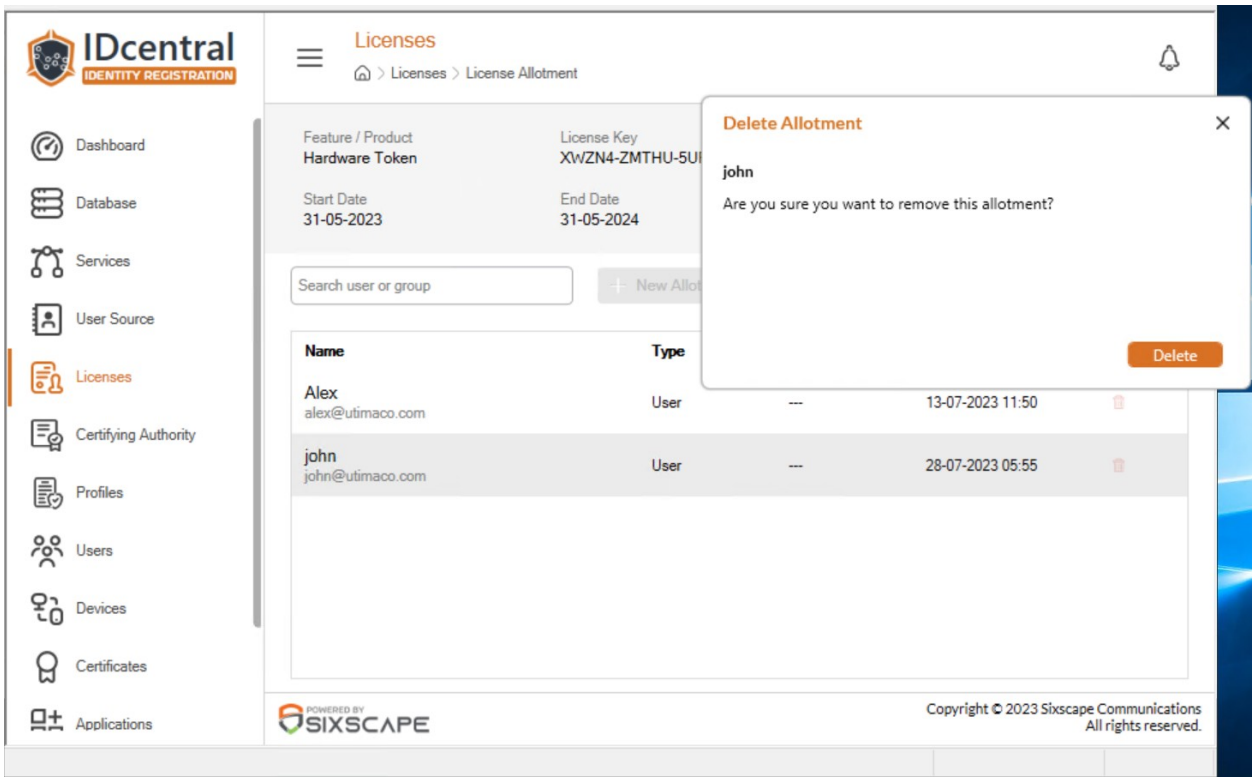


Figure 17 : Removal of user in License Allotment

3. On successful license allotment deletion, the entity information will be removed from the view.

6 Integrating IDcentral with Utimaco u.trust Identify

6.1 Generate a Client Certificate to Authenticate to u.trust Identify PKI

You must generate a client certificate signed by CA in u.trust Identify PKI so that it can authenticate itself while requesting a certificate for end users.

6.1.1 Generate CSR for Client

1. From Microsoft Windows, click **Start**.
2. In the Search programs and files field, type **certmgr** and select **Manage computer certificates**.
3. Right-click the **Personal folder**.
4. Select **All Tasks** > **Advanced Operations** > **Create Custom Request**.

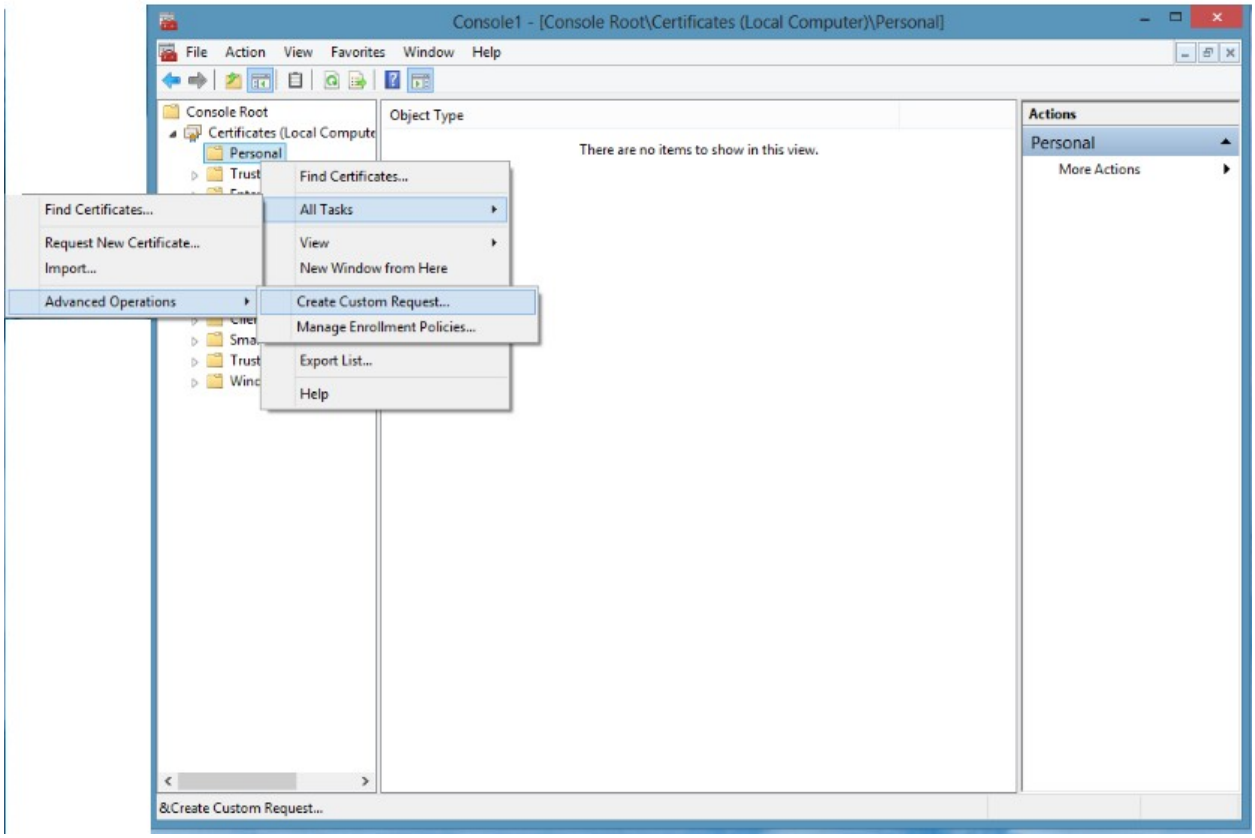


Figure 18 : Creating CSR for Client

5. The Certificate Enrollment wizard will open > click **Next**.

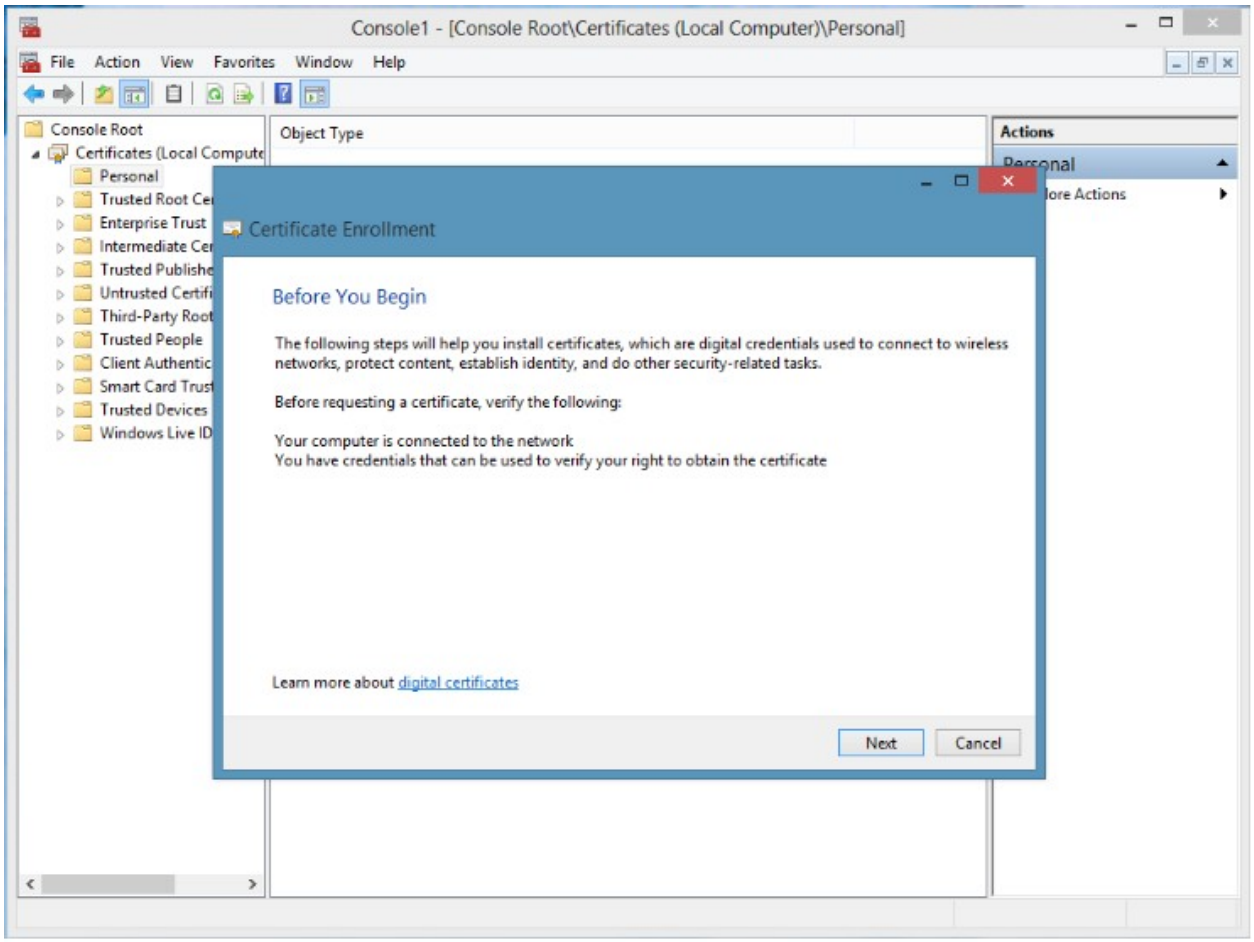


Figure 19 : Certificate Enrollment Window

6. Select the option to **Proceed without enrollment policy** > click **Next**.

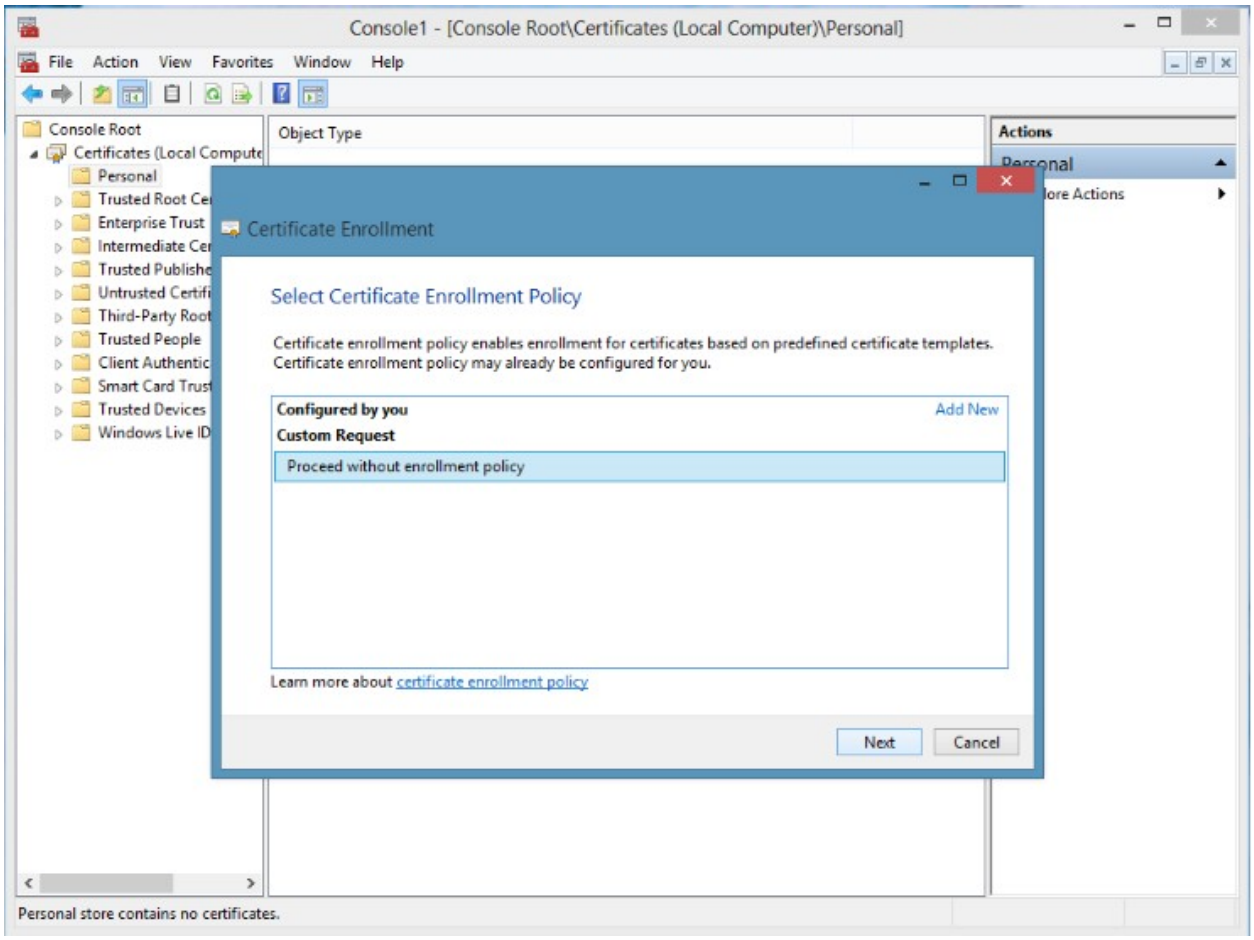


Figure 20 : Selecting Certificate Enrollment Policy

7. Click **Next** at the **Custom Request** window.

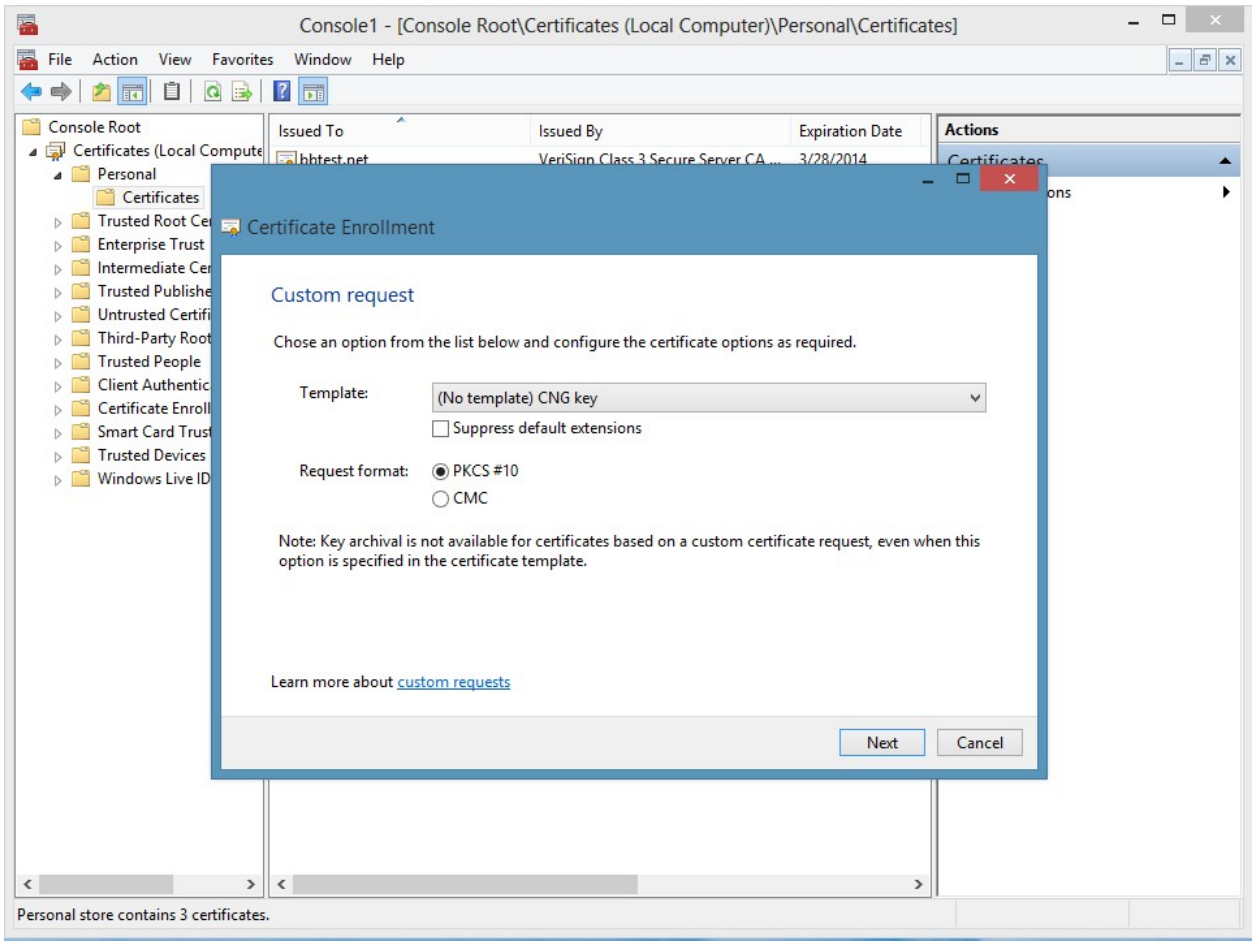


Figure 21 : Custom Request window

8. From the **Details** drop down menu click **Properties**.

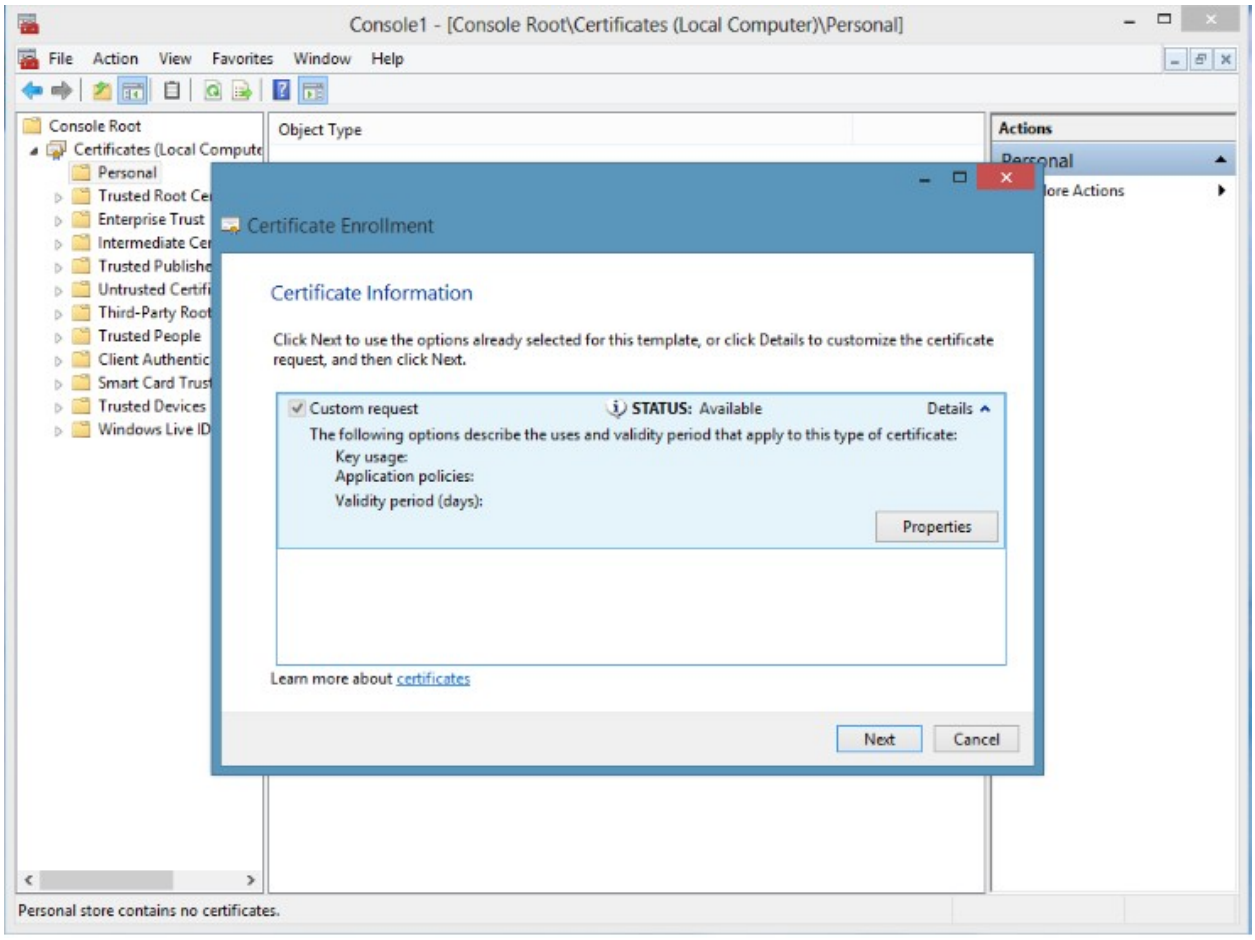


Figure 22 : Certificate Information window

9. Enter a **Friendly Name** of your choice.

Figure 23 : Certificate Properties window

10. Access the **Subject** tab > in the **Subject name: Type**: field add the following distinguish name values:

Example:

- CN = <Username>: The technical user in the CMS group of the AD.
- O = <Organization>: The registered organizational name the certificate belongs to.
- C = <Country/region>: The two letter ISO country code.

- DC = <Domain>: This is the domain name which has been assigned by the CMS Administrator and which is used in this system. Example: DC=demopkilocal.

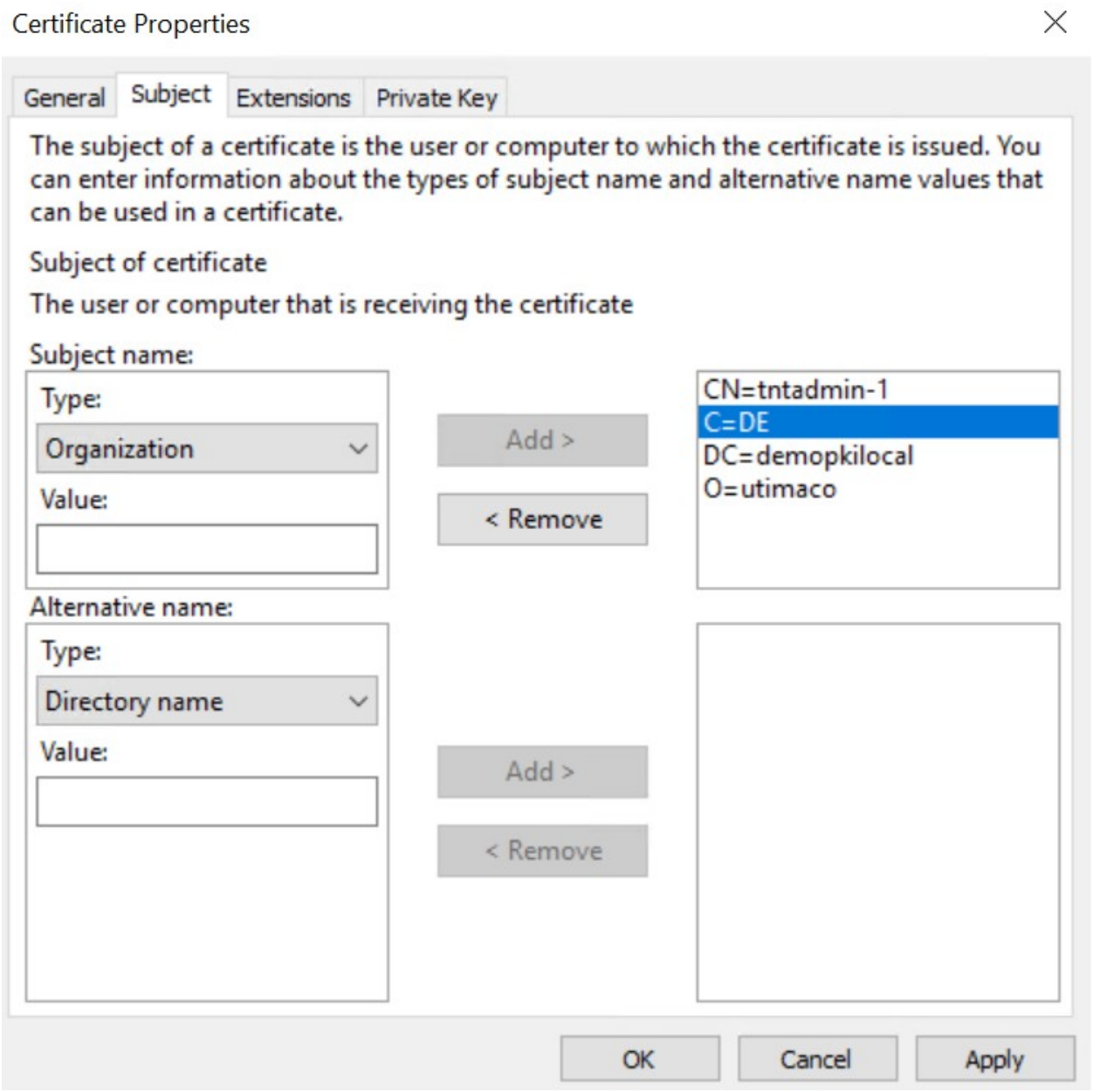


Figure 24 : Certificate Properties Window

For a CMP Client Certificate, the content of the "Subject" field must be generated with the CN and DC.

11. Click on **Extensions**.

a. Add below **Key usage** extensions.

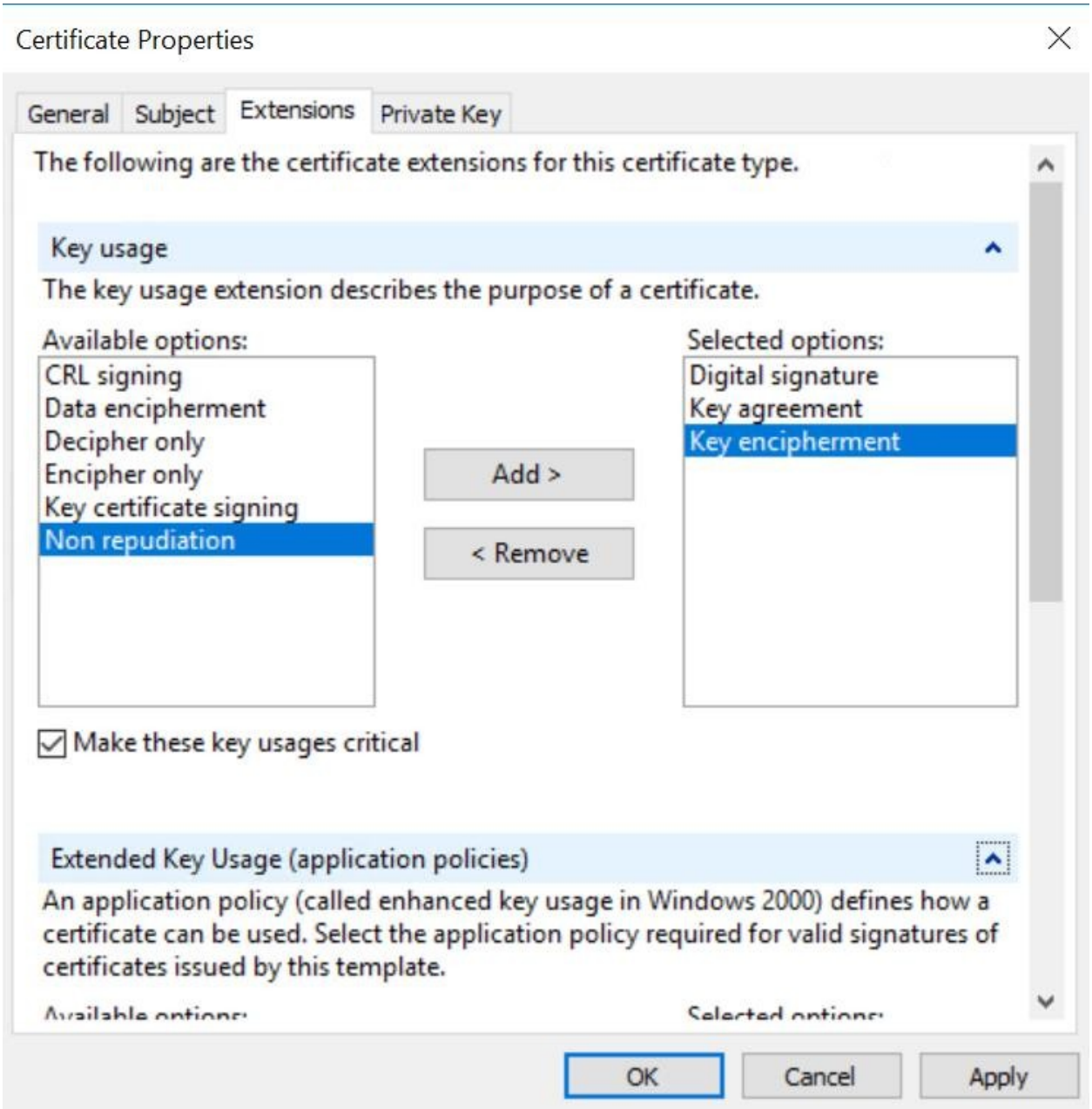


Figure 25 : Certificate Properties window

b. From **Extended Key usage** select Server Authentication and Client Authentication.

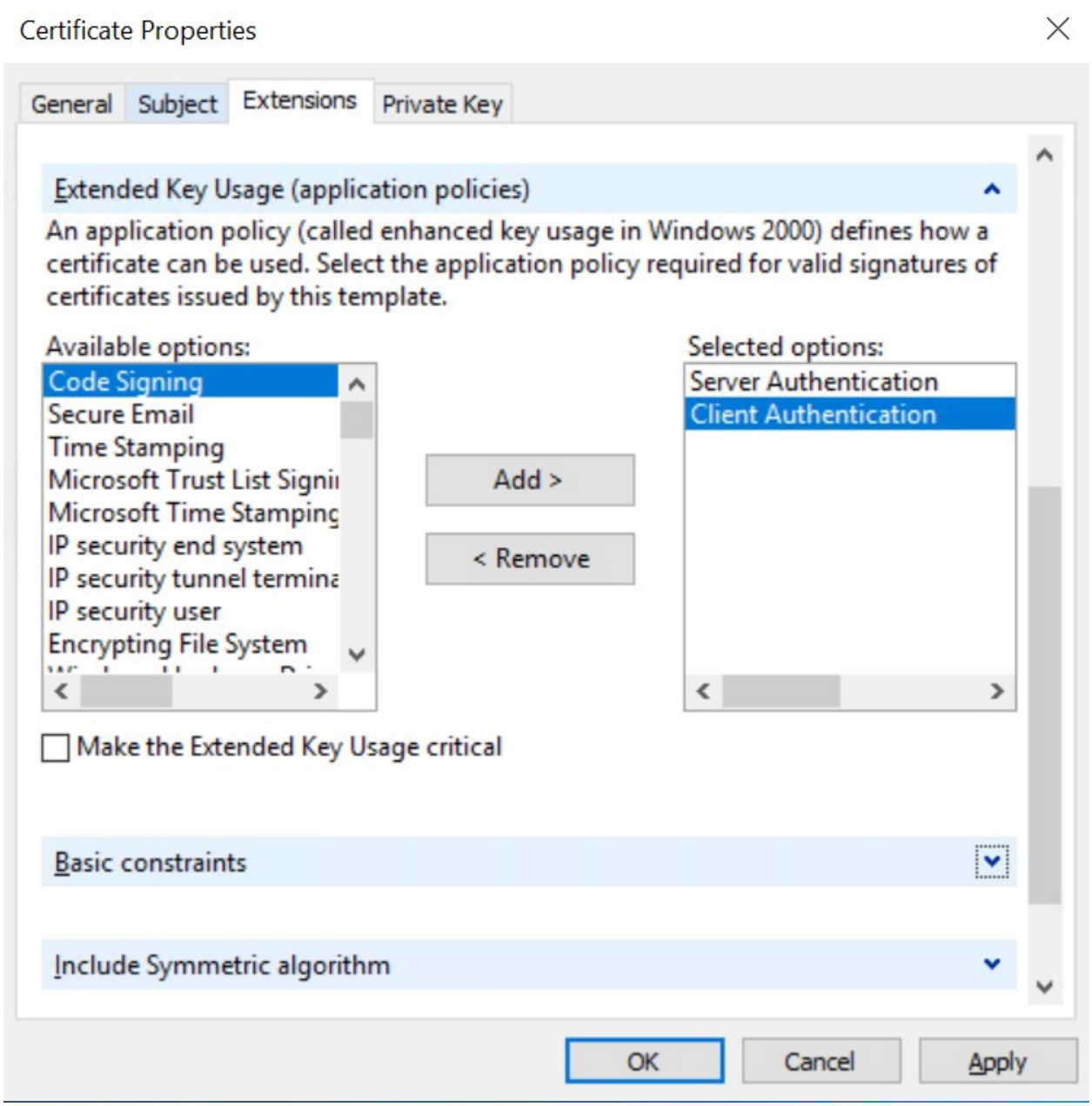


Figure 26 : Certificate Properties window

c. Enable **Basic constraint**s and set path length value as 0.

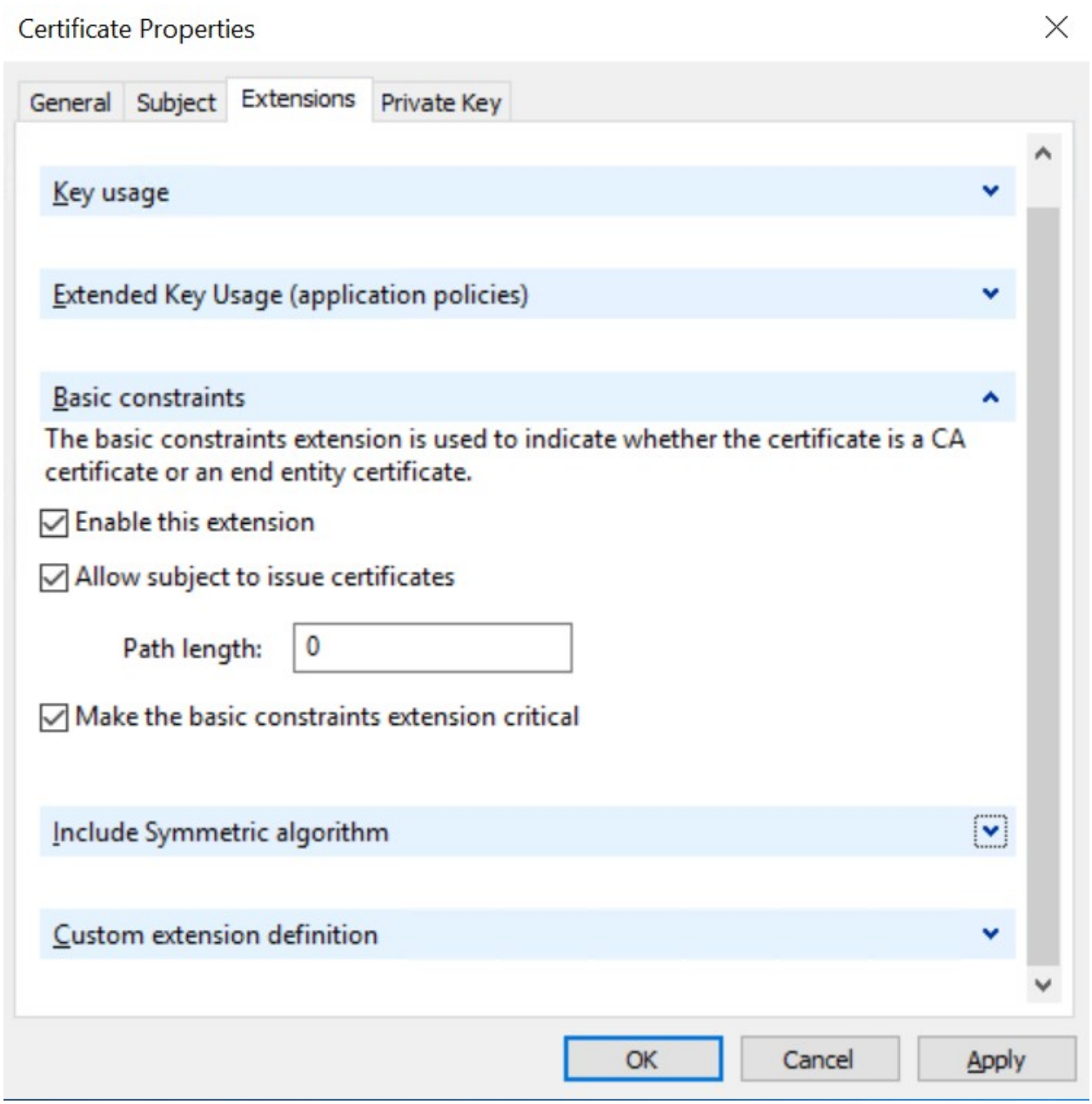


Figure 27 : Certificate Properties window

12. Click the **Private Key** tab > click the drop down for **Key options** > select **Key size**: 2048 and check the option to **Make private key exportable** > Click **OK**.

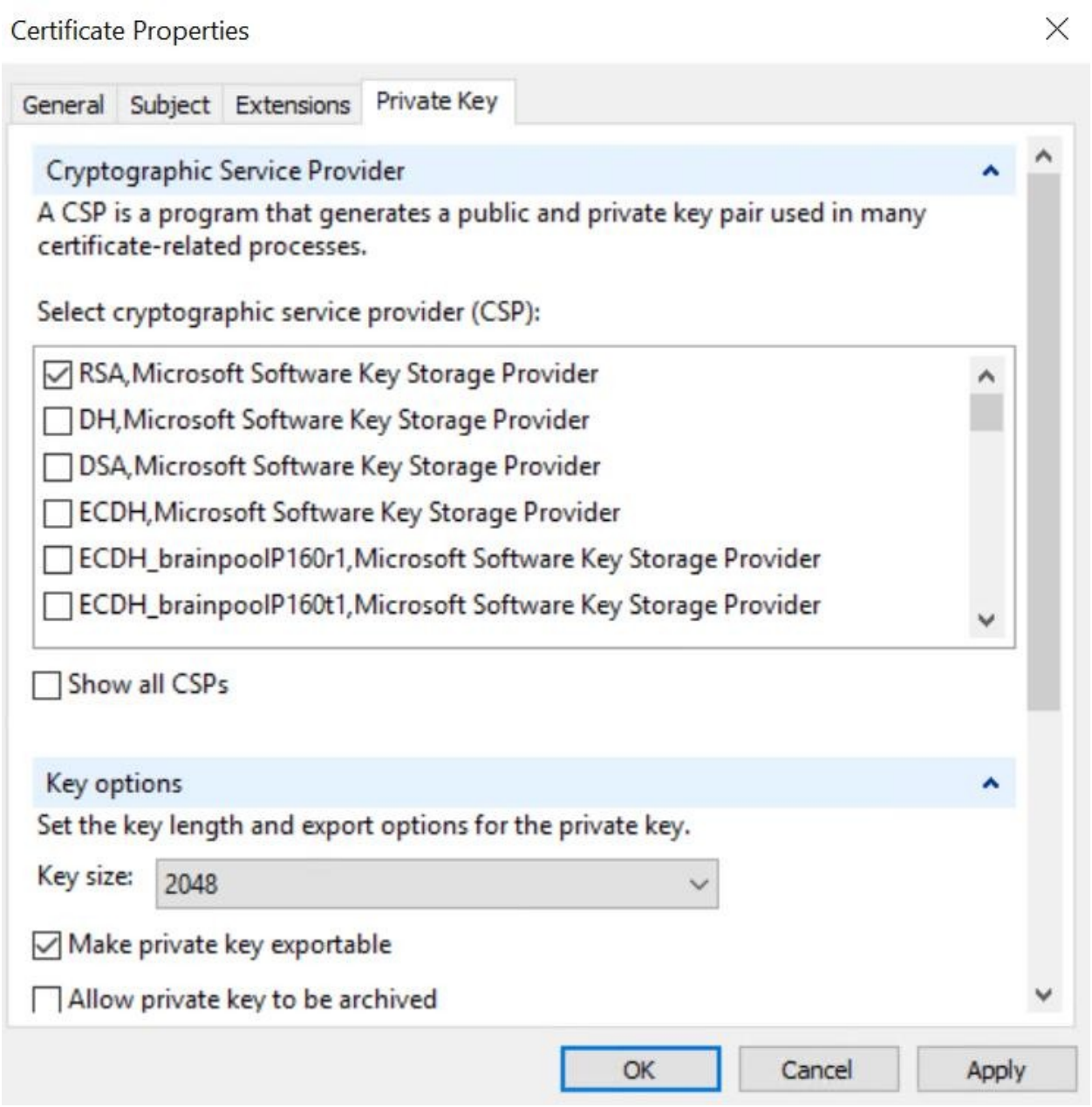


Figure 28 : Certificate Properties window

13. Click **Next** > Click **Browse**.

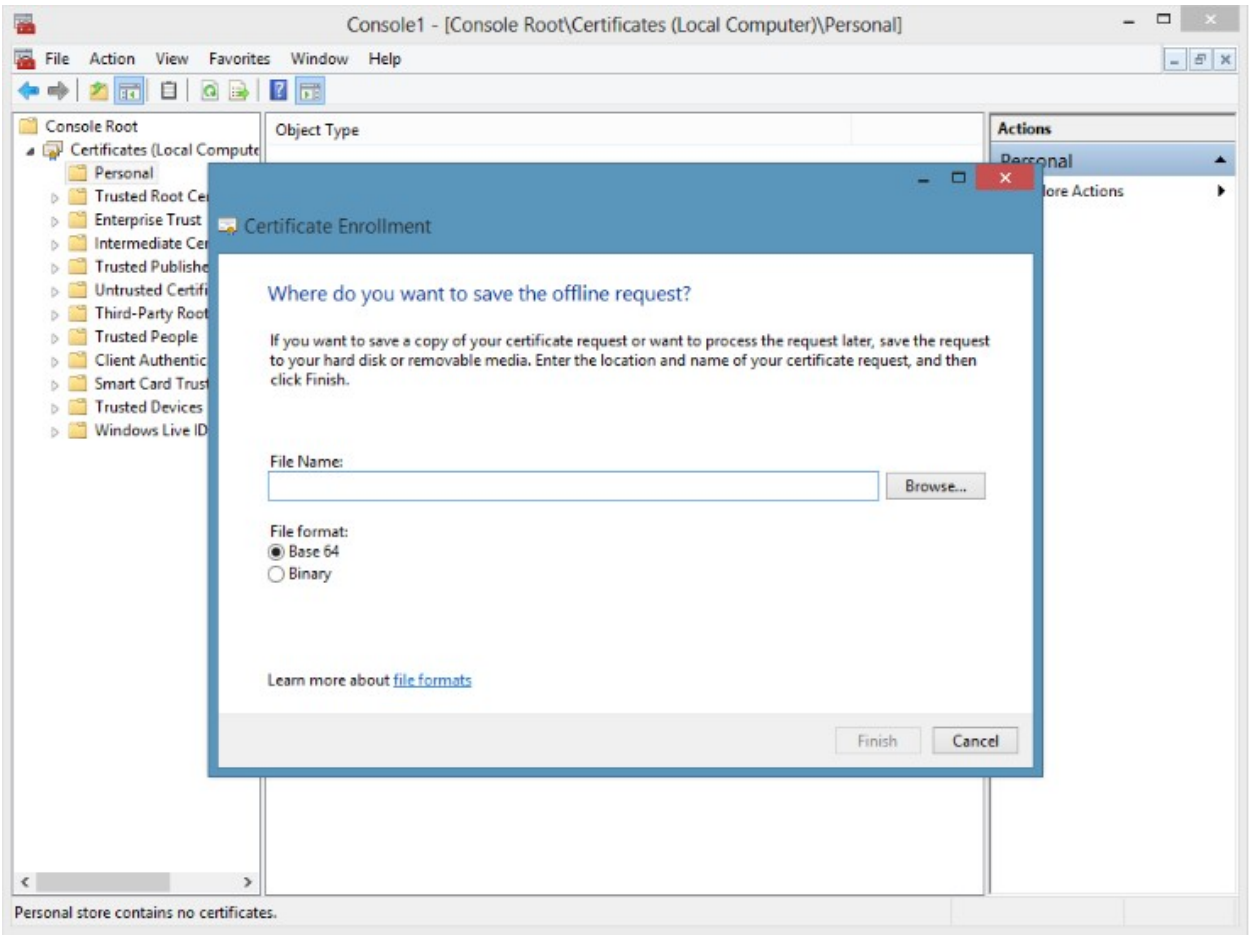


Figure 29 : Saving Offline Request

14. Select a location to save the CSR file. Enter a name for the file and click **Save**.

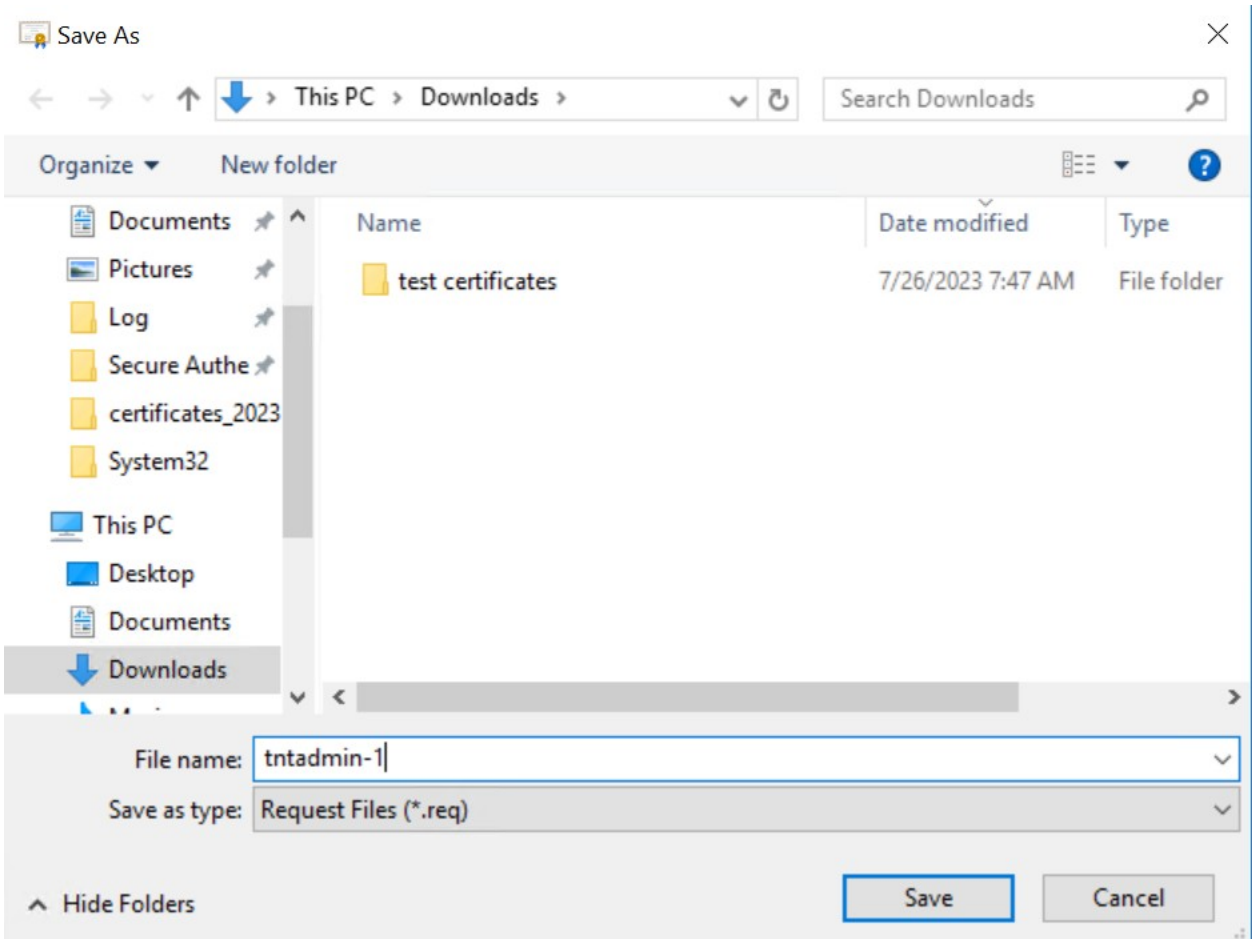


Figure 30 : Save As window

15. Click **Finish.**

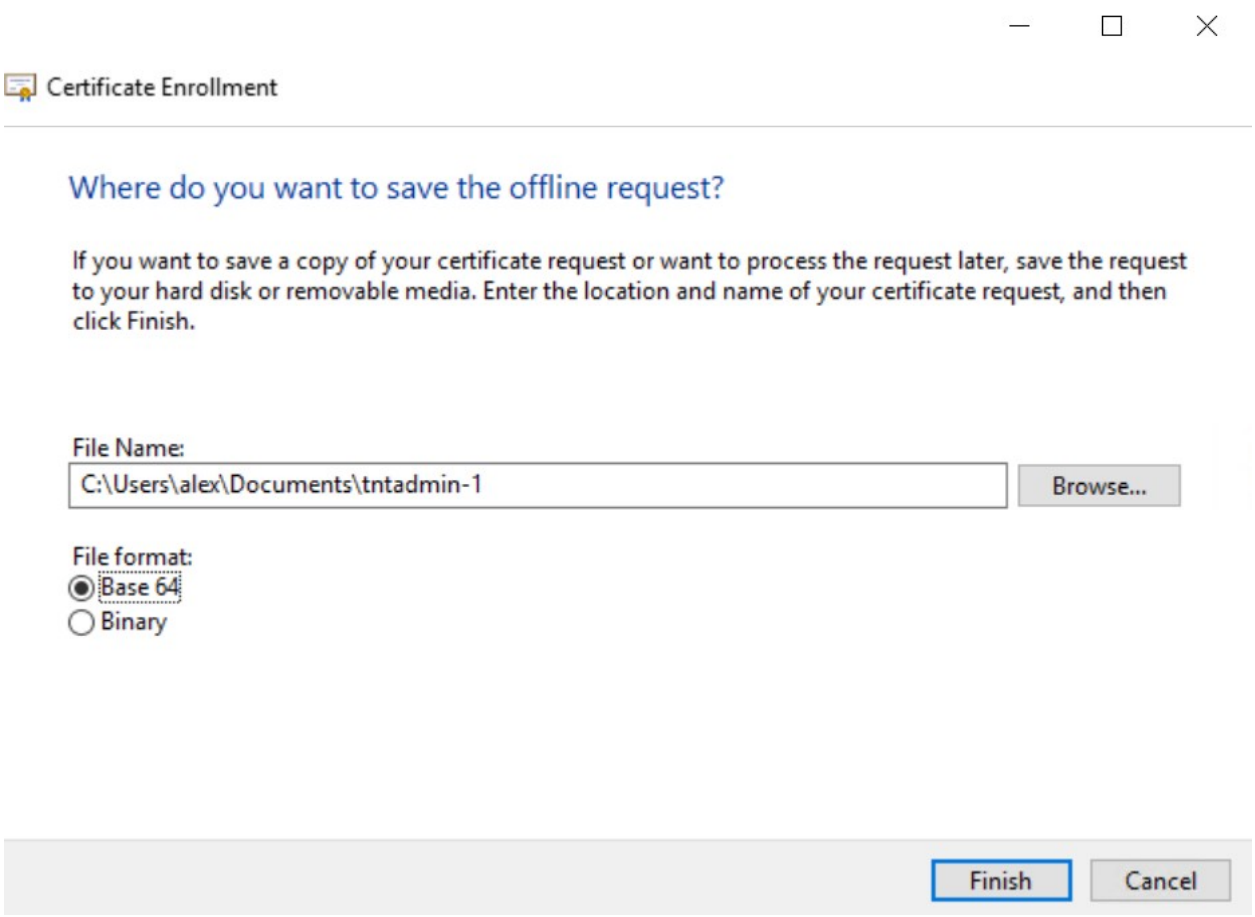


Figure 31 : Finish CSR generation

16. The CSR file will be saved at the selected location.

6.1.2 Upload CSR file to CMS for Creating Client Certificate

1. Login to CMS web as tenant administrator.
2. Navigate to **Certificate Requests**.
3. Click on **Upload New Request**.
4. Click on **Select** and select the CSR file.
5. Select certificate type as `CMP_CMS_USER_DEMOPKI-INFRA-CA_utimaco`.

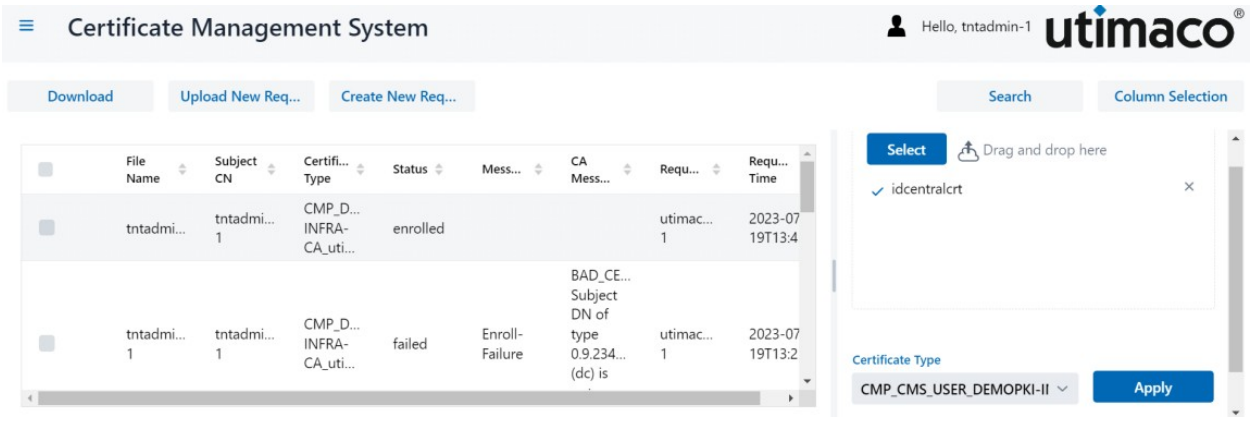


Figure 32 : Upload CSR

6. Click on **Apply**.
7. After few seconds the CSR will get signed by the CA.
8. Navigate to **Certificates**.
9. Select the certificate that was issued and click on **Download**. A zip file will be downloaded that contains signed certificate.

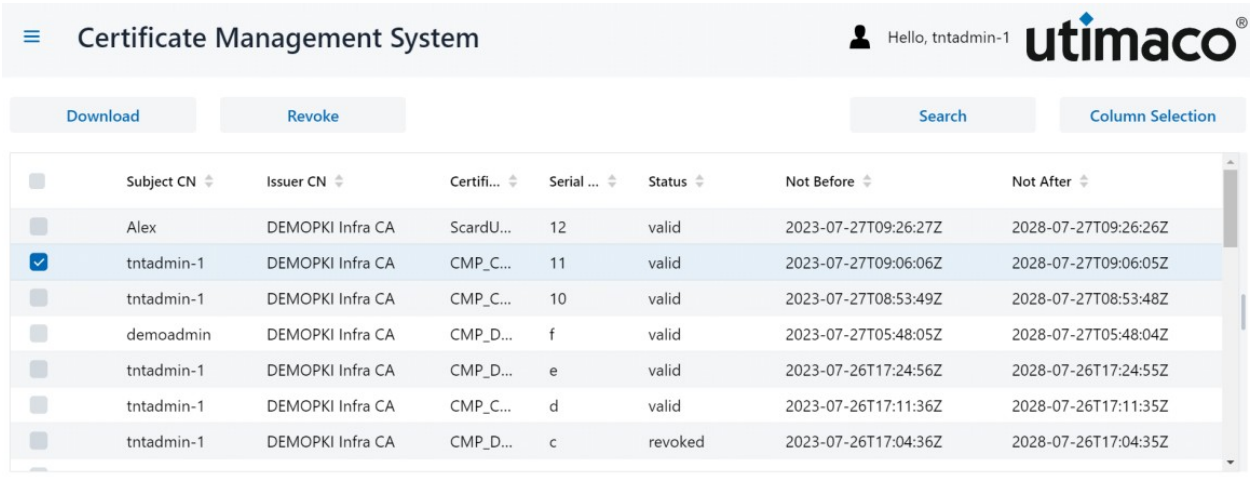


Figure 33 : Download client certificate

6.1.3 Install and Export Client Certificate

1. From Microsoft Windows, click **Start**.
2. In the Search programs and files field, type **certmgr** and select **Manage computer certificates**.

3. Go to the **Certificates -Local Computer** > **Personal** > **Certificates** folder in the Certificate tree.

4. Right-click on the **Certificates** and select **All Tasks** > **Import**.

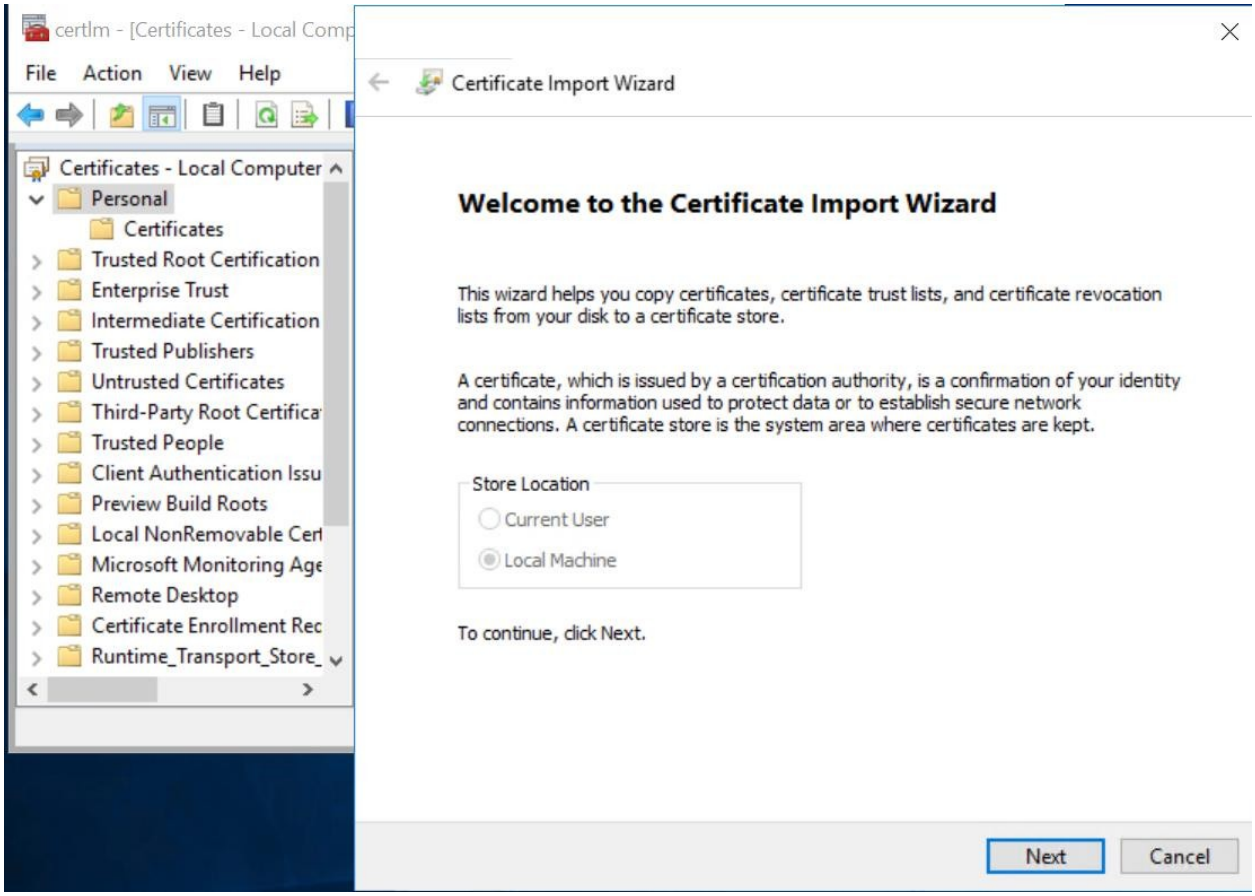


Figure 34 : Import client certificate

5. Select the signed certificate file that you have downloaded from CMS Web and click the **Open** button.

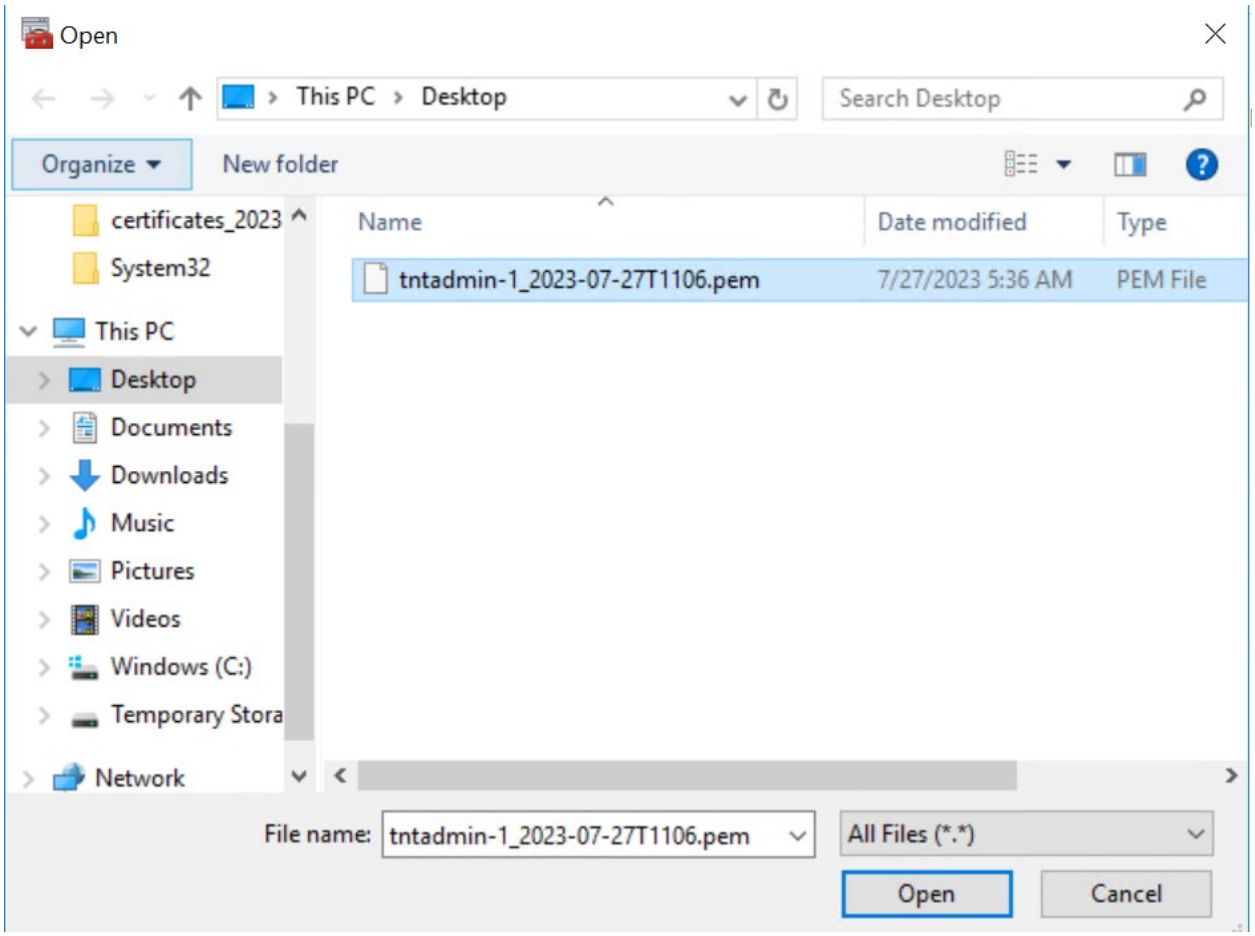


Figure 35 : Select client certificate

6. On **Certificate Import Wizard** click the **Next** button.

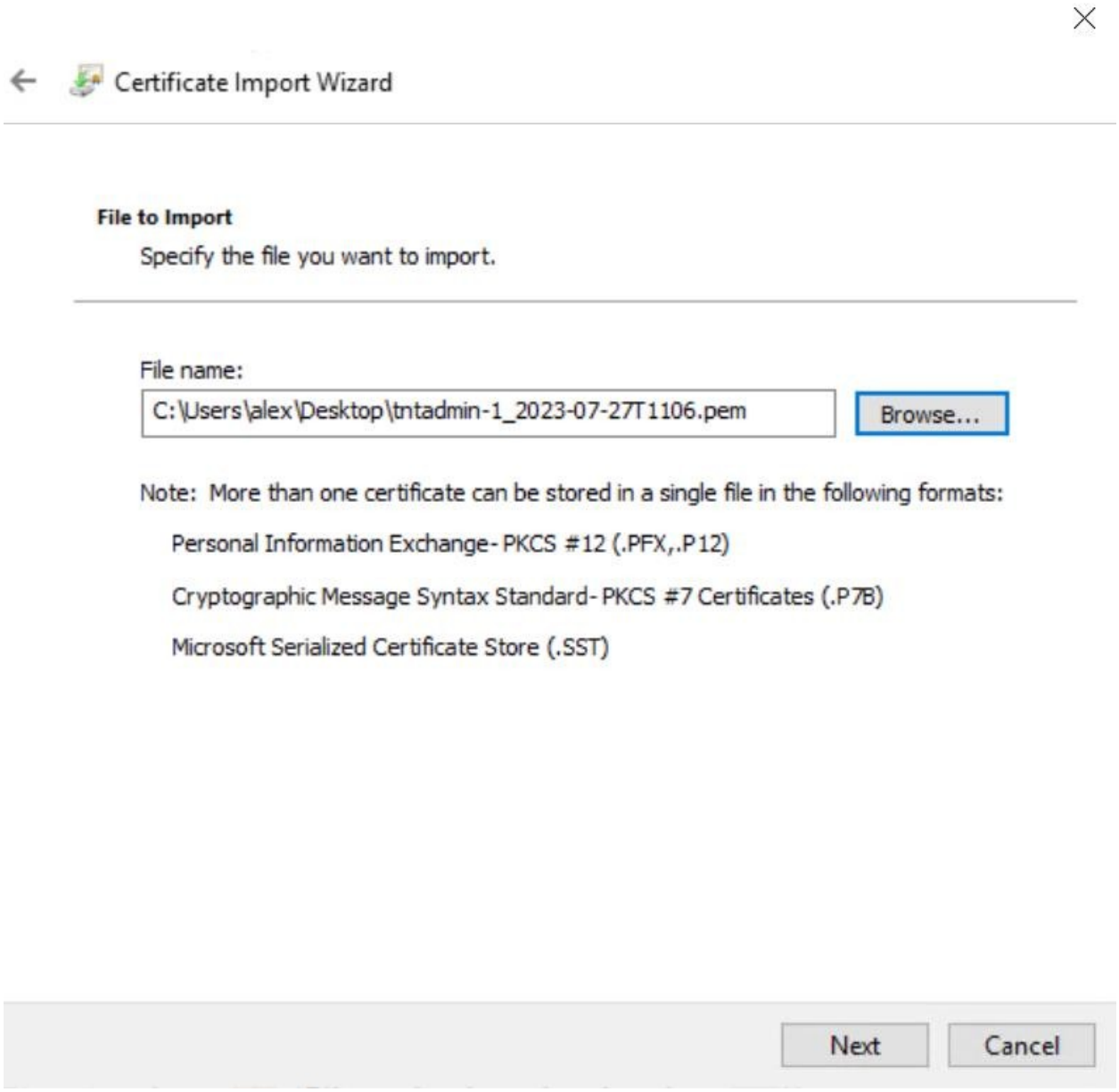


Figure 36 : Certificate Import Wizard

7. Select **Personal** as certificate store and click **Next**.

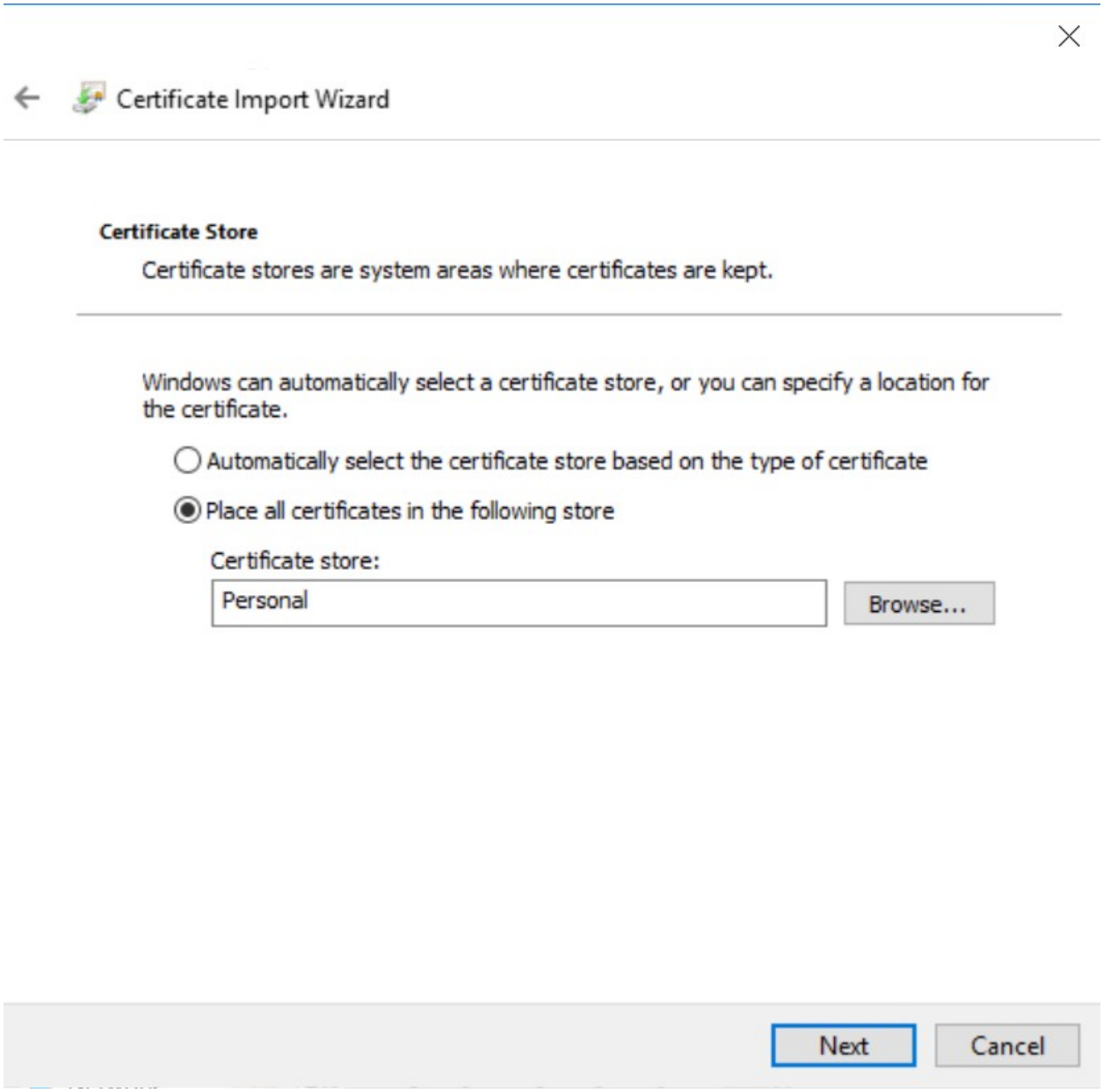


Figure 37 : Select Certificate Store

8. Click on **Finish**.

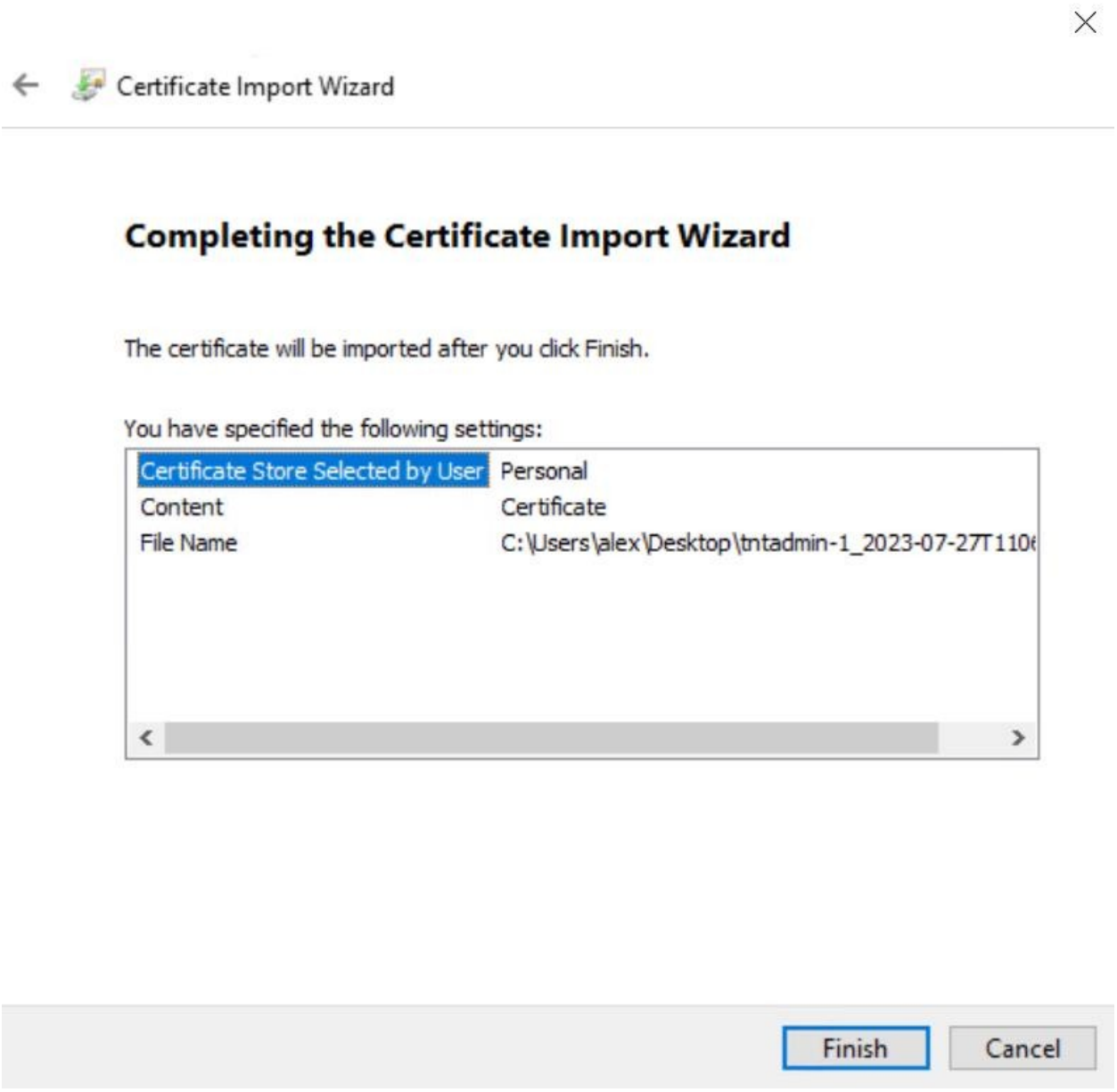


Figure 38 : Finish window

You will get a message **Import Successful**.

9. Refresh the certificate list and you will notice the presence of your new certificate, with a key icon over the certificate icon to indicate the presence of a private key.

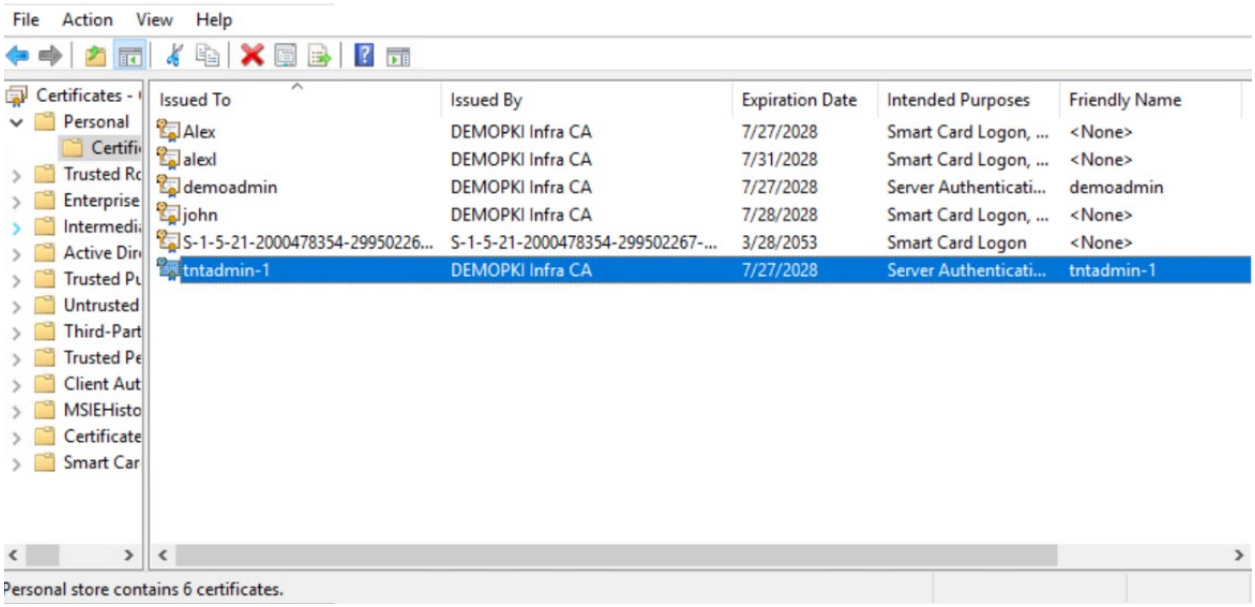


Figure 39 : Verifying installed certificate

10. Export the newly generated certificate, right-click on tntadmin-1 certificate and Select **All Taks** > **Export...**

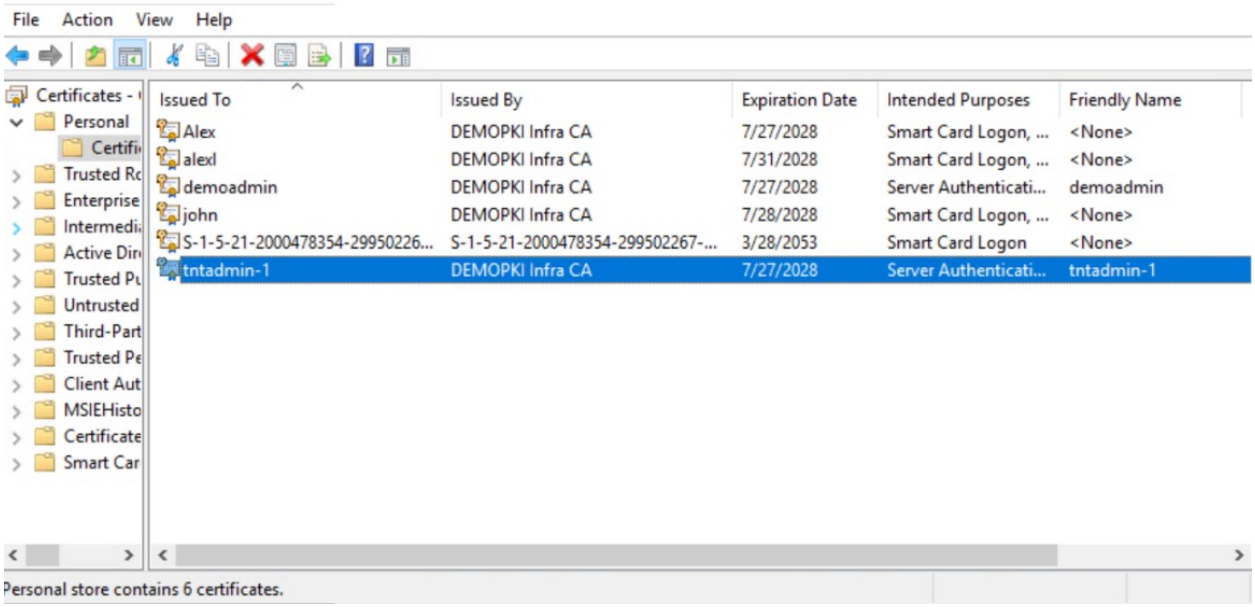


Figure 40 : Selecting Certificate to export

11. Click the **Next** button to continue.

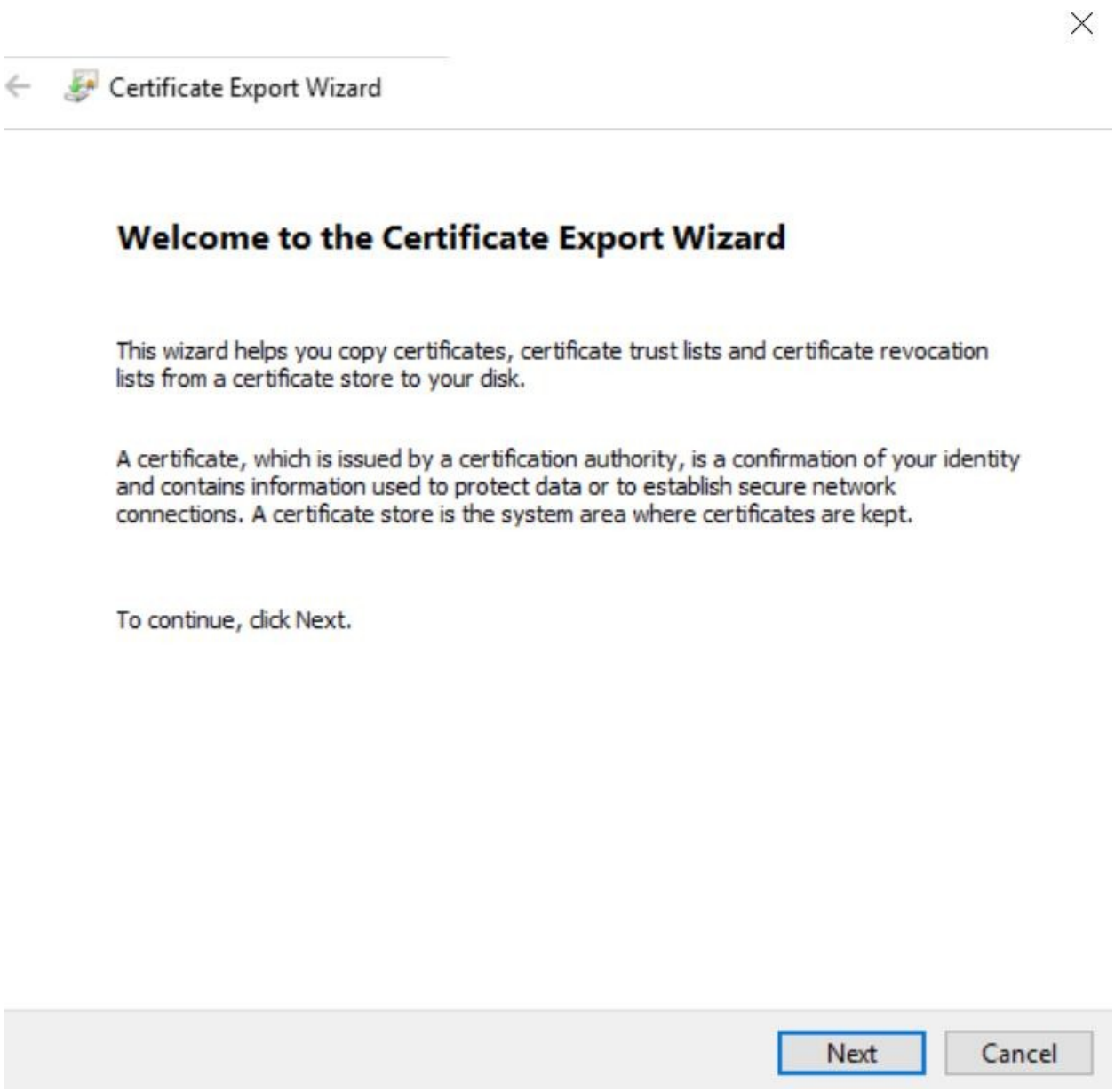


Figure 41 : Certificate Export Wizard

12. Select **Yes, export with private key** option and click the **Next** button.

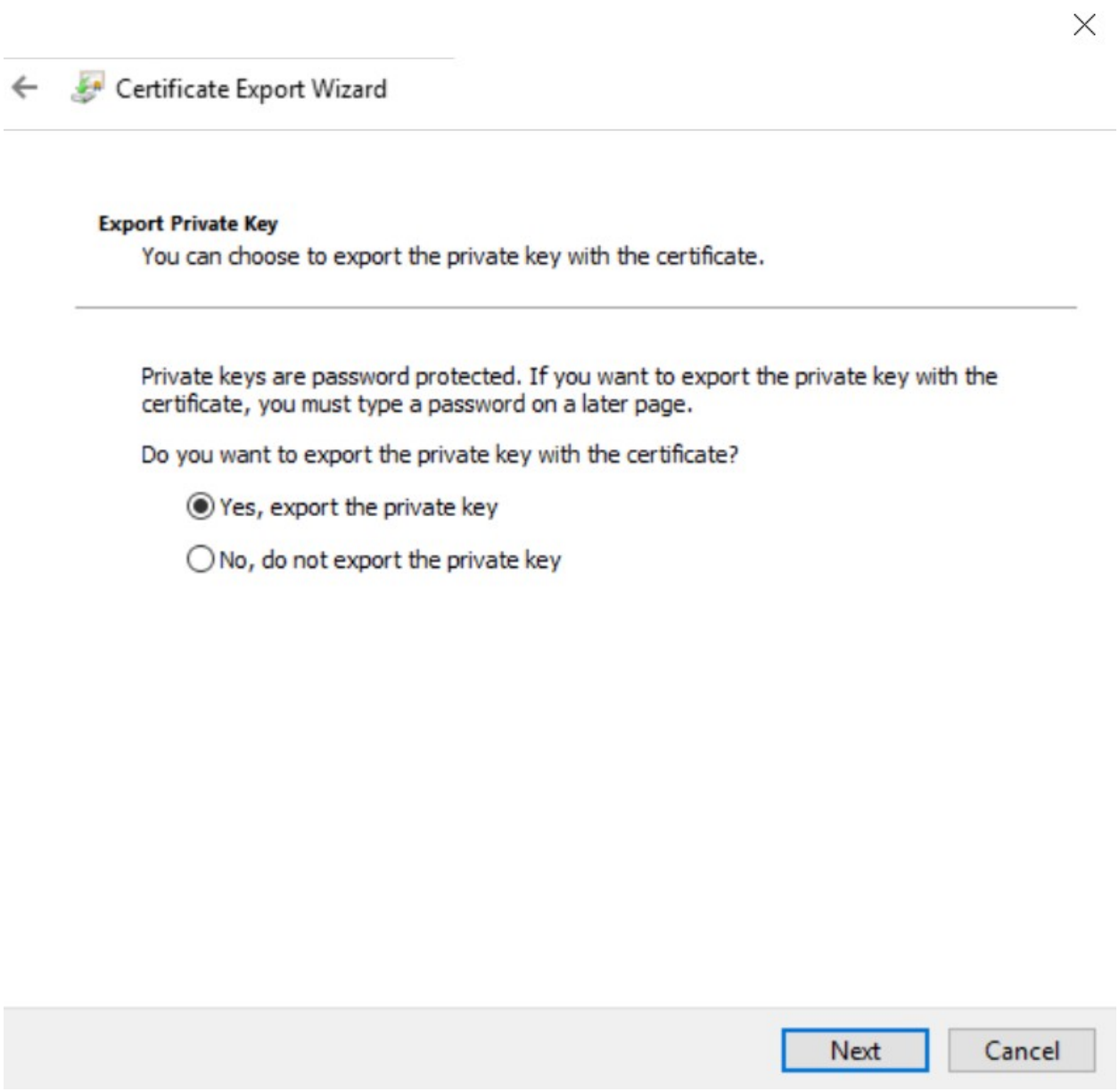


Figure 42 : Selecting export with private key

13. Select **Include all certificates in the certification path if possible** and **Export all extended properties.**
14. Click on the **Next** button.

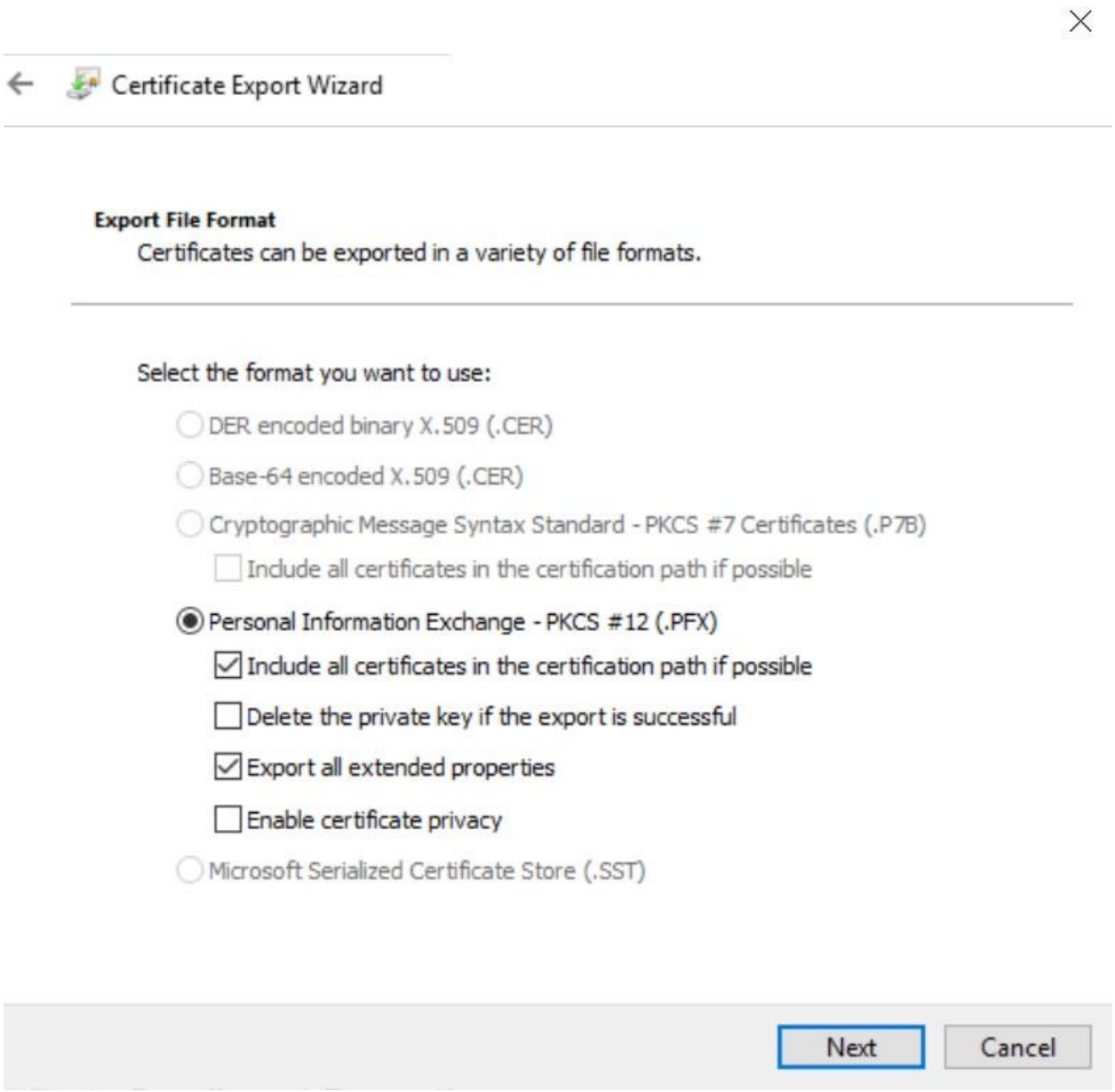


Figure 43 : Certificate Export Wizard for file format

15. Check the **Password** option and enter any strong password. Click **Next**.

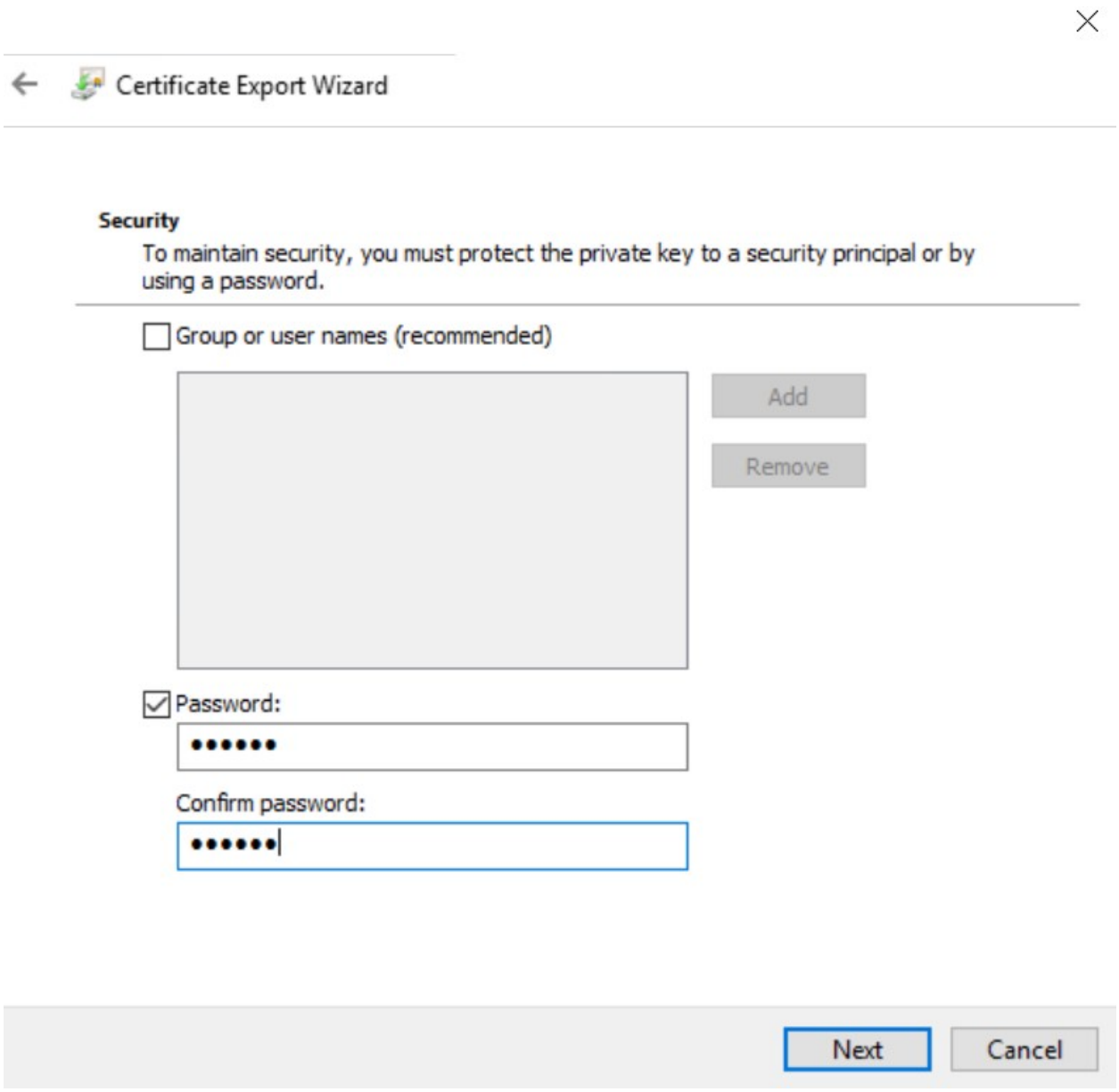


Figure 44 : Enter the password

16. It will ask to save the certificate with key file. Click **Browse**
17. Select location and provide file name.

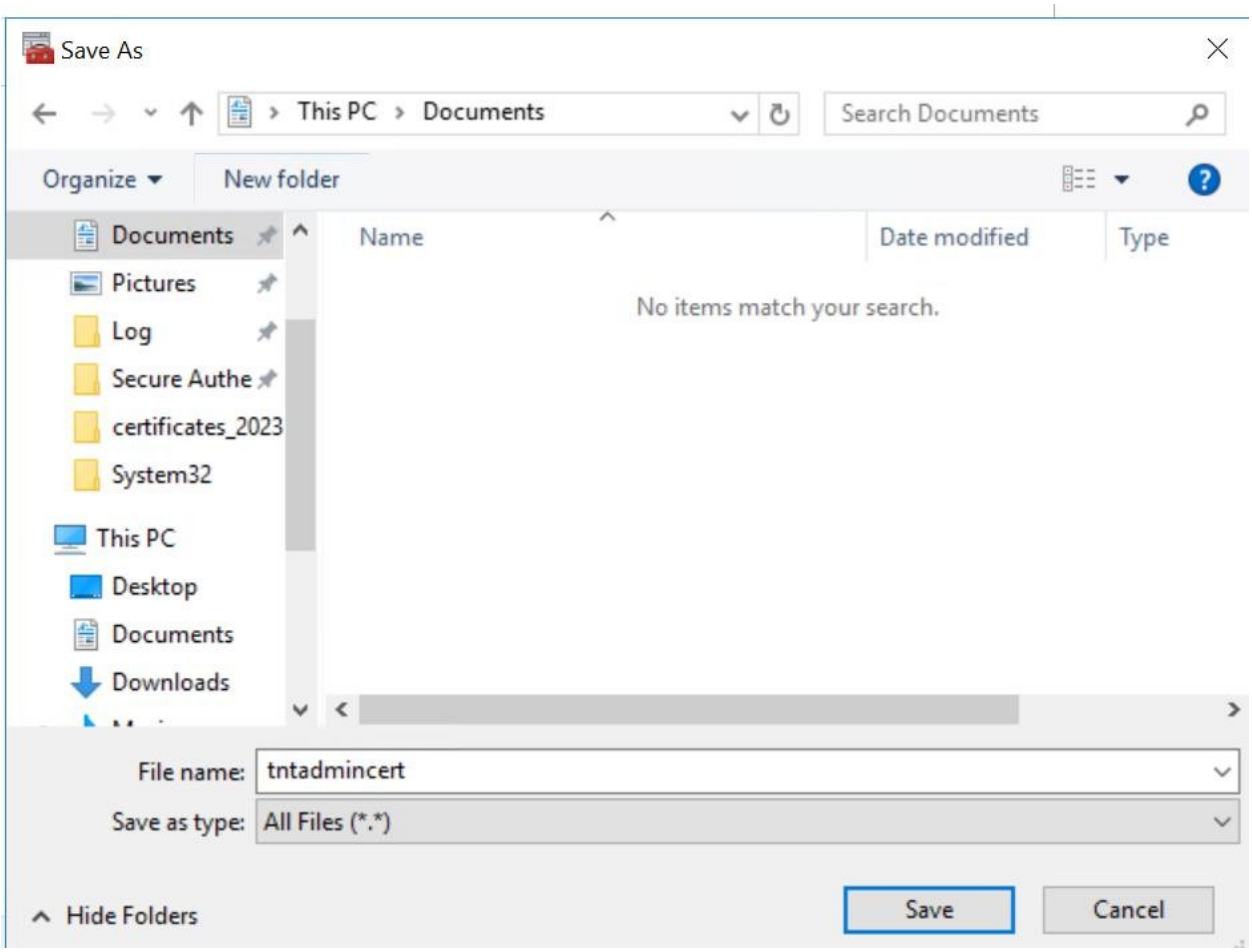


Figure 45 : Save certificate

18. Again, click **Next**.

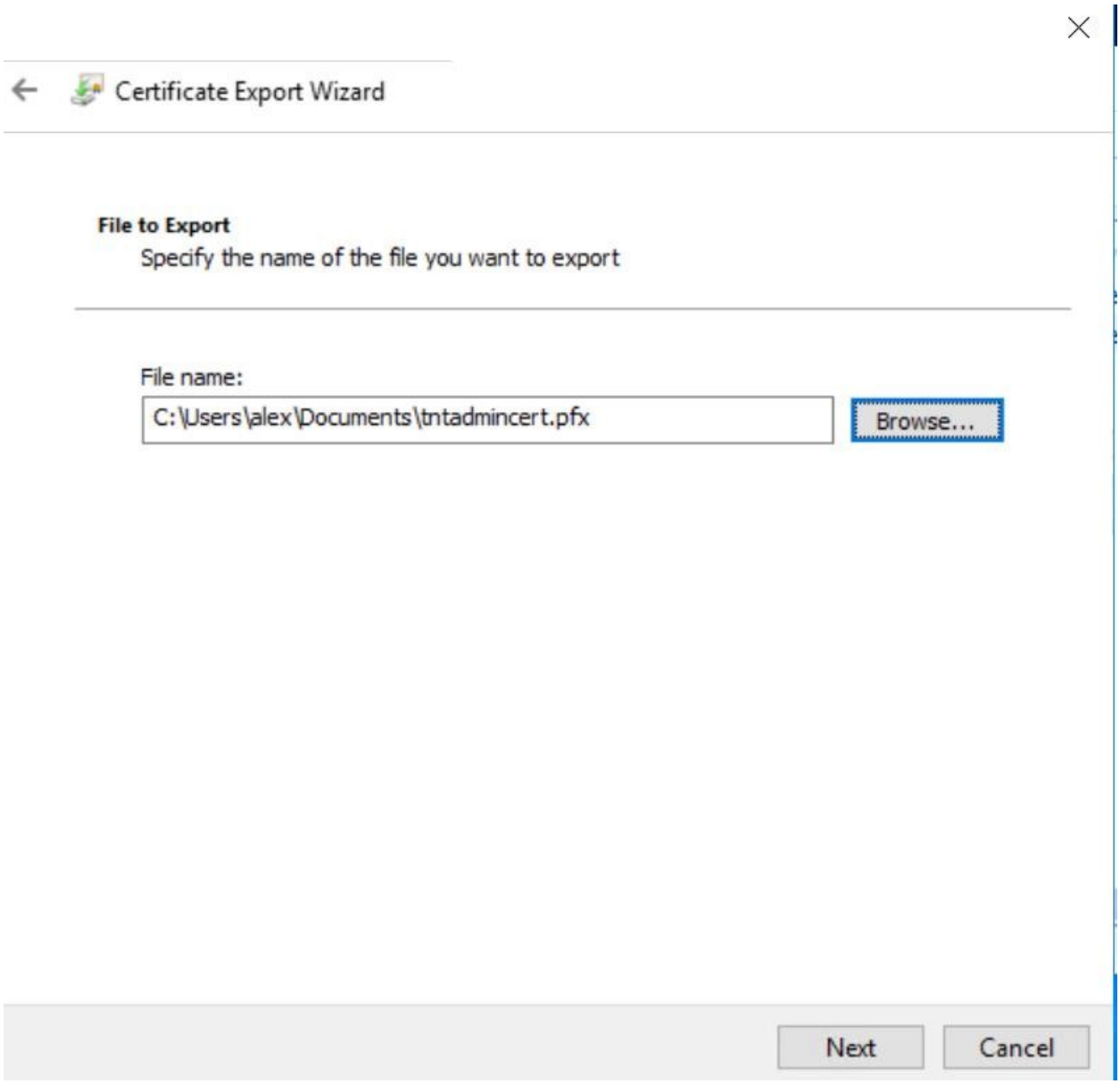


Figure 46 : Certificate Export wizard

19. Click the **Finish** button.

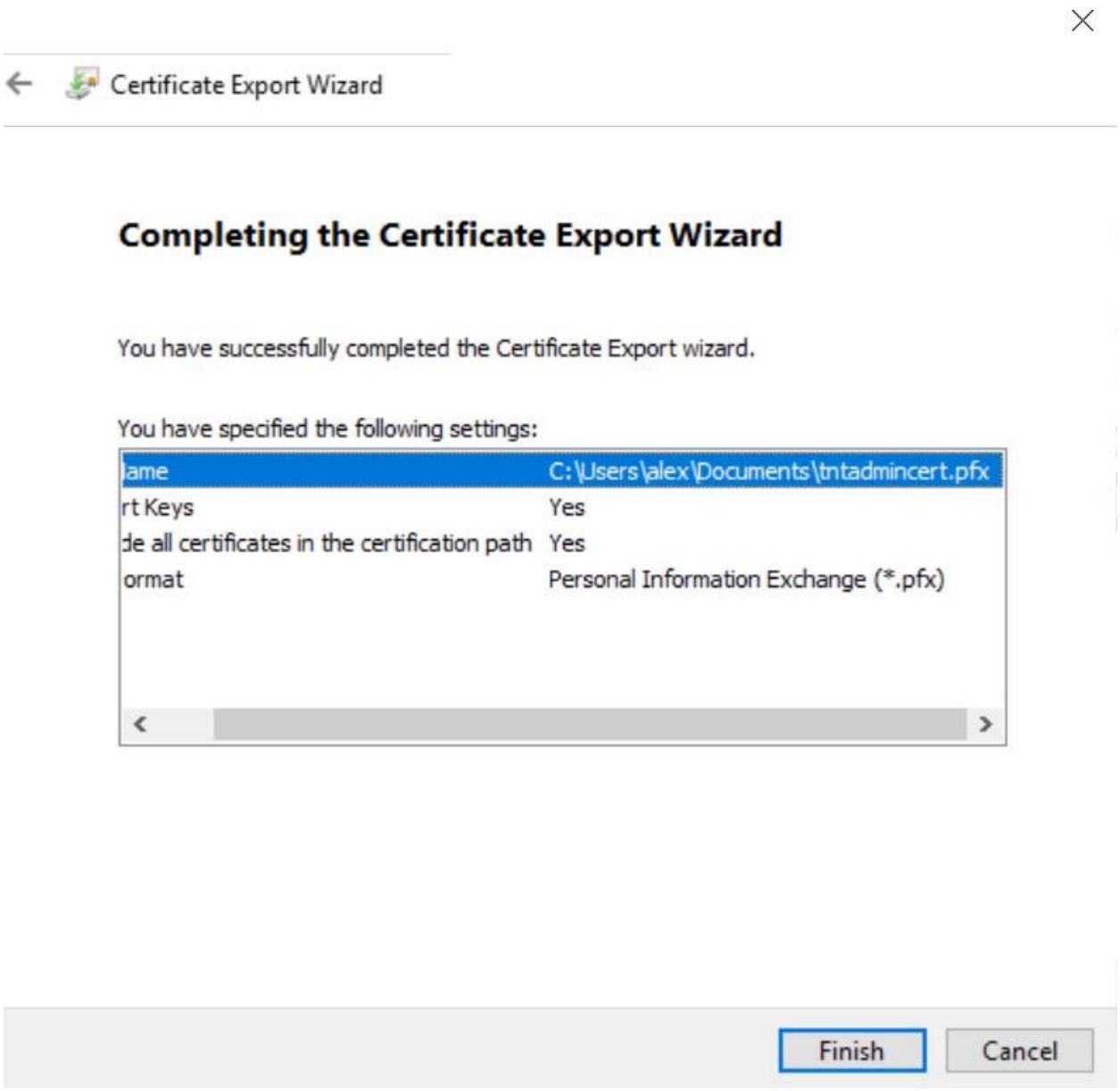


Figure 47 : Certificate Export Wizard finish window

6.2 u.trust Identify CA Configuration on IDcentral

This section describes in detail the configuration steps to set up u.trust Identify PKI Certificate Authority in IDcentral Identity Registration administrator snap-in.

6.2.1 CA Configuration

1. Open IDcentral Identity Registration snap-in in MMC (Microsoft Management Console).

2. Navigate to **Certificate Authority** section from the left panel options.
3. Click on **Add Hierarchy**.

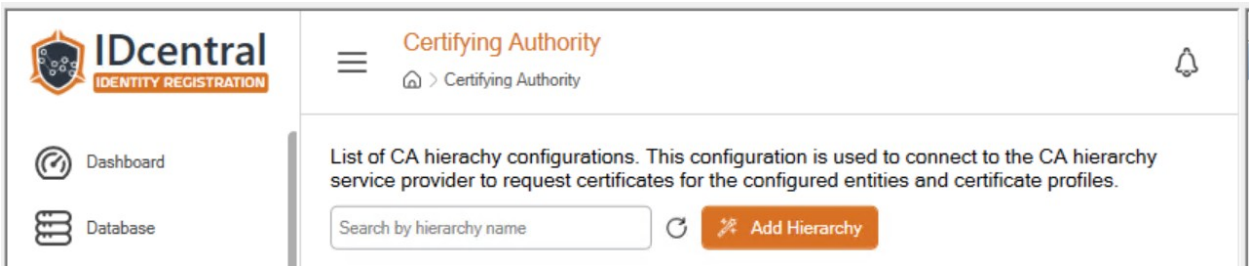


Figure 48 : Certifying Authority window

4. Choose Provider as **u.trust Identify – Utimaco** from the dropdown list.
5. Provide the following necessary information.

Parameters	**Values**
Hierarchy Name	Enter the CA name as configured in the u.trust's Certificate Management System
CA Certificate	Upload the CA certificate. Please note that the CA chain must be trusted in the Idcentral server.
API client certificate	Upload the client certificate to be used for authenticating to the CMPv2 interface of u.trust Identify.
CA URL	Enter the URL of CMPv2 interface of u.trust Identify. For example: https://<FQDN des CMS>:<HTTPS-PORT>/cmp
Requestor Name	Name of support person or account

Parameters	Values
Requestor Phone	A support phone number
Requestor Email	A support person or account's email address

Table 5: List of parameters and values

6. In Issuing CA Certificate Click on **Upload** to select the issuing CA certificate that will be issuing the smartcard certificates.

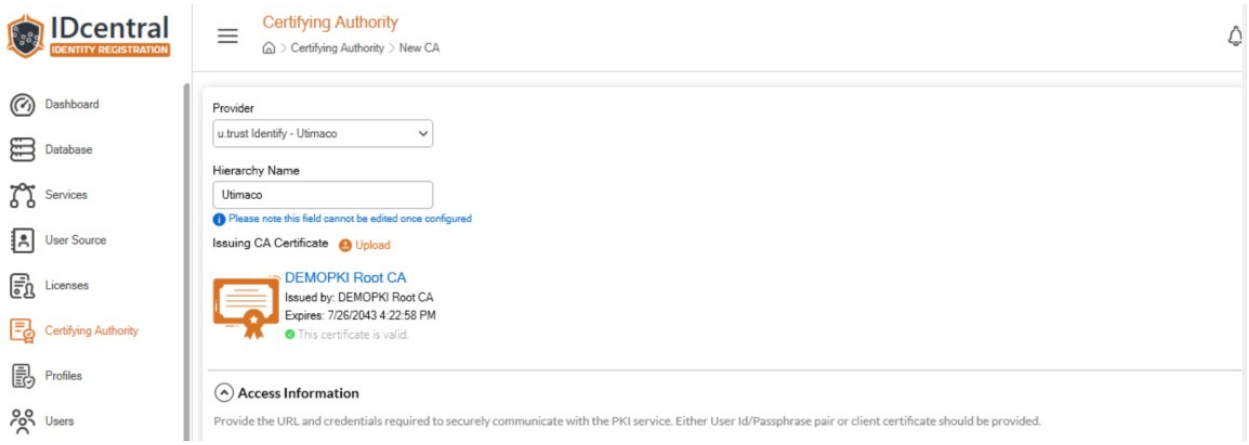


Figure 49 : Root CA certificate

7. In **Client Certificate** click on **Upload** to browse the client certificate that is used to authenticate CMPv2 interface.
8. Select the client certificate pfx file that you have exported earlier with private keys from file browser and click **Open**.
9. Enter the passphrase for the client pfx certificate and click **OK**.

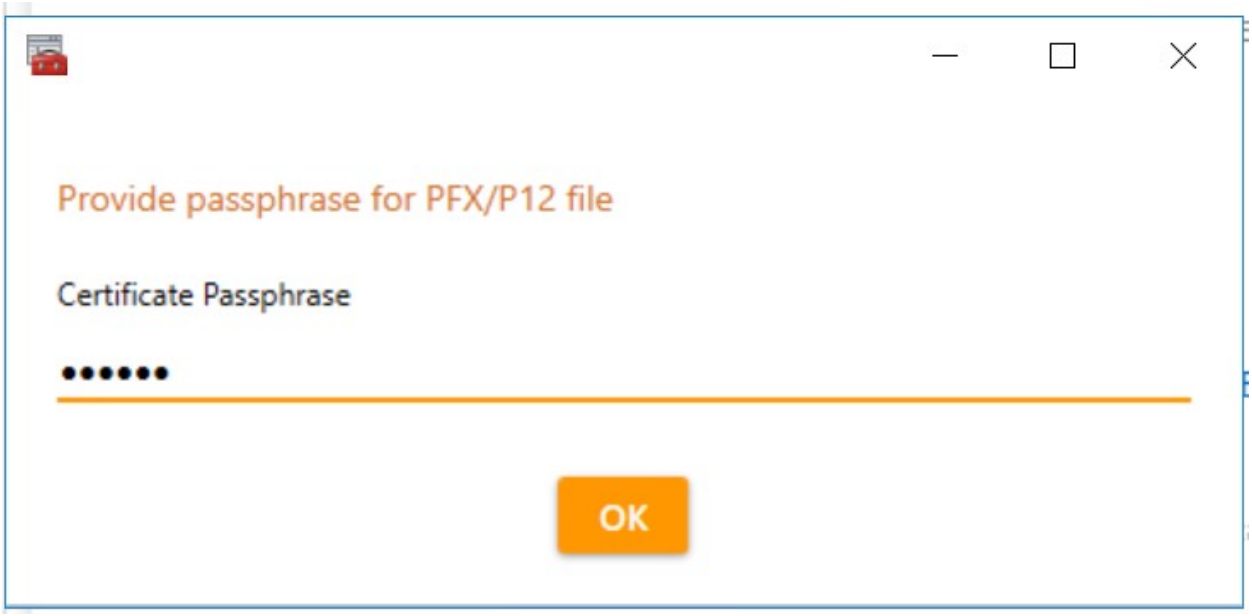


Figure 50 : Certificate passphrase

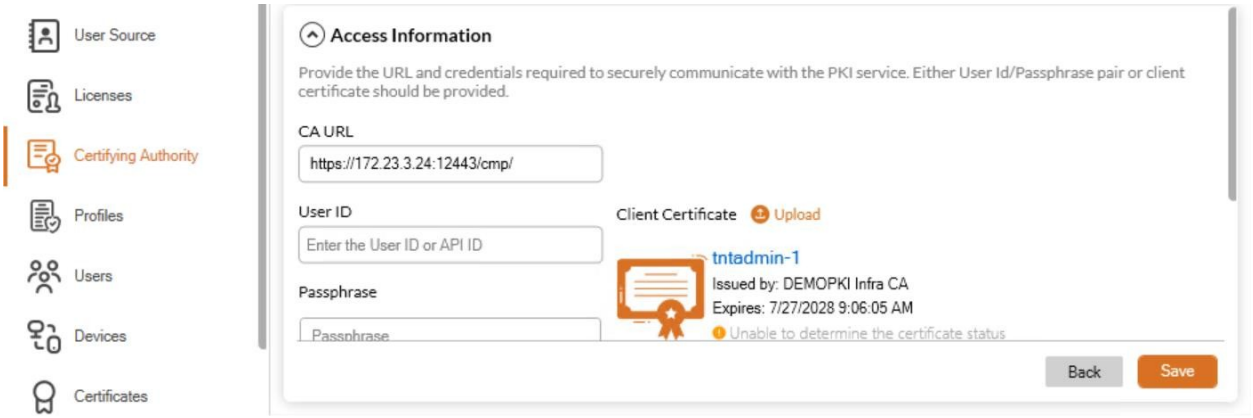


Figure 51 : Upload client certificate

10. Click **Save** to proceed saving the CA configuration.
11. On success, the saved CA configuration will be listed in the **Certificate Authority** tab.

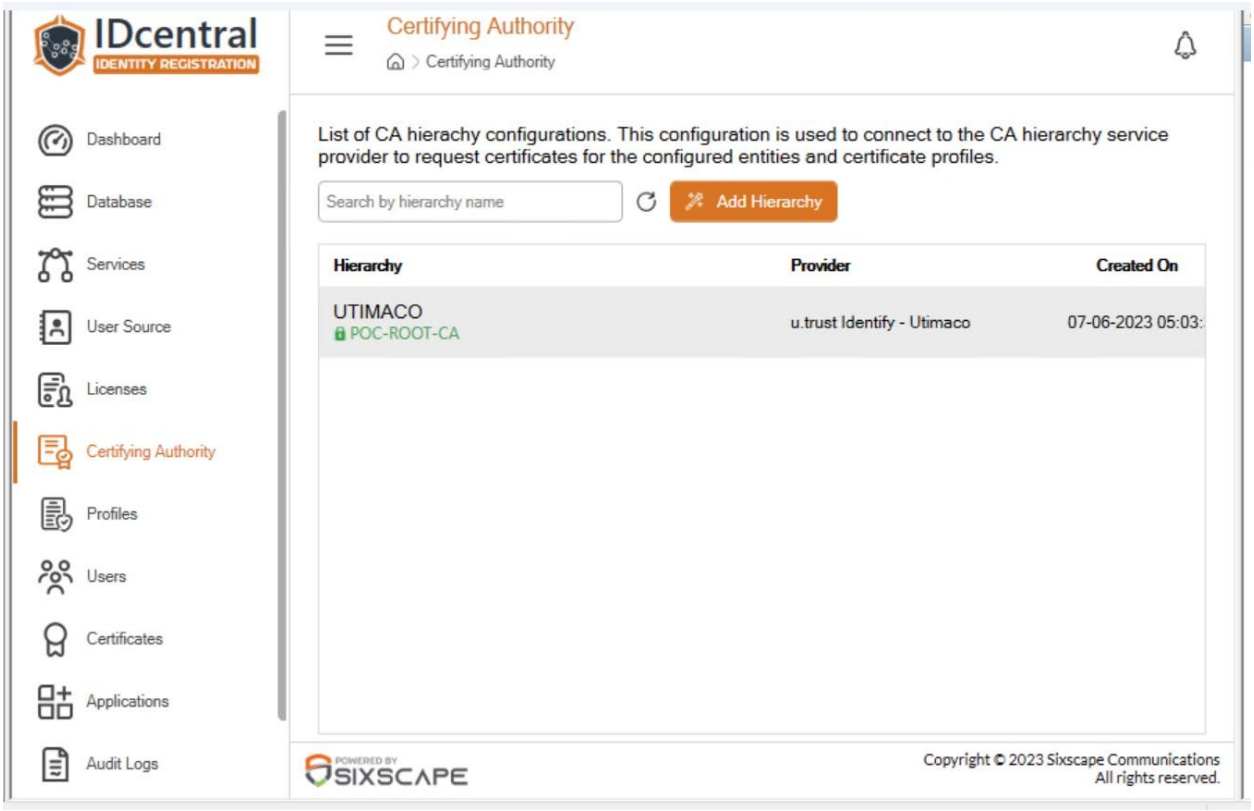


Figure 52 : Verifying added CA

6.2.2 Certificate Profile Creation

1. Navigate to **Profiles** section from the left panel options.
2. Choose **Certificate Profile** from the dropdown.

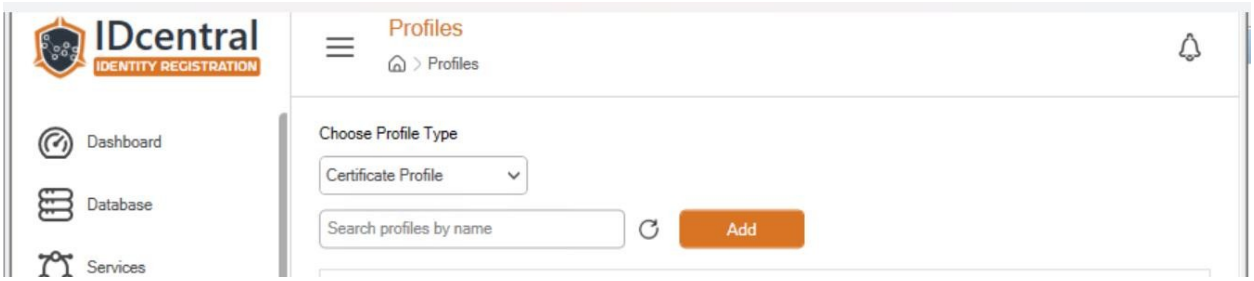


Figure 53 : Profiles window

3. Click on **Add**.
4. Provide the following information.

Parameters	Values
Profile Name	Provide a suitable name for the certificate profile
Hierarchy	Choose the configured issuing CA name from the hierarchy list
Certificate Type	Choose MS Smart Card Authentication for smartcard certificate profile
Product Code	Provide the certificate type name configured in the certificate profile configuration of u.trust Identify CMS. For example: ScardUPN
Platform	Choose suitable OS platform from the list for which the profile has been created. If applicable for all platforms, choose ANY
Key Algorithm	Choose suitable KeyAlgorithm from the list
Hash Algorithm	Choose suitable Hash Algorithm from the list
Keystore Type	Choose Microsoft CSP/CNG from the list as certificate has to be generated within the smartcard
Keystore Name	Provide a suitable keystore name
Validity (in days)	Provide the certificate validity in days
Validity Offset (in seconds)	Provide the certificate validity offset in seconds

Parameters	Values
Renewal Threshold (in days)	Number of days before the certificate expiry to initiate certificate renewal
Validation Threshold (in seconds)	Frequency interval in seconds during which the certificate validation allowed for clients

Table 6: List of parameters and values

5. Click **Save** to proceed with certificate profile configuration.

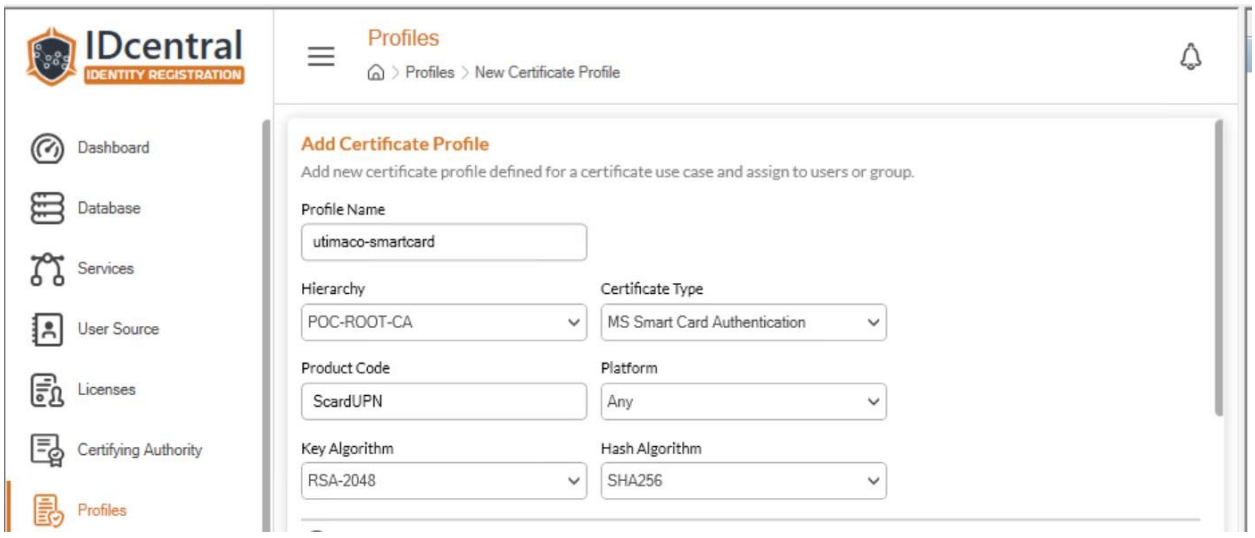


Figure 54 : Adding certificate profile

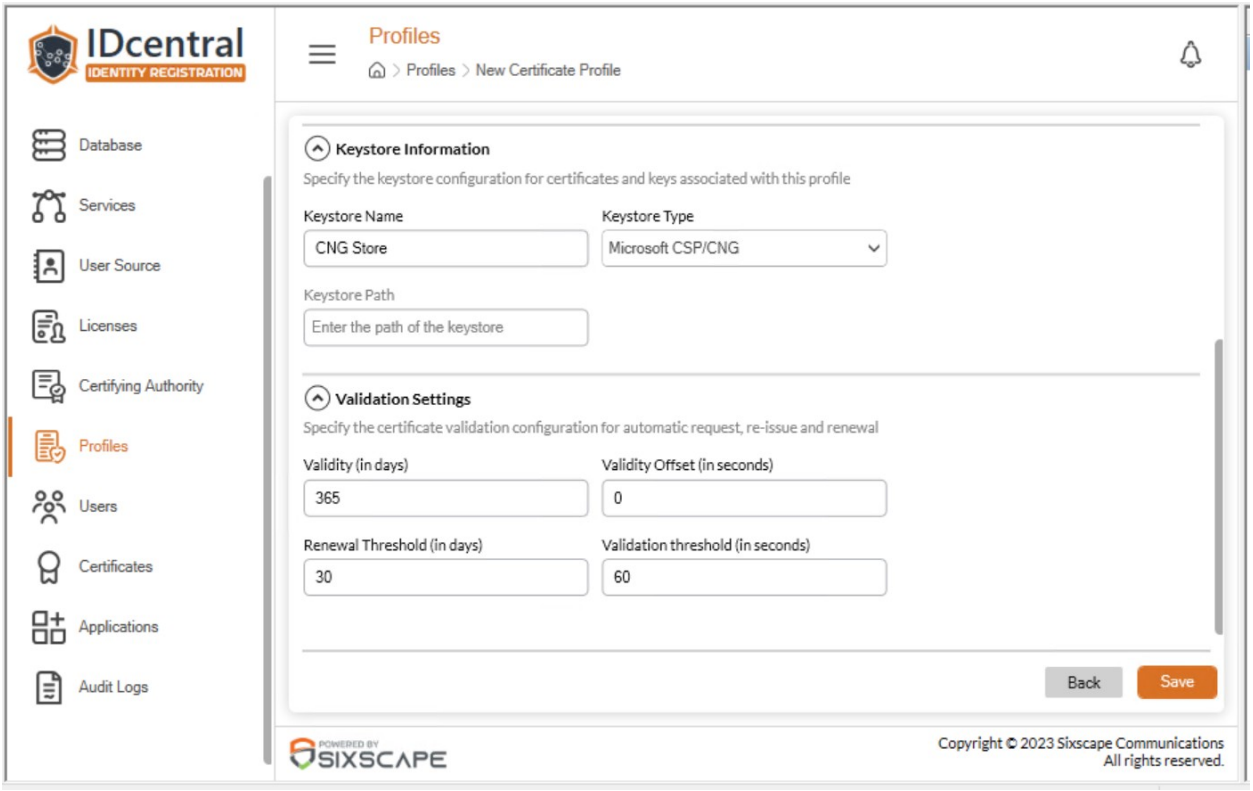


Figure 55 : Adding certificate profile

6. On success, the Certificate profile saved will be listed in the **Profiles** tab.

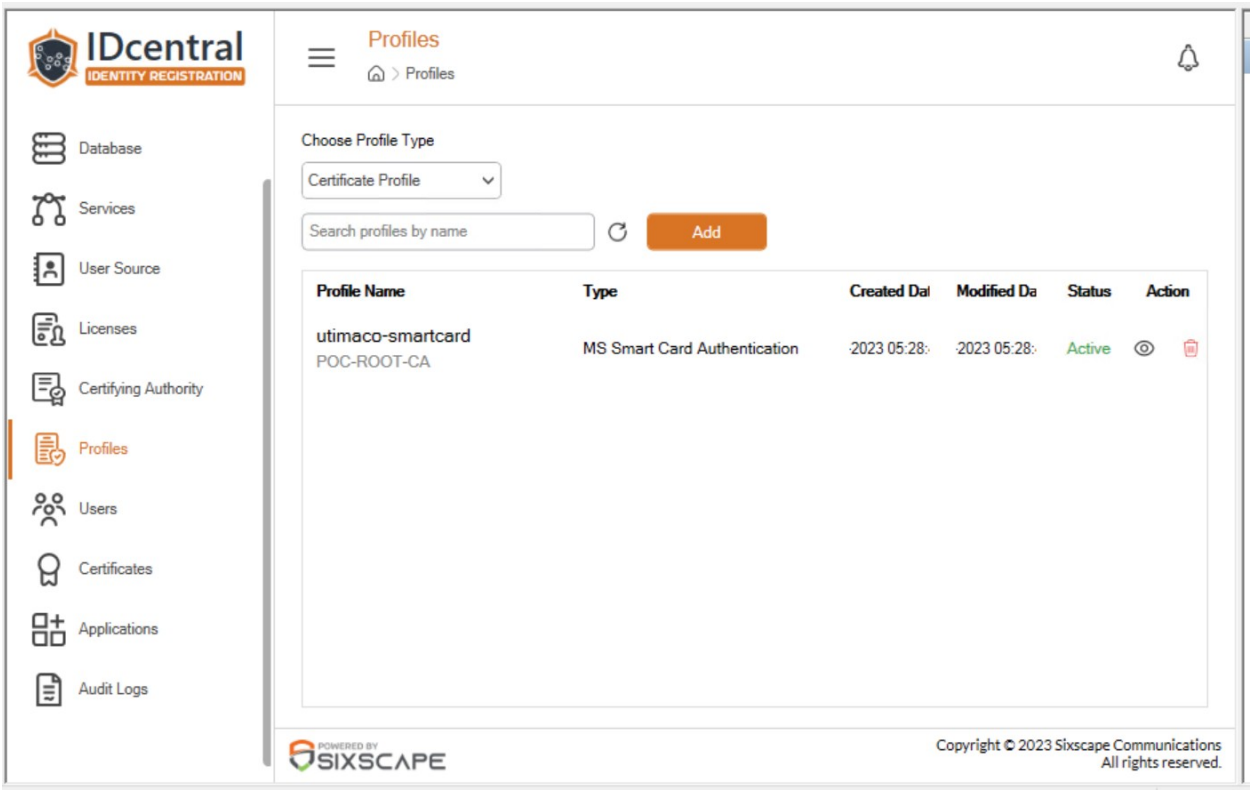


Figure 56 : Listing Certificate profiles

6.2.3 Certificate Profile Assignment

This section describes in detail the certificate profile assignment to a user or a group.

1. Click on the **View** icon from the certificate profile's view.
2. Click on the **Assignments** tab control. This view lists all the users or groups assigned to the profile.
3. Click on **New Assignment**.

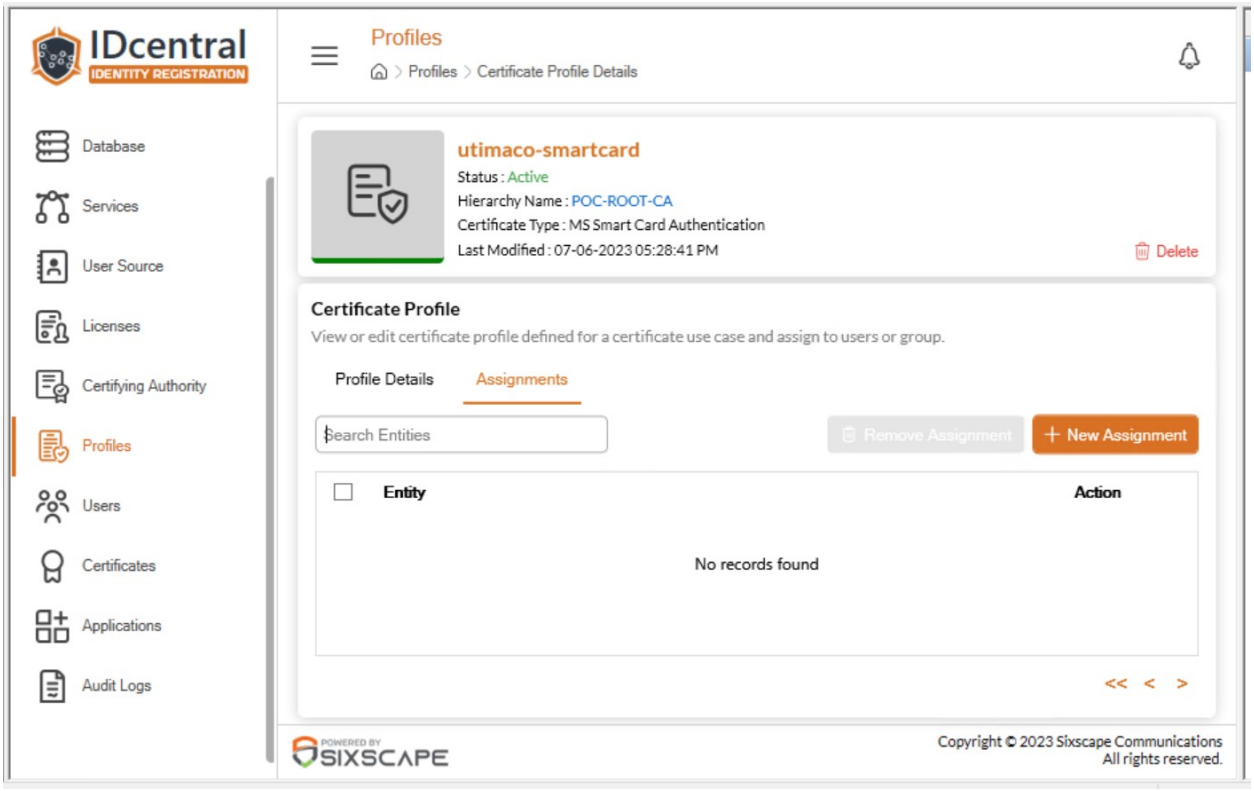


Figure 57 : Certificate Profile New Assignment

4. User **Directory Selection** panel opens on the right side.
5. Search for the required user/group and choose the same to move it to the selected records. You can sync directory to update the users and groups.
6. After selecting all the required users/groups, click on **Select**.

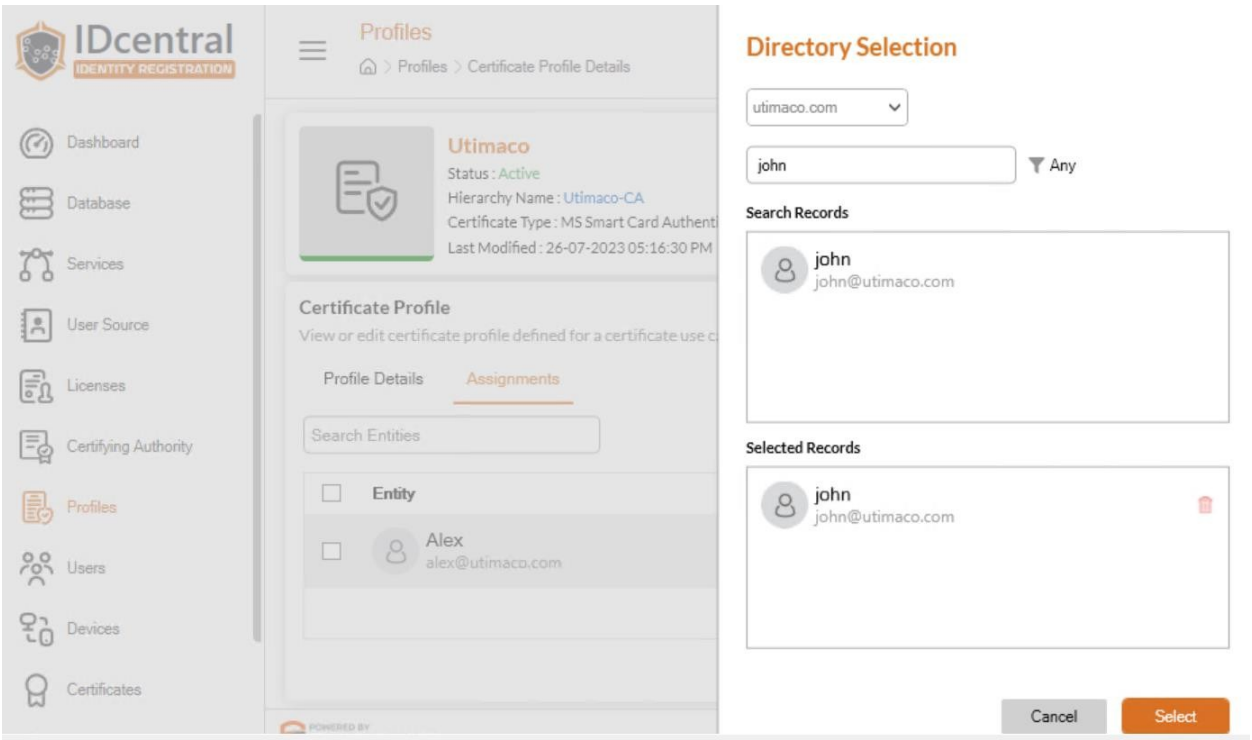


Figure 58 : Selection of user/group

7. User/Group chosen will be successfully assigned and listed in the assignments view.

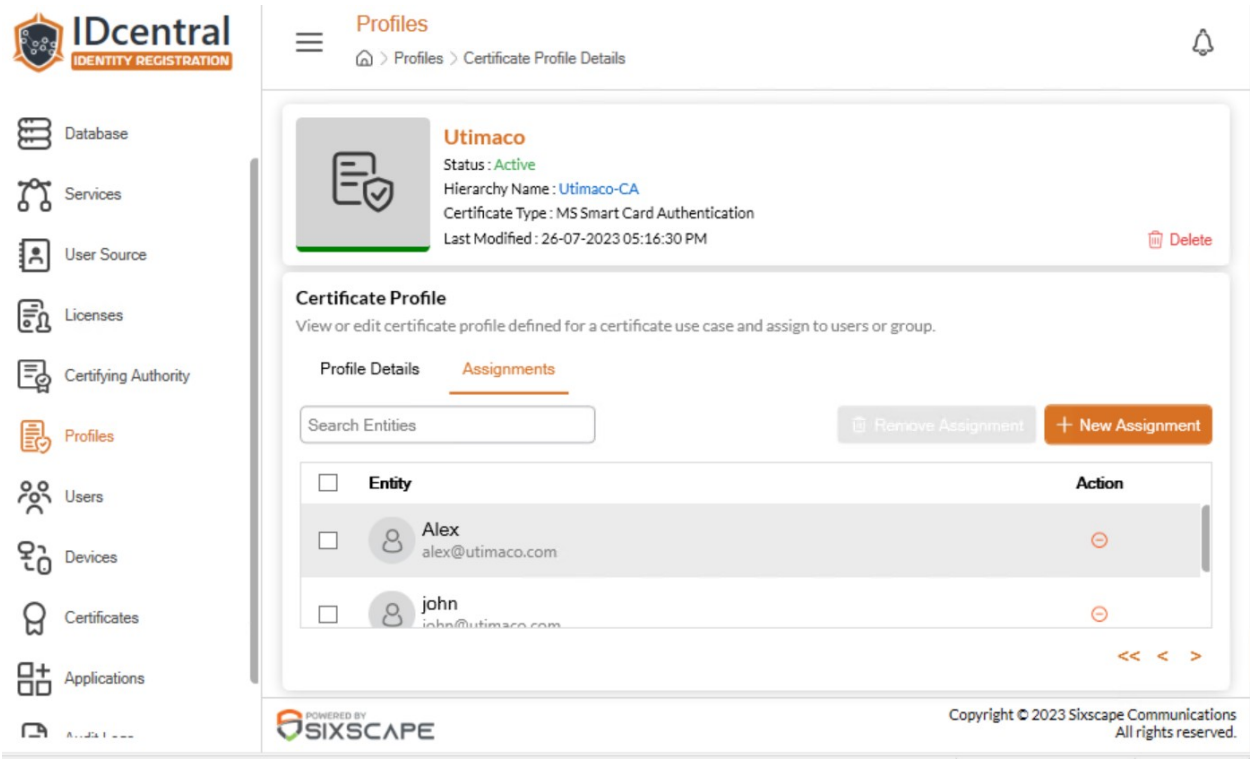


Figure 59 : Assignments view

6.2.4 Removal of User or Group from Certificate Profile

This section describes the steps to unassign certificate profile assignment for a user/group.

1. To unassign a user/group, select the check box to the left of the chosen entities.
2. Click on **Remove Assignment**.
3. Click on **Remove** on the confirmation dialog to delete the entity assignment.

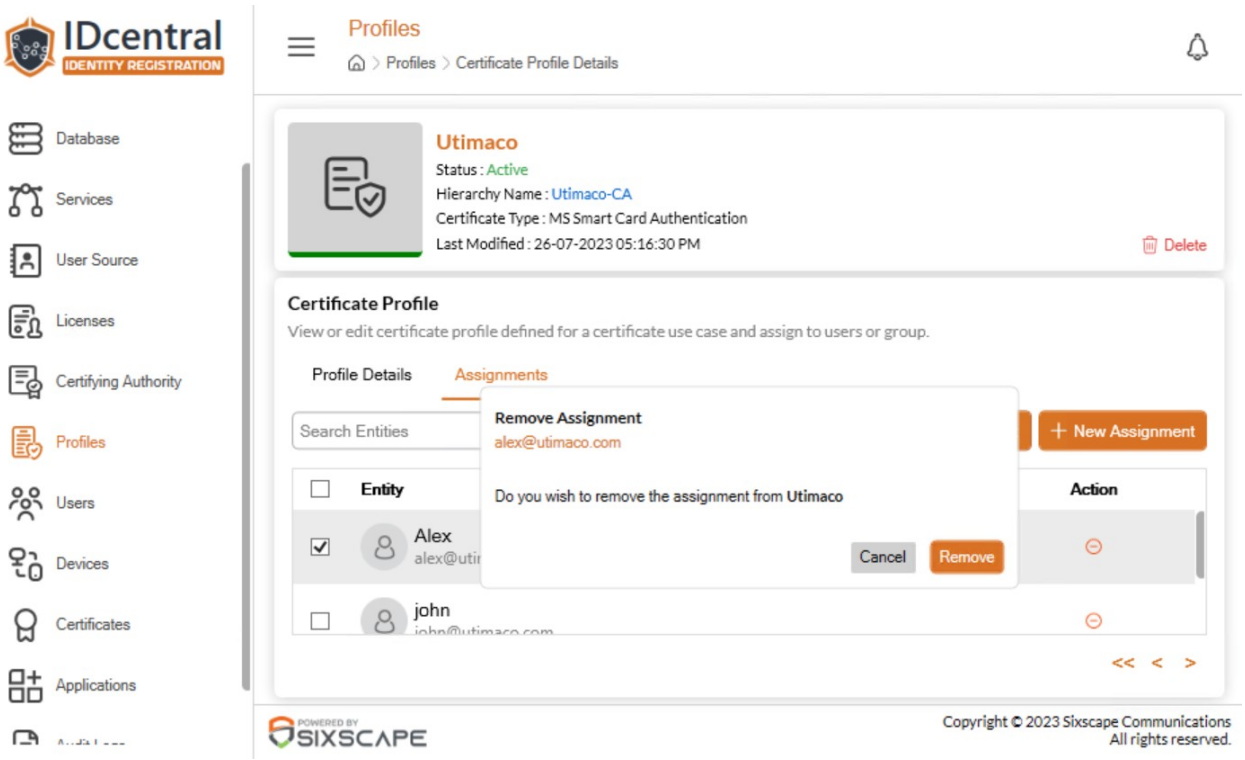


Figure 60 : Remove assignment

6.3 Device Provisioning

Device tab will appear on the IDcentral Identity Registration Management Snap-in only when Device License is activated. Once the license is activated and a user is assigned a license, details appear on the Device tab.

For activating device license, follow the steps mentioned in the section *IDcentral Smartcard License Configuration.*

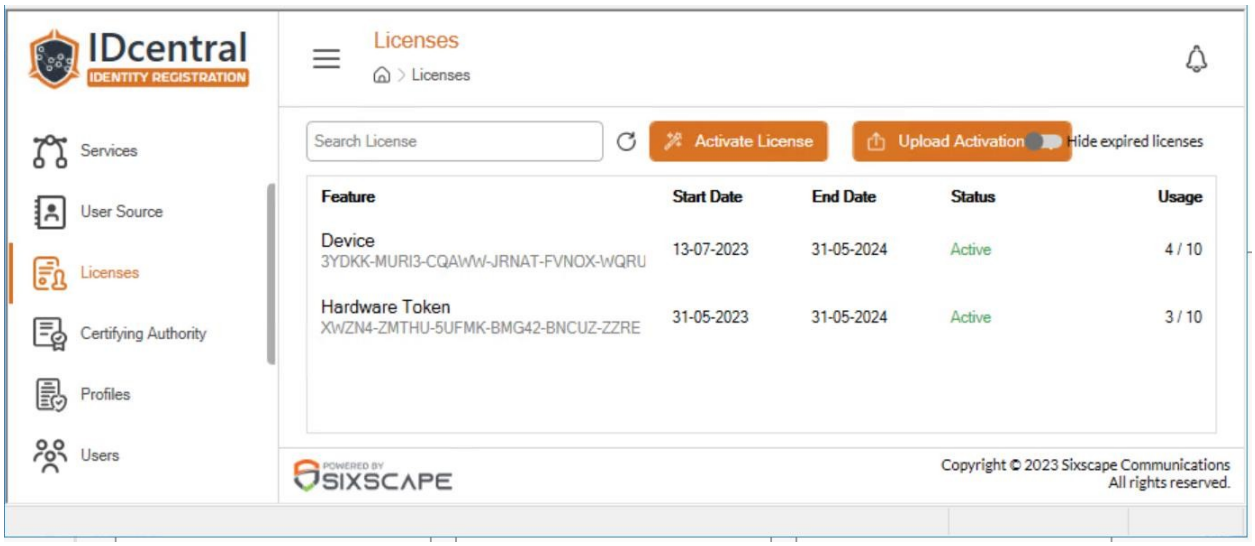


Figure 61 : Verifying device license

Once a device is registered to IDcentral Identity Registration, the device information will be listed under Devices view.

6.4 Device License Allotment to User

1. Navigate to **Licenses** view from the left panel options.
2. Click on **Device** license entry.
3. Click on **New Allotment.**

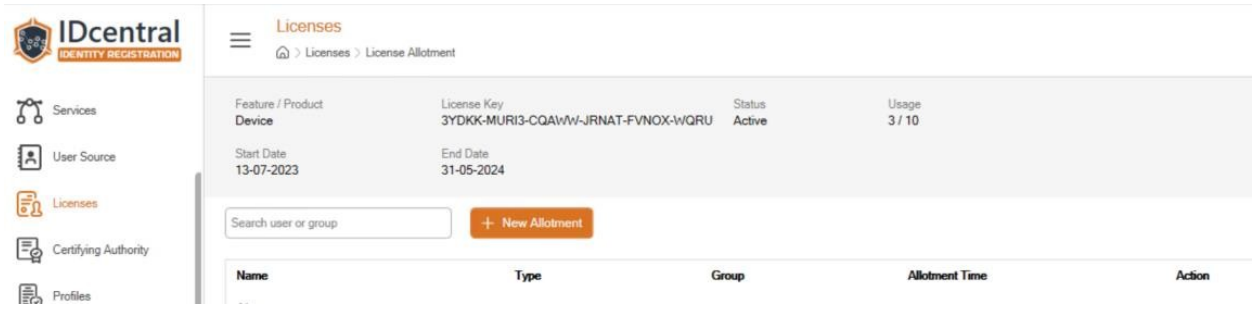


Figure 62 : Device license allotment

4. **Directory Selection** panel will be displayed on the right side. Search for a user or group in the search box.

5. Search for the required user/group and choose the same to move it to the selected records.

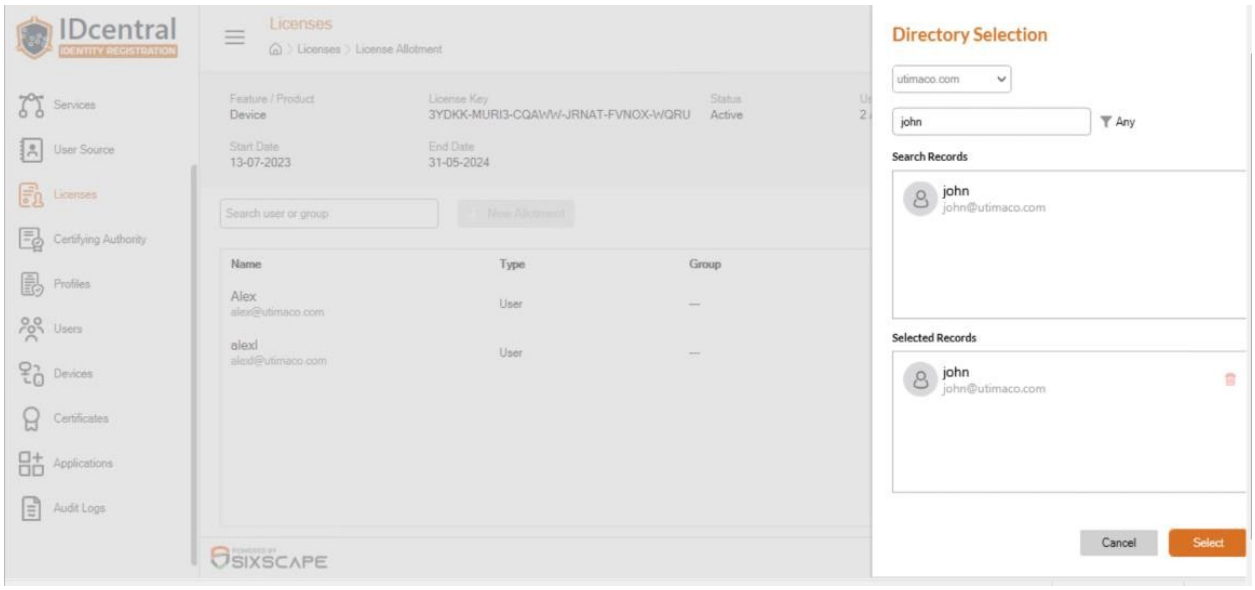


Figure 63 : Add user/group to device license

6. On successful entity license allotment, the entity information will be listed in the view.

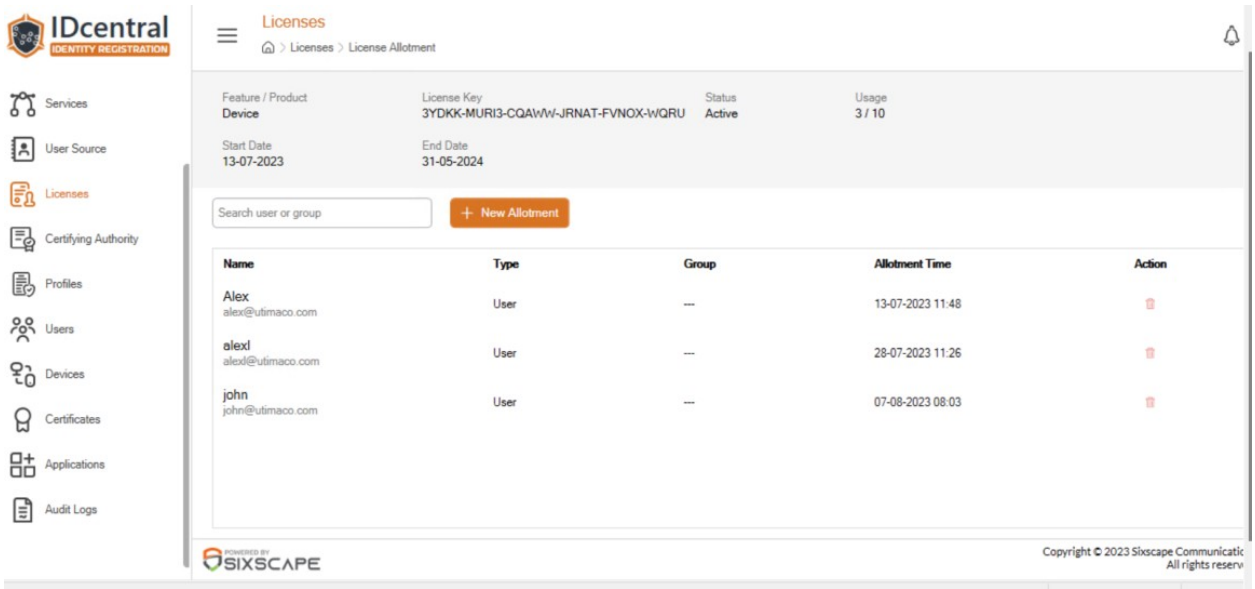


Figure 64 : License Allotment Window

6.5 Removal of Device License Allotment

This section describes the steps to unassign license allotment for any user/group.

1. To unassign the entity, click on the **delete** icon (right side).
2. Click on **Delete** in the displayed confirmation dialog to delete entity allotment.

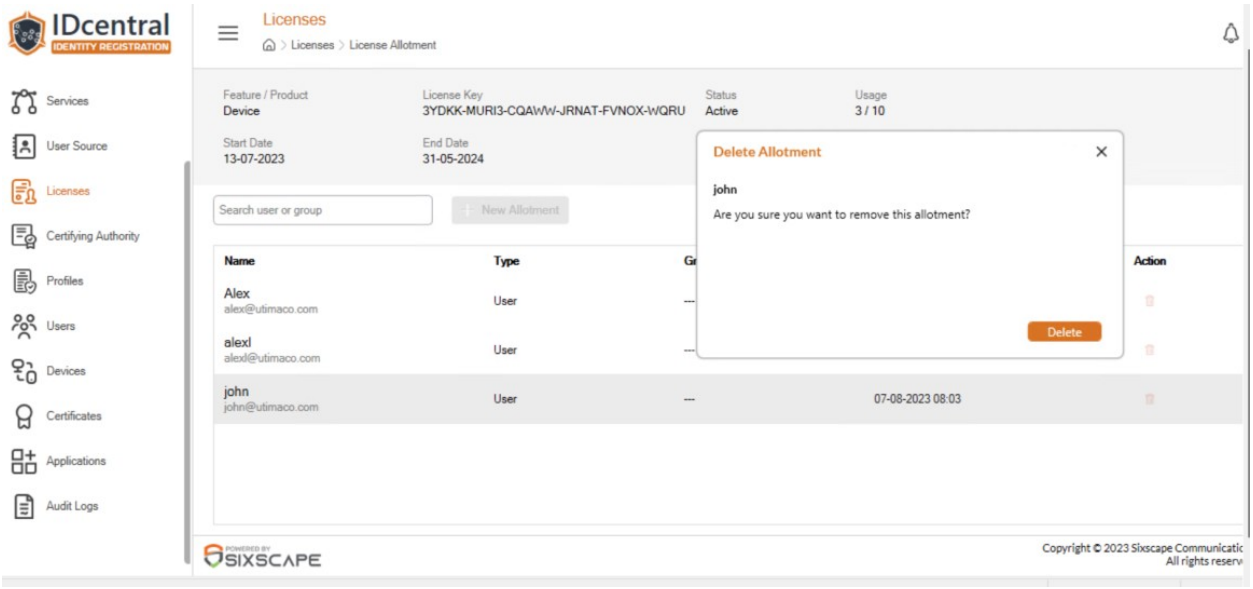


Figure 65 : Delete License Allotment

3. On successful license allotment deletion, the entity information will be removed from the view.

The administrator can have a workflow for approving a device which was self-registered by user prior to device activation by reviewing its properties.

7 Secure Authentication Suite Smartcard Certificate Enrollment

7.1 Secure Authentication Suite Installation

The following section describes the installation of the Secure Authentication Suite application.

1. Log on to the domain joined machine with user which was assigned Hardware Token and Device License.
2. Go to the folder where you have downloaded SAS software.
3. Double-click on the Secure Authentication Suite application installer.

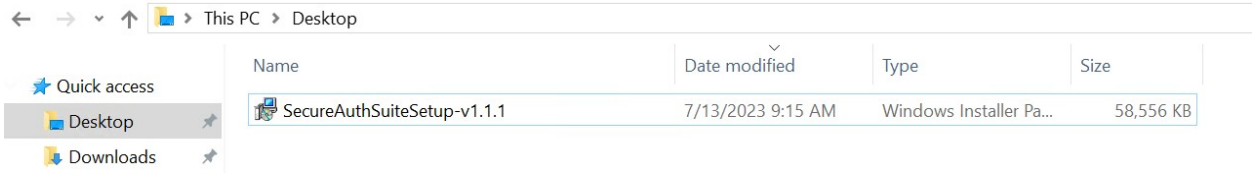


Figure 66 : Secure Authentication Suite software

4. The installer will launch. Click **Next**.

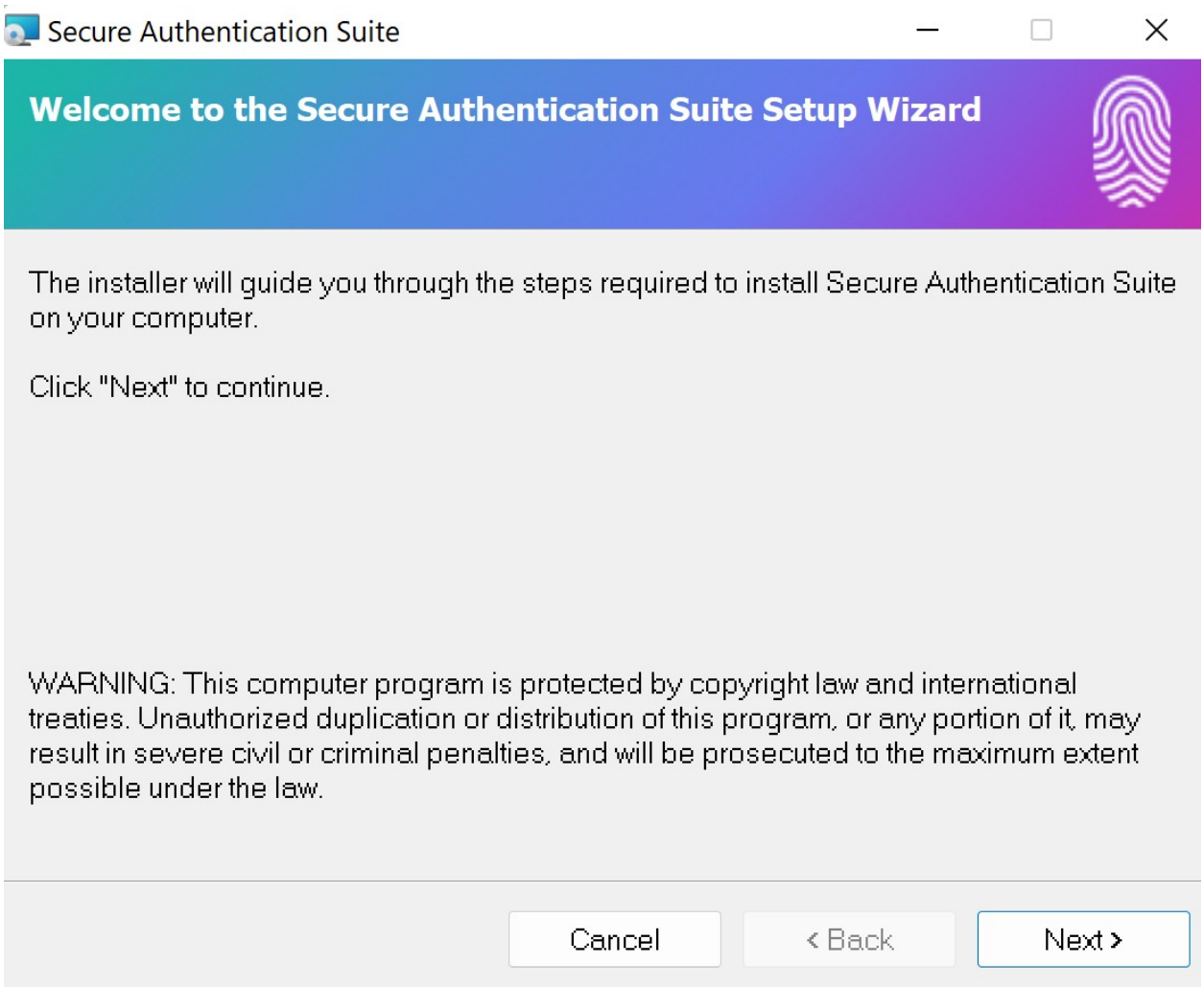


Figure 67 : Installer window

5. Select **Everyone** to install for all users within the same machine. Select **Just me** to install specifically for a single user within the machine. Click **Next.**

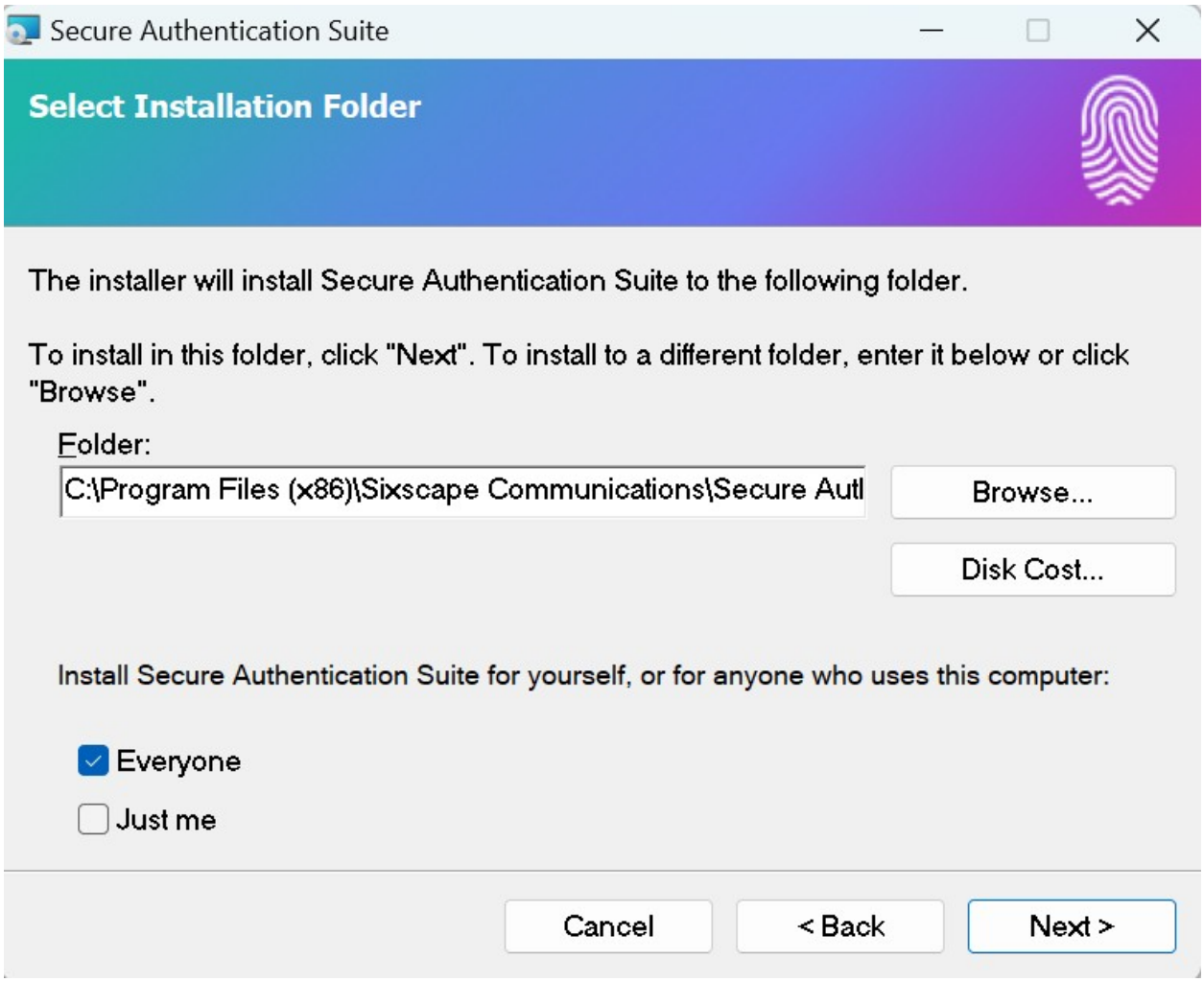


Figure 68 : Select Installation Folder and user

6. To start installation, click **Next.**

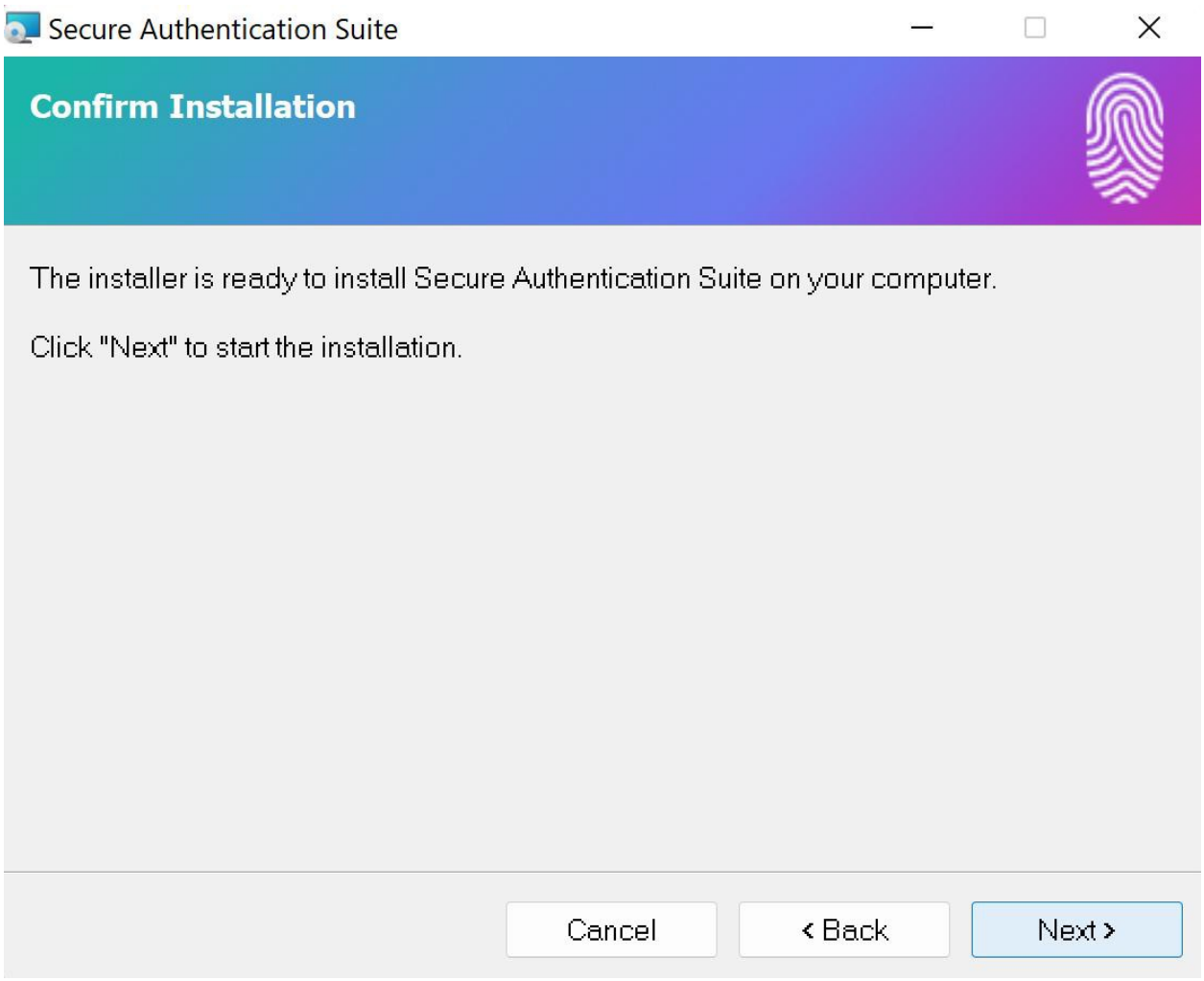


Figure 69 : Confirm Installation

7. Click **Close** after the installation has completed.

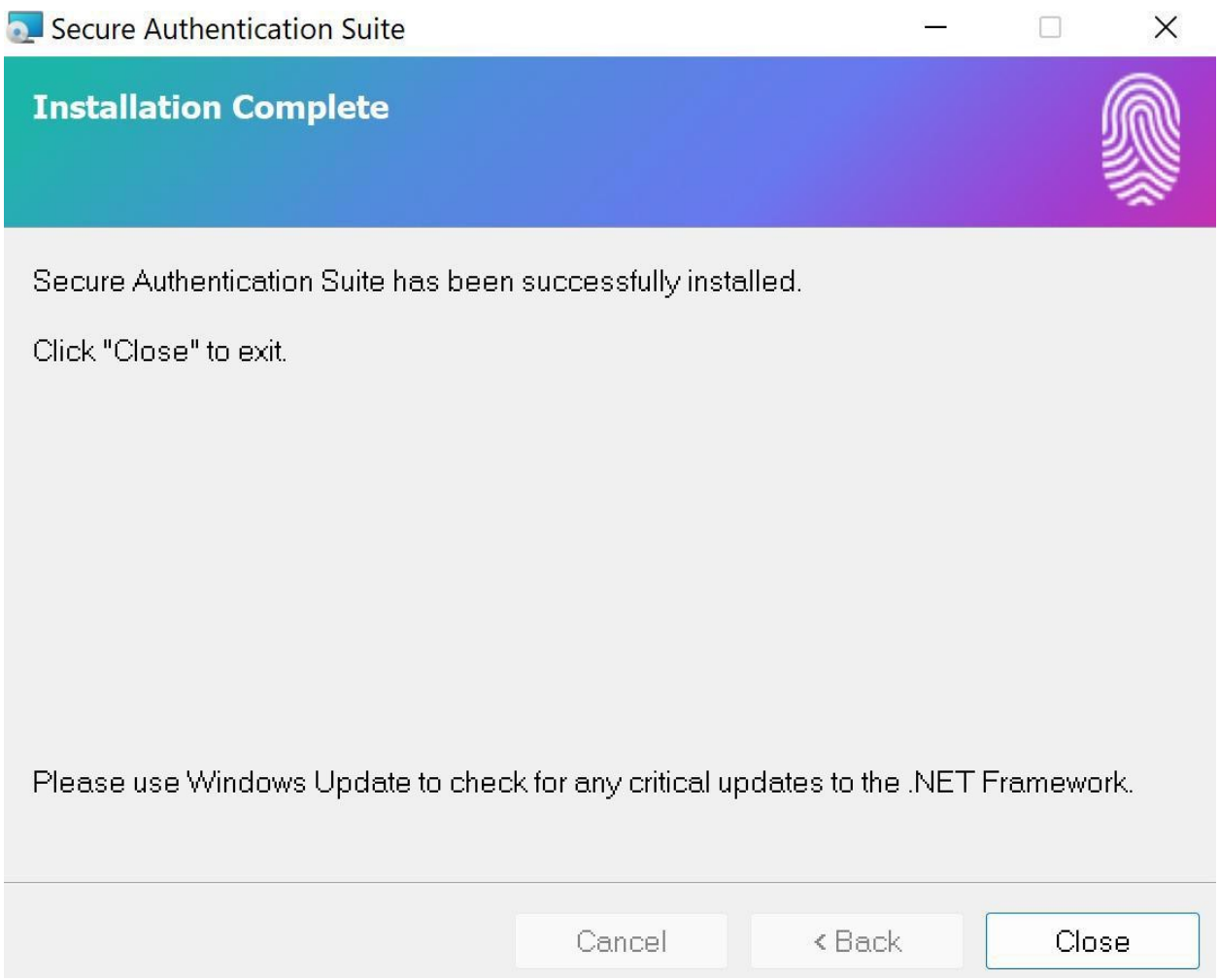


Figure 70 : Installation Complete window

8. Search for **Secure Authentication Suite** in windows search to open the application.

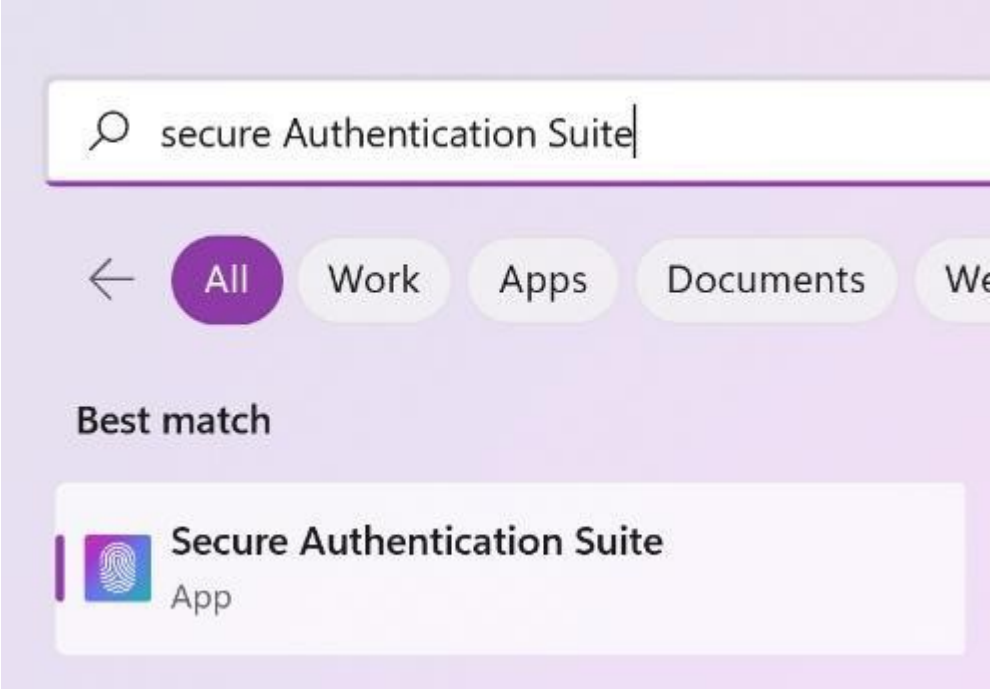


Figure 71 : Starting Secure Authenticate Suite

9. Click on the application name. The application will be launched in windows tray section.

Figure 72 : SAS Initializing window

10. To hide and open the application, use the application's tray icon.

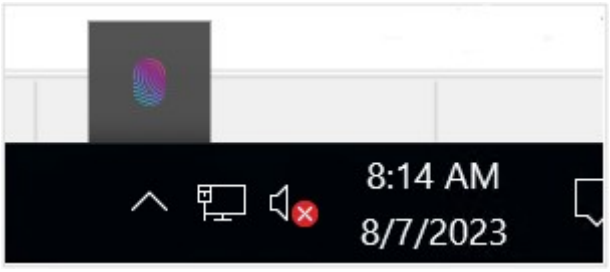


Figure 73 : System tray

7.2 (Optional) Enabling Virtual smart card

In this step, you will create the virtual smart card on the client computer by using the command-line tool, `Tpmvscmgr.exe`. You must have TPM supported machine to enable Virtual Smartcard.

To create the TPM virtual smartcard:

1. On a domain-joined computer, open a Command Prompt window with Administrative credentials.

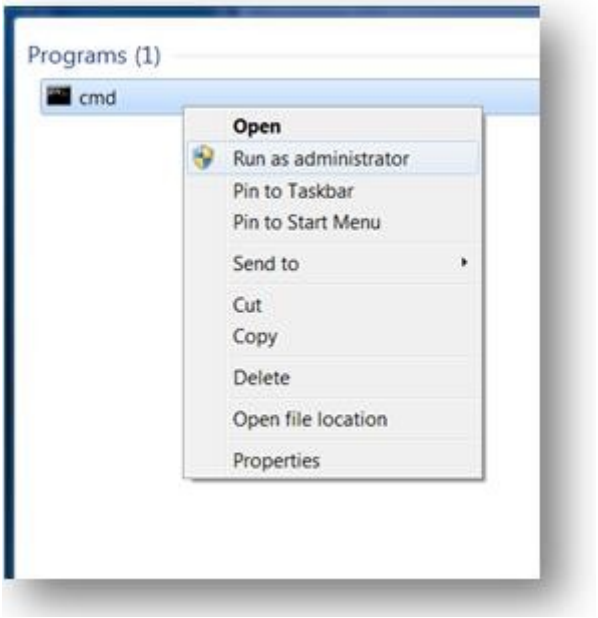


Figure 74 : Open elevated command prompt

2. In the command prompt, type the following command, and then press ENTER.

›_ Console

```
C:\Windows\System32>tpmvscmgr.exe create /name TestVSC /pin default /adminkey
random /generate

Using default PIN: 12345678 Creating TPM Smart Card...

Initializing the Virtual Smart Card component... Creating the Virtual Smart Card
component...

Initializing the Virtual Smart Card Simulator...

Creating the Virtual Smart Card Simulator... Initializing the Virtual Smart Card
Reader...

Creating the Virtual Smart Card Reader...

Waiting for TPM Smart Card Device...

Authenticating to the TPM Smart Card...

Generating filesystem on the TPM Smart Card...

TPM Smart Card created.

Smart Card Reader Device Instance ID = ROOT\SMARTCARDREADER\0000

C:\Windows\System32>
```

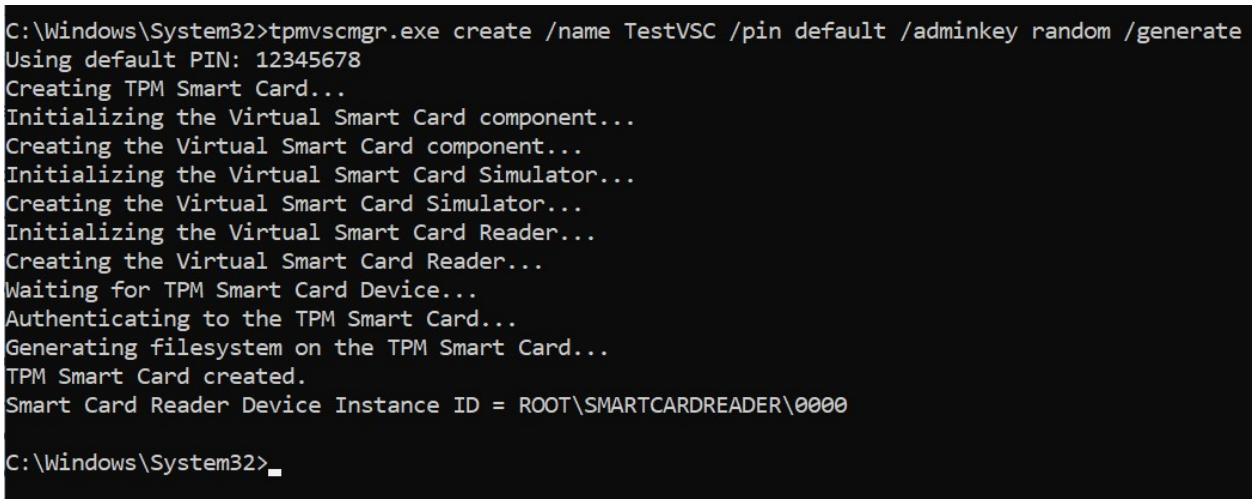


Figure 75 : Virtual smartcard

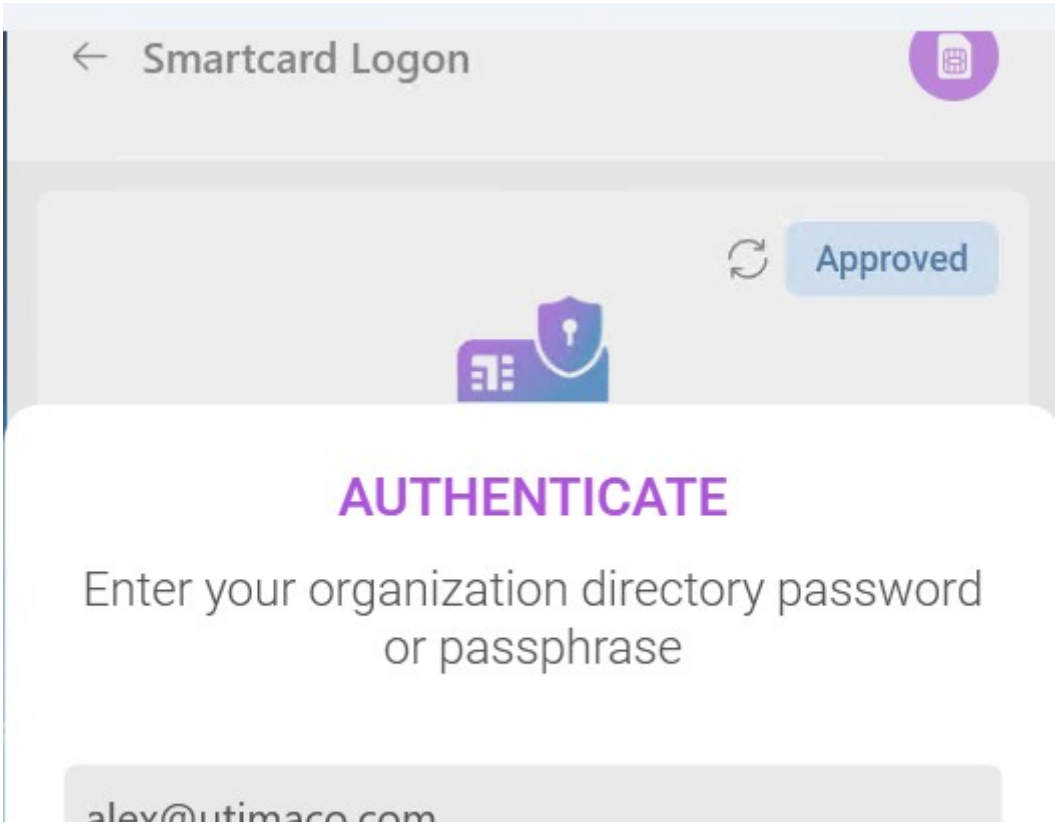
3. This will create a virtual smart card with the name TestVSC and generate the file system on the card. The PIN will be set to the default, 12345678. To be prompted for a PIN, instead of `/pin` default you can type `/pin` prompt.

Wait several seconds for the process to finish. Upon completion, Tpmvscmgr.exe will provide you with the device instance ID for the TPM Virtual Smart Card. Store this ID for later reference because you will need it to manage or remove the virtual smart card.

7.3 Smartcard Certificate Enrollment

This section describes in detail the smartcard certificate enrolment steps using the SAS application. Before starting the device certificate enrolment, confirm whether IRPService is running.

1. From system tray, open the SAS application.
2. Provide the logon device user's email address or user principal name in username textbox. Note that the domain name will be auto filled from the username.
3. Click on **Connect**.



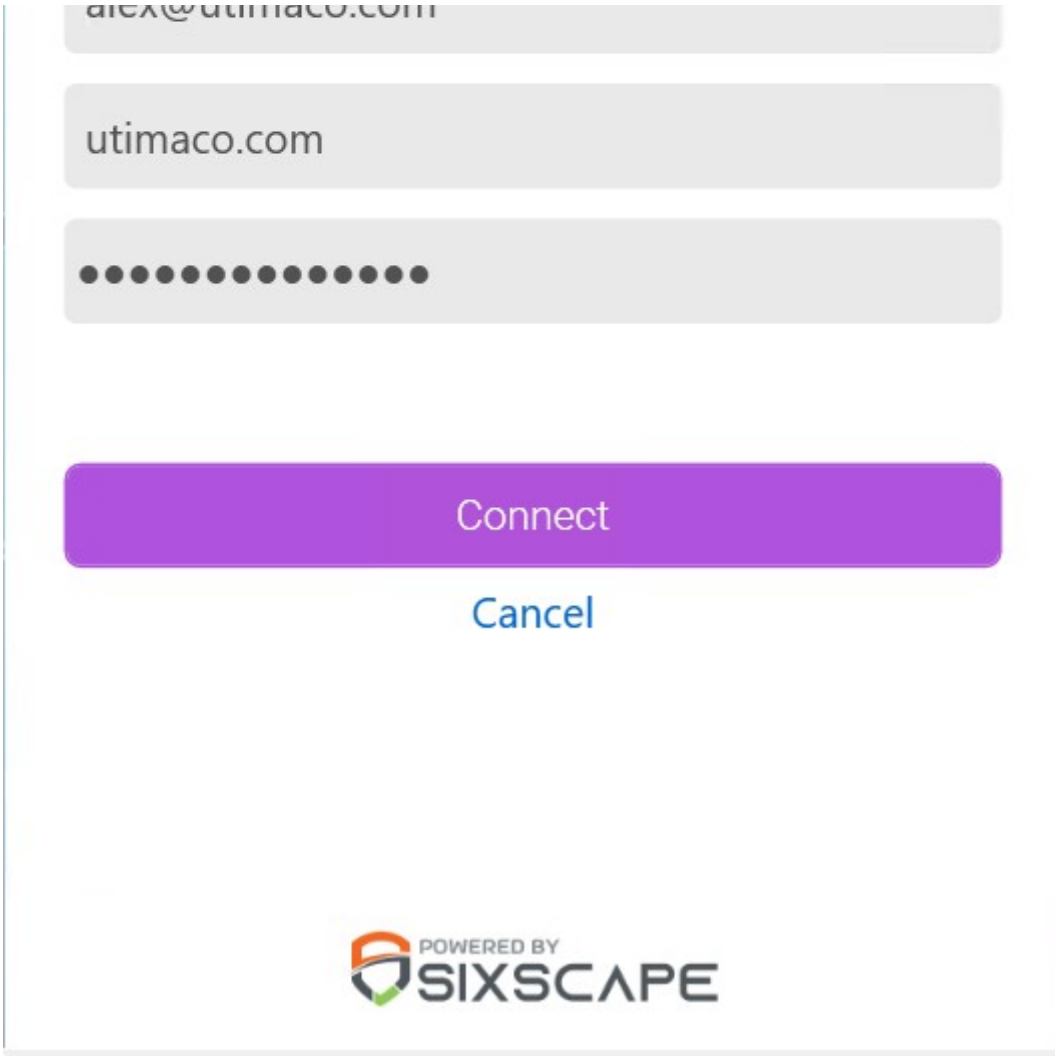


Figure 76 : Authenticate user window

4. While authenticating user credential with IRP service, **Authentication in progress** screen will be displayed.

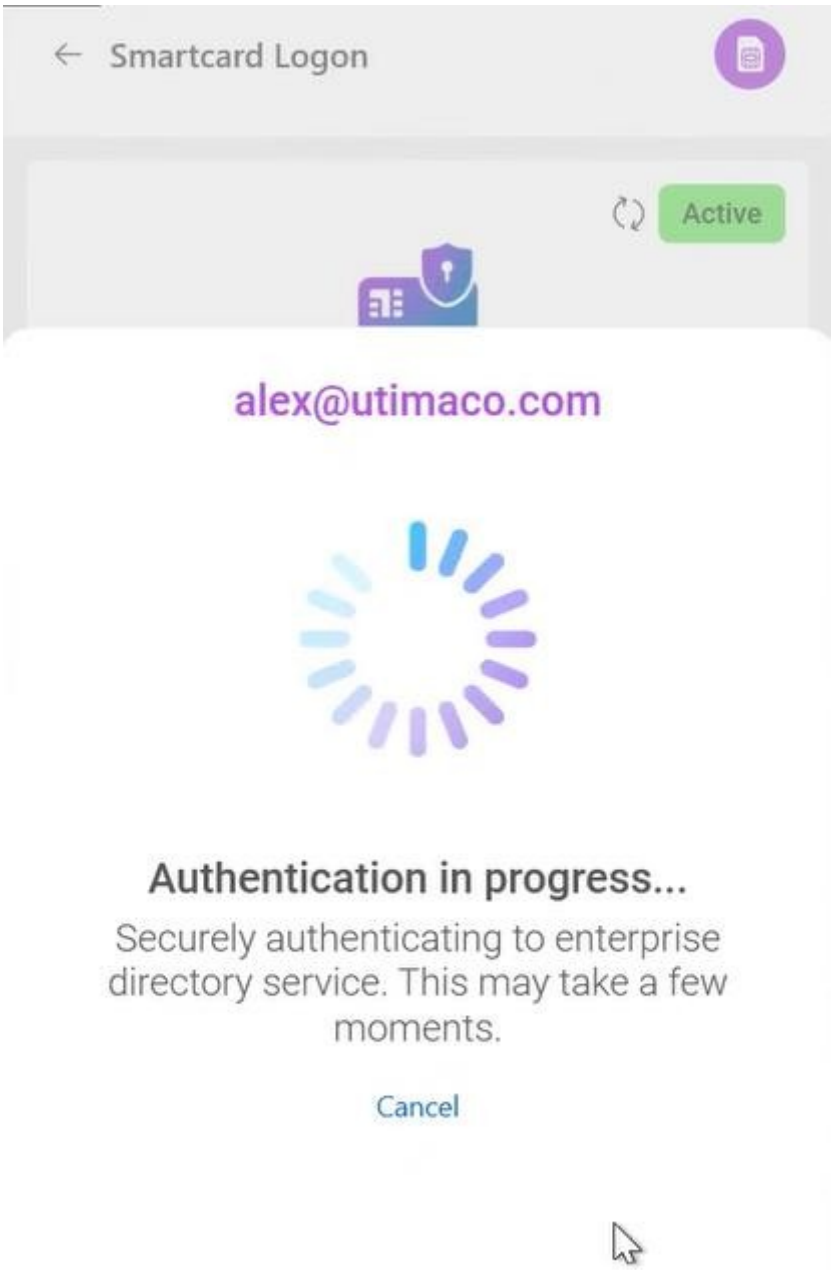


Figure 77 : Authentication in progress window

5. On successful user authentication, a list of products view will be displayed.
6. If device user is allotted with **Hardware Token** license in IDcentral Identity Registration, **Smartcard Logon** will be enabled and in Inactive status. If license is not allotted, then the product status would be Unavailable.

7. Click on **Smartcard Logon** to initiate device registration.

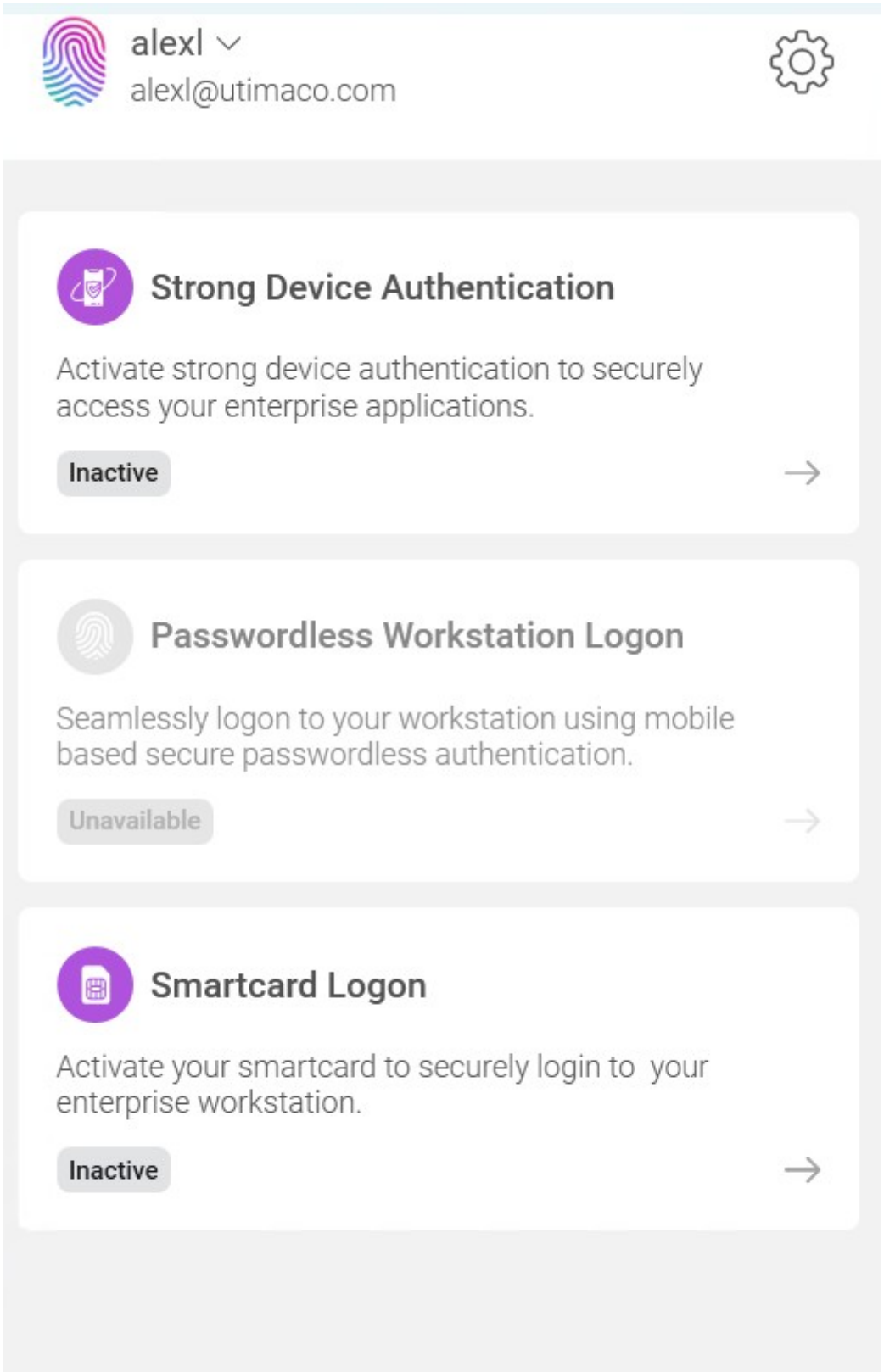


Figure 78 : Smartcard Logon activation

8. **Begin Registration** view will be displayed. Click on **Begin.**

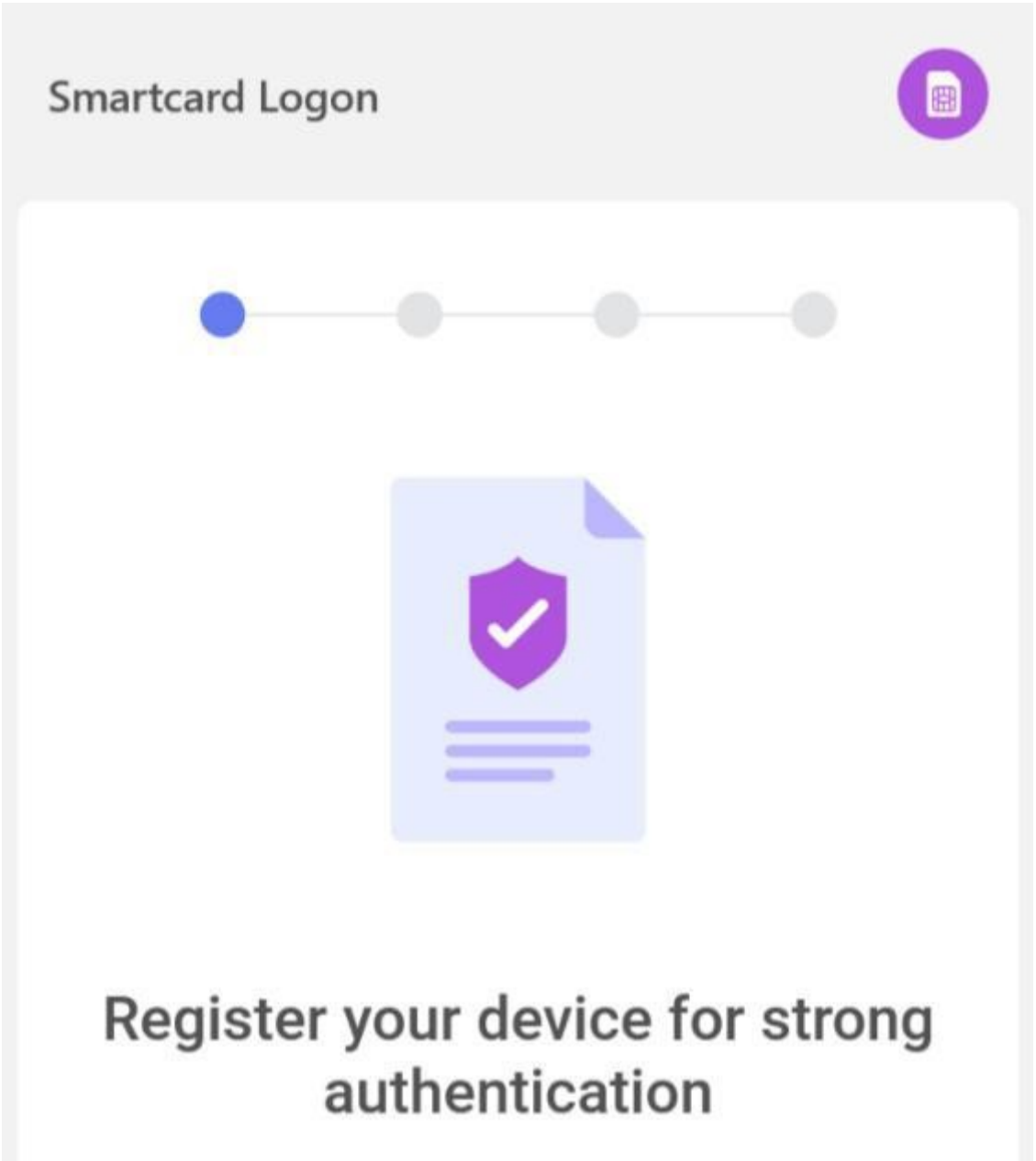


Figure 79 : Registration window

9. If smartcard is not connected to the window's device, **Windows Security** dialog will be prompted to connect the necessary smartcard.
10. Now plug in your smartcard. Smartcard name will be displayed on the screen.

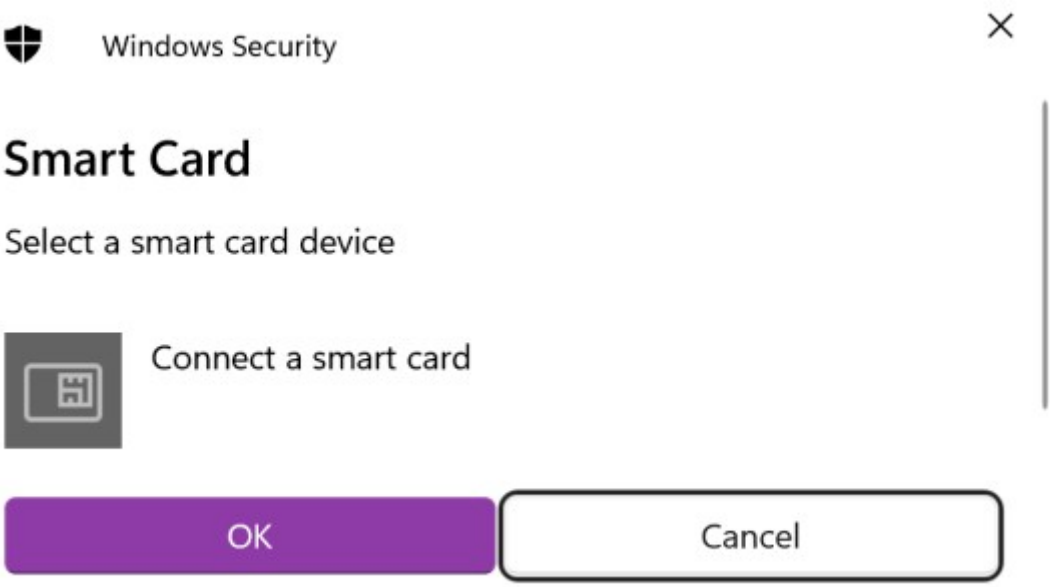
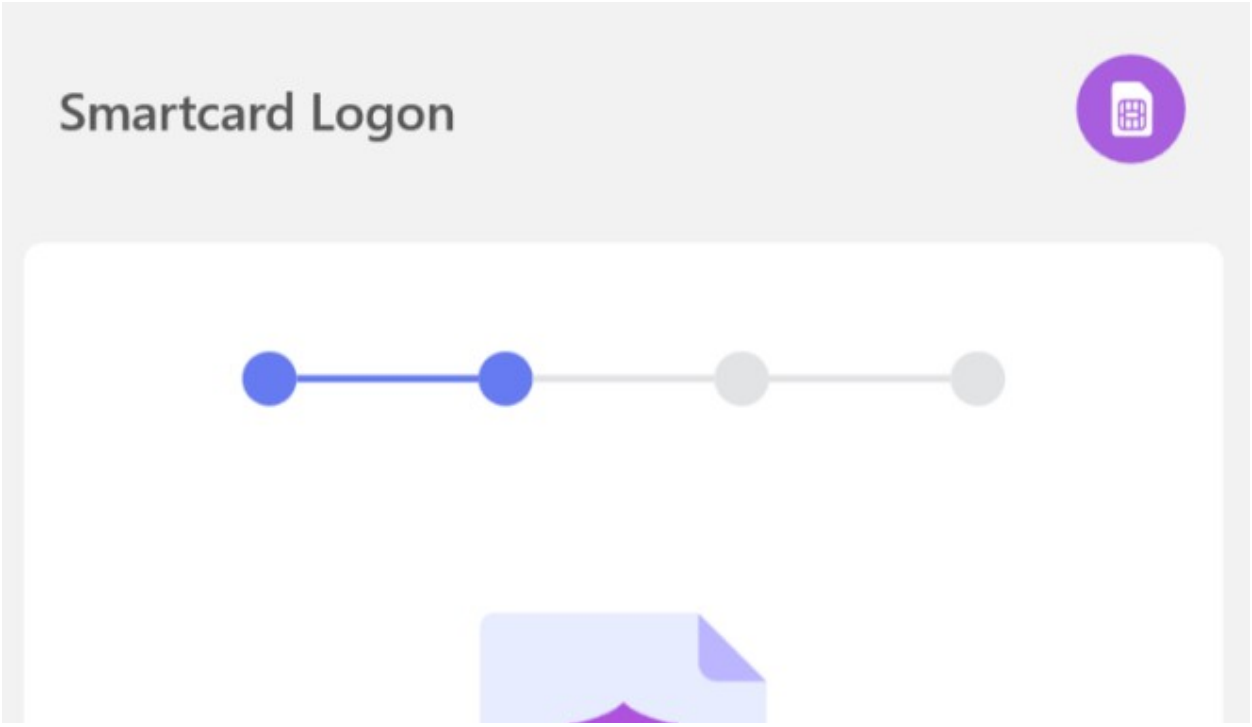


Figure 80 : Smart Card plugin window

11. Click **OK** to proceed with device registration.
12. Now the application fetches smartcard device properties and registers the device to IDcentral Identity Registration.
13. On successful registration, **Awaiting for approval** view will be displayed.



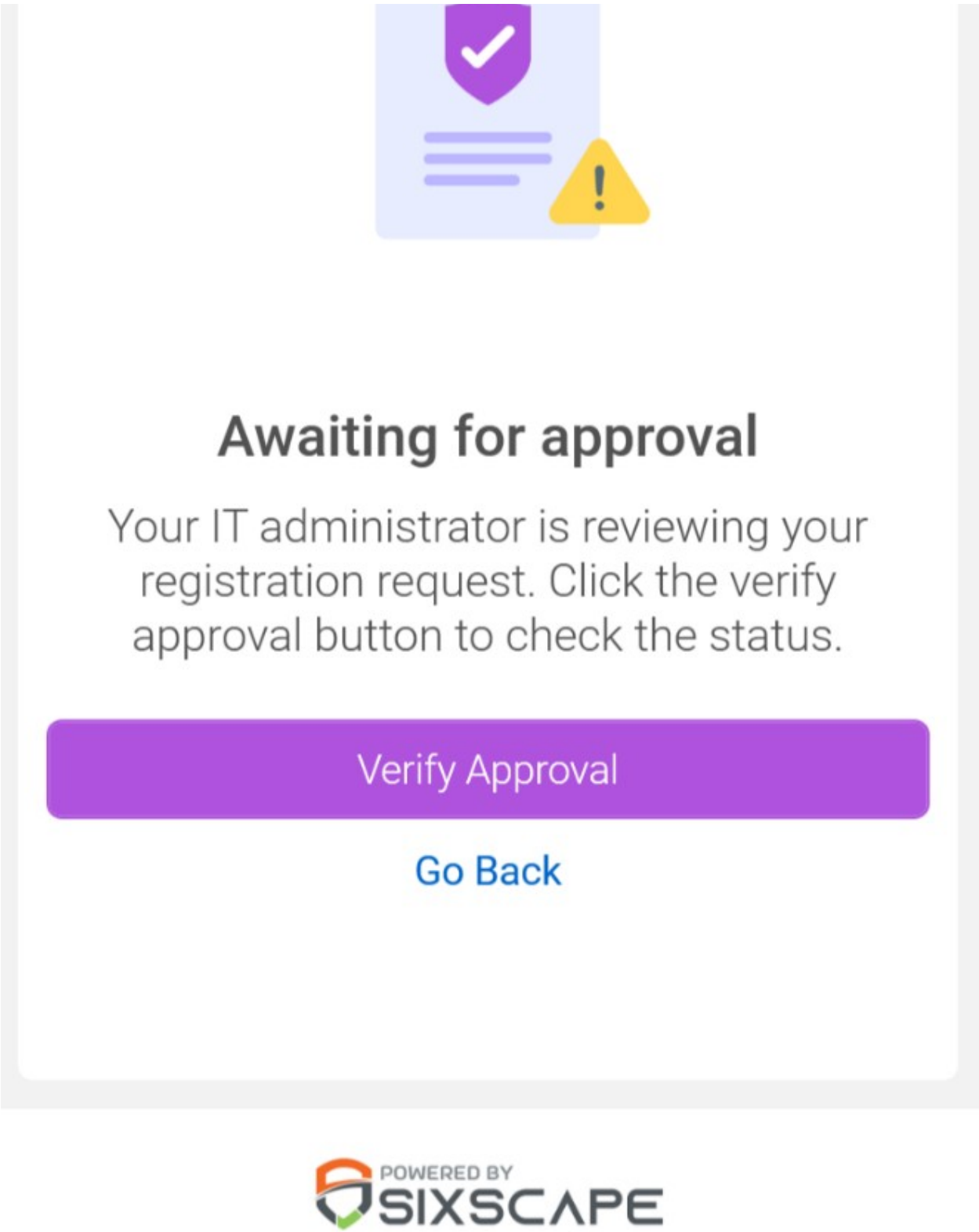


Figure 81 : Verify approval window

14. Go to the IDcentral machine. The administrator can view the device's properties and choose to approve the device from IDcentral Identity Registration Devices view.
15. Go Back to SAS application. Click on **Verify Approval**. If smartcard device is approved by the IDcentral administrator, device activation process will be initiated. If it is not, **Device** detail's view will be navigated to view the current device status. To check on device status updates, click on **sync** button on the top right corner of the view.
16. While activating the smartcard device, Windows prompts to enter smartcard PIN to provision certificate within the smartcard. Enter the smartcard PIN in the dialog and click **OK.**

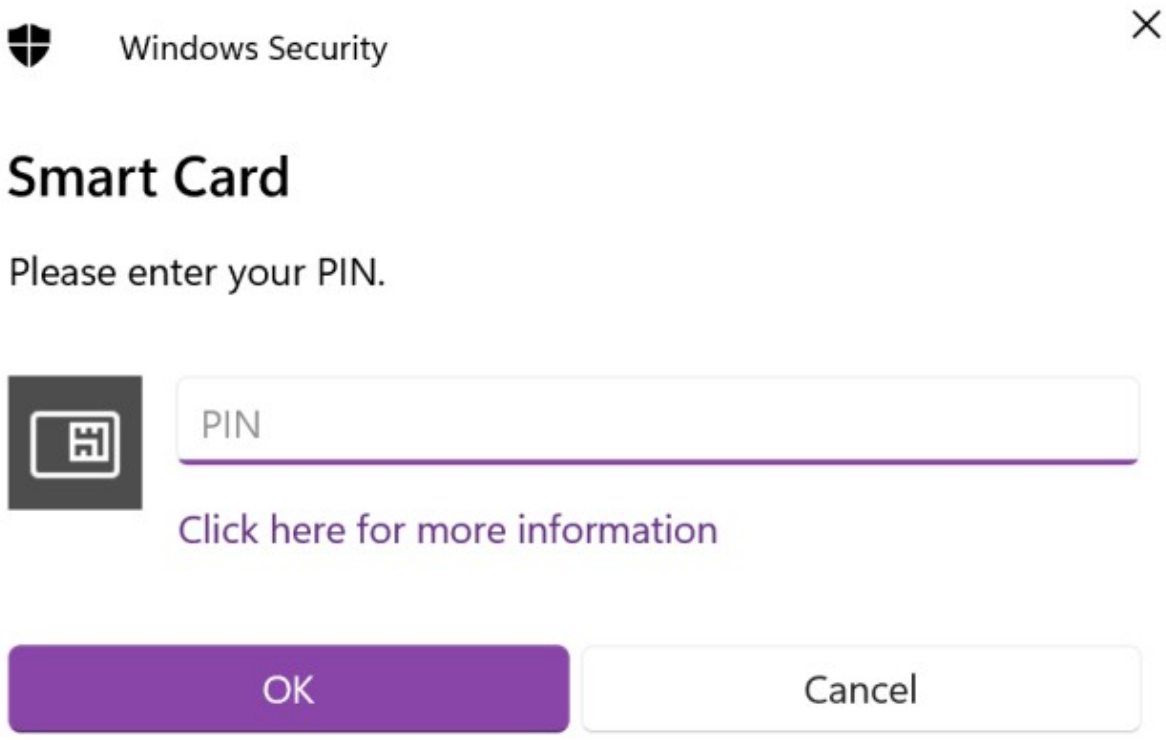


Figure 82 : Smartcard PIN prompt

17. On successful smartcard certificate provision, success completion screen will be displayed. Click **OK.**
18. In device detail's view, the smartcard device now will be in **Active** status.

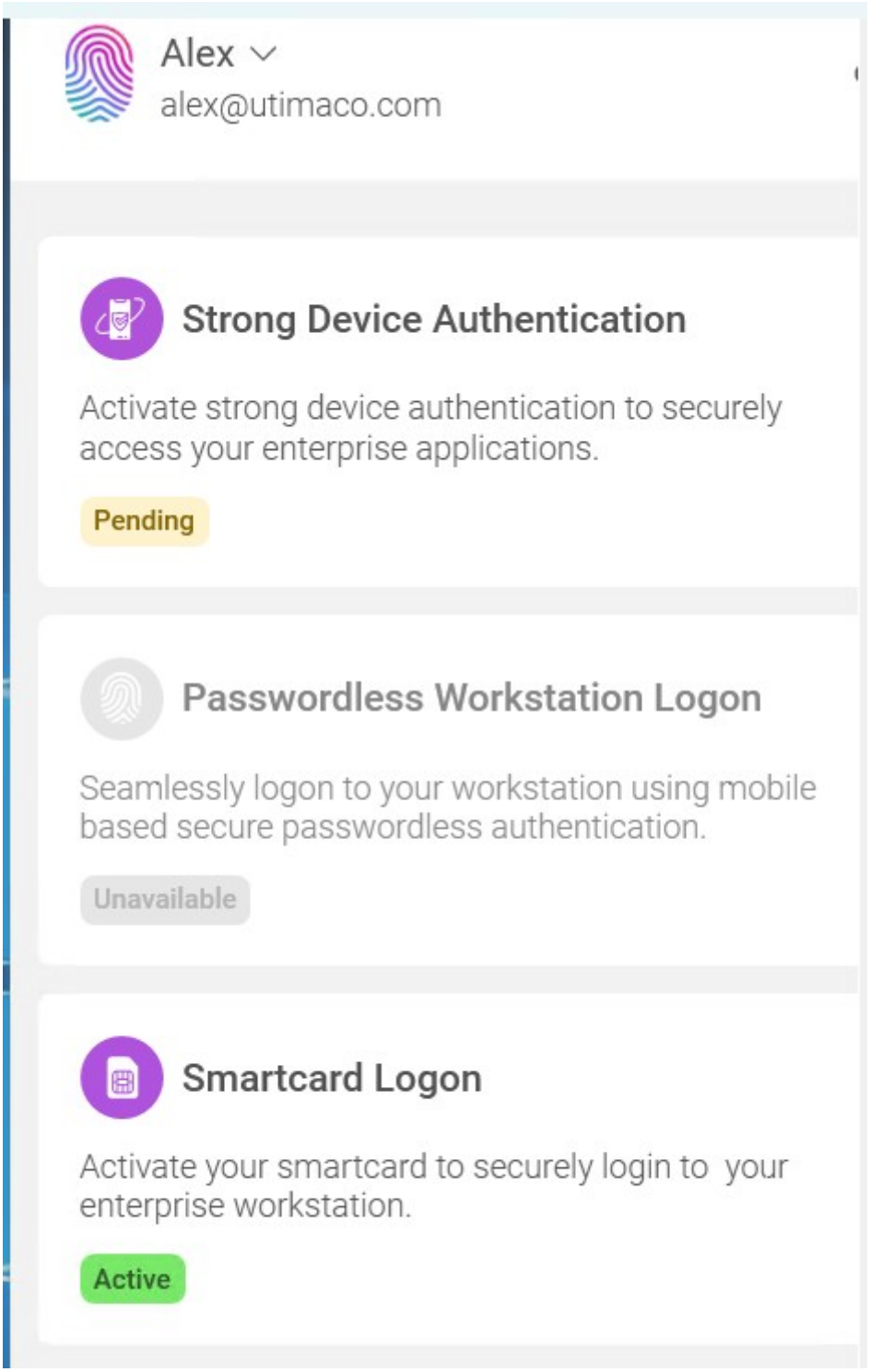


Figure 83 : Verifying active status for Smartcard Logon

19. Click on **Certificates** to view device certificate information.

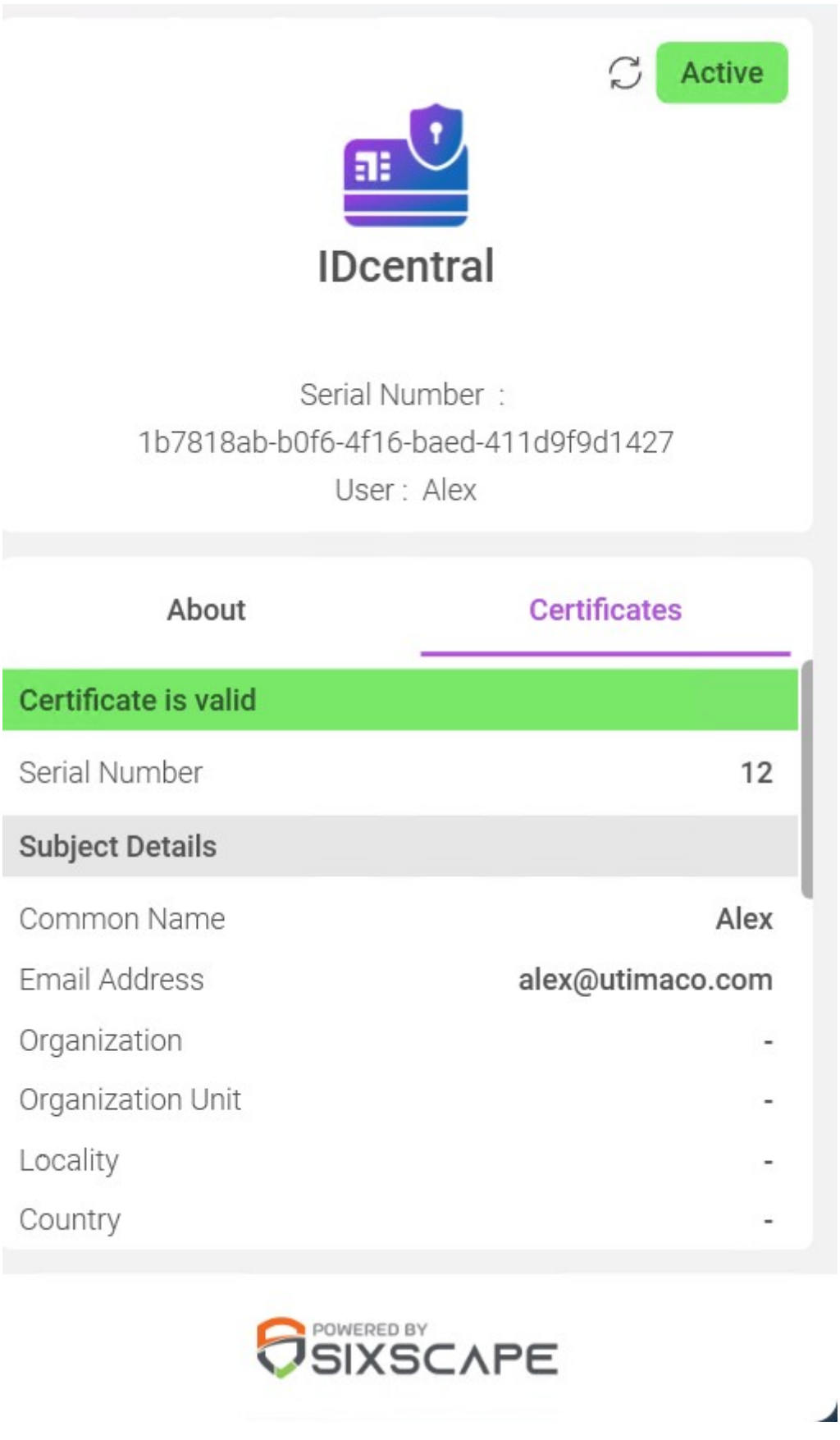

Active
IDcentral
Serial Number :
1b7818ab-b0f6-4f16-baed-411d9f9d1427
User : Alex
About
Certificates
Certificate is valid
Serial Number
12
Subject Details
Common Name
Alex
Email Address
alex@utimaco.com
Organization
-
Organization Unit
-
Locality
-
Country
-
POWERED BY
SIXSCAPE

Figure 84 : Viewing certificate information

7.4 Verify Smartcard Certificate from CMS Web

1. Log in into Certificate Management System as tenant administrator.
2. Click on the **Certificates** tab from CMS and verify the newly generated certificates gets listed with certificate type ScardUPN.

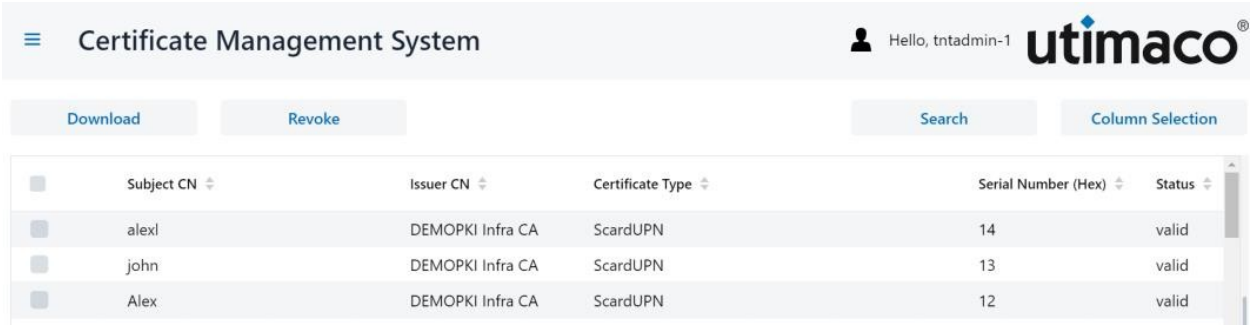


Figure 85 : Verifying smartcard certificate in CMS

This completes the integration of IDcentral with Utimaco u.trust Identify.

8 Troubleshooting

Error	Diagnosis
uti-demopki-cms-service | 2023-07-19T12:25:07.271974301Z 2023-0719T14:25:07,271 | INFO | de.exceet.cms.server.cmp.CmpServlet:661 | CMP: Error occurred: signature is not valid	ca-list -v DEMOPKI-INFRA-CA 1. ca-update -signerConf 'device-name?hsmsimulator%algo?SHA256withECDSA%slot?1%hcfctx-id?hcf-session-ctx%key-label?DEMOPKIINFRA-CA' -name DEMOPKI-INFRA-CA 2. ca:ca-restart 3. ca-list -v DEMOPKI-INFRA-CA

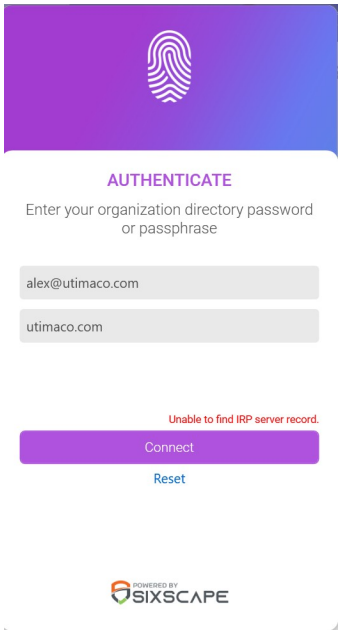
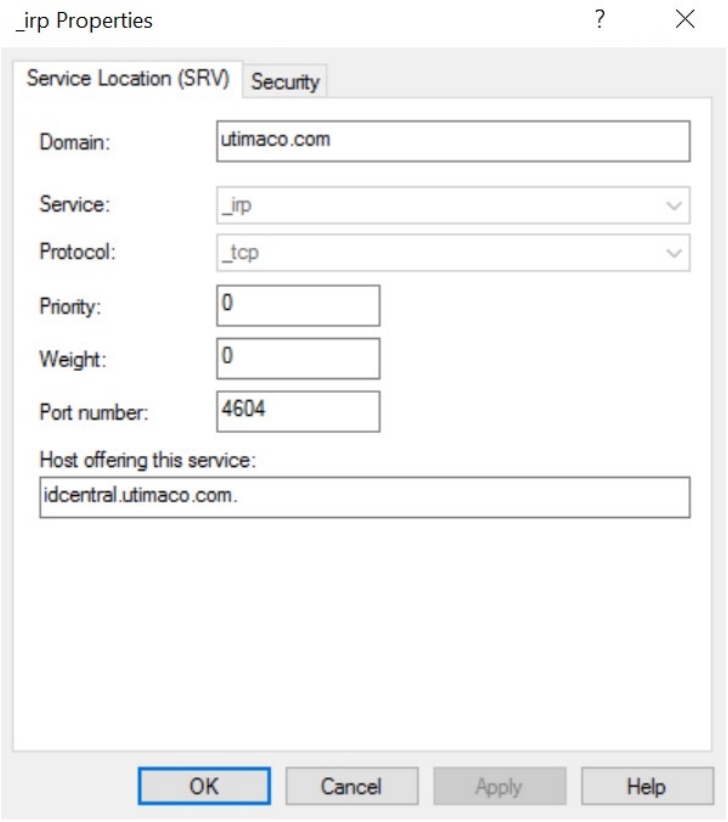
Error	Diagnosis
Unable to find IRP Server record in SAS 	Add DNS SRV Record to DNS pointing to IDcentral Service. E.g. _irp._tcp.utimaco.com TTL IN SRV 10 20 4604 irp.utimaco.com.  Verify with nslookup. 

Table 7: List of errors and their diagnoses

9 Further Information

This document forms a part of the information and support which is provided by Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All u.trust Identify product documentation is also available at the Utimaco IS GmbH website: *https://utimaco.com/*.

10 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.