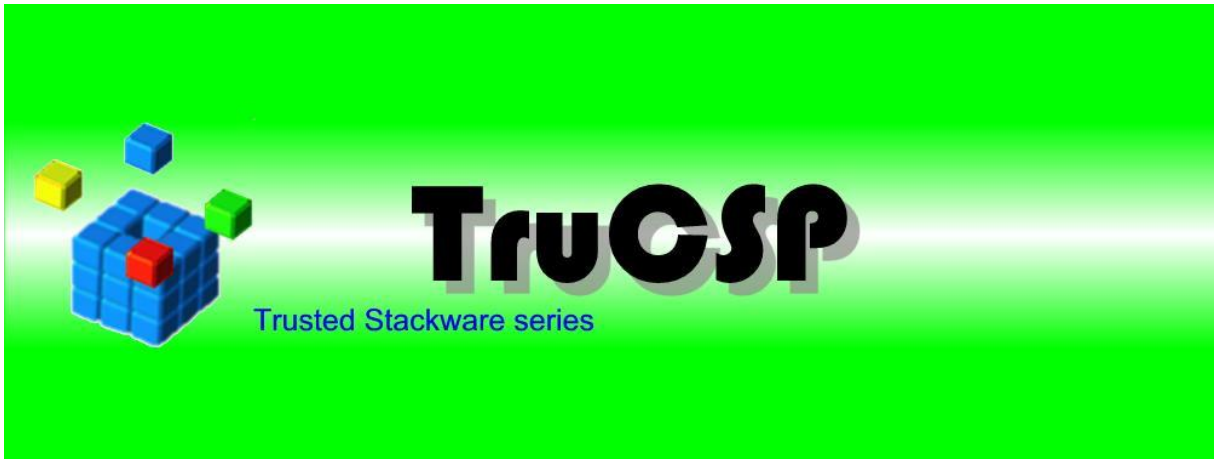
TruCSP

Windows Cryptographic Provider with TruGate Authentication

User's Guide

Rev. 1.0.4



D.O.I-Net Co., Ltd.

Disclaimers

1. D.O.I-Net Co., Ltd. shall not take responsibility for any direct and indirect damage caused by the descriptions stated in this document or other injustices.
2. It is not intended to consent to any rights including the patent rights of any third party or our company with this document.
3. It is prohibited to reprint or reproduce some or all parts of this document without permission.
4. D.O.I-Net Co., Ltd. may change the specifications listed in this document without a notice for the purpose of improvement.

When you export these products, please follow the necessary procedures by confirming the foreign exchange, foreign trade methods, and regulations such as the U.S. export control laws.

Revision History

Rev.	Date	Details
1.0.0	2012/04/17	Issued.
1.0.1	2013/05/09	Added Windows 8, Windows Server 2012 to Supported OSs. Changed Trial Period.
1.0.2	2014/12/04	Modified descriptions of Supported OSs.
1.0.3	2015/07/21	Added Windows 10 to Supported OSs.
1.0.4	2023/10/27	Changed Supported OSs.

Index

Figure Index

1. Introduction

This User's Guide explains the operation of TruCSP produced by D.O.I-Net Co., Ltd. (D.O.I-Net).

2. Operating Conditions

a. Supported OSs

Windows 10 32bit/64bit
Windows 11
Windows Server 2016
Windows Server 2019

b. Supported Authentication Framework

TruGate ver.5.0.10 or above

c. Applicable Authentication Devices

Depends on TruGate. For details, please refer to the TruGate User's Guide.

d. Necessary Device Plug-ins

Depends on TruGate. For details, please refer to the TruGate User's Guide.

e. Installation Requirements

TruGate must be installed.

f. Operational Requirements

TruGate must be installed and initially configured so that it can be used for authentication. "Enabling TruStack Gina" is optional, but be sure to register the template for the authentication device you will be using. For details, please refer to the TruGate User's Guide.

3. Product Summary

a. Contents of Product

TruCSP consists of two modules: a certificate storage provider, TruStack Certificate Store Provider (hereinafter referred to as TSCert), and a cryptographic service provider, TruStack Cryptographic Service Provider (hereinafter referred to as TSCSP).

TSCert extends the certificate storage function provided by Microsoft CryptoAPI, and

works in conjunction with TruGate, an authentication framework product provided by D.O.I-Net, to add authentication functionality to access certificates.

TSCSP is equipped with an API that is compliant with Microsoft CryptoSPI (System Program Interface) and provides cryptographic services that comply with Microsoft CSP standards. Like TSCert, TSCSP works in conjunction with TruGate, an authentication framework product provided by D.O.I-Net, and is publicly available. This adds an authentication function to access the private key pair storage location.

Note: TSCert and TSCSP use TruGate as an authentication framework. Please prepare TruGate separately for use.

b. Package

2 types of installer packages are prepared; one for PCs with a single license edition, and another for PCs with a volume license edition.

i. Single License Edition

This is a package mainly for personal users. It comes with the exe installer package. The trial period is 1 month. No restrictions are set during the trial period.

ii. Volume License Edition

This is a package mainly for corporate users. It comes with the msi installer package. You cannot uninstall it from "Apps and Features" of the OS installed on the PC. Uninstall it from “Active Directory server” or “re-launched msi installer”. Either 32bit version or 64bit version is available. The trial period is 3 months. No restrictions are set during the trial period.

4. Restrictions and Warnings

1. The maximum size of a certificate that TSCert can store is just under 2KB after encoding.
2. TSCert cannot store multiple certificates. Only new writing or rewriting of a single certificate is possible.
3. In TSCert, certificate revocation lists and certificate trust lists cannot be stored in the TSCert vault.
4. When importing an existing certificate to the TSCert store using the OS's "Certificate Import Wizard", select "Automatically select certificate store based on certificate type".
5. In TSCSP, the maximum length of public keys that can be stored is up to 1024 bits.
6. TSCSP does not allow storing multiple key pairs. Only a single key pair can be written to or deleted.

5. Installation and Uninstallation Procedure

Note: Please check the Installation Requirements before installing TruCSP. In installing and uninstalling, please log on with the administrator privilege of the local computer.

a. Installation

A dialog box shown below appears when you execute TruCSP Trusted Stackware Crypto Service Provider.exe. Click the "Next" button.

Figure 1 Setup Wizard Welcome Dialog Box

Read "SOFTWARE LICENSE AGREEMENT" shown in the dialog box carefully, and click the "I accept the terms in the license agreement" radio button if you agree, then click the "Next" button.

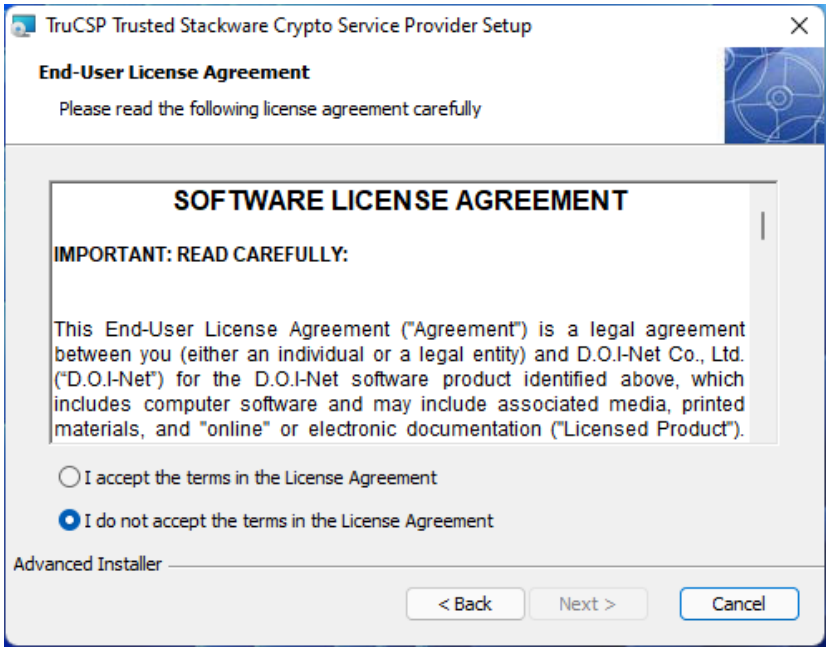


Figure 2 SOFTWARE LICENSE AGREEMENT

When the Setup Type dialog box is displayed, select the setup type according to your usage environment.

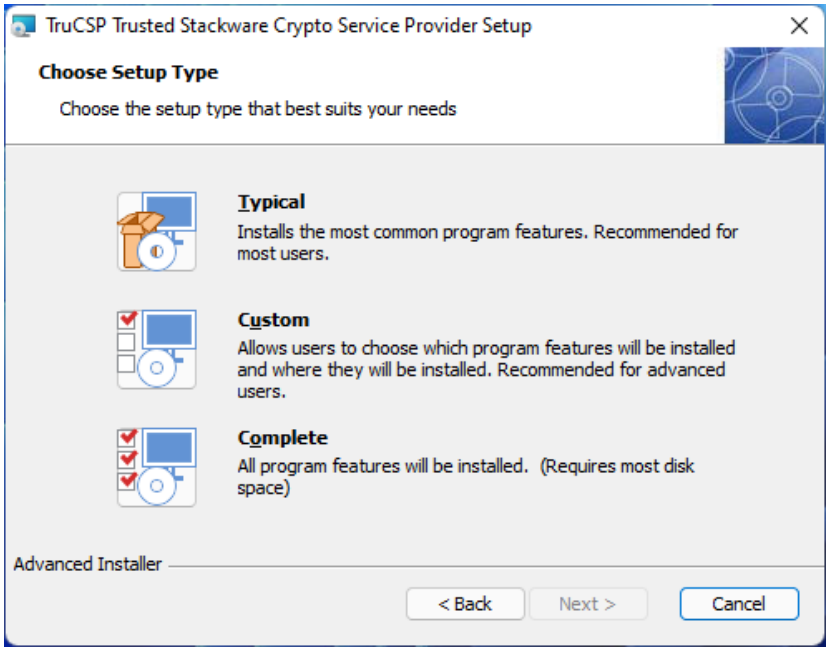


Figure 3 Setup Type Selection Dialog Box

Click the "Install" button unless you need to change. If you need to make some changes, click the "Back" button and return to the dialog box where you want to make changes.

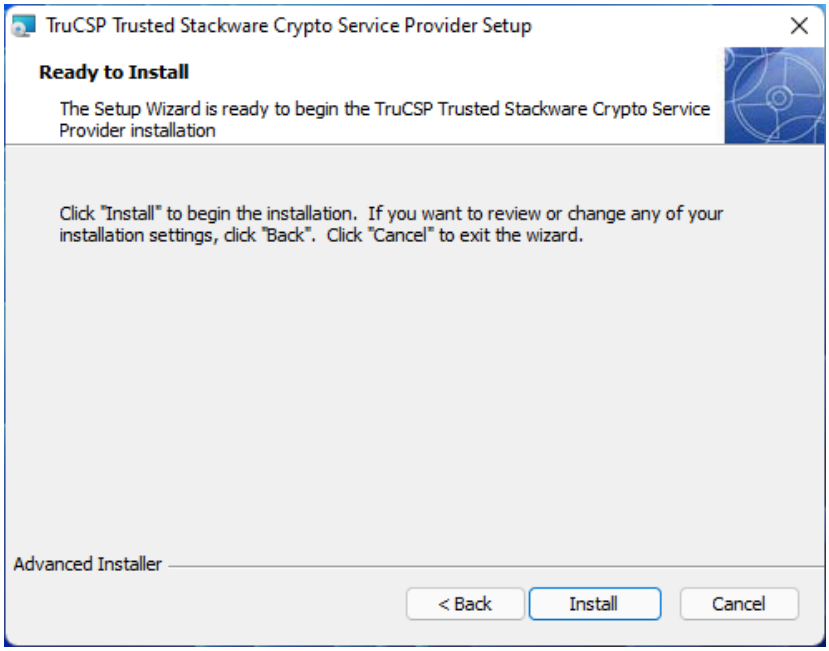


Figure 4 Ready to Install Dialog Box

During installation, the following indicator dialog box will be displayed.

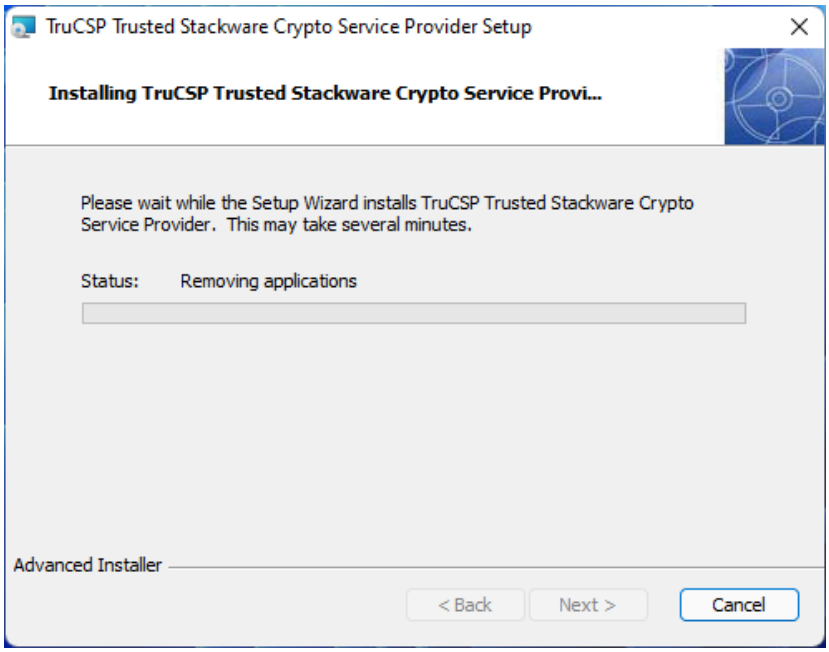


Figure 5 Installation Indicator Dialog Box

When installation is finished, the following installation completion dialog will be displayed. Click the "Finish" button.

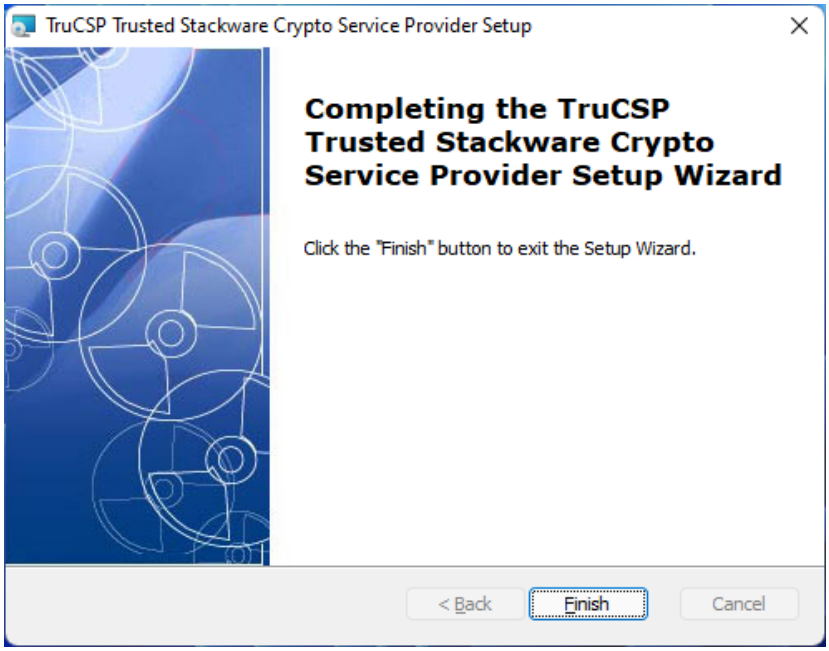


Figure 6 Installation Complete Dialog Box

b. Uninstallation

Select “TruCSP Trusted Stackware Crypto Service Provider” from "Apps and Features" of the OS.

The following is an operation example with Windows 11.

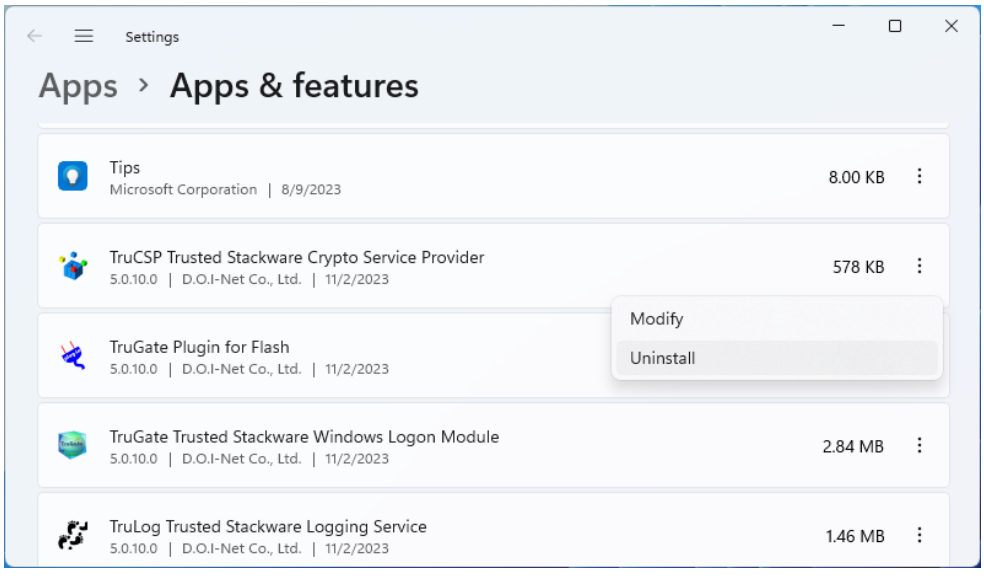


Figure 7 Apps and Features Dialog Box

Then click “Uninstall”, and uninstall TruCSP following the message.

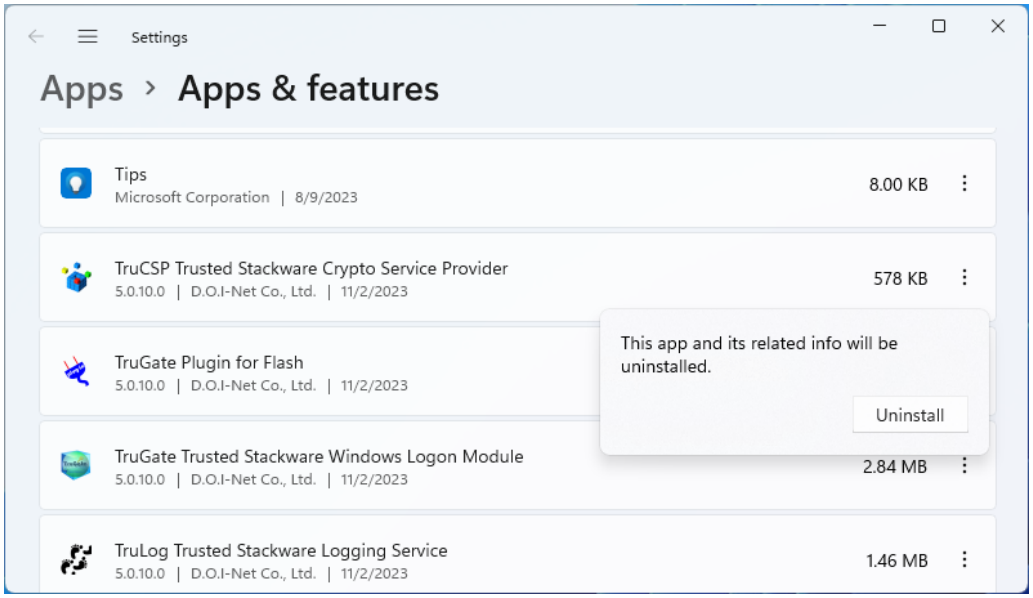


Figure 8 Confirmation of Program Uninstallation Dialog Box

During uninstallation, the following indicator dialog box will be displayed.

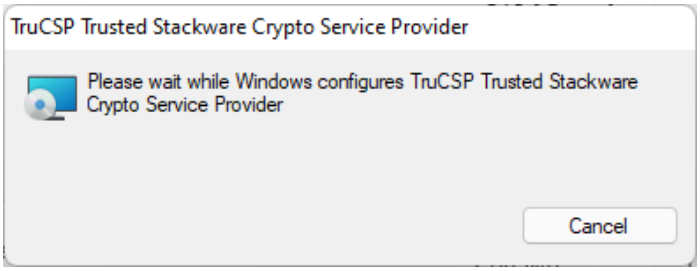


Figure 9 Uninstall Indicator Dialog Box

When uninstallation is completed, the indicator dialog box will disappear.

6. Operation

a. License Verification

The following popup message will be displayed during the trial period. If the message is shown, click the “OK” button.

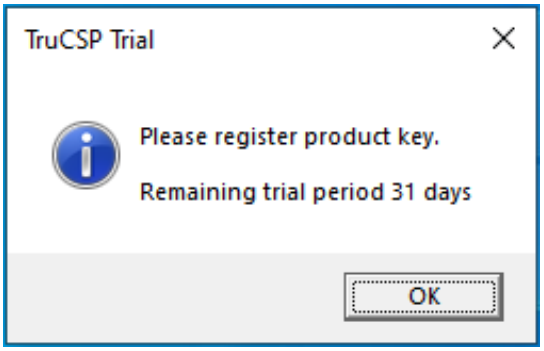


Figure 10 Trial Period Message

Note: Trial period is 1 moth for the single license edition, and 3 months for the volume license edition. You cannot use TruCSP after the trial period expires. Please register the product key to use TruCSP continuously.

When the trial period is over, the dialog box as follows will be displayed. To keep using it, enter the product key in the edit box, then click the “OK” button. To terminate the trial, click the “Cancel” button, and uninstall TruCSP.

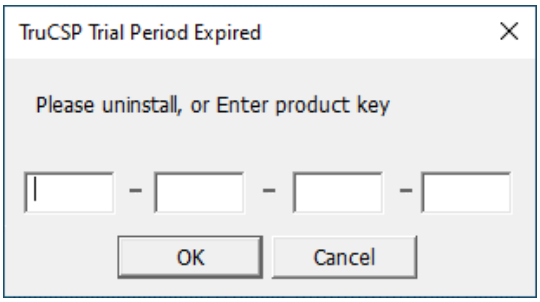


Figure 11 Trial Period Expired Warning Message

b. How to confirm the registration status of TruCSP Certificate Store Collection

1. After installing TruCSP, reboot the system and log on to TruGate, or enable TruStack Gina if you have not enabled it.
2. Start MMC, open the certificate console file you created, and start the certificate console.

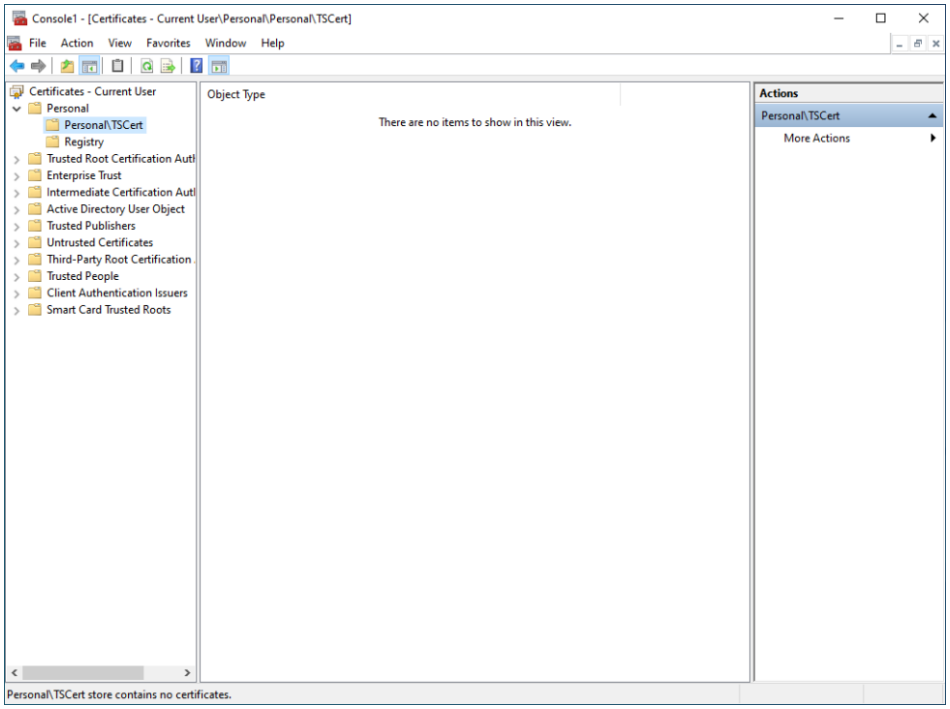


Figure 12 Launch Certificate Console

If you have not yet created a certificate console, follow the steps below to create one.

(a) Right-click "Start" and then click "Run".

(b) When the "Run" dialog box appears, enter mmc and click the "OK" button.

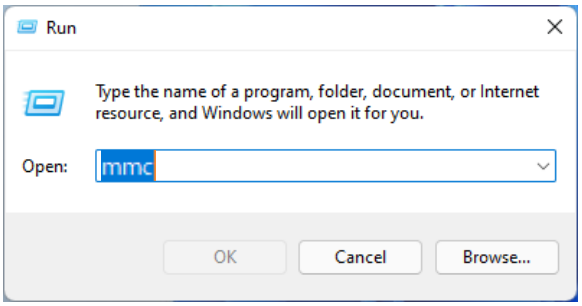


Figure 13 Run mmc

(c) A console screen will be displayed.

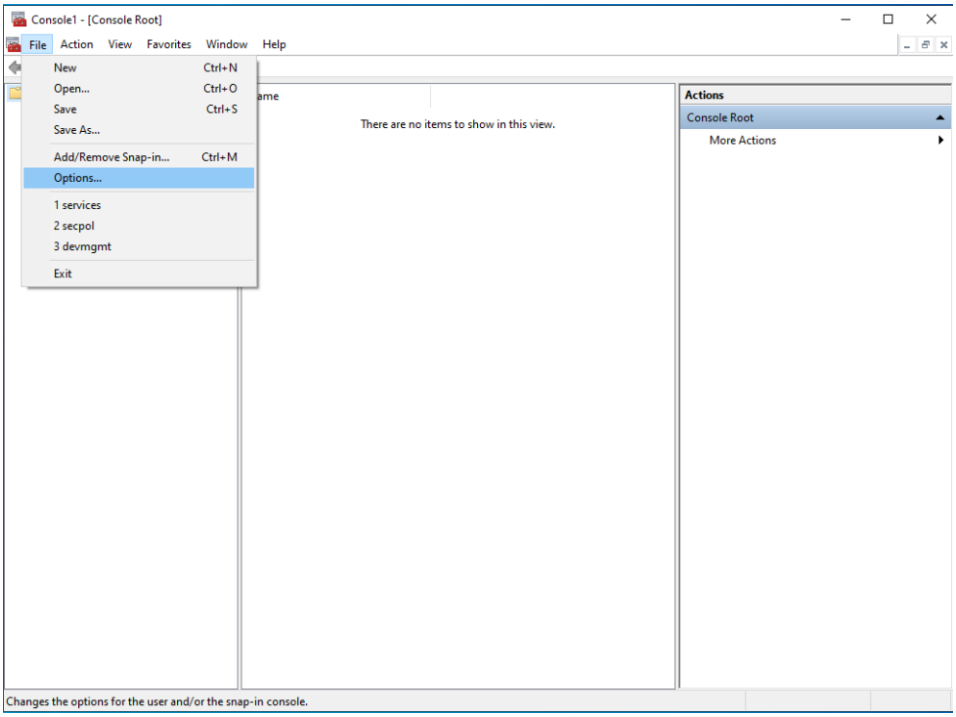


Figure 14 Launch MMC

(d) From the console screen, select “File” – “Add/Remove Snap-in...”.

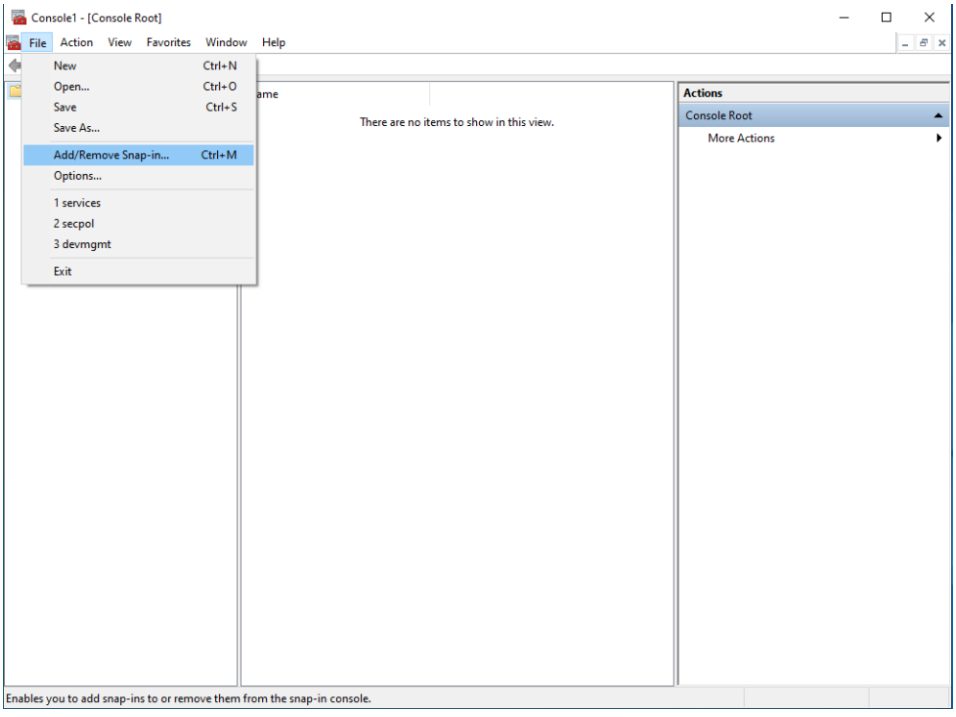


Figure 15 Select Add or Remove Snap-ins

(e) When the Add or Remove Snap-ins screen appears, select "Certificates" from the available snap-ins and click the "Add" button.

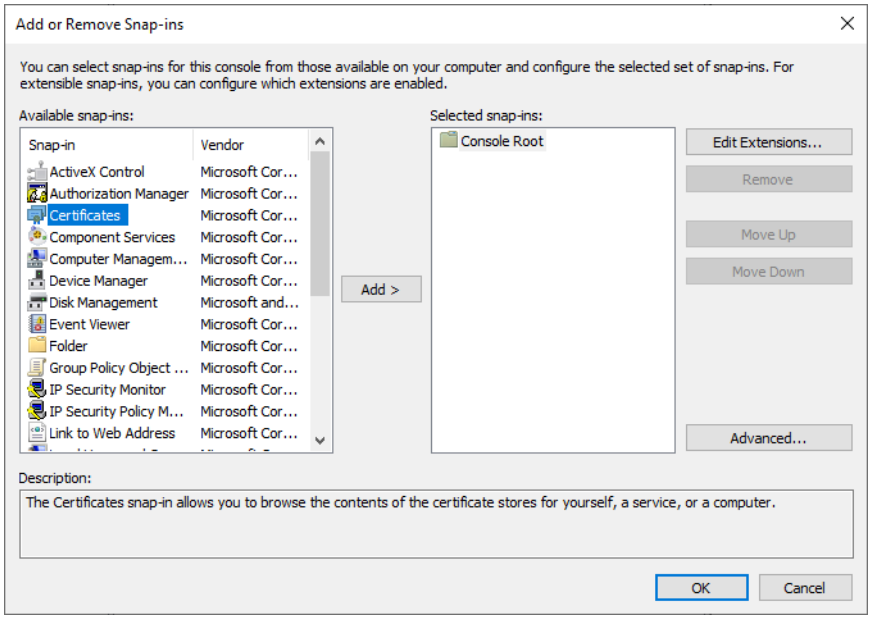


Figure 16 Add Certificates Snap-in

(f) When the Certificates snap-in screen appears, select “My user account” radio button and click the “Finish” button.

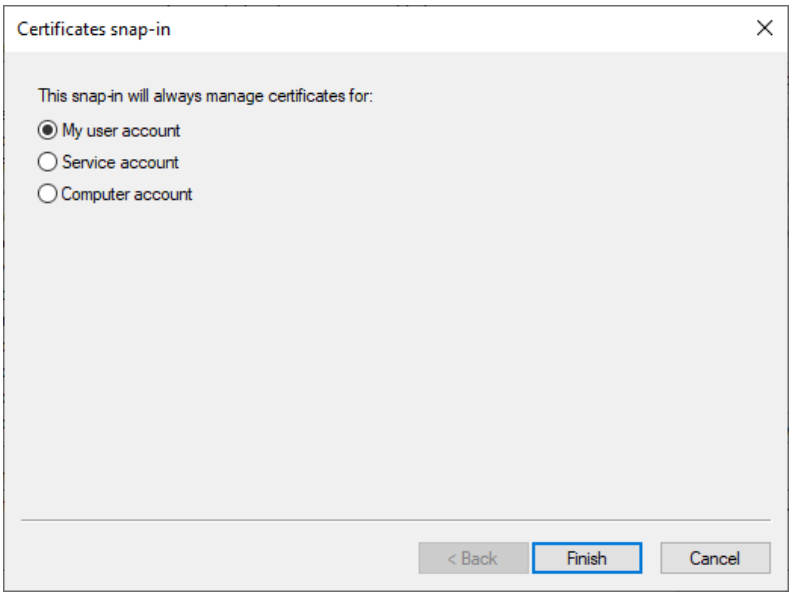


Figure 17 Certificates Snap-in

(g) When you return to the Add or Remove Snap-ins screen, click the “OK” button to close the Add or Remove Snap-ins screen.

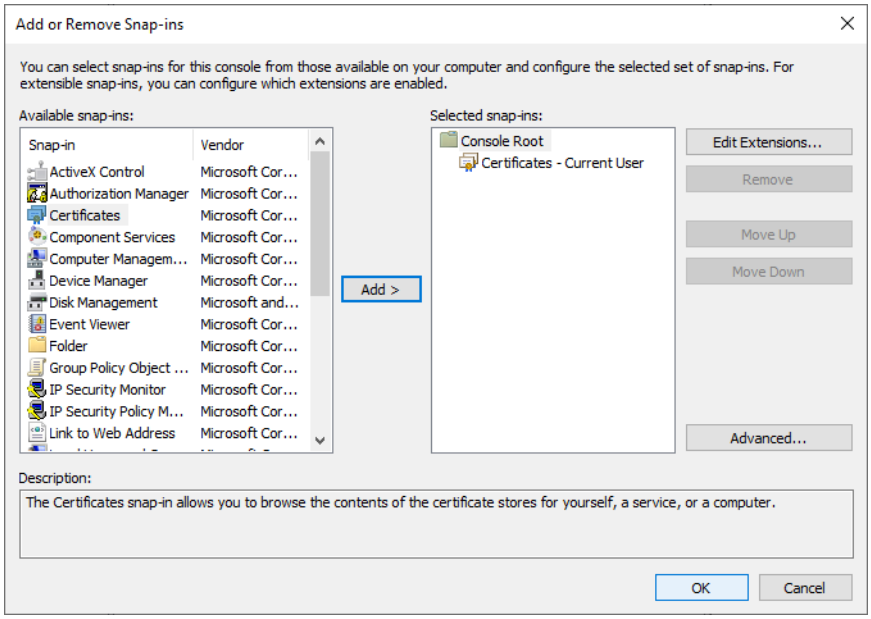


Figure 18 Certificates Snap-in is selected

(h) When you return to the console screen, select "File" - "Save As...".

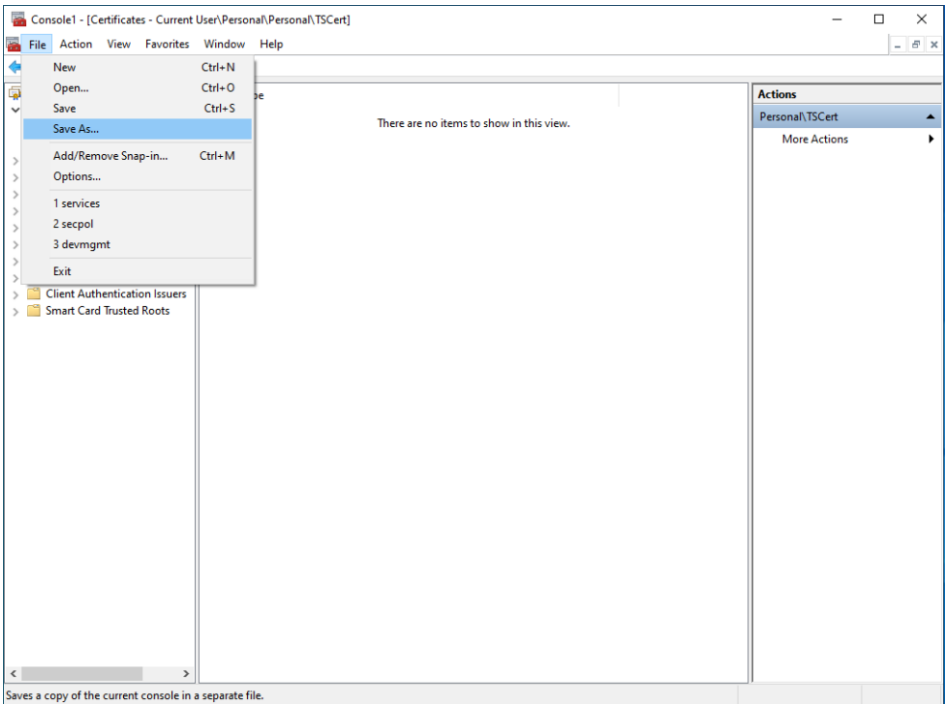


Figure 19 Save Console as

(i) When the Save As screen appears, type "Certificate" as the file name and click the "Save" button.

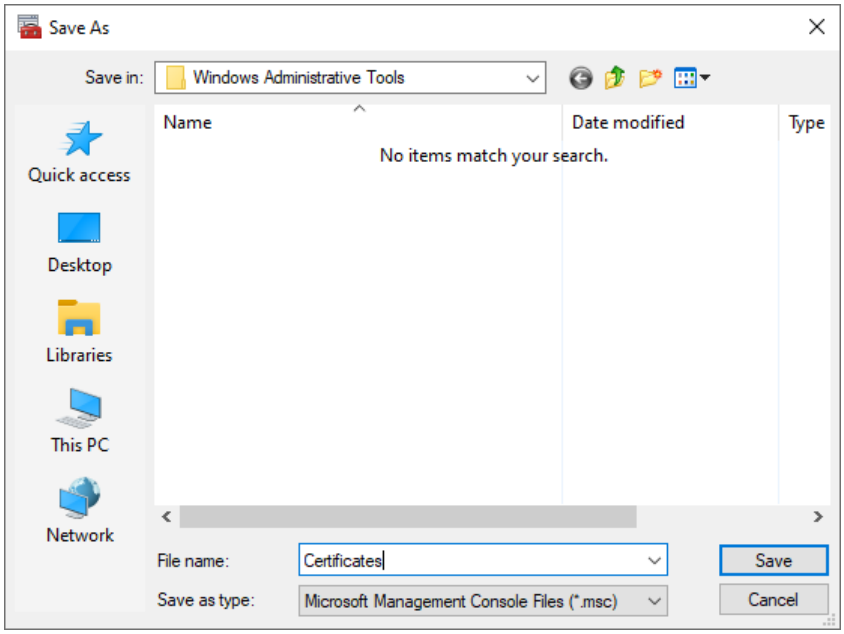


Figure 20 Save As File Name

3. When the Certificate console screen is displayed, right-click on the certificate and select "View" - "Options".

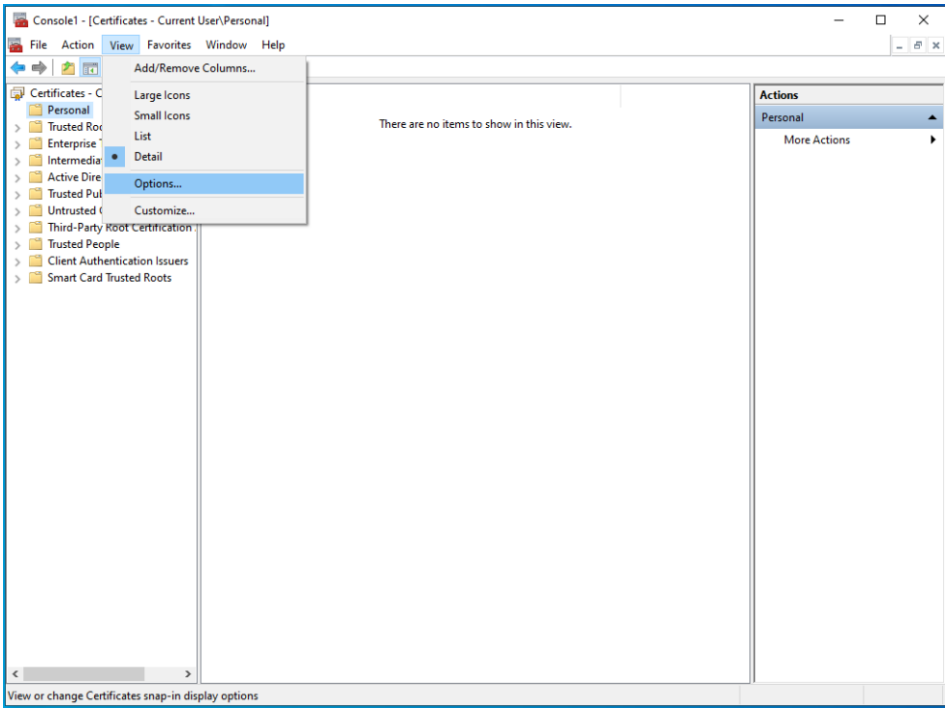


Figure 21 Certificates View Options

4. When the View Options screen appears, select the "Logical certificate store" radio button under "View mode" classification, check the "Physical certificate stores"

checkbox, and click the "OK" button.

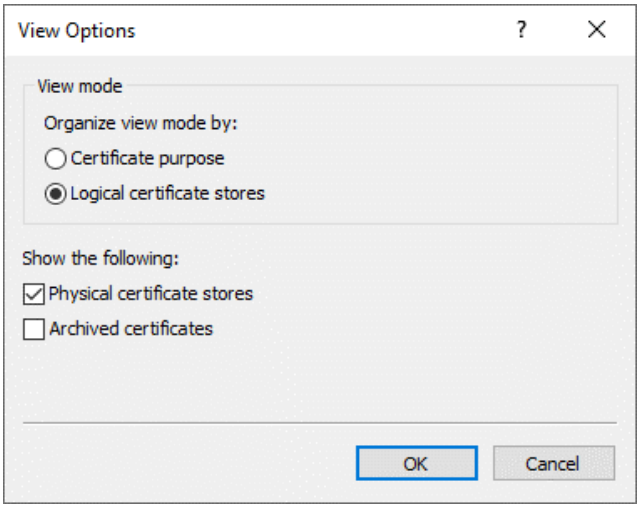


Figure 22 Configure View Options

5. If you return to the console screen and TruCSP is displayed under the "Personal" tree in the left pane, it is considered to have been successfully registered.

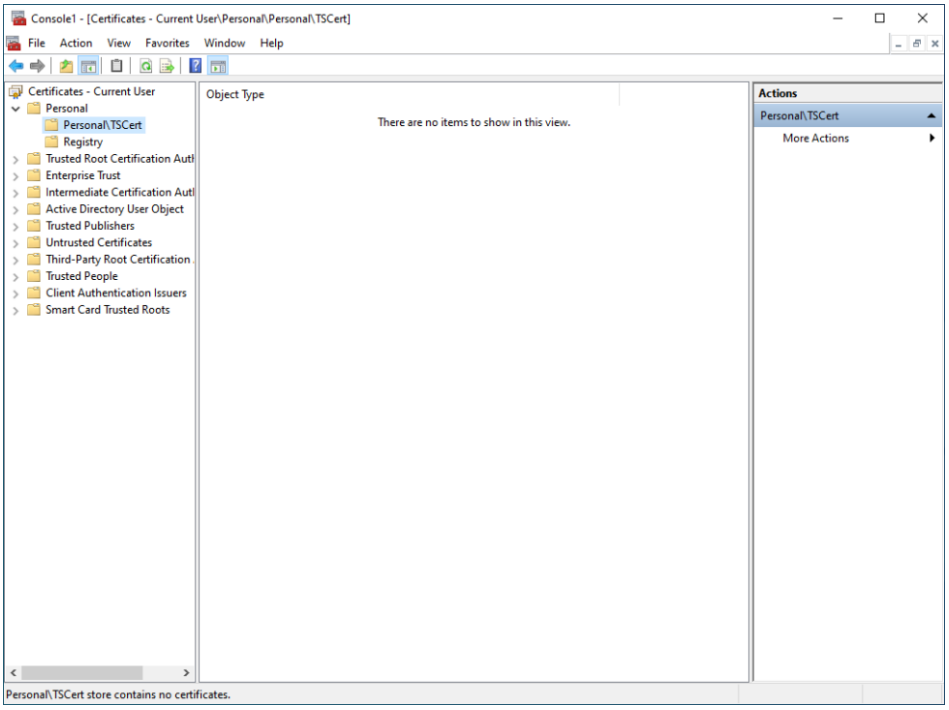


Figure 23 Console – TruCSP added

c. Get Digital ID by TruCSP

i. Get ID from Commercial CA

The following example uses VeriSign's Digital ID Services to store personal digital certificates in TruCSP.

1. Please log on at TruGate or enable your authentication device if you have not enabled TruStack Gina.
2. Launch your web browser and access VeriSign's Digital ID Services application site.

Figure 24 VeriSign Digital ID Request Site

3. When you click the "Apply" button, the page for selecting a web browser as shown below will be displayed, so please select the web browser in which you will use the electronic certificate. In this example, select Microsoft Internet Explorer.

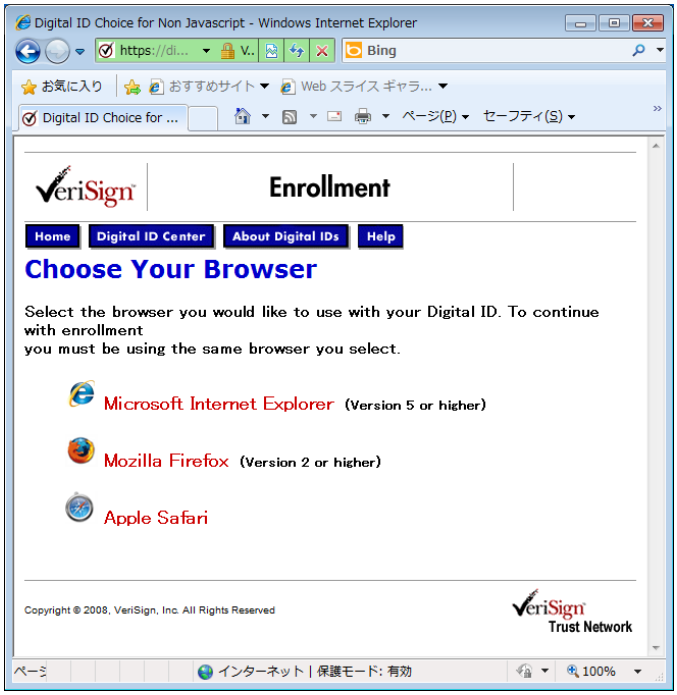


Figure 25 Web Browser Selection

4. If a screen like the one below appears after selecting Microsoft Internet Explorer, click the "Yes" button to continue.

Figure 26 Confirm proxy request for certificate

5. When you select a web browser, an application form page like the one below will be displayed. Fill out the form according to the questions on the screen.

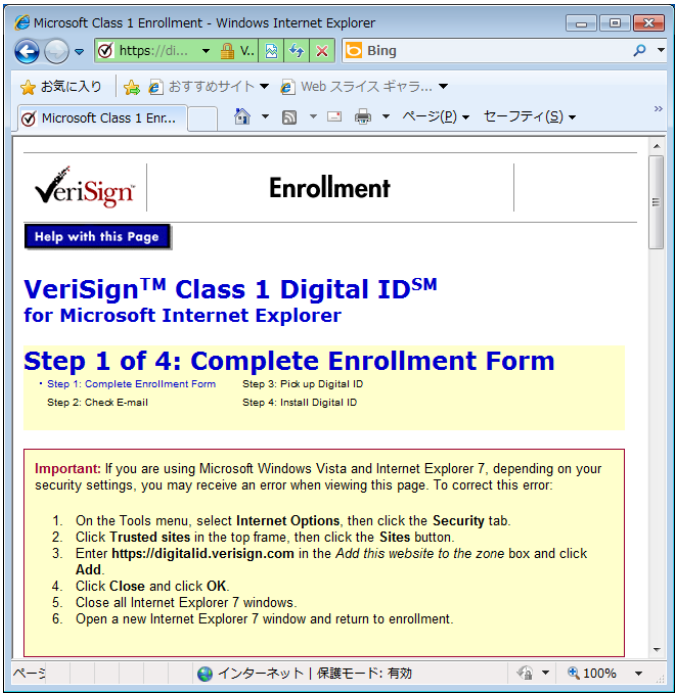


Figure 27 Digital ID Request Enrollment Form

6. First, enter your first name, last name, and email address to be included in your digital certificate.

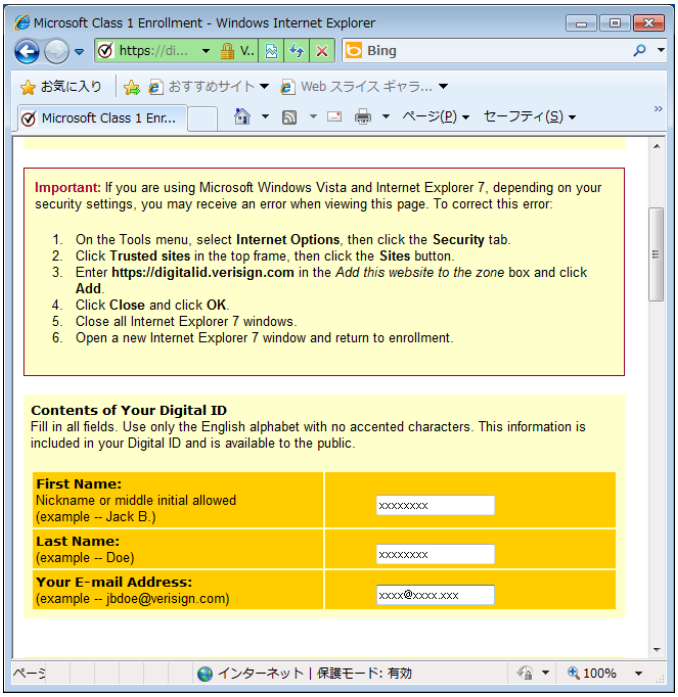


Figure 28 Contents of Digital ID

7. Next, enter the challenge phrase to be used for authentication such as reissuing

a digital certificate.

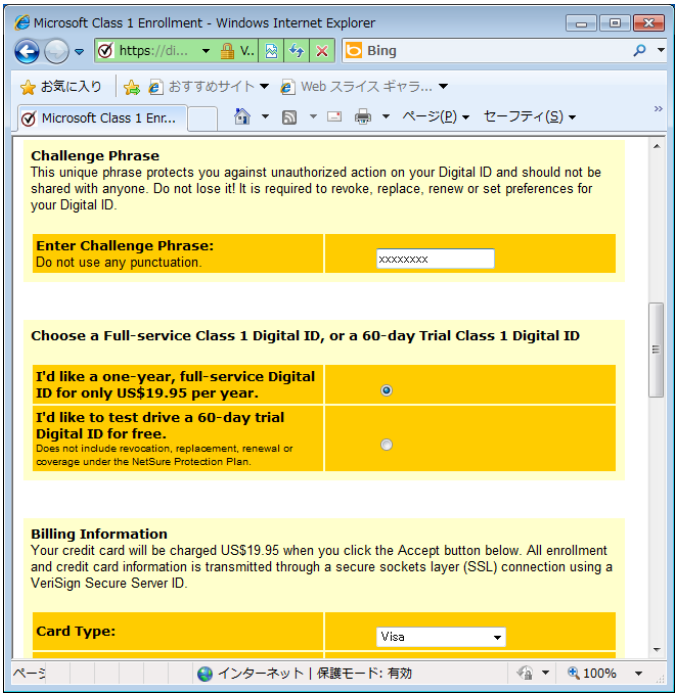


Figure 29 Challenge Phrase

8. Next, select the type of digital certificate you want to obtain. You can choose between a paid digital certificate valid for 1 year or a free evaluation digital certificate valid for 60 days. If you are using electronic certificates for the first time, we recommend that you obtain an evaluation electronic certificate and try it out.

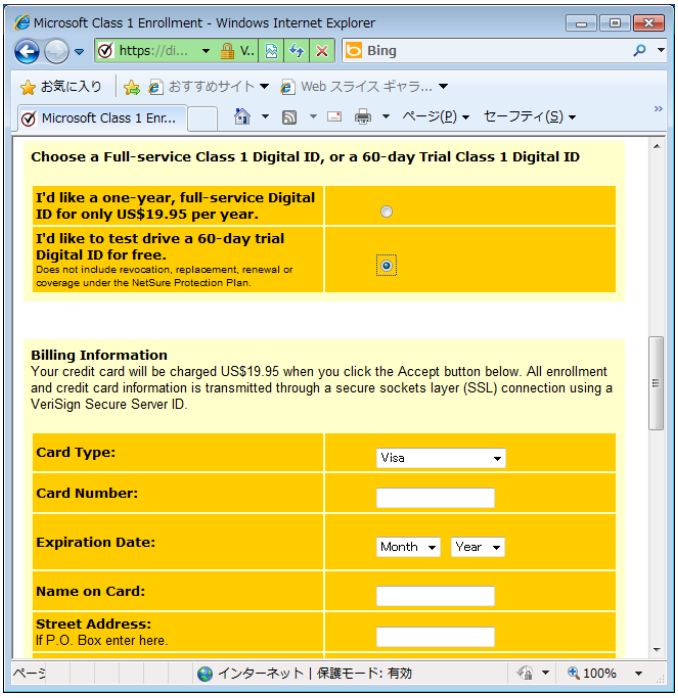


Figure 30 Digital ID Selection

9. Next, enter your credit card payment information if you selected a paid electronic certificate in the electronic certificate selection above. If you selected the free evaluation digital certificate when making the selection above, you do not need to enter this item.

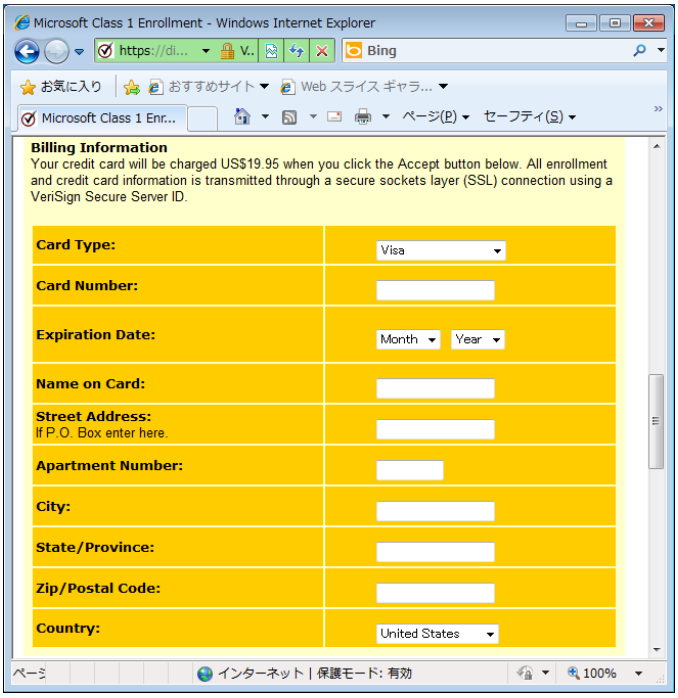


Figure 31 Billing Information

10. Next, when you move to the screen to select the cryptographic service provider you want to use, select "TruStack Cryptographic Provider v1.0" from the drop-down list.

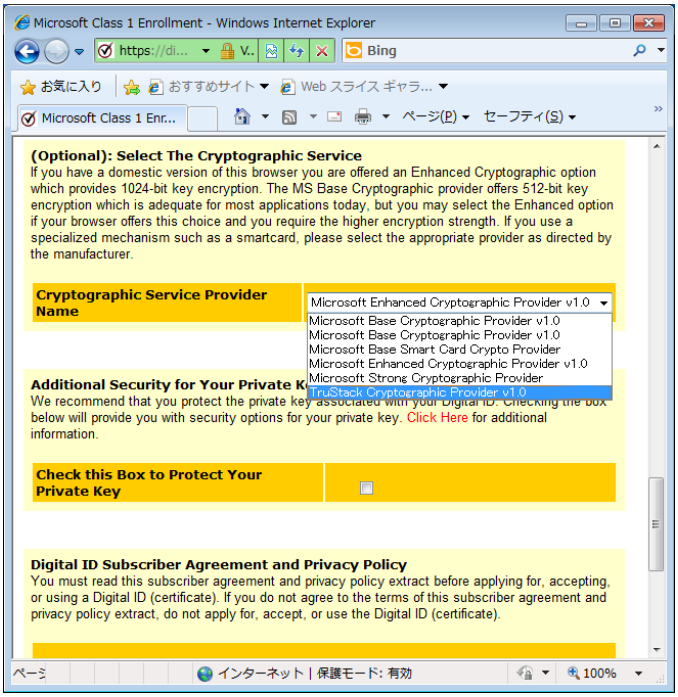


Figure 32 Cryptographic Service Provider Selection

11. Then check the "Protect private key" checkbox.

    Note: In this example, there is no setting item for "key length", but if there is an item for setting "key length" in other companies' CA services, be sure to set it to 1024 or less.

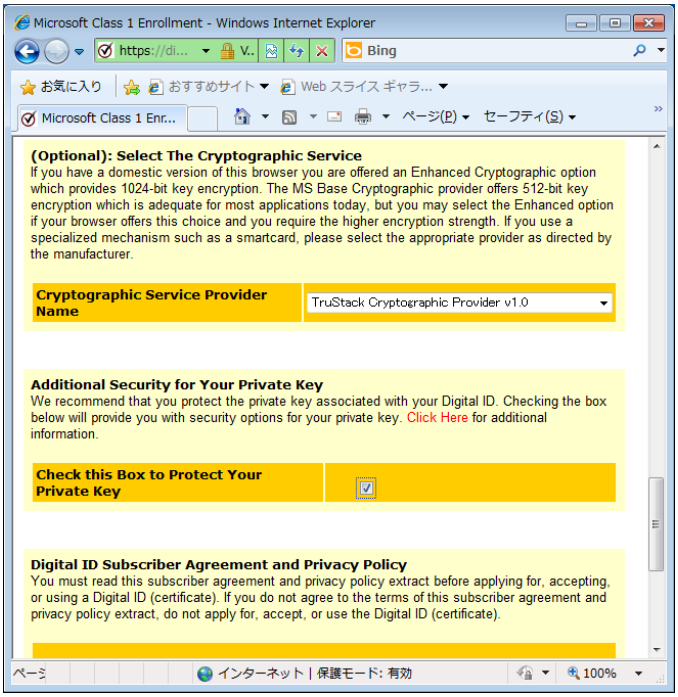


Figure 33 Protect Private Key

12. The Digital ID Subscriber Agreement and Privacy Policy is listed at the end of the application form page. Please read the contents carefully and click the "Accept" button if you agree.

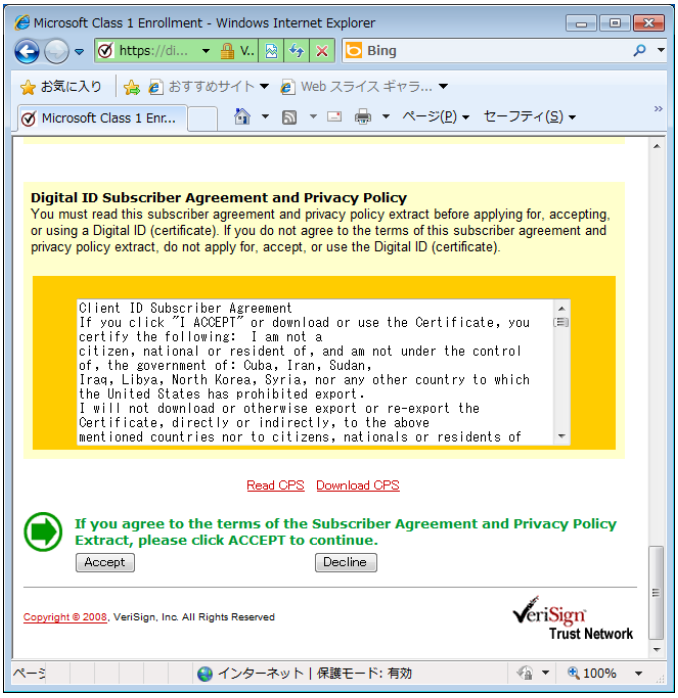


Figure 34 Digital ID Subscriber Agreement and Privacy Policy

13. When you click the "Accept" button, an e-mail confirmation screen will appear as shown below. If the e-mail is correct, click the “OK” button. If it is incorrect, click the "Cancel" button and return to the application form page to make corrections.

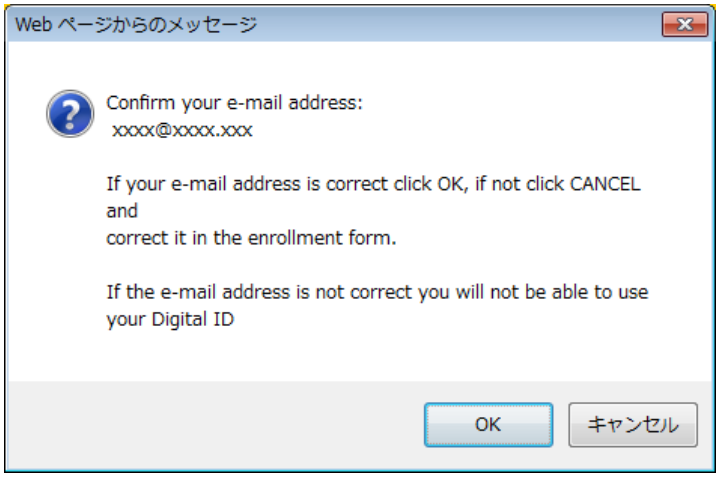


Figure 35 Confirm E-Mail Address of Digital ID

14. If the authentication device is unavailable, or if another certificate and public/private key pair are already registered in the storage area of the authentication device, an error screen like the one below will be displayed.

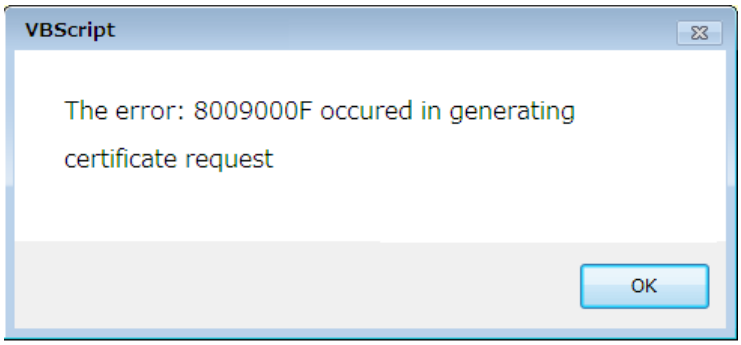


Figure 36 Digital ID Request Error Message

15. If an error like the one above occurs, click the "OK" button to display an example page of the cause of the error like the one below.
Note: If an error occurs, check the status of the authentication device, connect the authentication device, initialize the storage area, etc. (see What to do when a certificate request error/import error occurs), and then Please apply for the electronic certificate again.

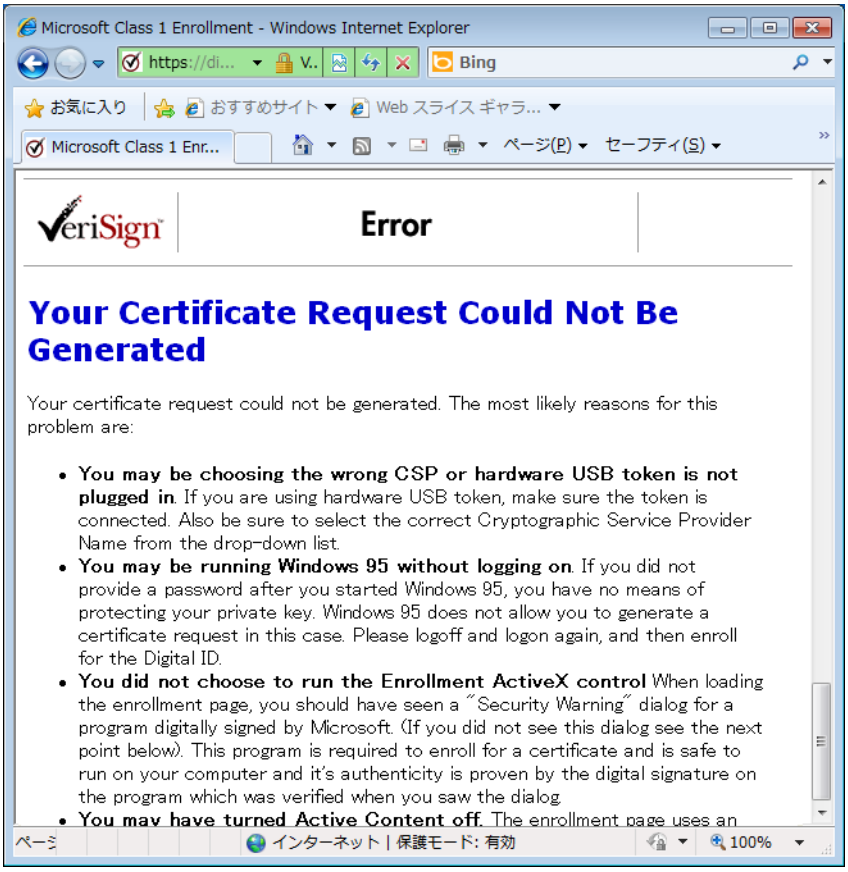


Figure 37 Example of Reasons for Digital ID Request Error

16. If your electronic certificate application is successful, you will be redirected to an e-mail confirmation page as shown below.

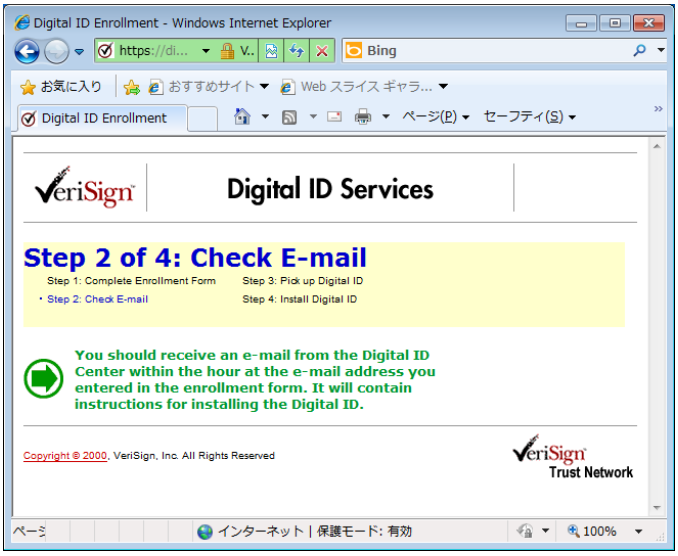


Figure 38 Check E-Mail

17. When the above screen appears, wait a while, then start the mailer and check the email from VeriSign. If your electronic certificate application is successfully accepted, you will receive an e-mail from VeriSign as shown below.

件名： Trial Class 1 VeriSign Digital ID Pickup Instructions

If you did not enroll for a Digital ID through VeriSign please do not follow the instructions below for picking up the ID.

QUICK INSTALLATION INSTRUCTIONS

To assure that someone else cannot obtain a Digital ID that contains your name and e-mail address, you must retrieve your Digital ID from VeriSign's secure web site using a unique Personal Identification Number (PIN).

Be sure to follow these steps using the same computer you used to begin the process.

Copy your Digital ID PIN
Your Digital ID PIN is:

Go to VeriSign's secure Digital ID Center
https://digitalid.verisign.com/enrollment/mspickup.htm

Paste (or enter) your Digital ID PIN
Then select the SUBMIT button to install
your Digital ID.

That's all there is to it!

****
INTERNATIONAL CUSTOMERS: International customers may be able to obtain local service and support from a VeriSign Affiliate.
Please visit http://www.verisign.com/international/class1.html.
****

Figure 39 Accepted Digital ID Request by VeriSign

18. Next, click the link to the Digital ID Center shown in the e-mail above. When the Pick up Digital ID page shown below is displayed, copy and paste the Digital ID PIN received in the e-mail into "Digital ID Personal Identification Number (PIN):" on the page, and click the "Submit" button. .

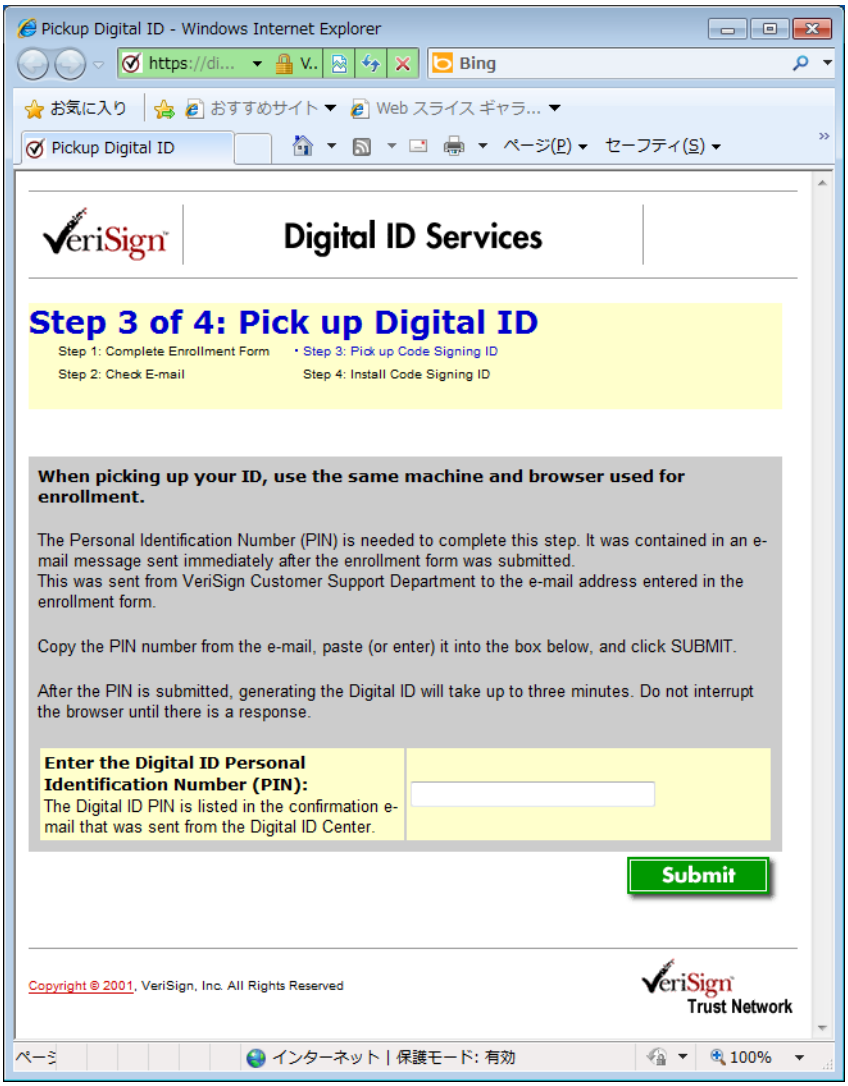


Figure 40 Digital ID Personal Identification Number (PIN)

19. Once the Digital ID is successfully generated, you will see the Install Digital ID page shown below. Check the displayed information, and if it is correct, click the "Install" button to install.

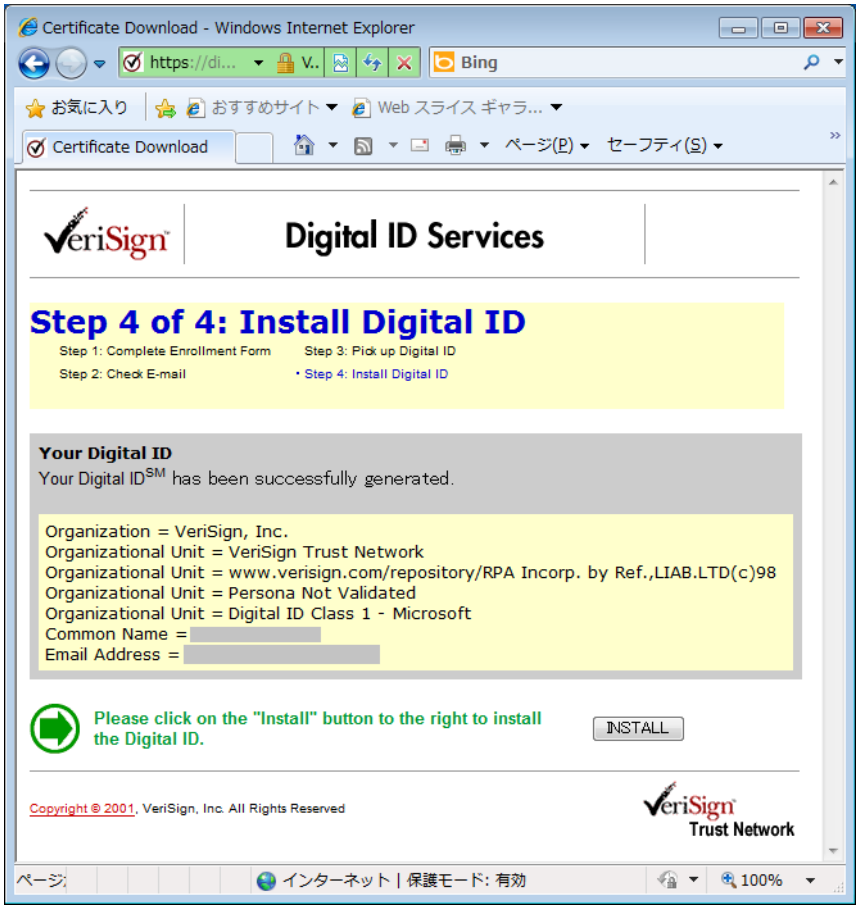


Figure 41 Install Digital ID

20. If a screen like the one below appears after clicking the "Install" button, please click the "Yes" button to continue.

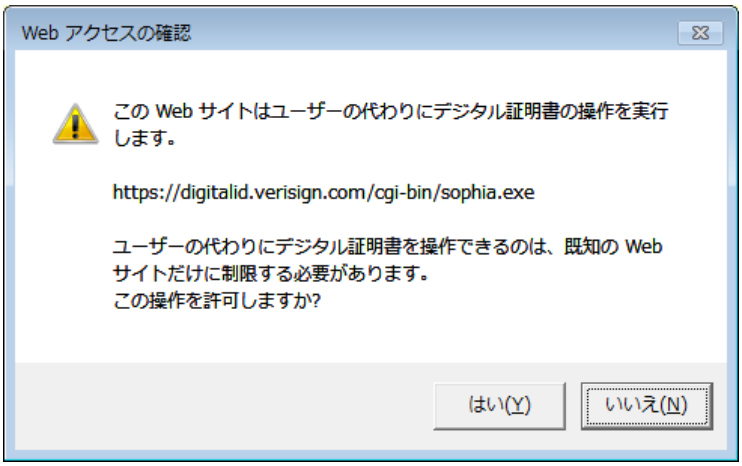


Figure 42 Confirm additional certificate

21. If the device authentication screen is displayed, perform device authentication.
22. If the digital certificate installation is successful, the digital certificate usage

settings page shown below will be displayed.

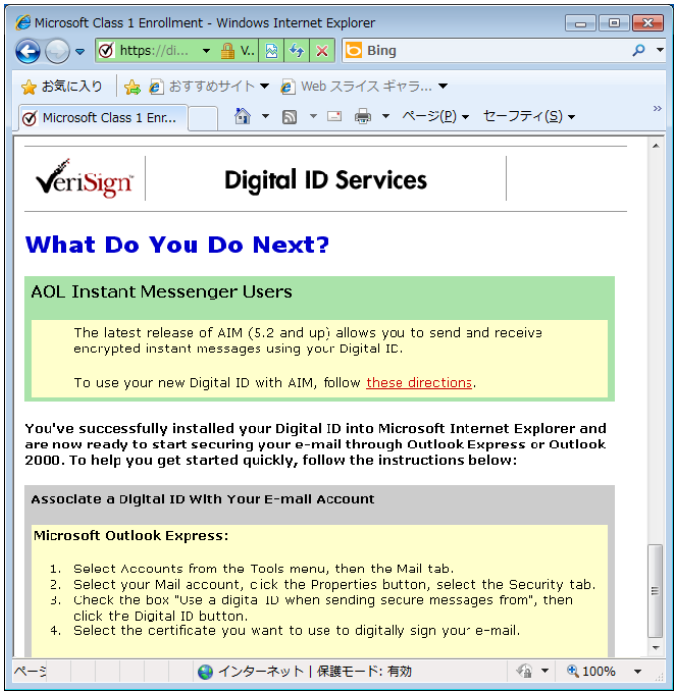


Figure 43 Configuration for Digital ID Usage

23. To check the installed digital certificate, select "Tools" - "Internet Options" from the Internet Explorer menu bar.

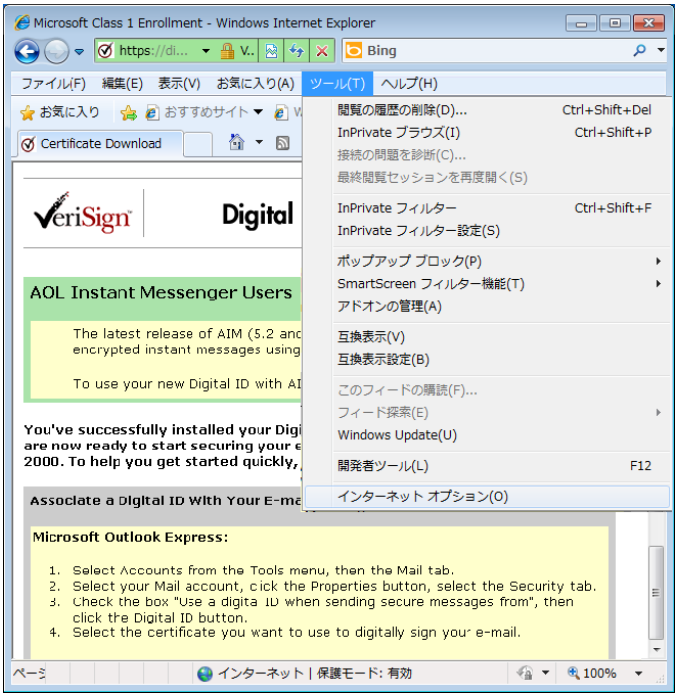


Figure 44 Launch Internet Options

24. When the Internet Options screen appears, select the “Content” tab.

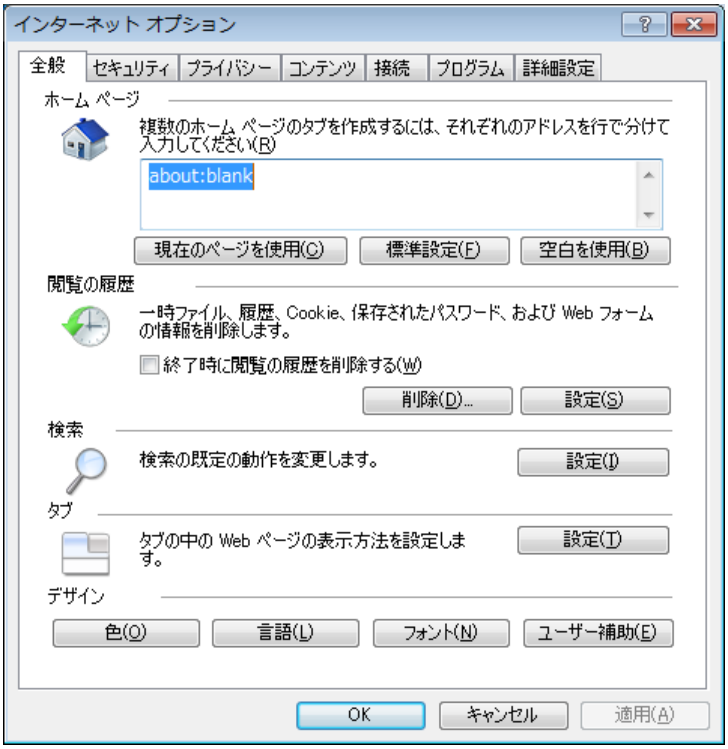


Figure 45 Internet Options Dialog box

25. When the Internet options display changes to content, click the "Certificate" button.

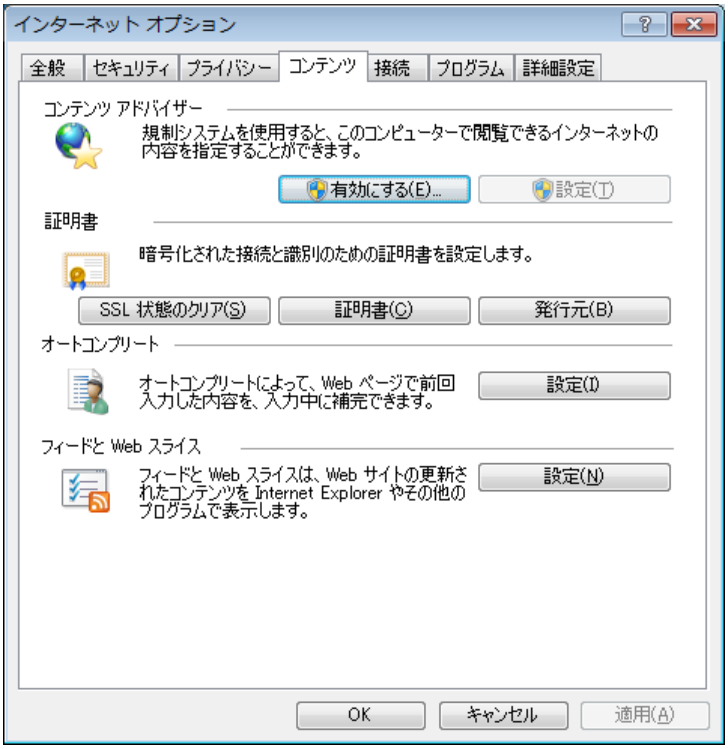


Figure 46 Show Contents

26. When the certificate screen appears, select the certificate you just installed and click the "View" button.

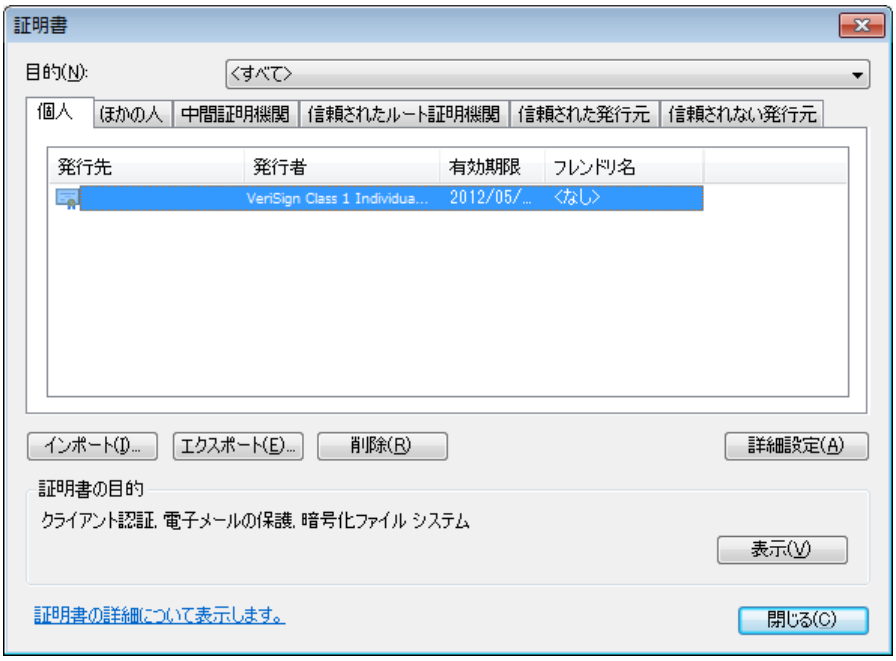


Figure 47 Confirm Digital ID

27. When the certificate information screen shown below is displayed, please check

that the information matches what you applied for.

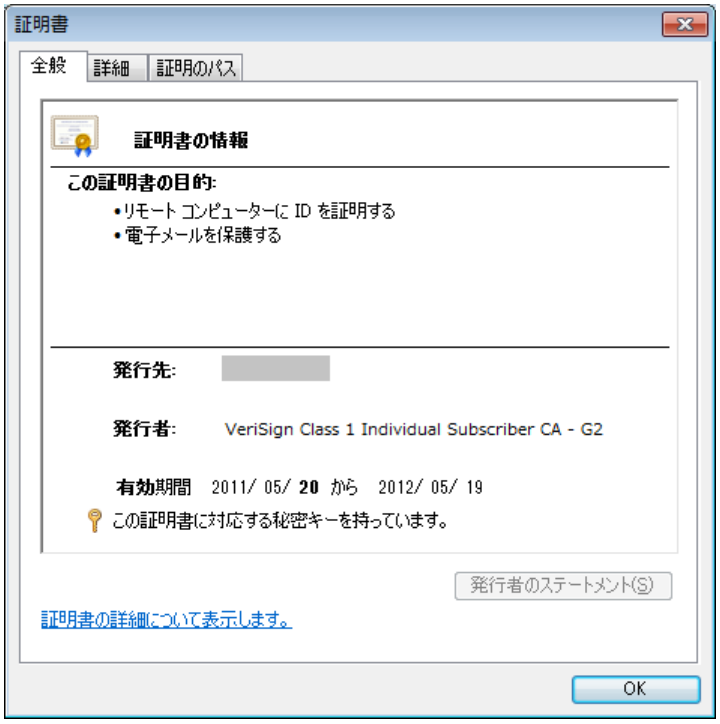


Figure 48 Information of Digital ID

28. Once the confirmation is complete, close each screen to exit.

ii. Get Certificate from Windows CA

The following is an example of storing a personal digital certificate in TruCSP from a CA configured in Active Directory.

To request a certificate from a CA in Active Directory from the client PC's certificate console, an enterprise CA must be configured on the server PC's OS.

Note: If the existing CA is a standalone CA, you cannot directly request a certificate from the CA in Active Directory from the certificate console of the client PC. In that case, request a certificate via the Windows CA's Certificate Services web page (http://servername/certsrv), just as you would from a commercial CA.

1) Configuration of CA

1. Log on to the server PC as an enterprise administrator.
2. Select "Start" - "Server Manager".

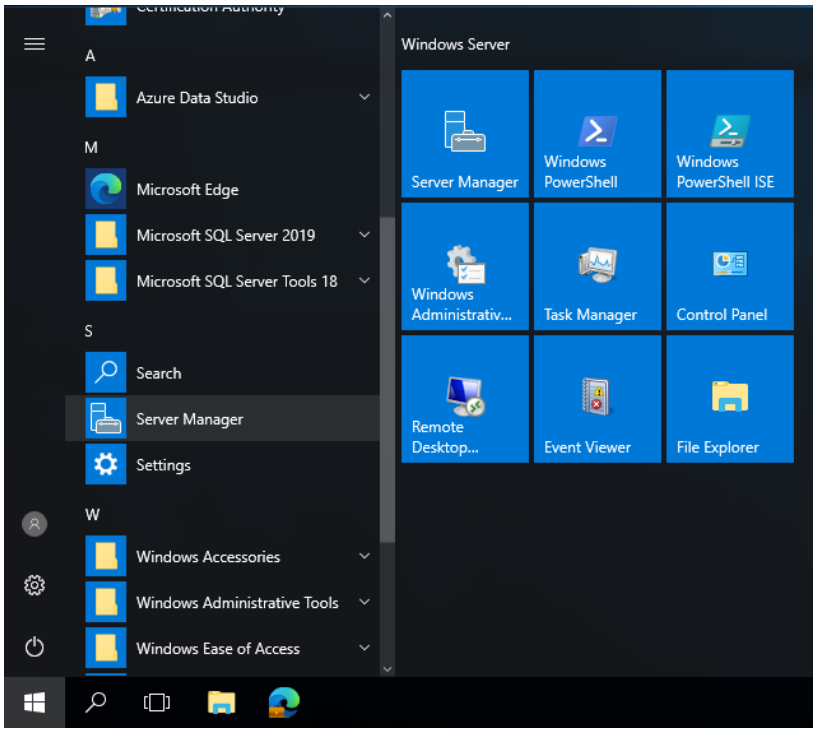


Figure 49 Launch Server Manager

3. When the Server Manager screen appears, click Add Role.

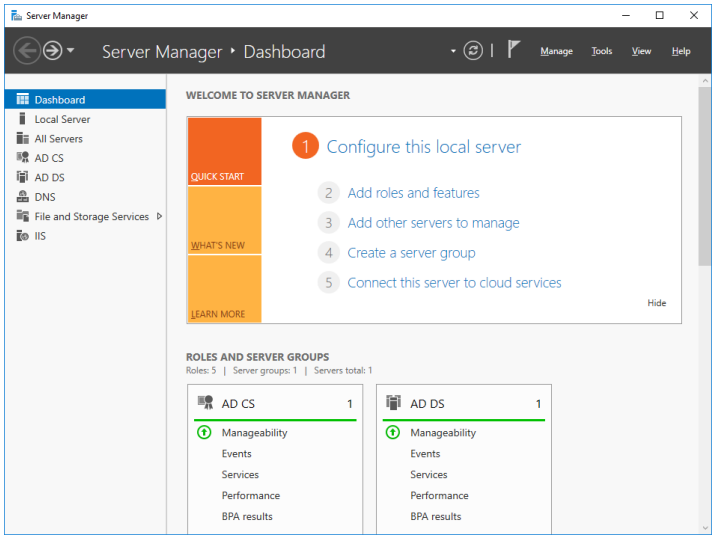


Figure 50 Server Manager Dashboard

4. When the Add Roles and Features Wizard screen like the one below appears, check the items in "Before you begin" and if there are no problems, click the "Next" button.

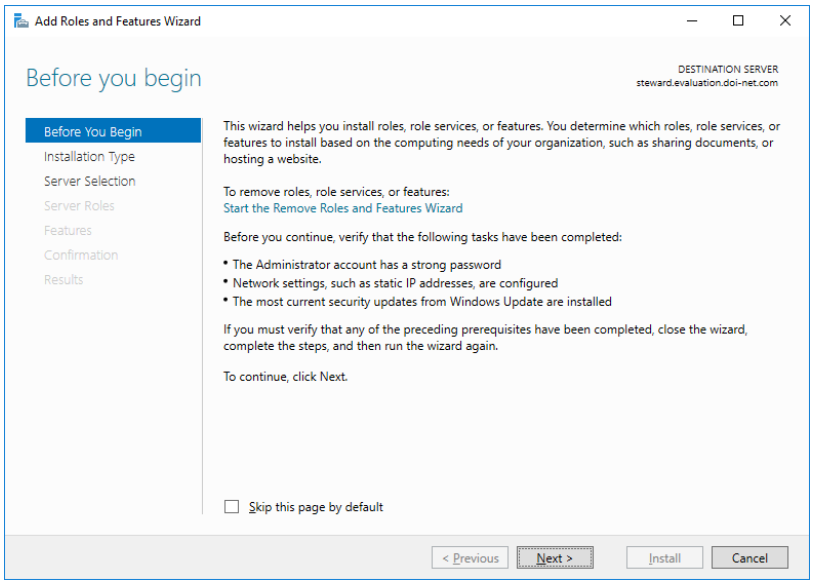


Figure 51 Add Roles and Features Wizard

5. When the “Select Installation Type” page appears, check the “Role-based or feature-based installation” radio button and click the Next button.

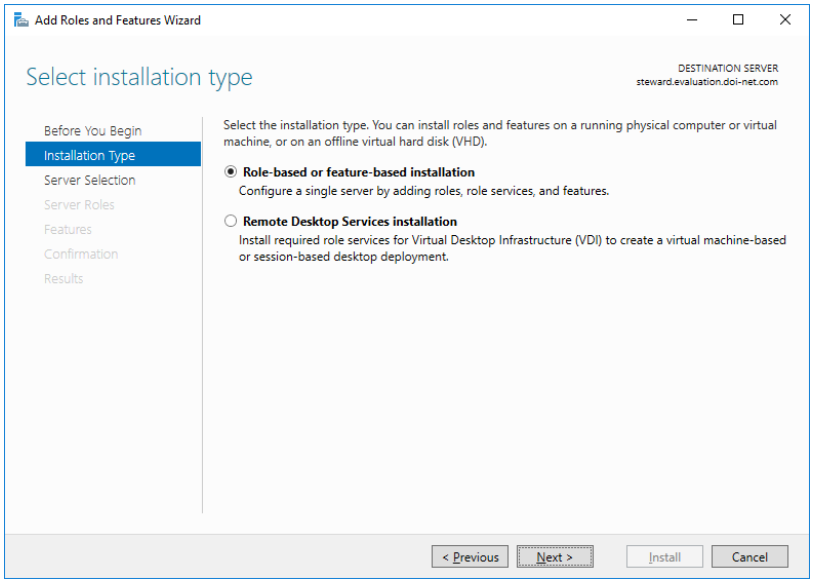


Figure 52 Select Installation Type

6. When the “Select Destination Server” page appears, select the target server from the server pool and click the Next button.

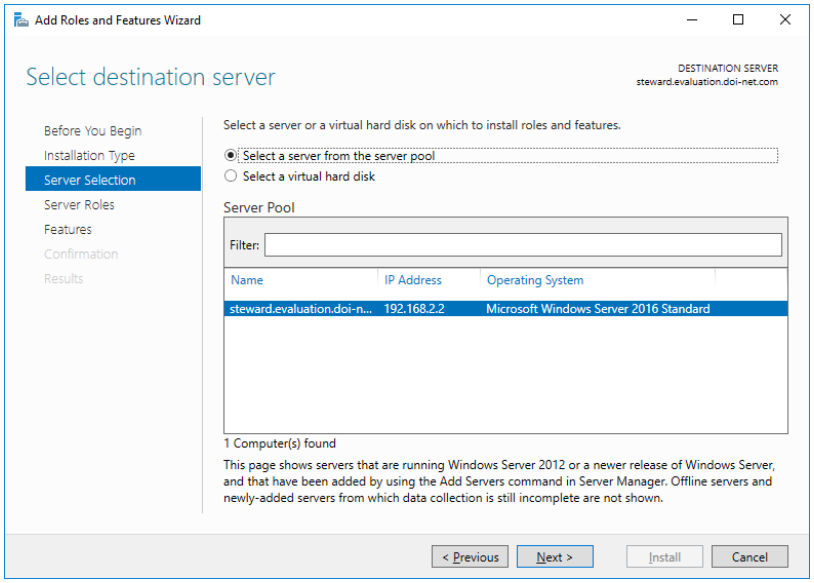


Figure 53 Select Destination Server

7. When the "Select Server Roles" page appears, check the "Active Directory Certificate Services" checkbox and click the "Next" button.

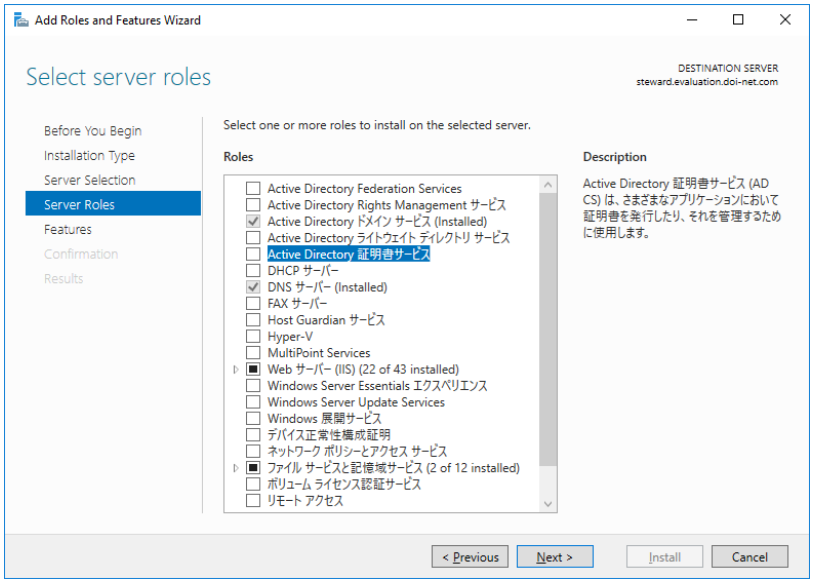


Figure 54 Select Server Roles

8. If you check the "Active Directory Certificate Services" checkbox, a confirmation screen for adding the following functionality will be displayed. If you are satisfied, click the “Add Features” button to continue.

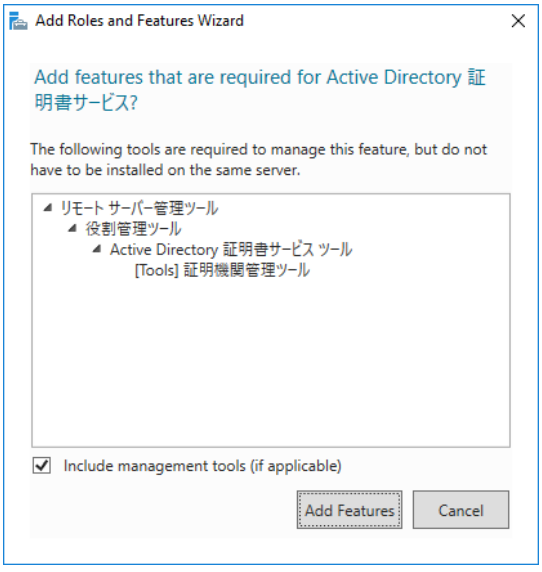


Figure 55 Add Features Confirmation

9. When the “Select Features” screen appears, check the items and if there are no problems, click the "Next" button to continue.

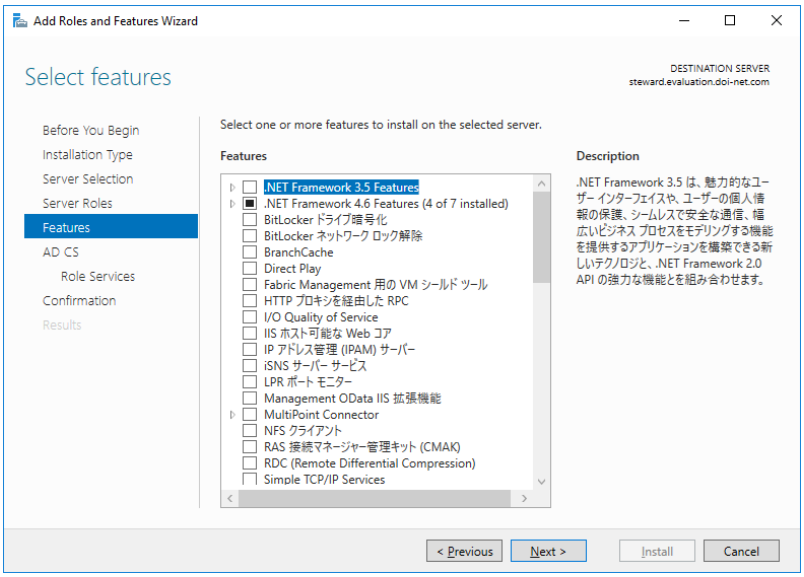


Figure 56 Select Features

10. If you check the "Active Directory Certificate Services" checkbox, the computer name and domain membership confirmation screen shown below will be displayed. If you are satisfied, click the “Next” button to continue.

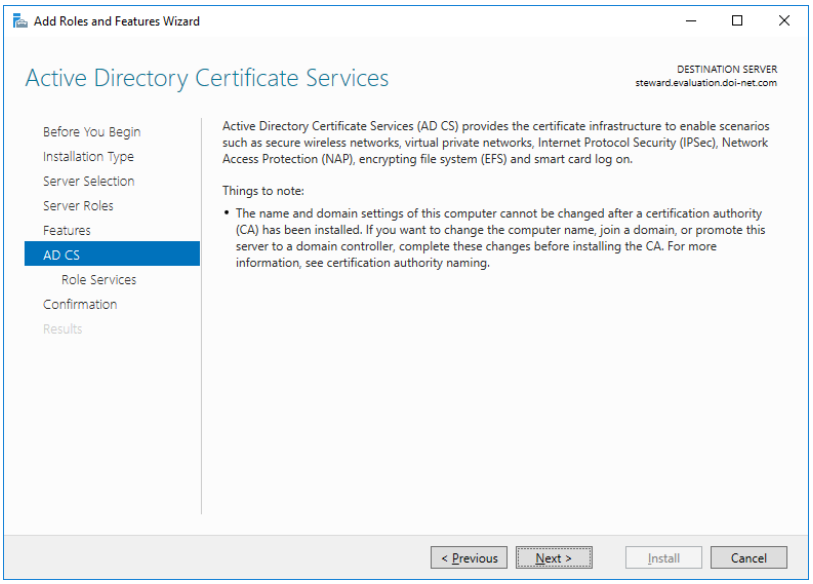


Figure 57 Active Directory Certificate Services

11. When the "Select Role Services" page is displayed, check the "Certification Authority Web Registration" checkbox to use the certificate service web page, and click the "Next" button.

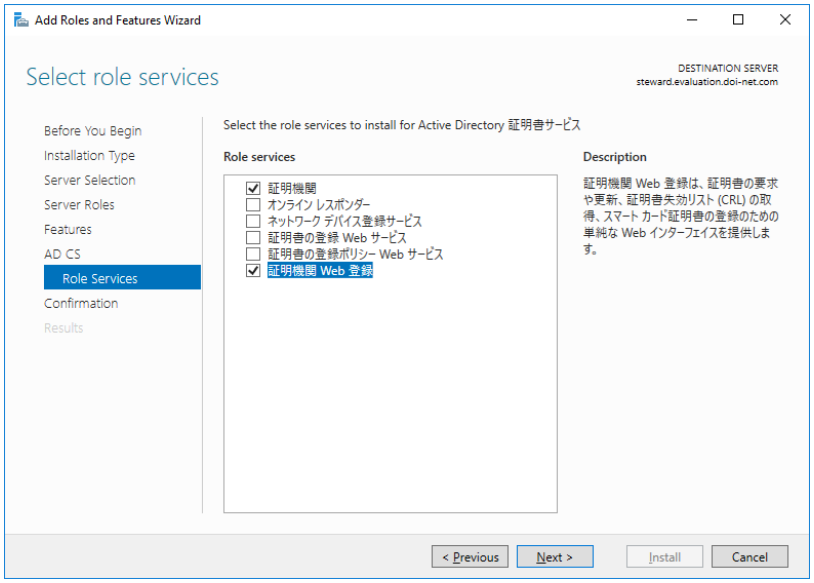


Figure 58 Select Role Services

12. If the optional feature is not installed in advance and "Certification Authority Web Registration" is checked, the screen shown below will be displayed. If everything is OK, click the “Install” button to continue.

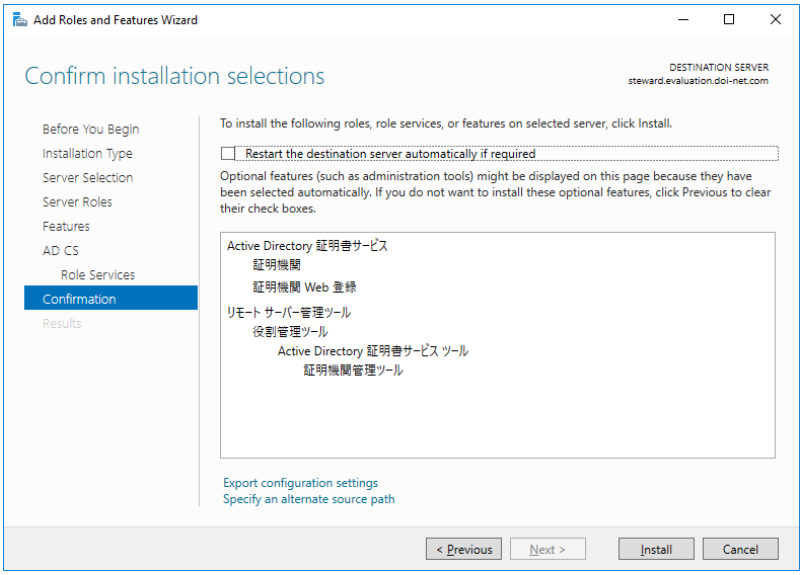


Figure 59 Confirm Installation Selections

13. Then, when the “Setup Type” page appears, select the setup type according to your network configuration and click the “Next” button.

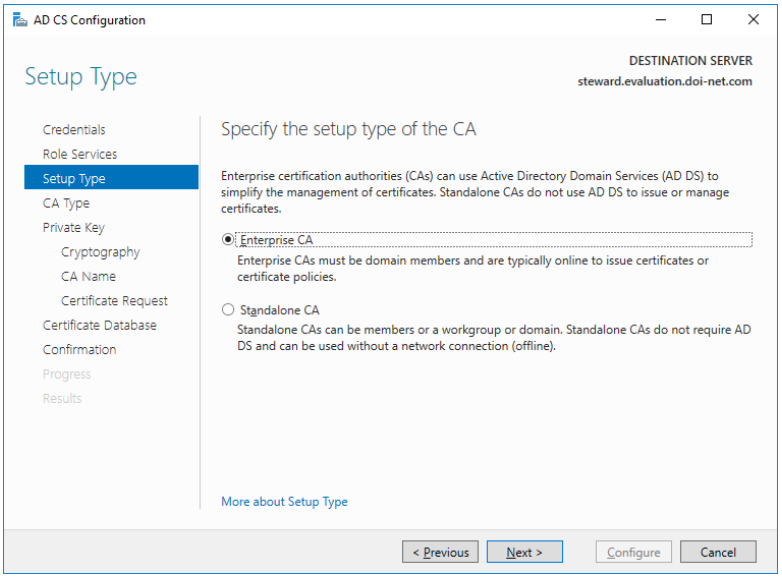


Figure 60 Setup Type

14. When the "CA Type" page is displayed, select the CA type you want to set up and click the "Next" button.

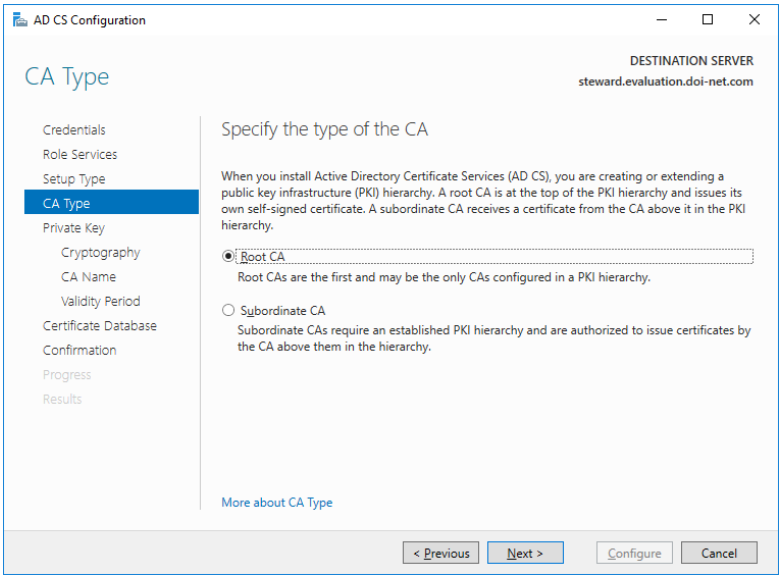


Figure 61 CA Type

15. When the "Private Key" screen appears, select the "Create a new private key" radio button and click the "Next" button.

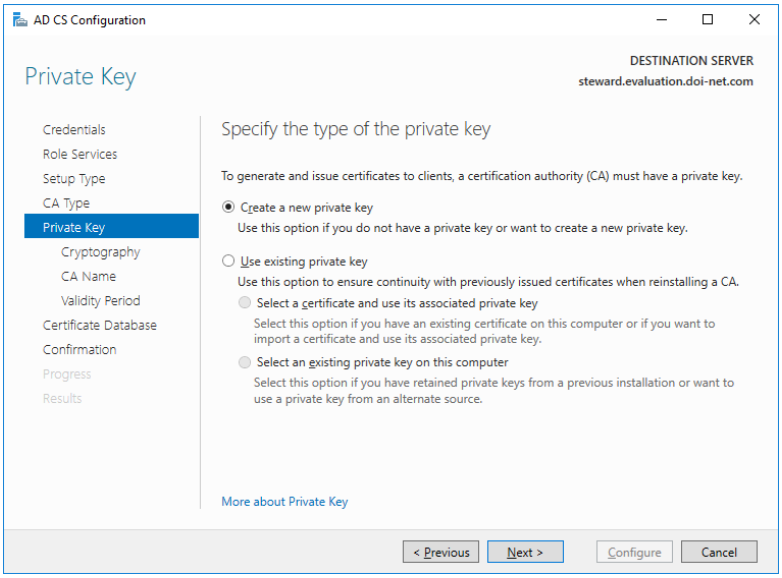


Figure 62 Private Key

16. Next, the “Cryptography for CA” page is displayed. Set the CSP, hash algorithm, key length, etc. you want to use, and click the "Next" button.

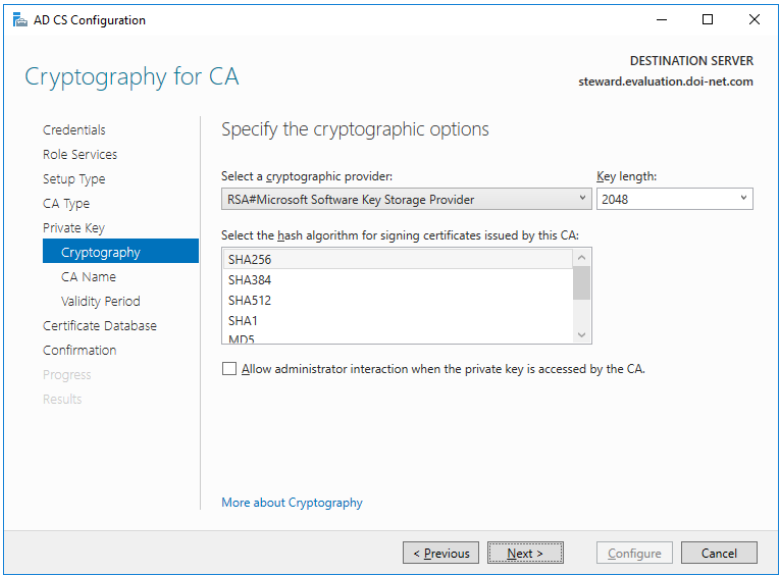


Figure 63 Cryptography for CA

17. When the “CA Name” page appears, optionally type the unique CA name you want to generate in the Common Name for this CA edit box and click the “Next” button.

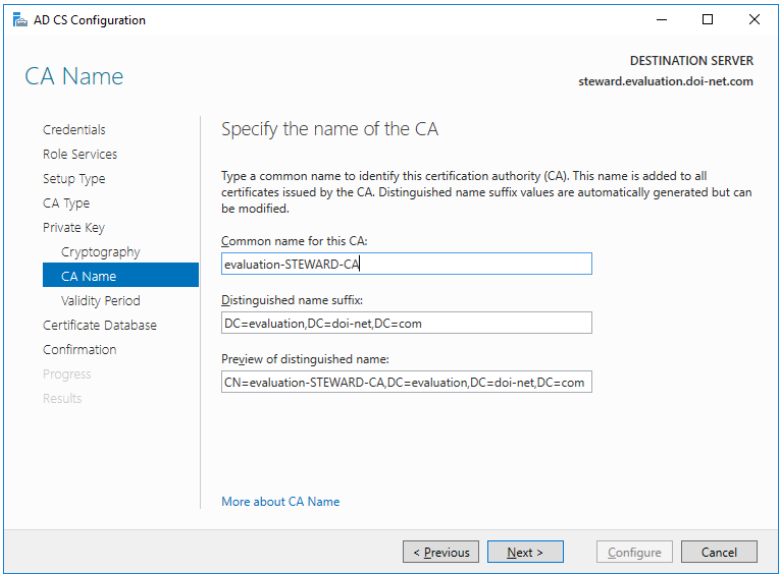


Figure 64 CA Name

18. When the “Validity Period” page appears, select the validity period if necessary and click the “Next” button.

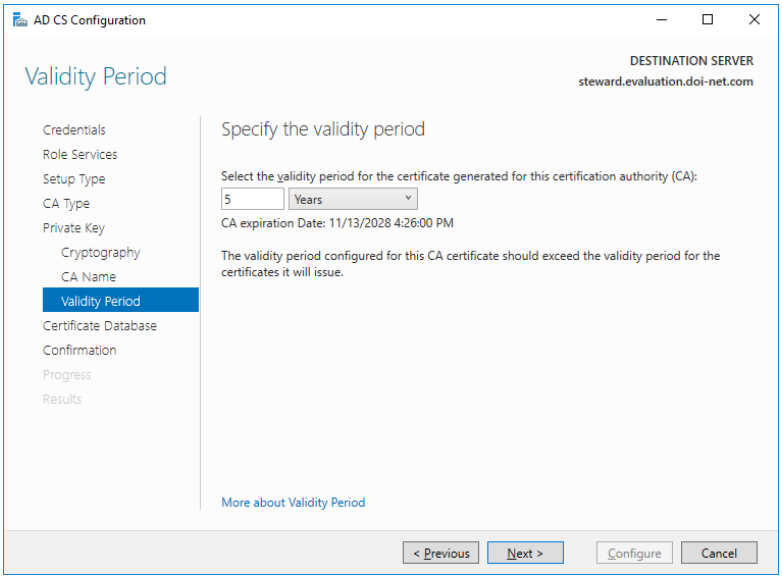


Figure 65 Validity Period

19. When the “CA Database” screen appears, change the location if necessary.

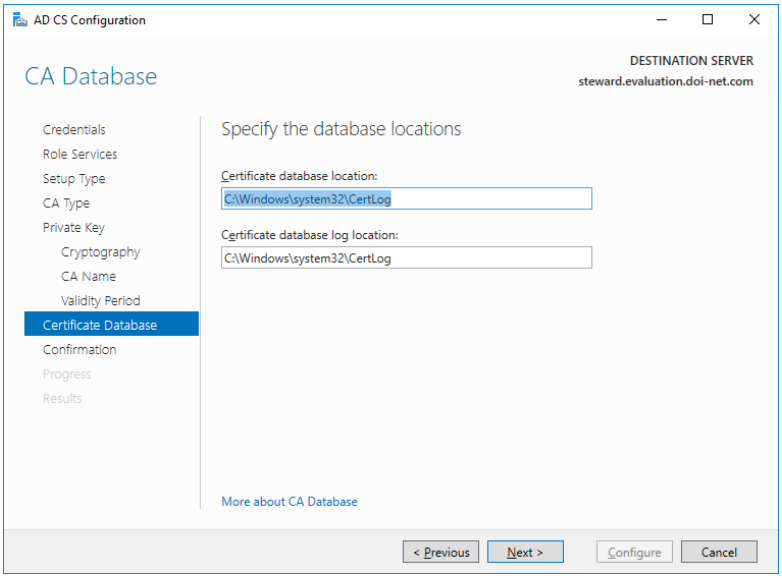


Figure 66 CA Database

20. When the “Confirmation” page appears, confirm that there are no issues and click the “Configure” button to continue.

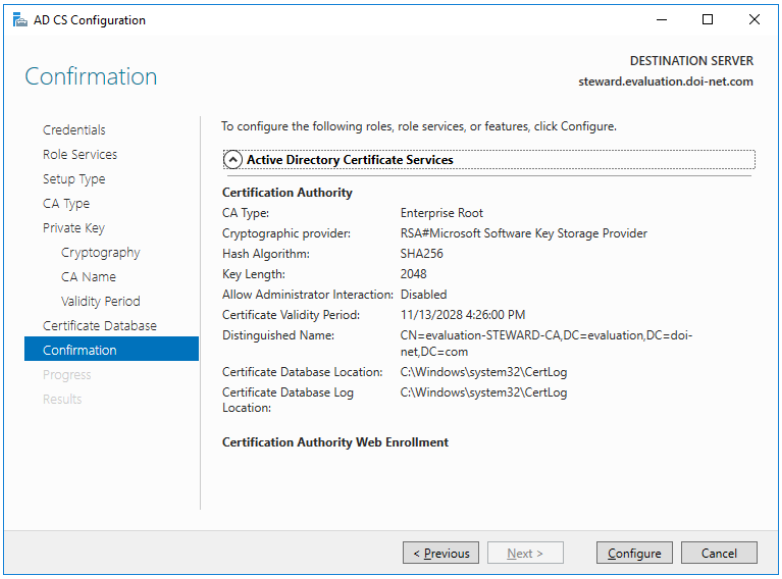


Figure 67 Confirmation

21. When the installation is complete, the “Results” page is displayed. If a problem occurs, eliminate the cause and install again.

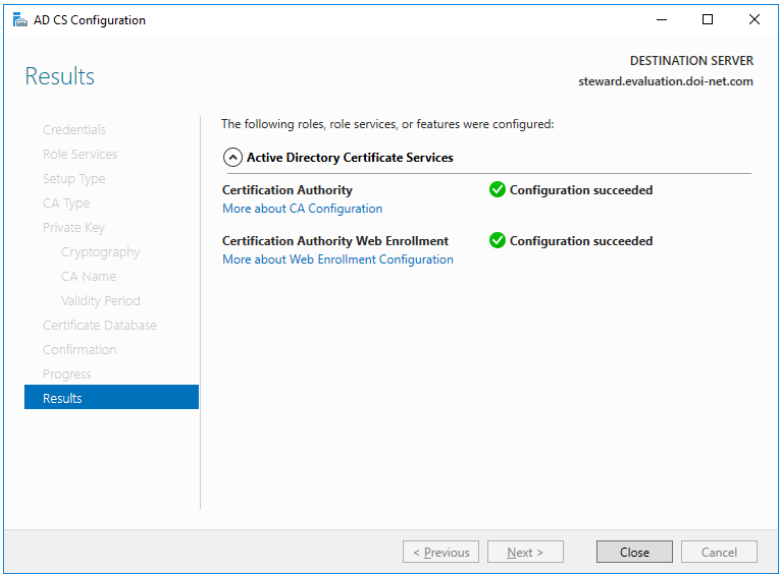


Figure 68 Results

22. Click the “Close” button to return to Server Manager, confirm that Active Directory Certificate Services is added to Roles, and exit.

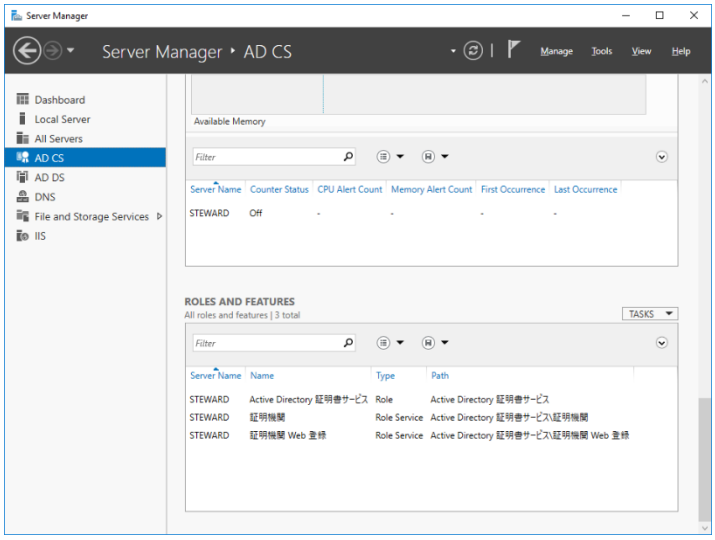


Figure 69 Confirm Server Manager

23. Next, select "Start" - "Windows Administrative Tools" - "Certification Authority".

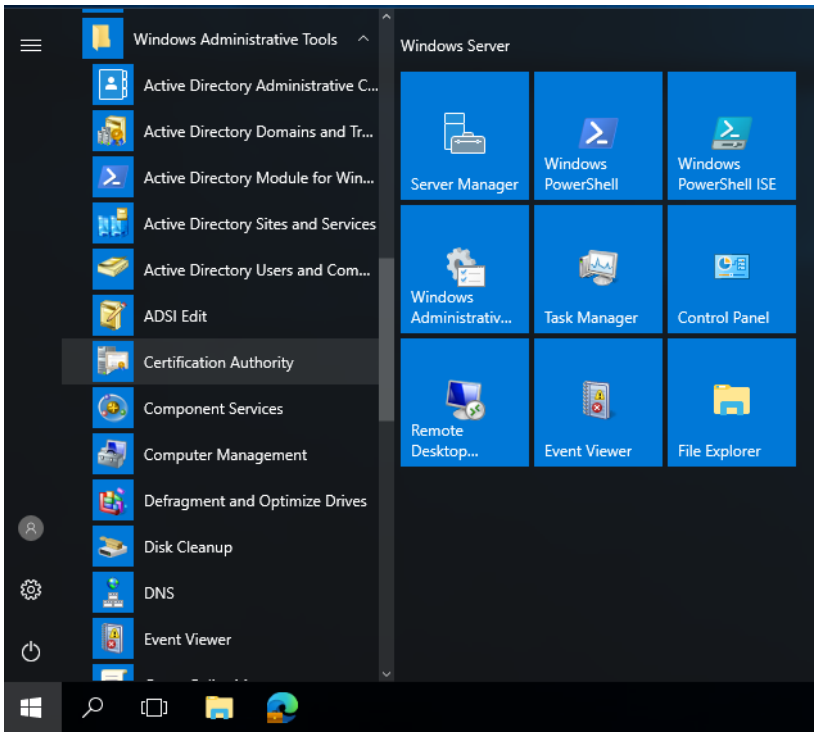


Figure 70 Certification Authority

24. When the “Certification Authority console” screen appears, select "Certificate Templates" from the left pane.

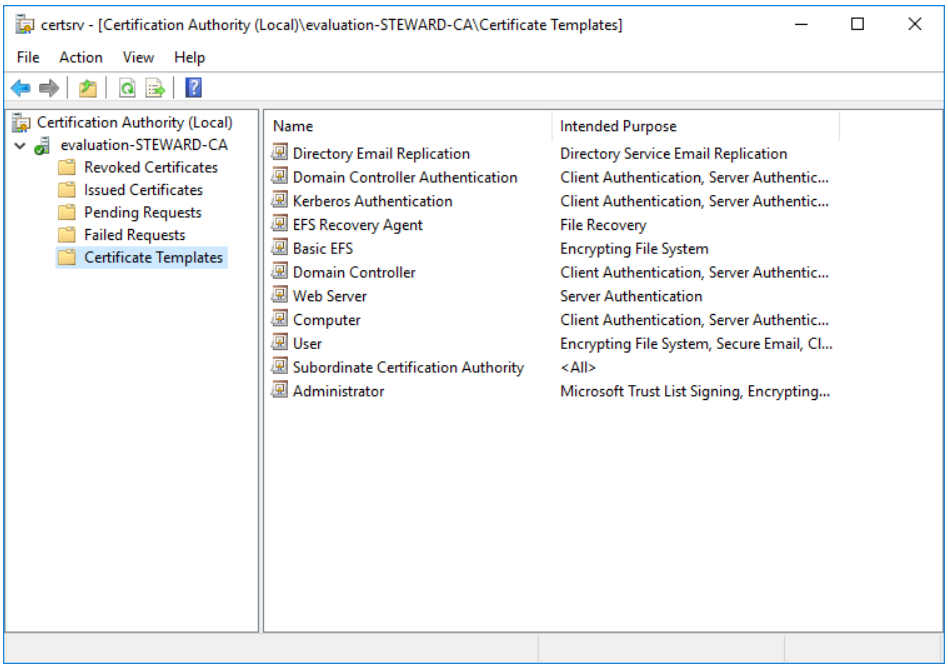


Figure 71 Certification Authority console

25. When the list of issued certificate templates is displayed in the right pane,

click the right mouse button on "Certificate Templates". When the pop-up menu appears, select “Manage”.

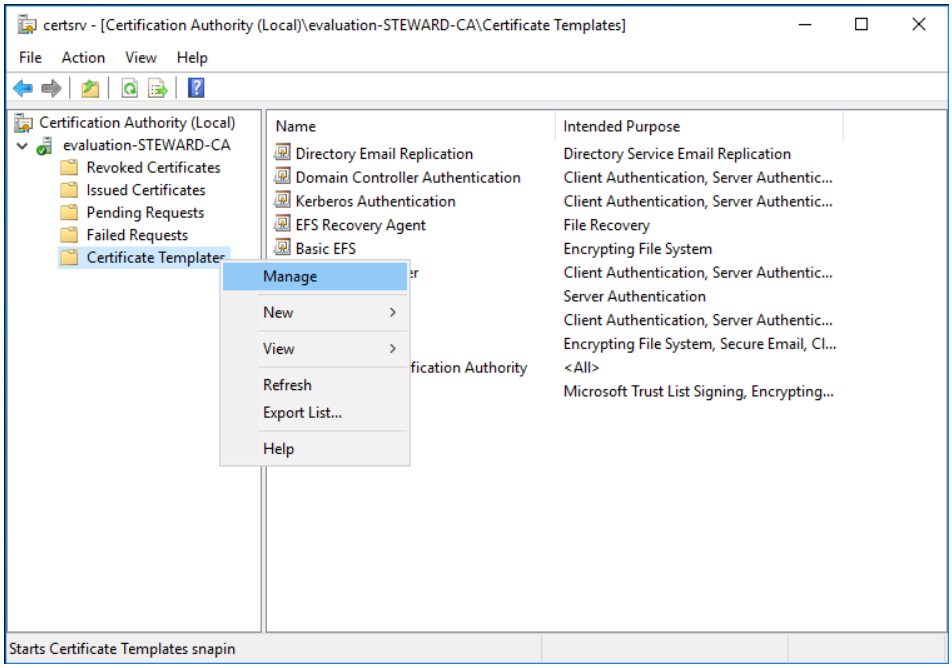


Figure 72 Manage Certificate Templates

26. When "Manage" is selected, the “Certificate Templates Console” screen shown below will be displayed.

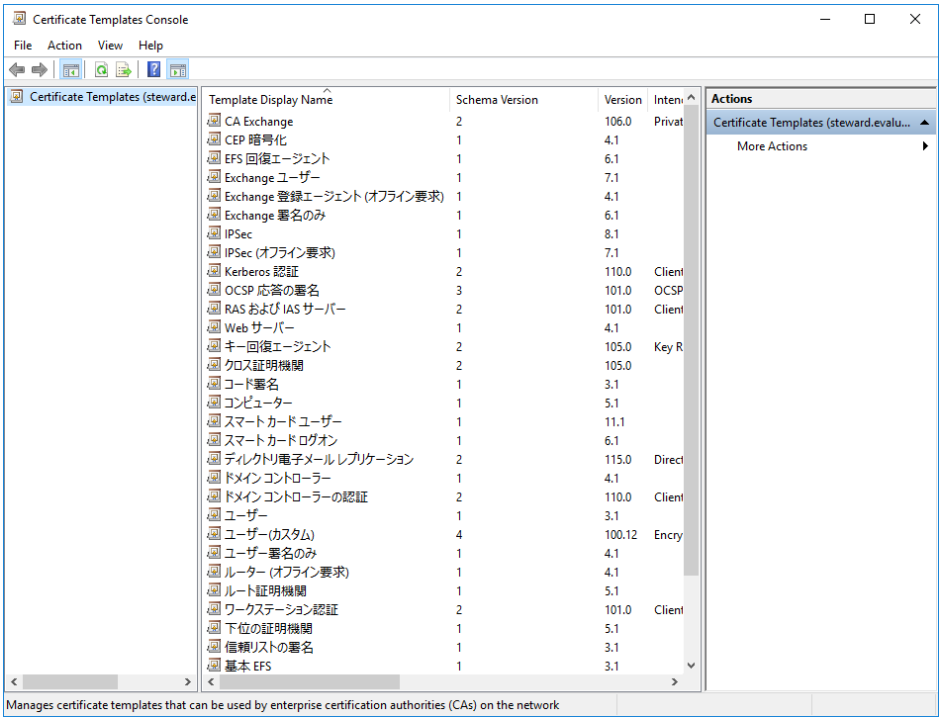


Figure 73 Certificate Templates Console

27. When the “Certificate Templates Console” screen is displayed, click the right mouse button on "User" in the right pane. When the pop-up menu appears, choose “Duplicate Template”.

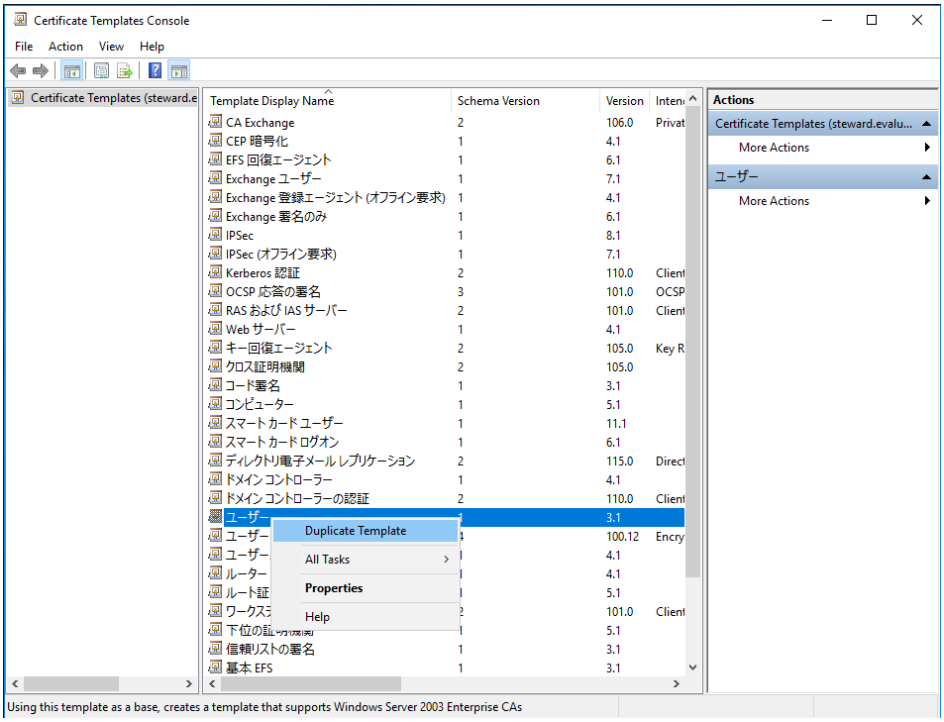


Figure 74 Duplicate Template

28. When “Duplicate Template” is selected, the “Properties of New Template” screen as shown below will be displayed. Select “Compatibility” tab, and select the template version you need according to your usage environment.

Figure 75 Properties of New Template - Compatibility

29. Next, select the "General" tab and enter any name (in this example, User(Custom) and User(Custom)) in "Template Display Name" and "Template Name" respectively. Change the validity period and renewal period if necessary.

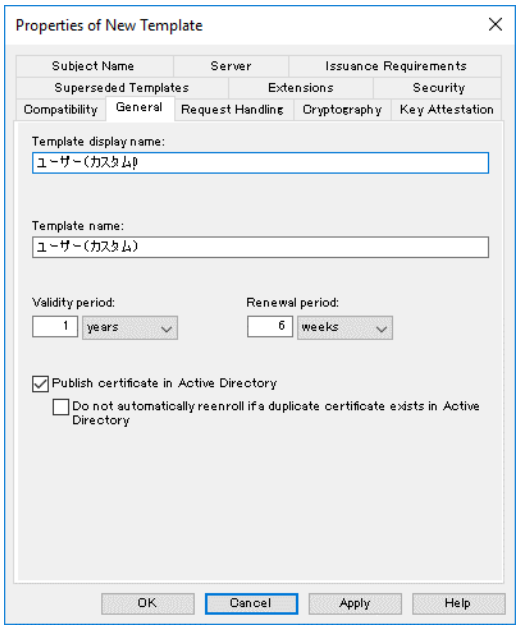


Figure 76 Properties of New Template - General

30. Next, after selecting the "Cryptography" tab, set the "Minimum key size" to 1024 or less, select the "Requests can use any provider available on the subject's computer" radio button, and click the "Apply" button. After that,

click the "OK" button.

Note: If you want to limit the CSP choices available to end users, click the "Requests must use one of the following providers" radio button. In that case, TruCSP must be installed on the server PC in advance. If you wish to use this type of usage, please contact us.

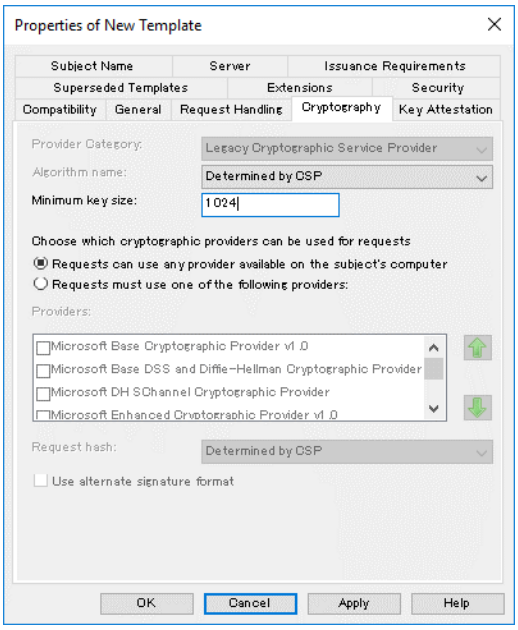


Figure 77 Properties of New Template - Cryptography

31. When you return to the “Certificate Templates Console” screen, select "File" - "Exit" from the menu bar to finish creating the certificate template.

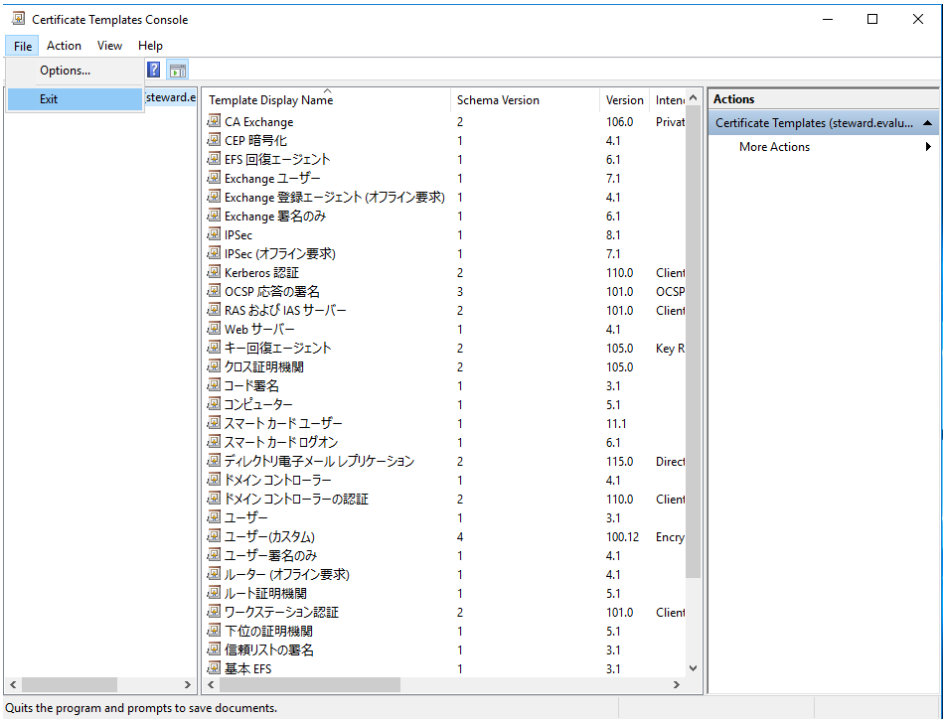


Figure 78 Exit Certificate Templates Console

32. When you return to the “Certification Authority console” screen, click the right mouse button on "Certificate Templates". When the pop-up menu appears, select "New" - "Certificate Template to Issue".

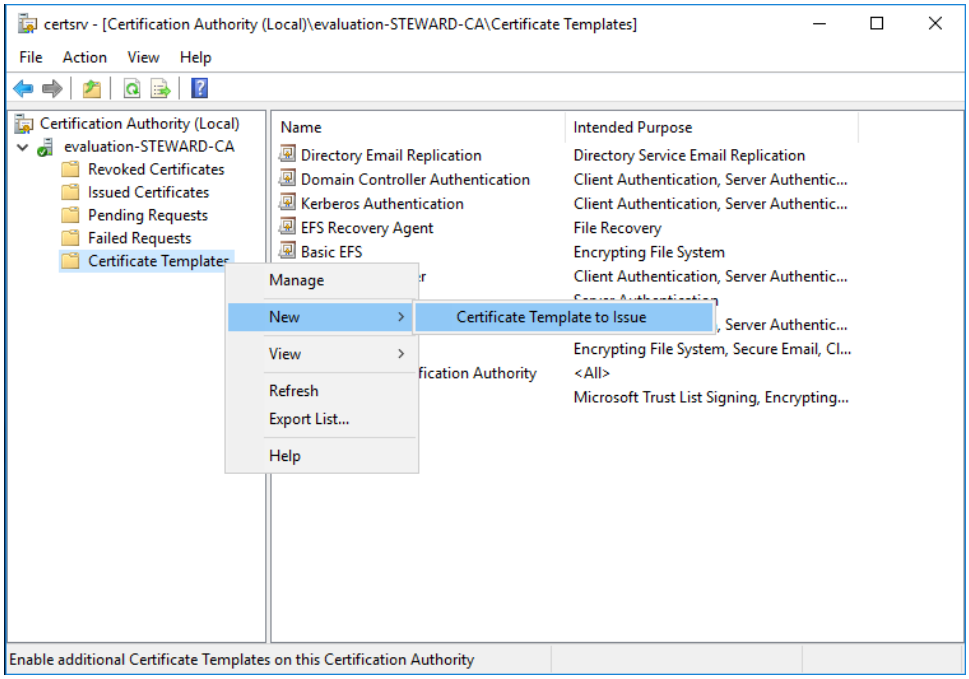


Figure 79 Issue Certificate Template

33. When the “Enable Certificate Templates” screen is displayed, select the

certificate template created earlier (in this example, User(Custom)) and click the "OK" button.

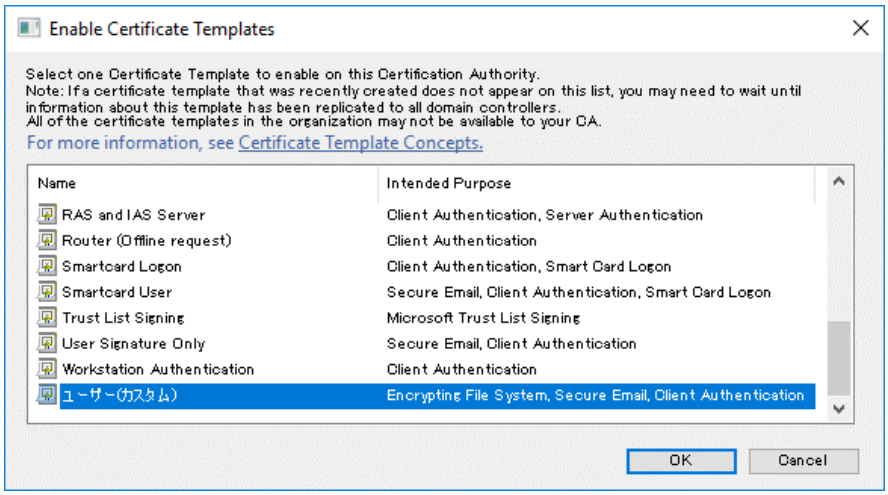


Figure 80 Enable Certificate Templates

34. When you return to the “Certification Authority console” screen, confirm that the certificate template selected in the previous section (in this example, User(Custom)) has been added to the list of issued certificate templates, and select "File" from the menu bar. - Select "Exit" to finish the settings.

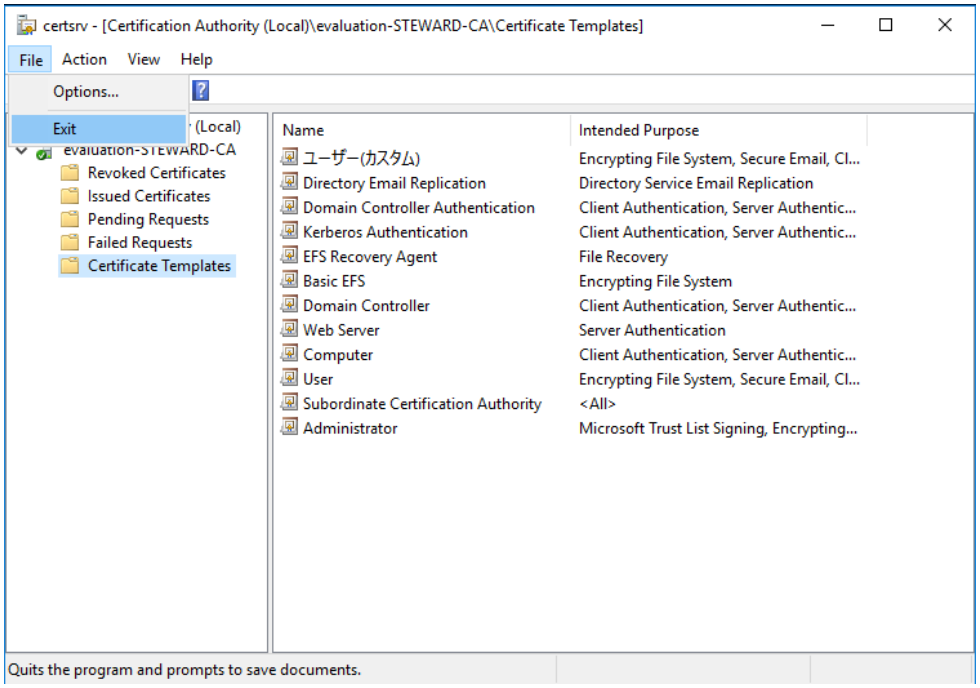


Figure 81 Exit Certification Authority console

2) Request for Certification

1. Log in to the client PC using TruGate, or enable the authentication device if TruStack Gina is not enabled.
2. Launch MMC, open the “Certificates console” file you created earlier, and start the Certificate console.

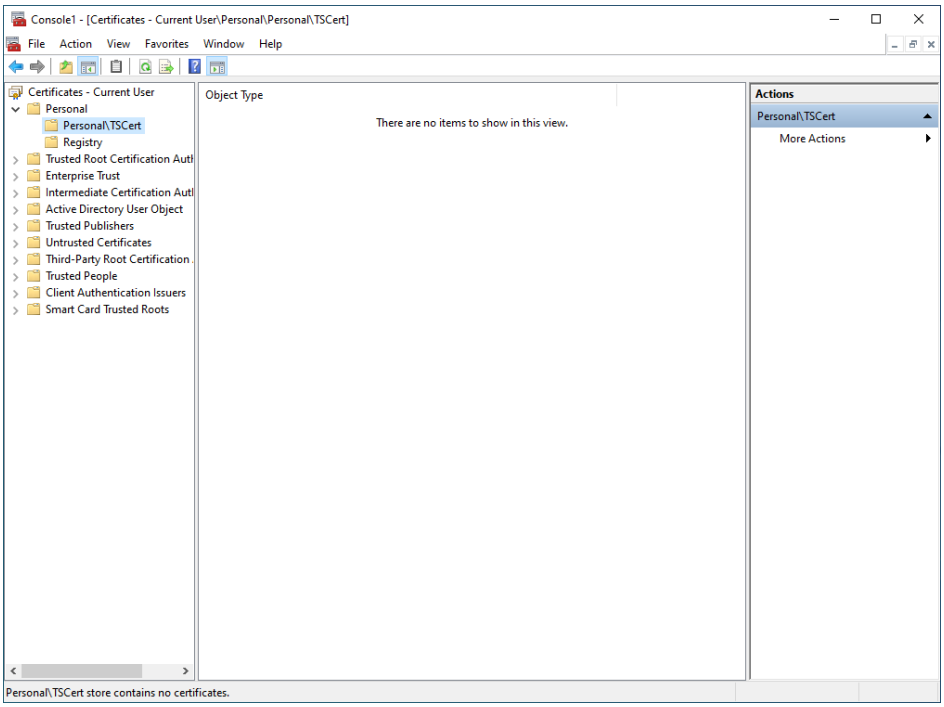


Figure 82 Launch Certificates console

3. When the “Certificate console” starts, right-click on "TSCert" in the left pane, and when the pop-up menu appears, select "All Tasks" - "Request a New Certificate…".

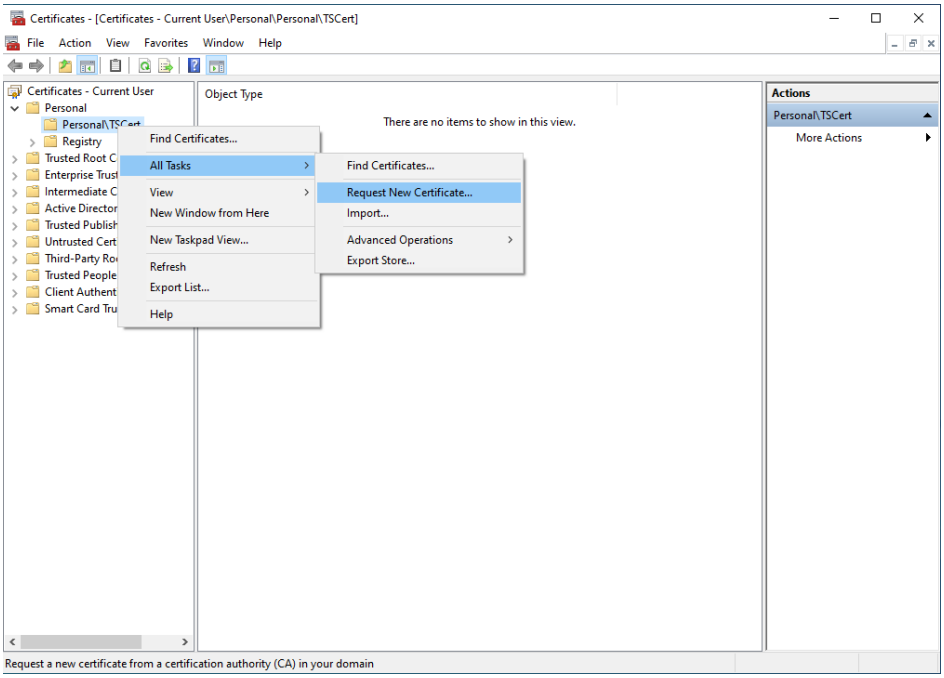


Figure 83 Request New Certificate

4. Follow the steps below to register the certificate.

   (a) When the "Before You Begin" page appears, check the contents and click the "Next" button.

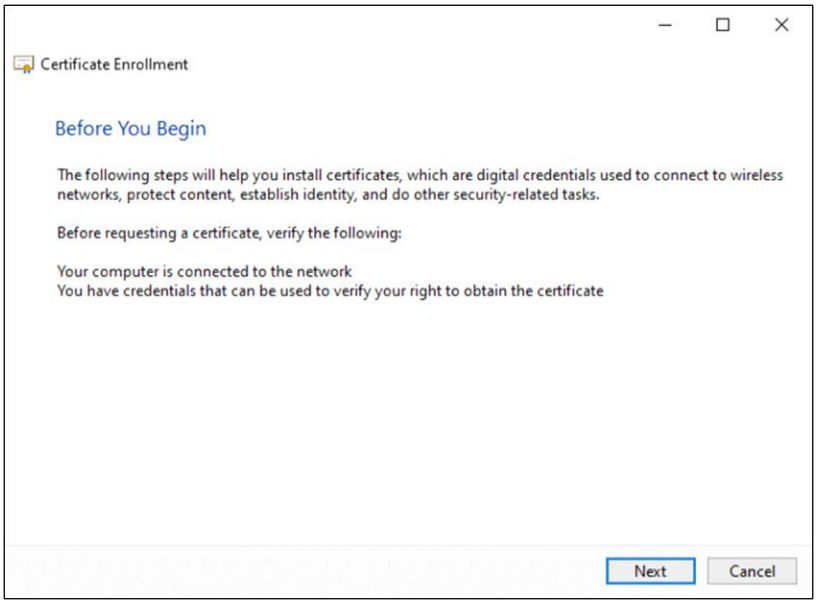


Figure 84 Certificate Enrollment – Before You Begin

   (b) When the "Select Certificate Enrollment Policy" page appears, click the "Next" button.

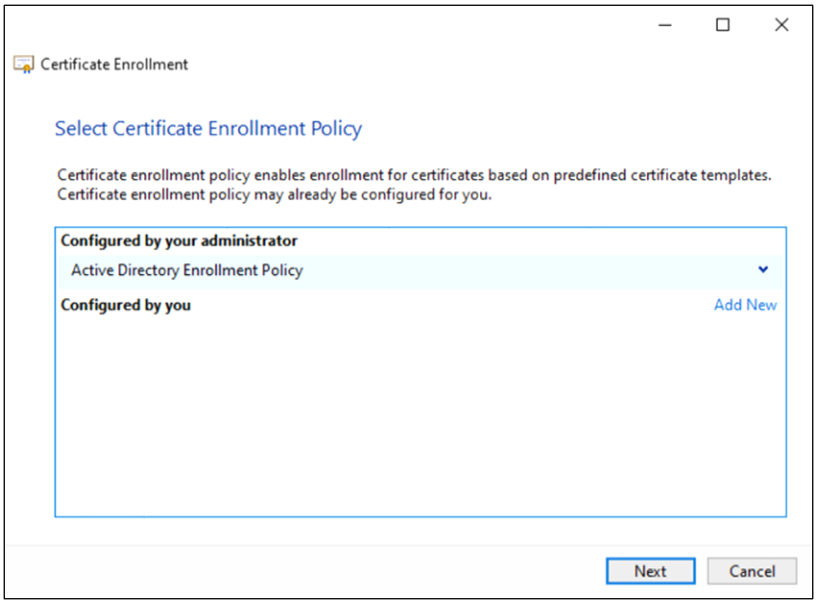


Figure 85 Certificate Enrollment – Select Certificate Enrollment Policy

(c) Next, when the " Request Certificates" page is displayed, first select the certificate template newly issued by the CA (in this example, "User(Custom)"), and then click the "Details" button. .

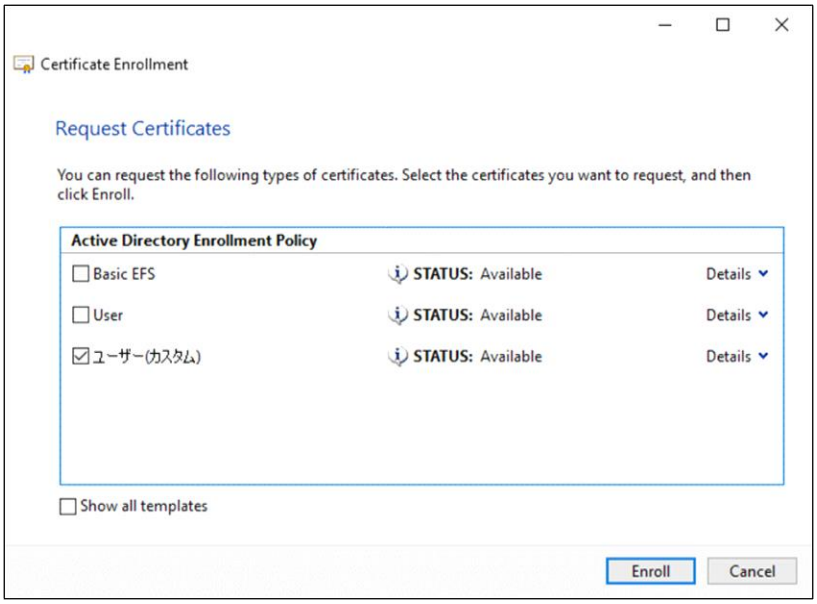


Figure 86 Certificate Enrollment – Request Certificates

(d) When the details of "User(Custom)" are expanded, click the "Properties" button.

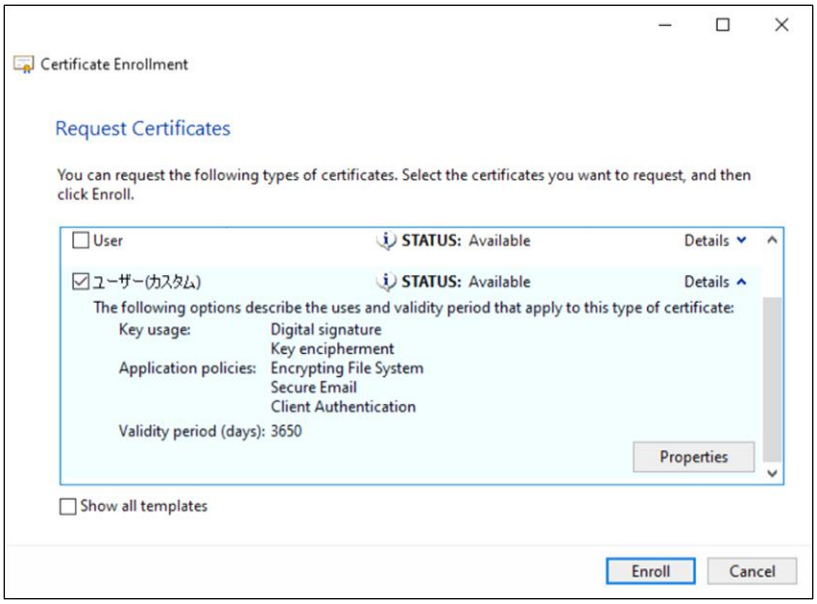


Figure 87 Certificate Enrollment – Details

(e) When the “Certificate Properties” screen appears, click the “Private Key” tab.

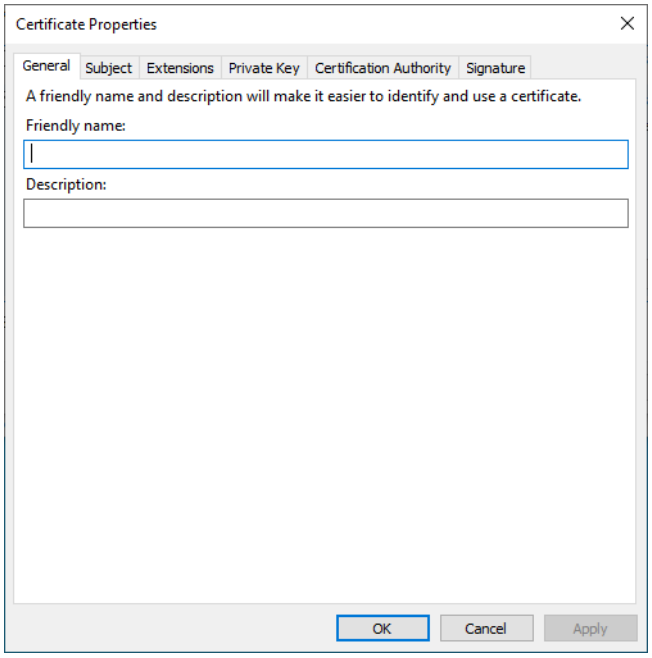


Figure 88 Certificate Properties

(f) When the “Private Key” page appears, click the "Cryptographic Service Provider" bar to display the cryptographic service provider selection screen. Check the "TruStack Cryptographic Provider v1.0" checkbox and uncheck all other cryptographic service provider

checkboxes.

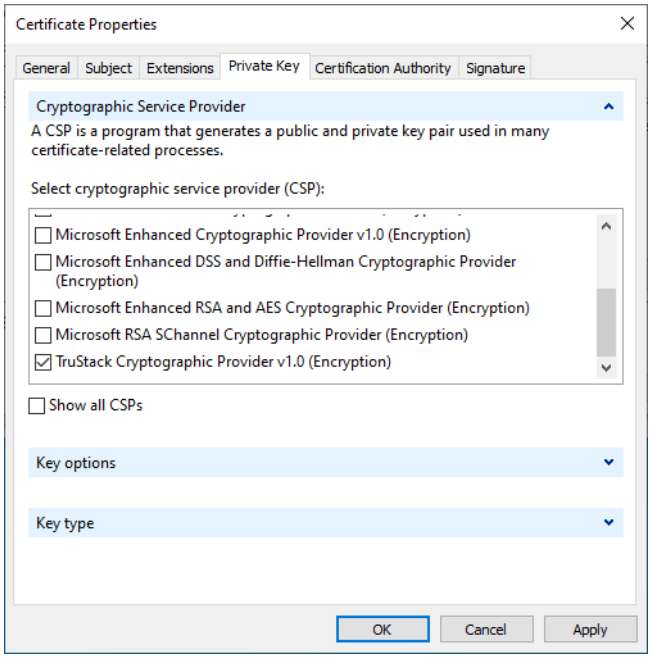


Figure 89 Certificate Properties – Private Key

(g) Next, click on the "Key Options" bar to display the options, then set "Key Size" to 1024 or less, and check the "Make private key exportable", "Allow private key to be archived", and "Strong private key protection" checkboxes. Click the "OK" button.

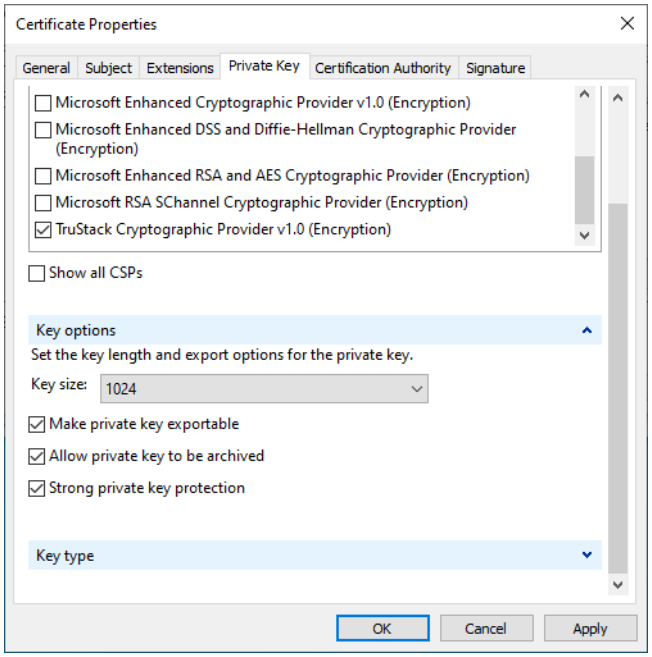


Figure 90 Key Options

(h) When you return to the “Request Certificates” page, click the “Enroll” button.

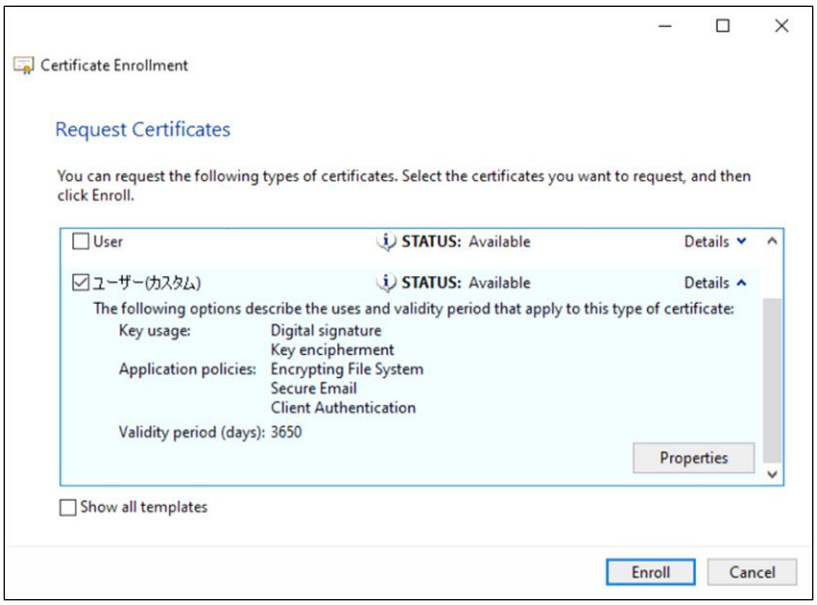


Figure 91 Enroll Certificate

(i) When enrollment is executed, a “Certificate Installation Results” page is displayed. When the certificate enrollment is successfully completed, a success message will be displayed in "Status" as shown in the figure below. Finally, click the "Finish" button to finish.

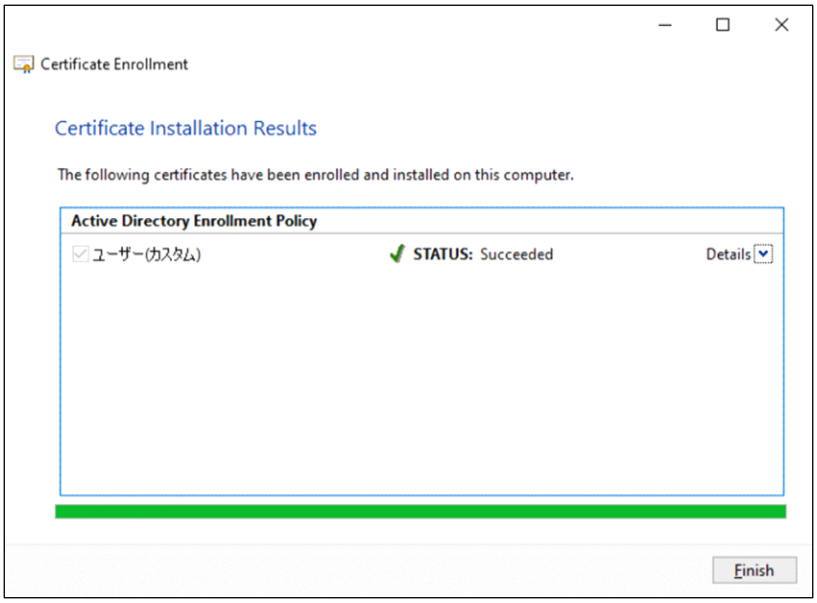


Figure 92 Certification Installation Results

Note: If an error occurs, check the status of the authentication device,

connect the authentication device, initialize the storage area, etc. (see What to do when a certificate request error/import error occurs), and then Please request the certificate again.

5. When you return to the “Certificates console”, confirm that the requested certificate has been generated in the "Active Directory User Objects" - "User Certificates" - "Certificates" folder.

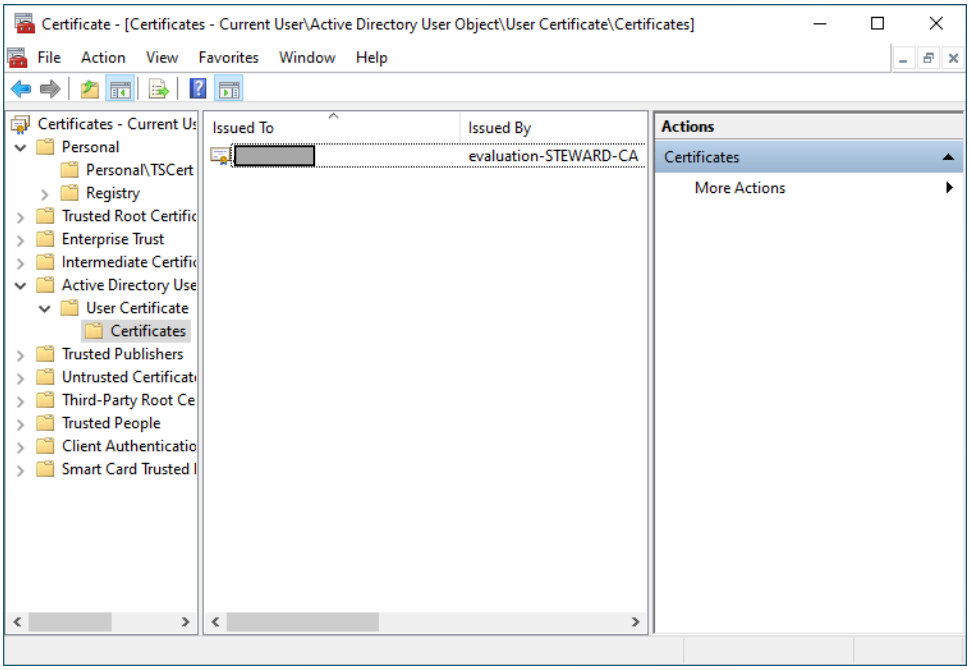


Figure 93 Confirm Generated User Certificate - AD

6. Similarly, confirm that the certificate is displayed in the "Personal" - "TSCert" - "Certificate" folder.

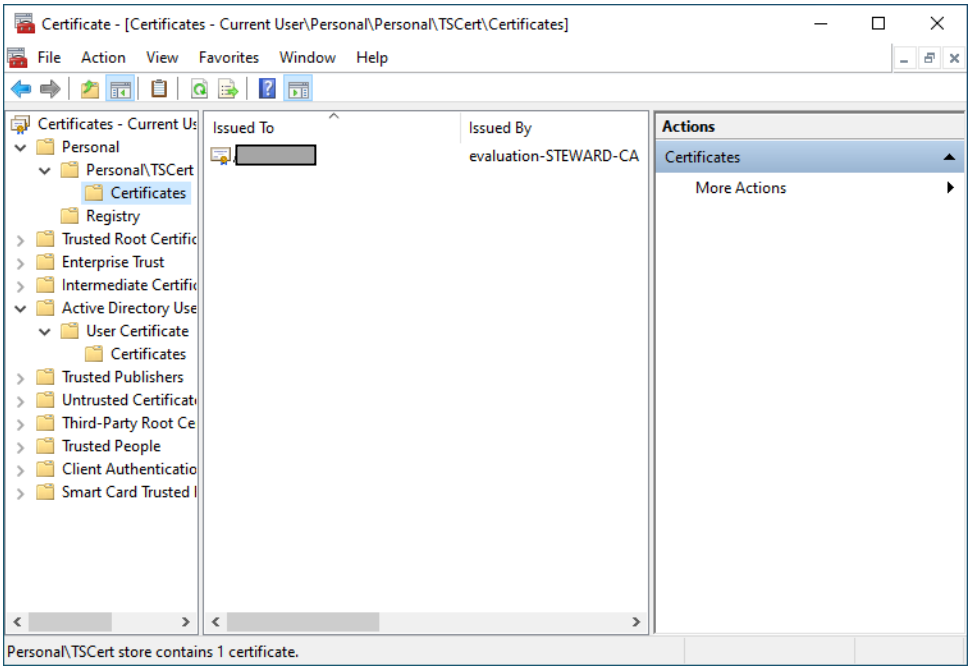


Figure 94 Confirm Generated User Certificate - Personal

7. Once confirmed, select "File" - "Exit" from the “Certificate console” screen to exit.

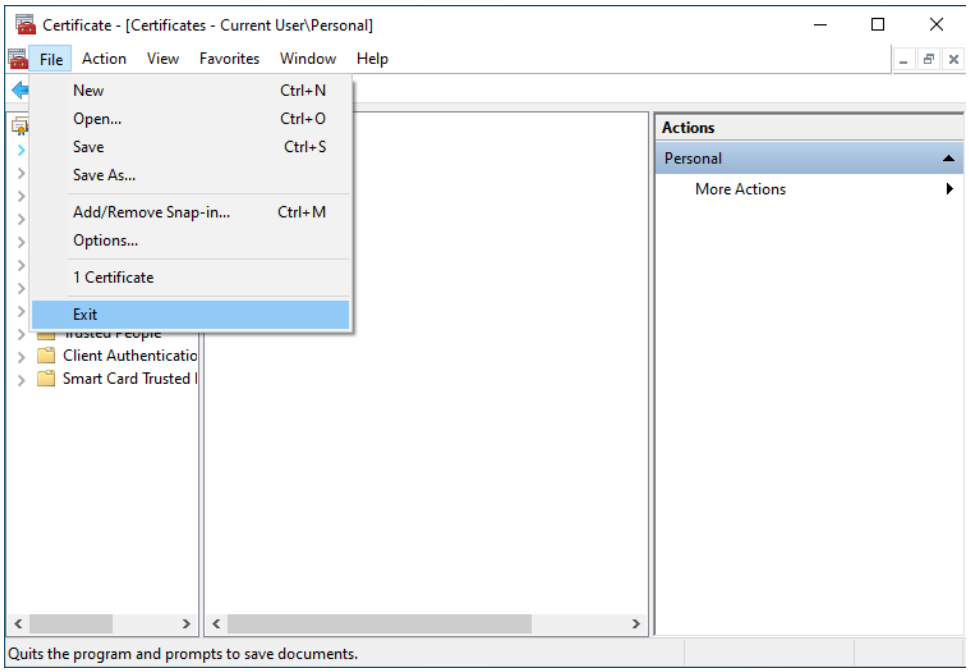


Figure 95 Exit Certificate console

d. How to apply TruCSP to Application

The following is an example of how to configure Outlook Express to use a certificate obtained by specifying TruCSP as the CSP type in an application.

1. Please log on at TruGate.
2. Start Outlook Express and select "Tools" - "Accounts" from the menu bar.

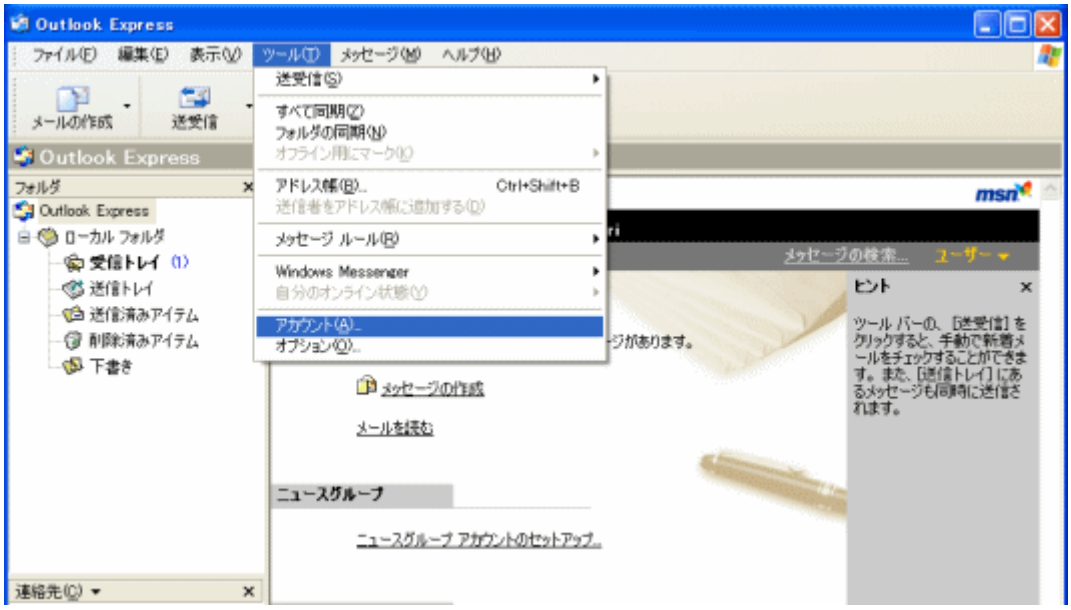


Figure 96 Launch Outlook Express

3. When the Internet Accounts screen shown below appears, select the "Mail" tab.

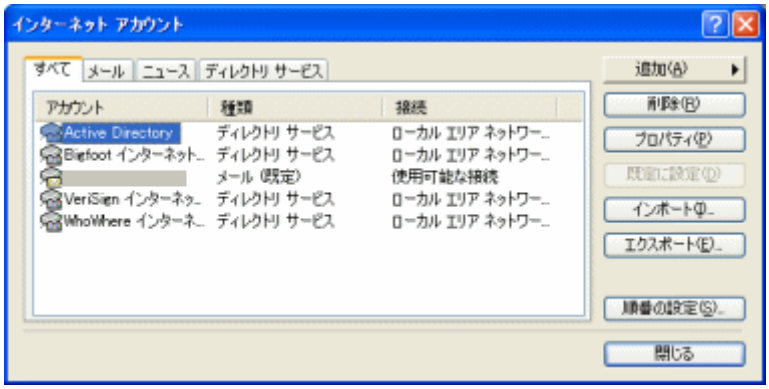


Figure 97 Internet Accounts Dialog

4. When the content of the Internet Accounts screen changes to Mail, select the account that uses the electronic certificate and click the "Properties" button.

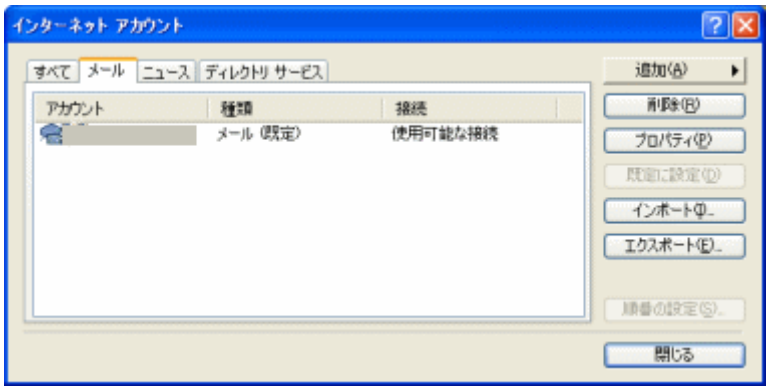


Figure 98 Show Mail Account

5. Next, when the email account properties screen appears, select the Security tab.

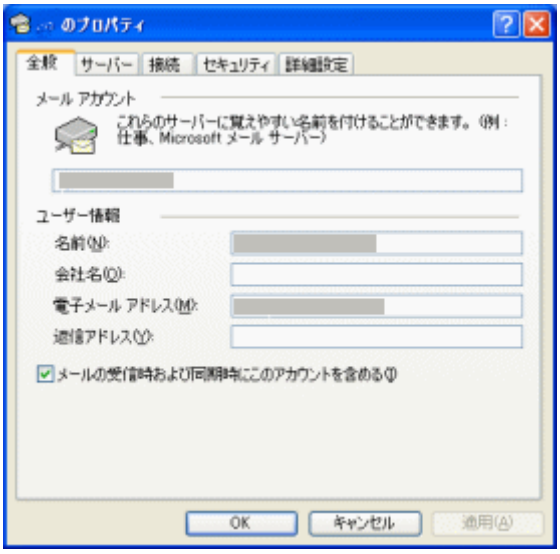


Figure 99 Mail Account Property

6. When the email account properties screen changes to security, click the "Select" button for "Signing Certificate".

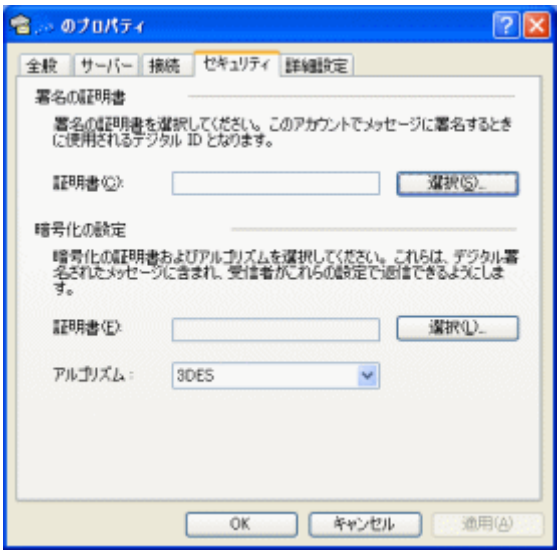


Figure 100 Security – Signing Certificate

7. Next, when the certificate selection screen shown below is displayed, select the digital certificate obtained by specifying TruCSP as the CSP type, and click the "Show Certificate" button.

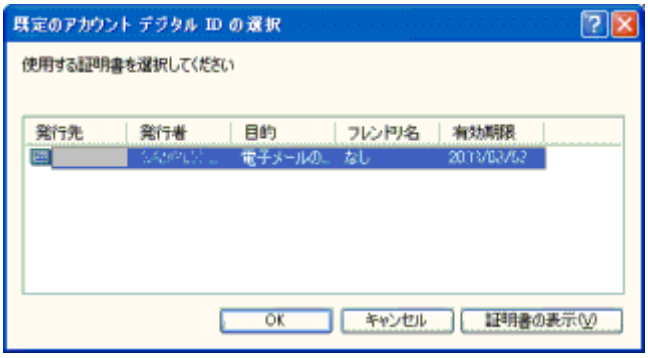


Figure 101 Select Certificate

8. When the certificate information screen shown below is displayed, confirm that it is the correct certificate and click the "OK" button. Please check carefully if you have multiple certificates installed.

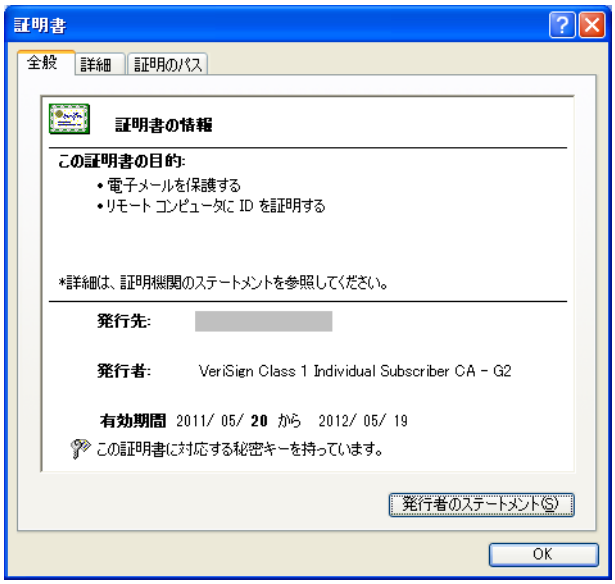


Figure 102 Certificate Information

9. When you return to the email account properties screen shown below, click the "Select" button for "Cryptography Settings".

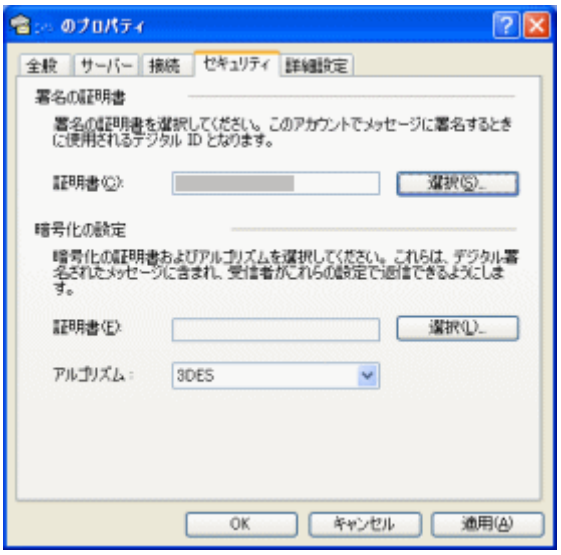


Figure 103 Security – Cryptography Settings

10. Next, when the certificate selection screen shown below is displayed, select the electronic certificate obtained by specifying TSCSP as the CSP type, and click the "OK" button.

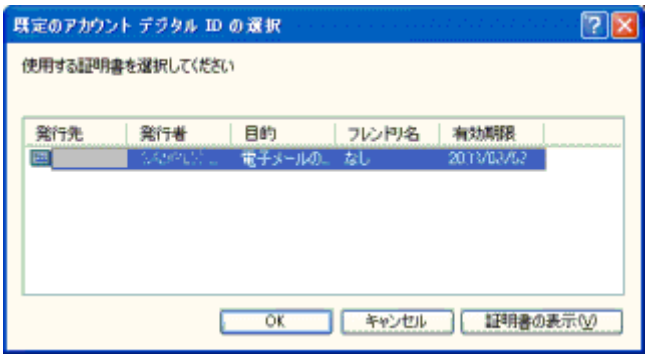


Figure 104 Select Certificate

11. When you return to the email account properties screen shown below, click the "OK" button.

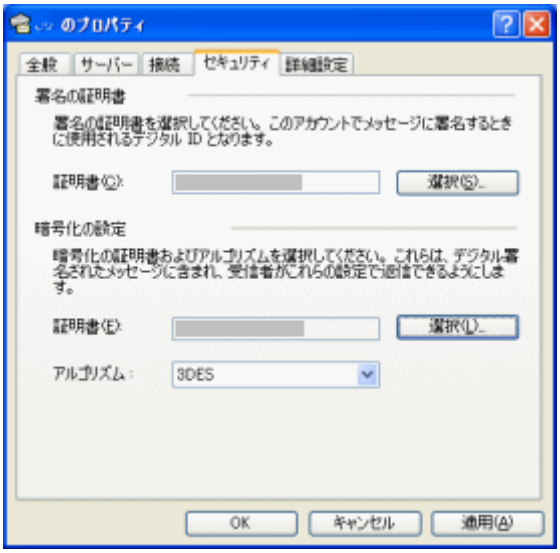


Figure 105 Exit Mail Account Property

12. When you return to the Internet Accounts screen shown below, click the “Close” button to exit.

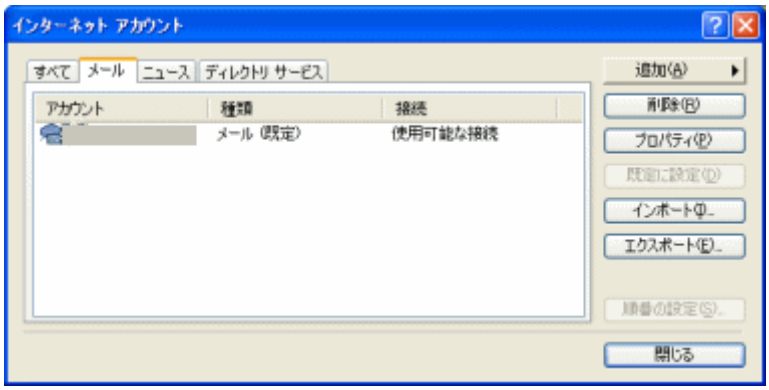


Figure 106 Exit Internet Account Dialog

e. Import Certificate and Public/Private key pair

Please prepare the certificate file (PFX file, etc.) you wish to register in advance. Follow the steps below to import the certificate file into the certificate store.

1. Please log on at TruGate or enable your authentication device if you have not enabled TruStack Gina.
2. Start MMC, open the certificate console file you created earlier, and start the Certificate console.

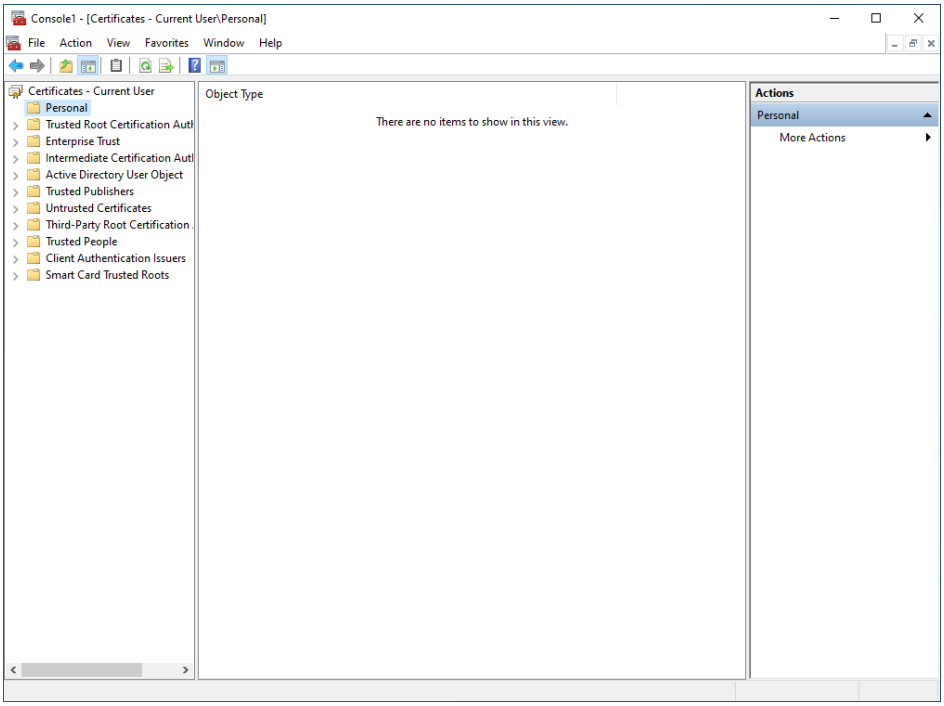


Figure 107 Launch Certificate console

3. Expand “Personal” – “TSCert” in the left pane of the Certificate console and verify that no certificates are displayed in the right pane.

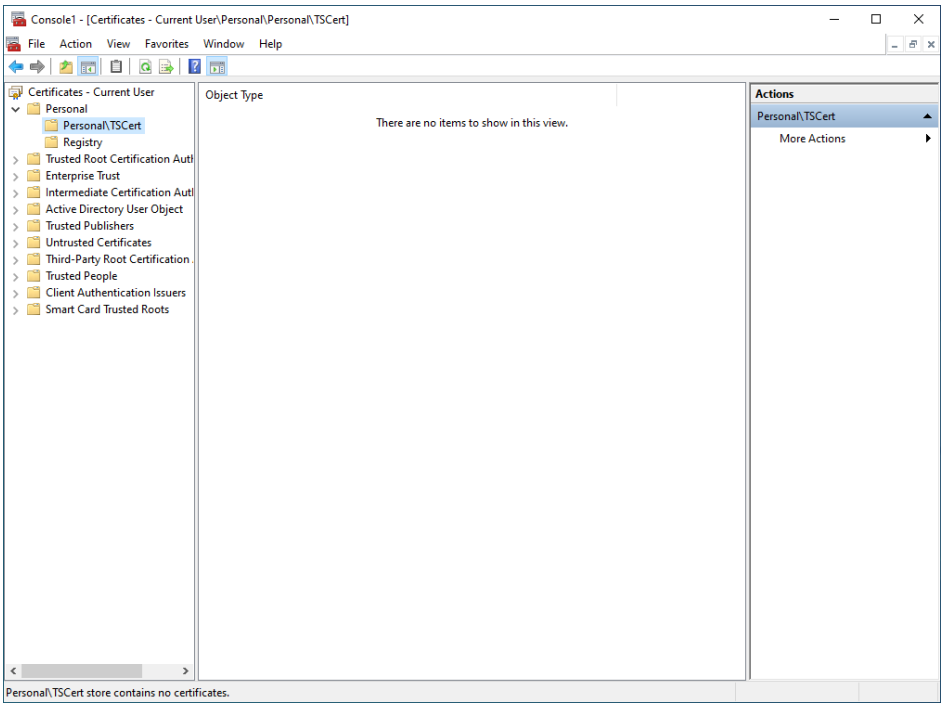


Figure 108 Certificate console – no certificate registered

4. Right-click on "TSCert" in the left pane to display the pop-up menu, and select "All Tasks" - "Import...".

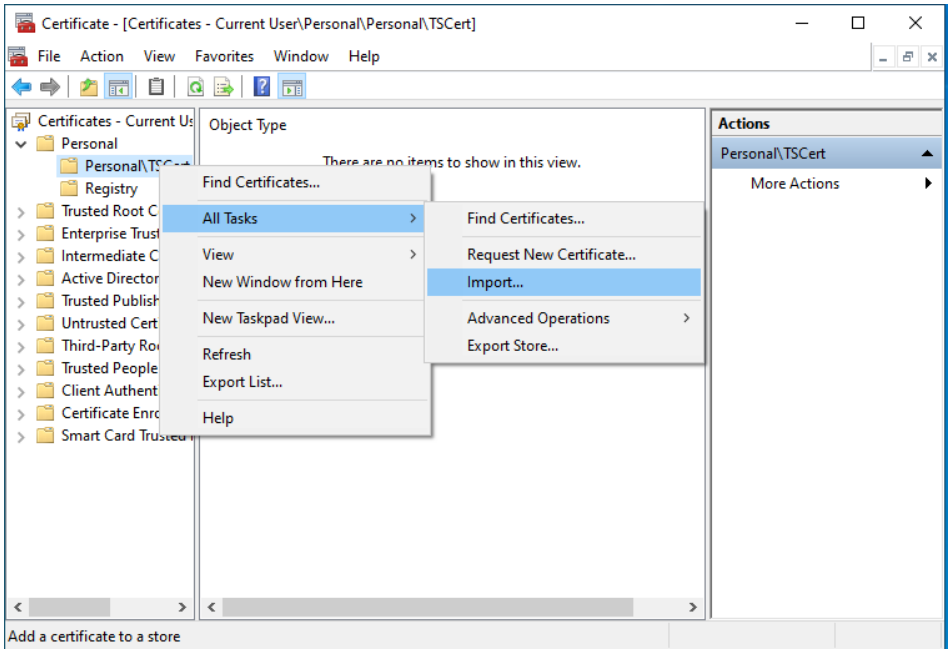


Figure 109 Run Certificate Import

5. Follow the steps below to import the certificate.

   (a) When the Certificate Import Wizard screen appears, click the "Next" button.

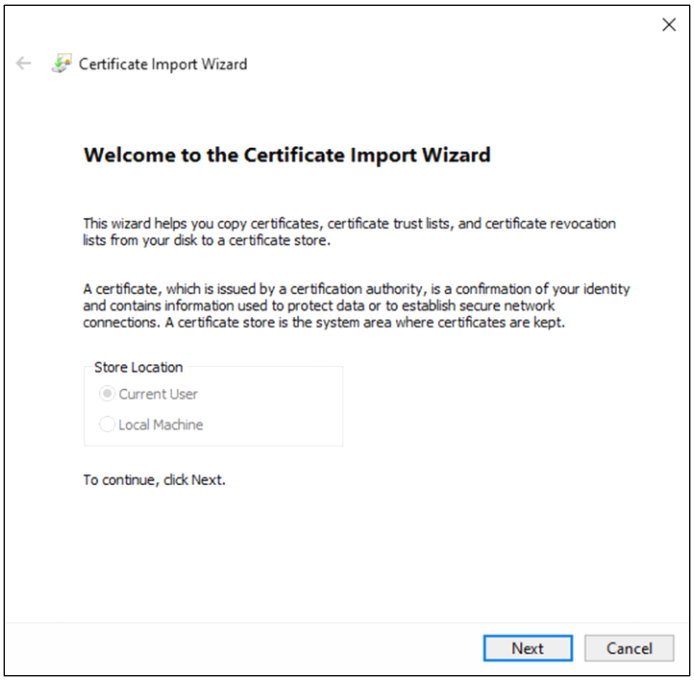


Figure 110 Launch Certificate Import Wizard

(b) When the screen for specifying the certificate file to import is displayed, click the "Browse..." button.

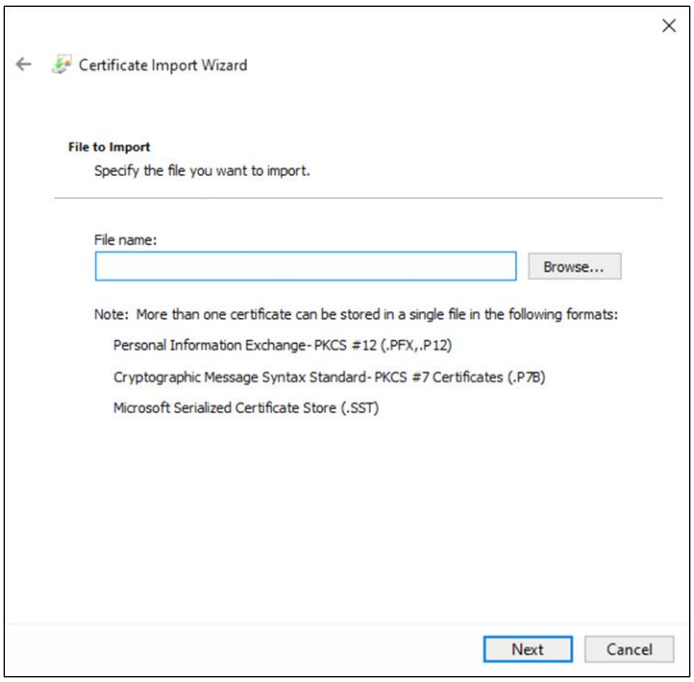


Figure 111 Certificate Import Wizard - File to Import

(c) After specifying the saved pfx file, click the "Open" button.

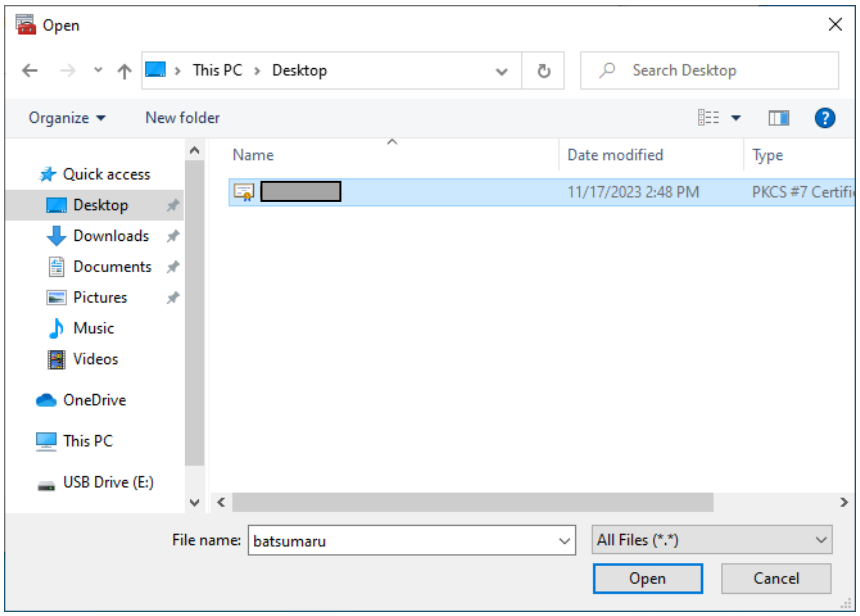


Figure 112 Certificate Import Wizard - Specify Open File

(d) When you return to the screen for specifying the certificate file to import, click the "Next" button.

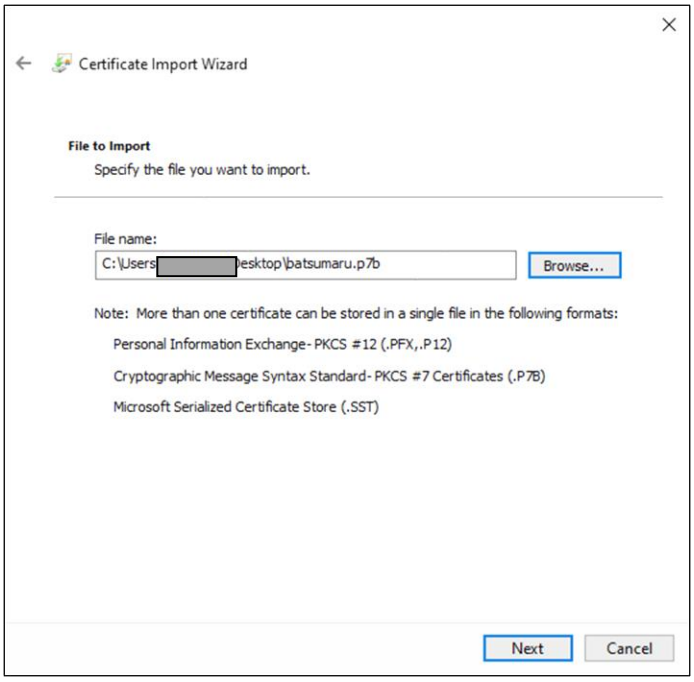


Figure 113 Certificate Import Wizard - Specified File to Import

(e) When the password entry screen appears, enter the password you set during export, check the "Enable strong private key protection" and "Make this key as exportable" checkboxes, and click the "Next" button. Click.

Note: If you import a certificate obtained by specifying a CSP type other than TruStack Crypt Service Provider into TSCert when obtaining the certificate, the public/private key pair will not be stored in TSCSP.

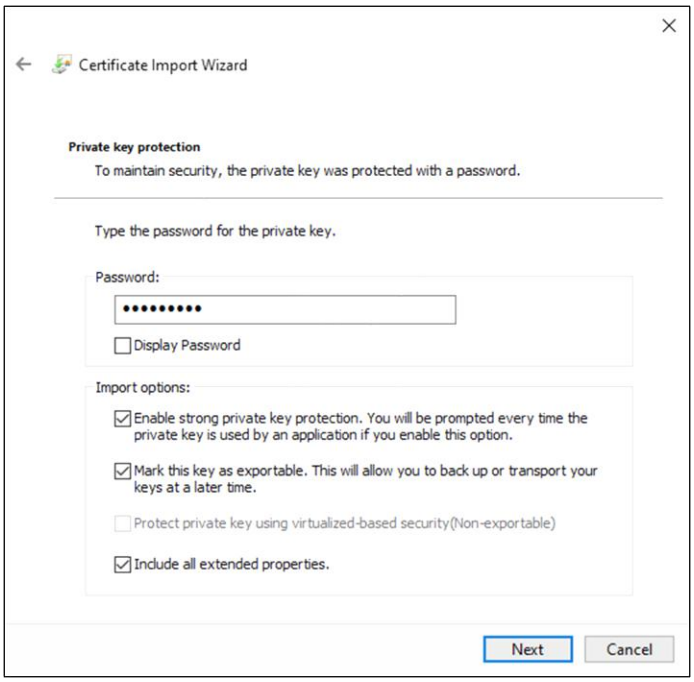


Figure 114 Certificate Import Wizard - Private Key Protection

(f) When the certificate store selection screen appears, select the "Automatically select the certificate store based on the type of certificate" radio button and click the "Next" button.

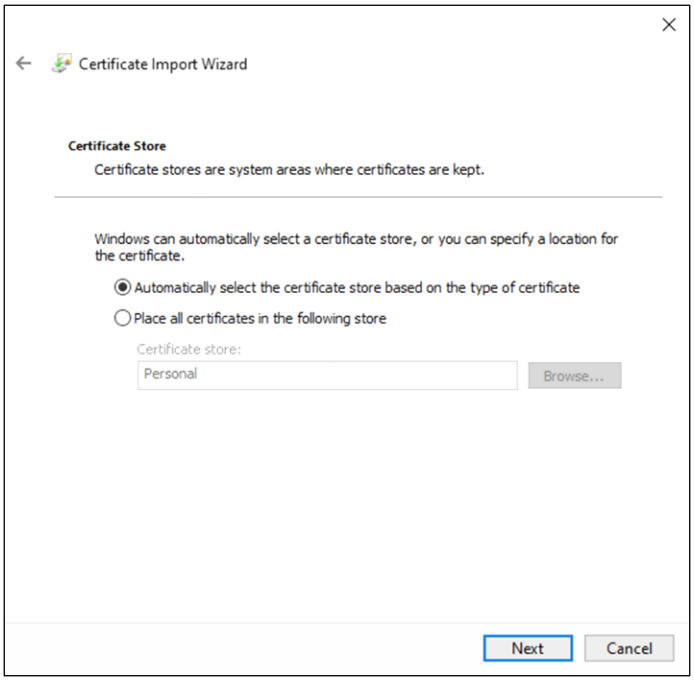


Figure 115 Certificate Import Wizard - Certificate Store

(g) When the Certificate Import Wizard completion screen appears, click the "Finish" button.

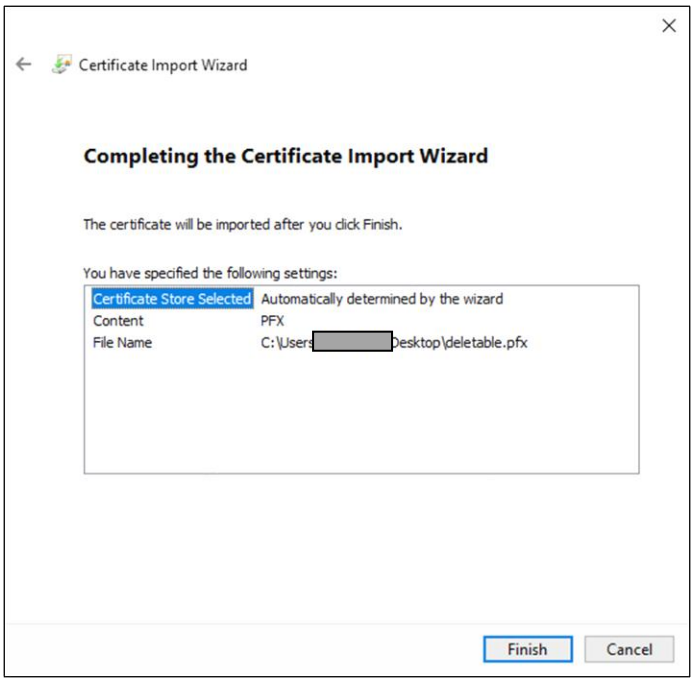


Figure 116 Complete Certificate Import Wizard

(h) If the device authentication screen is displayed, perform device authentication.

(i) If the import is successful, the following screen will be displayed. Click the “OK” button.

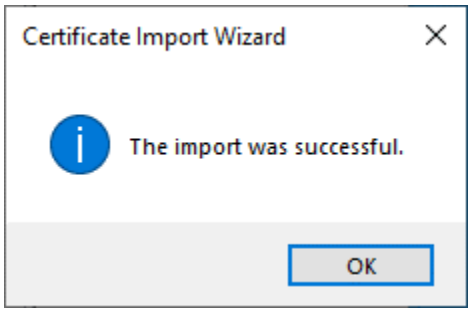


Figure 117 Import Successful

If the storage area of the authentication device used to store the certificate is not blank, the following error message will be displayed.

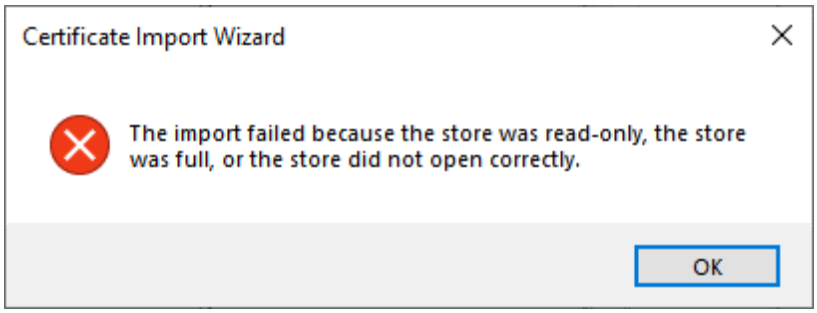


Figure 118 Import Error

Note: When an error message is displayed, check the status of the authentication device and perform tasks such as connecting the authentication device and initializing the storage area (see what to do when a certificate request error/import error occurs). After that, import the certificate again.

6. When the certificate import is finished and you return to the console screen, right-click "TSCert" in the left pane of the certificate console to display the pop-up menu, click "Refresh", and verify the certificate to the right pane is displayed.

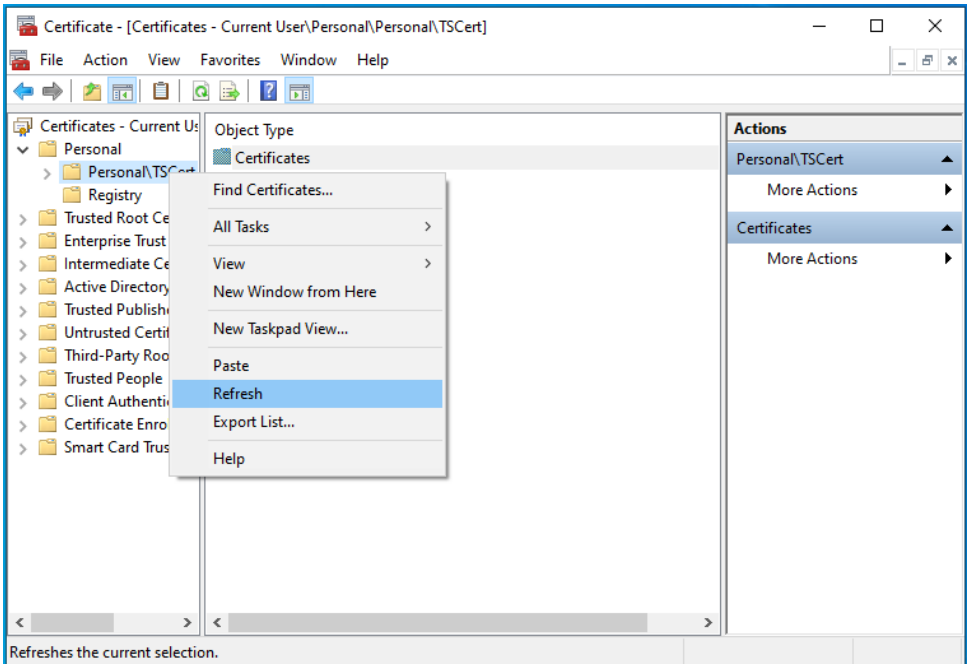


Figure 119 Refresh Certificate console

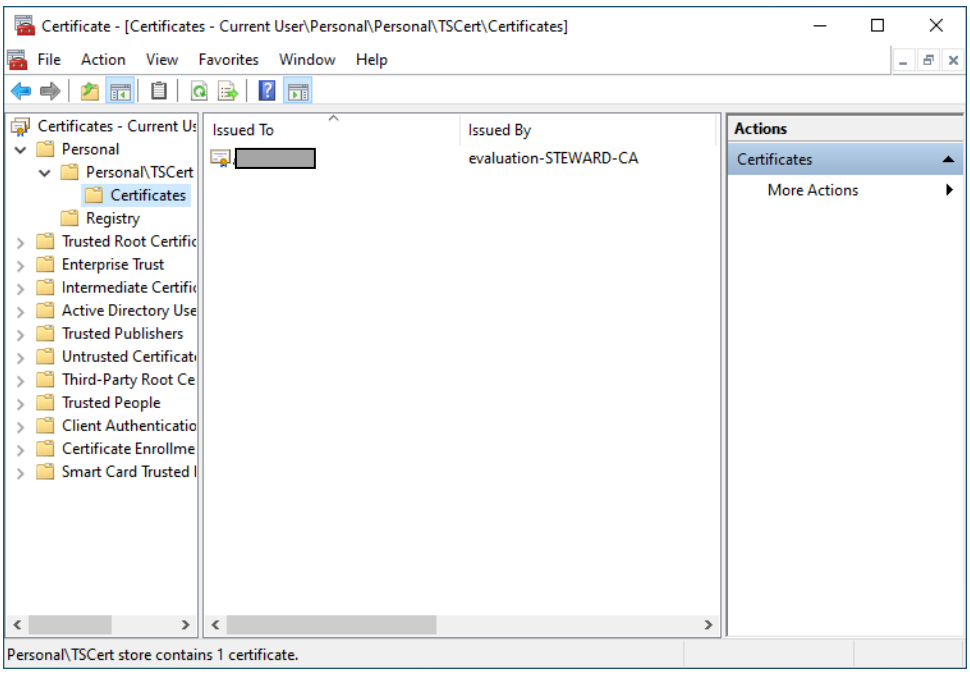


Figure 120 Verify Certificate displayed

7. Once confirmed, select "File" - "Exit" from the Certificate console screen to exit.

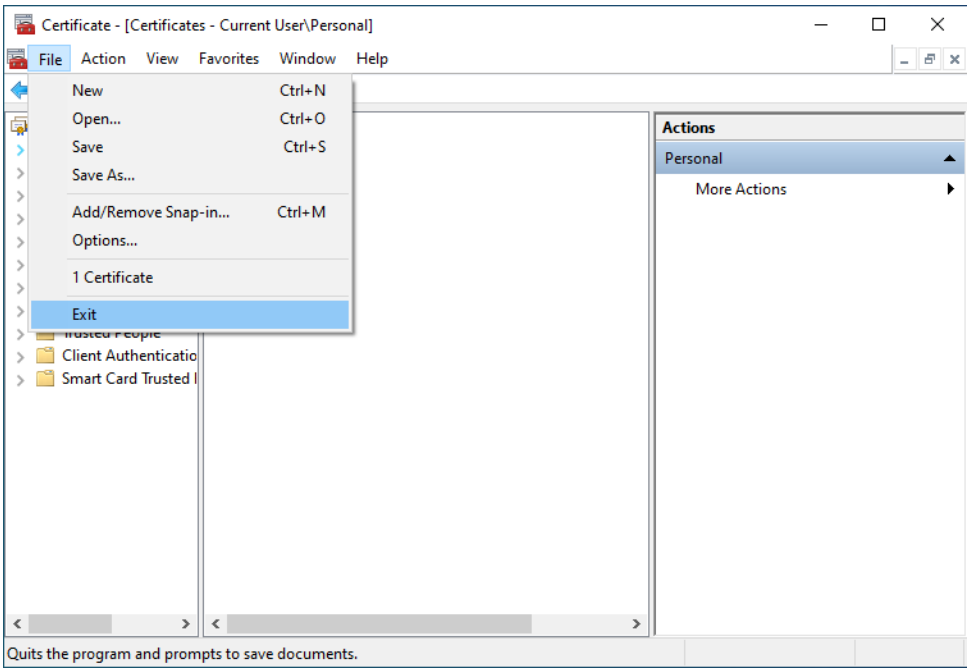


Figure 121 Exit Certificate console

f. Export and Delete Certificate and Public/Private key pair

If you want to delete the public/private key pair registered in the TSCSP storage area with TSCSP, follow the steps below to delete the private key when exporting the registered certificate.

1. Please log on at TruGate or enable your authentication device if you have not enabled TruStack Gina.
2. Start MMC, open the certificate console file you created earlier, and start the Certificate console.

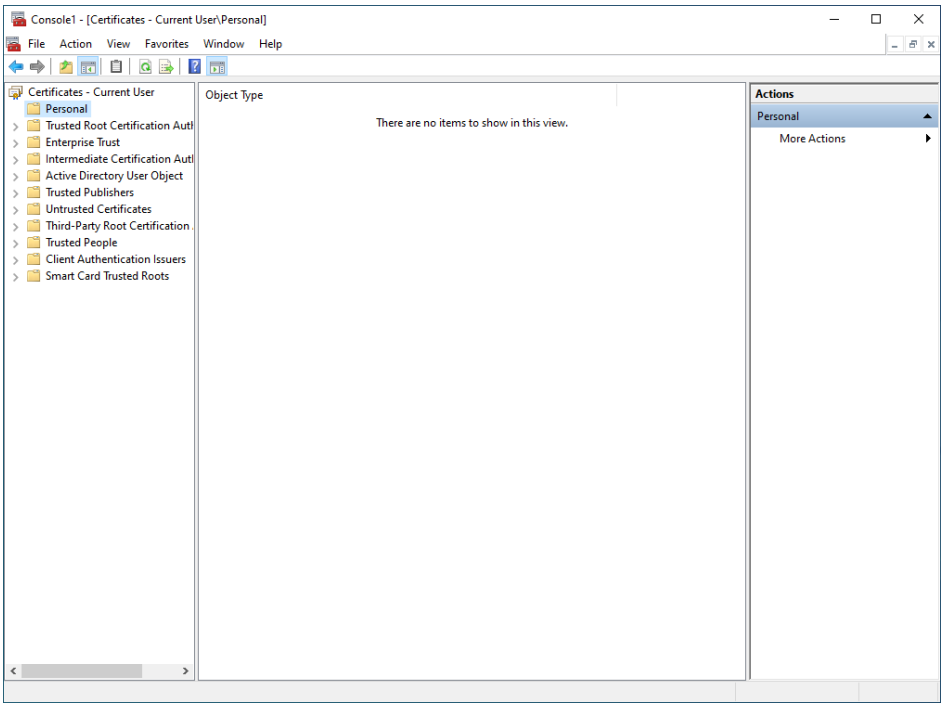


Figure 122 Launch Certificate console

3. Expand the left pane of the Certificate Console so that the right pane displays the certificate containing the key you want to delete.

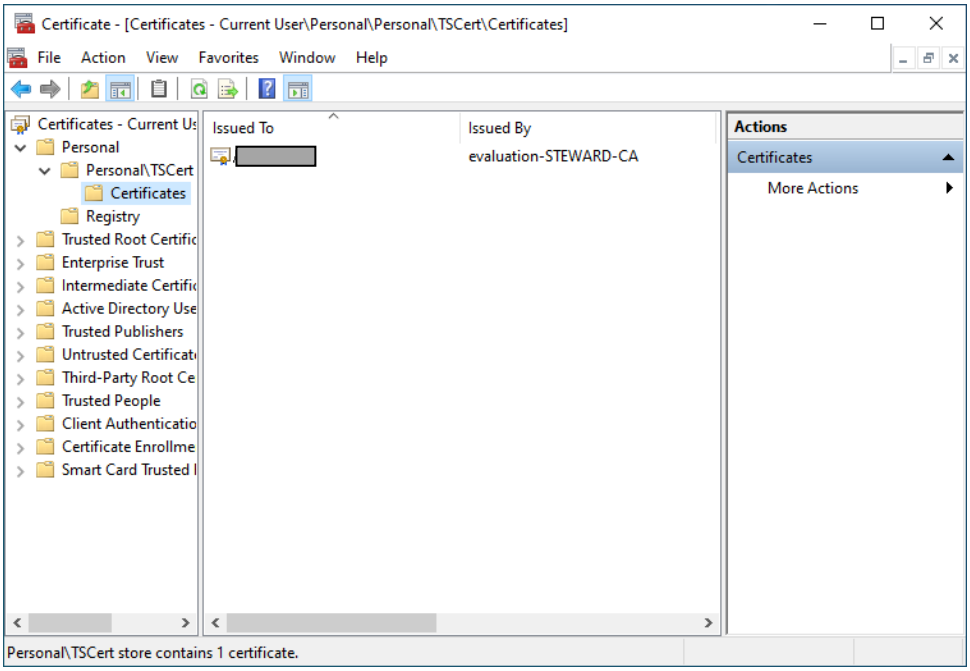


Figure 123 Show Certificate

4. Right-click the certificate to display the pop-up menu, then left-click “All Tasks” – “Export…”.

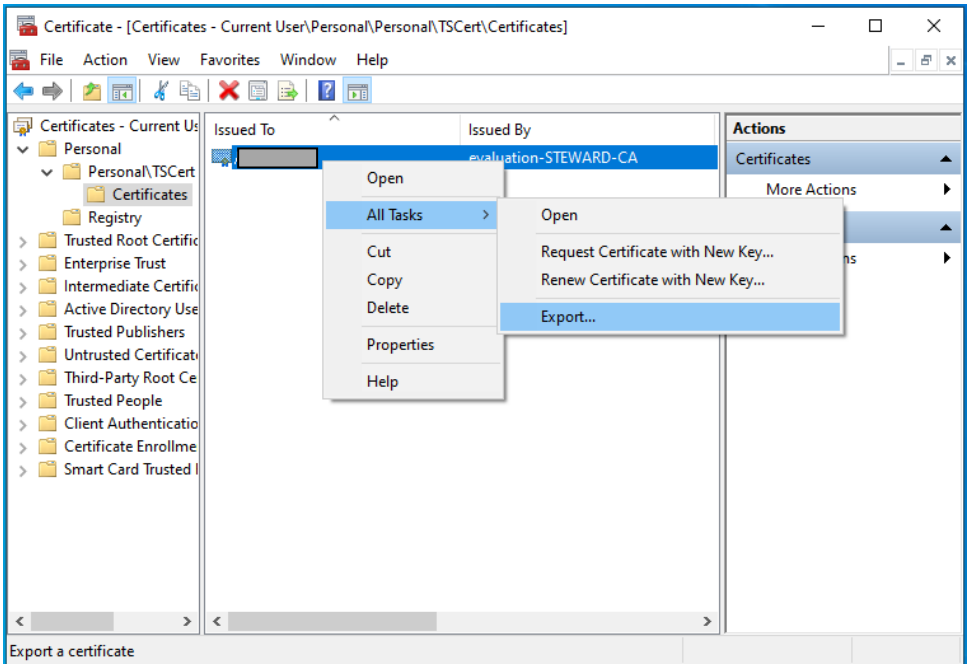


Figure 124 Run Certificate Export

5. Follow the instructions below for the certificate export wizard.
   (a) When the Certificate Export Wizard screen appears, click the "Next" button.

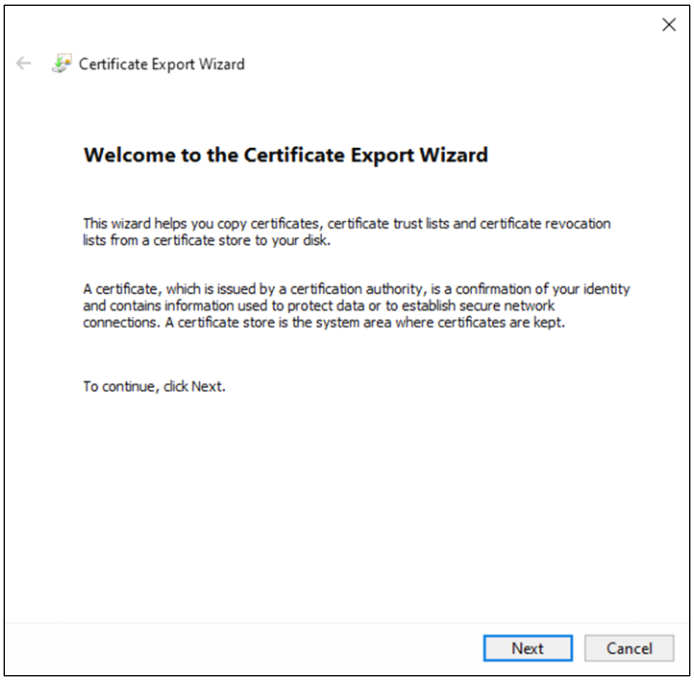


Figure 125 Launch Certificate Export Wizard

(b) In the Export Private Key specification, select the "Yes, export the private key" radio button.

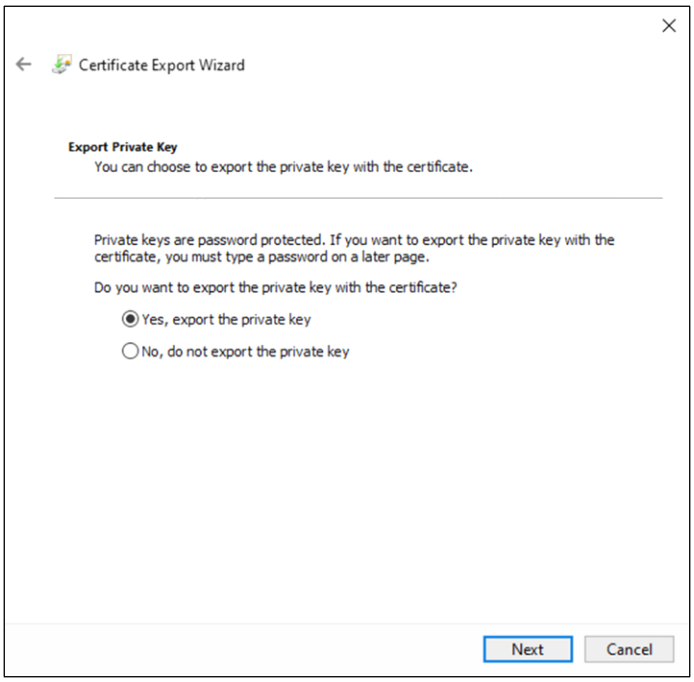


Figure 126 Certificate Export Wizard - Export Private Key

(c) When specifying the export file format, check the "Delete the private key if the

export is successful" checkbox.

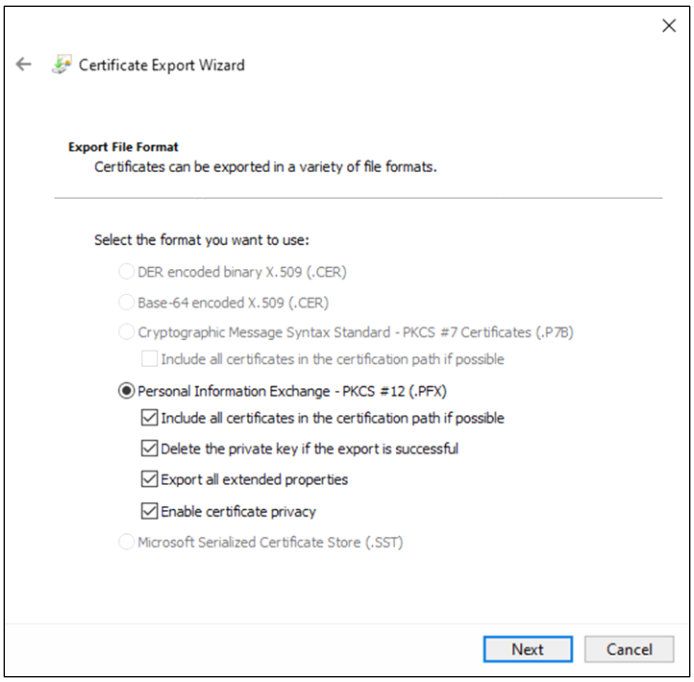


Figure 127 Certificate Export Wizard - Export File Format

(d) Then, when prompted for a password, type the password to protect the private key of the certificate you are exporting.

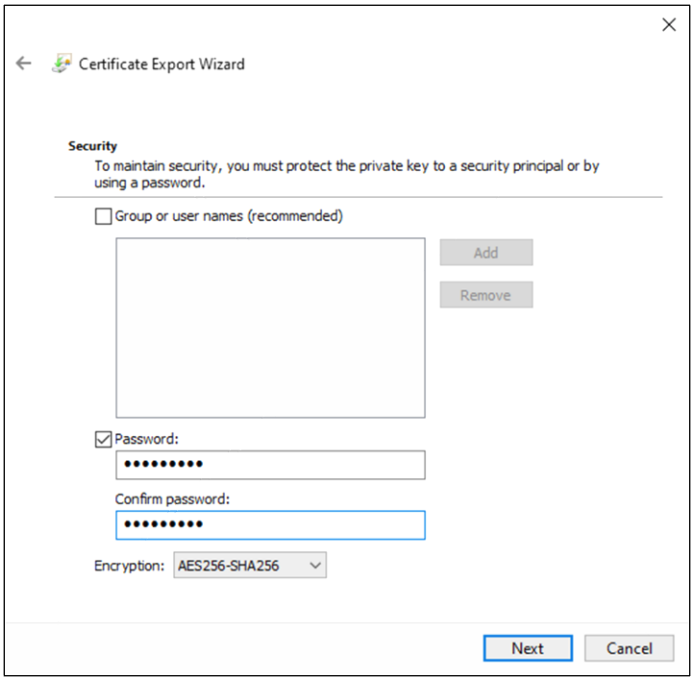


Figure 128 Certificate Export Wizard - Security

(e) Next, when the input screen for the file name to export appears, click the "Browse…" button.

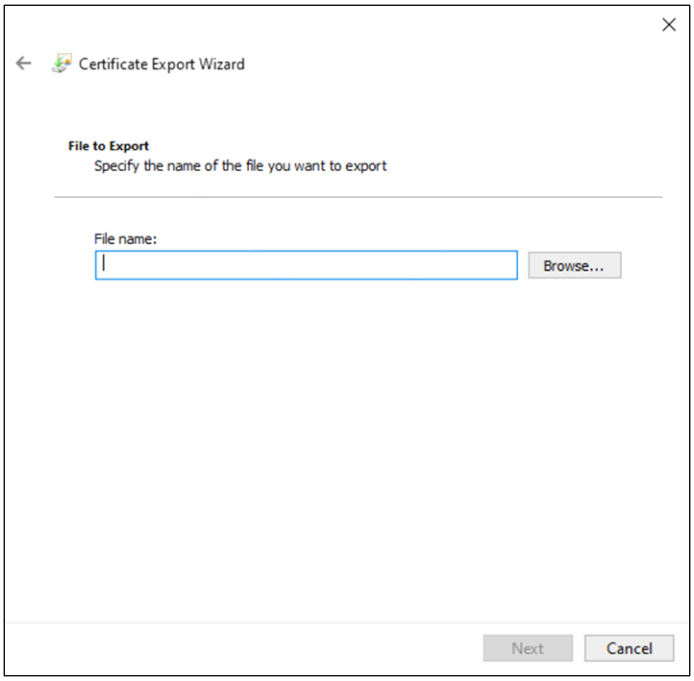


Figure 129 Certificate Export Wizard – File to Export

(f) Next, when the Save As screen appears, type the name of the file you want to export.

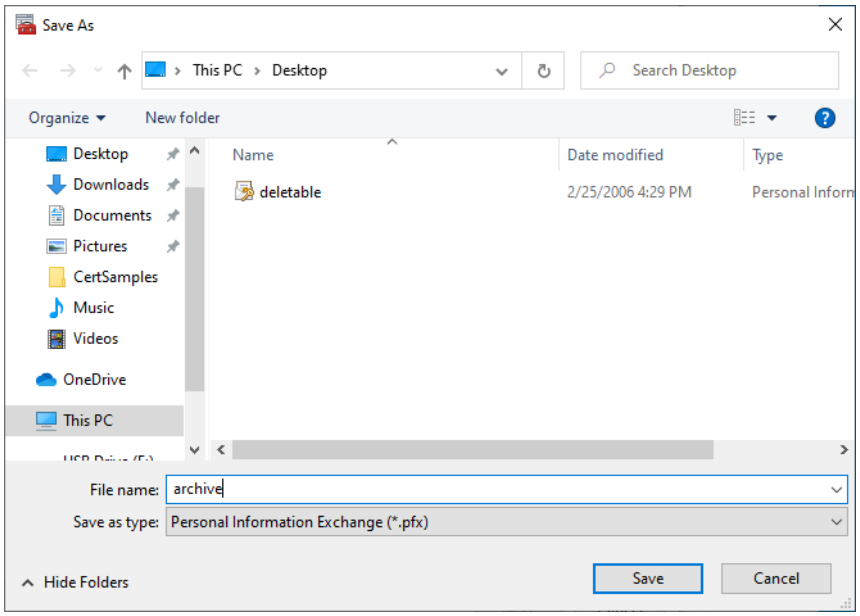


Figure 130 Certificate Export Wizard – Save As

(g) When you return to the screen for entering the file name to export, click the

"Next" button.

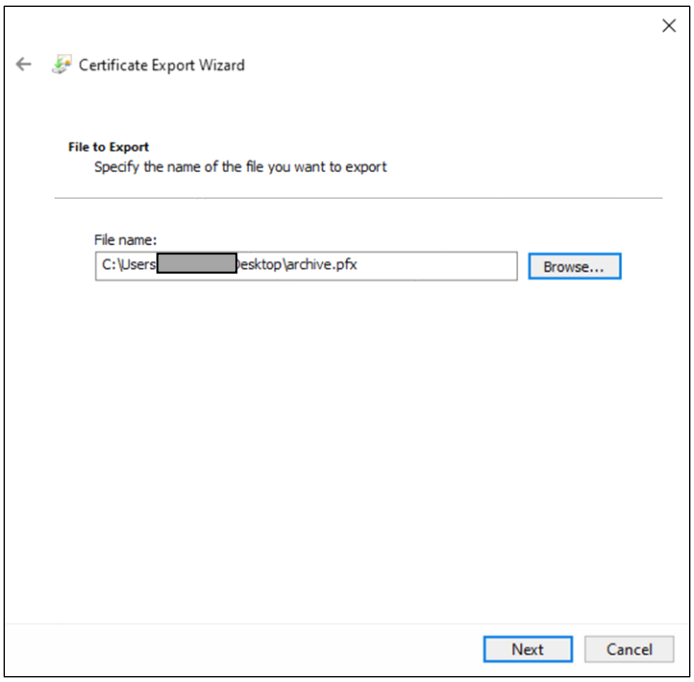


Figure 131 Certificate Export Wizard – Specify File to Export

(h) When the Certificate Export Wizard completion screen appears, click the "Finish" button.

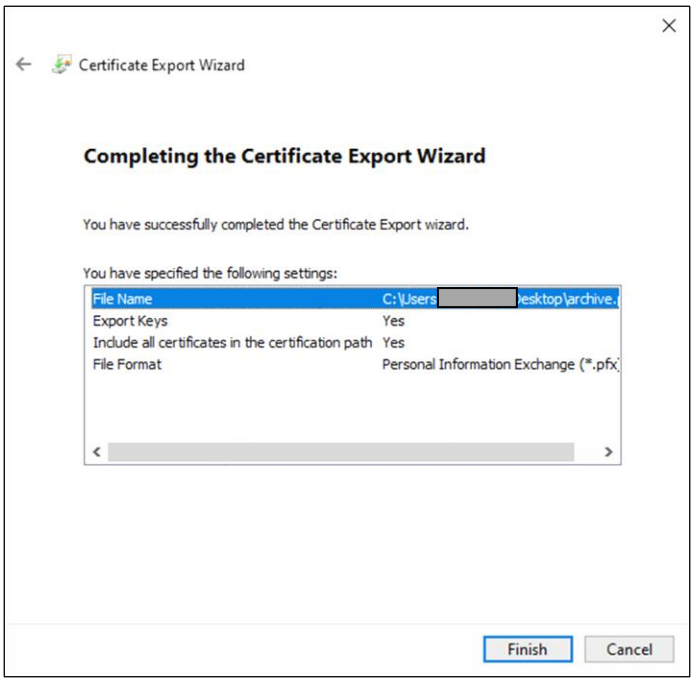


Figure 132 Complete Certificate Export Wizard

(i) If the device authentication screen is displayed, perform device authentication.

(j) If the export is successful, the following screen will be displayed. Click the “OK” button.

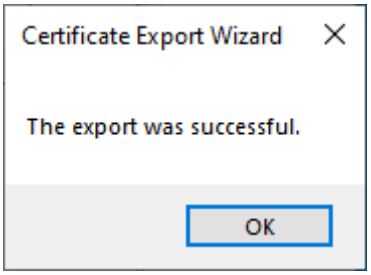


Figure 133 Export Successful

6. Once you have finished exporting the certificate and returned to the Certificate console, right-click the certificate again to display the pop-up menu, then left-click “Delete” to remove the certificate from the certificate store.

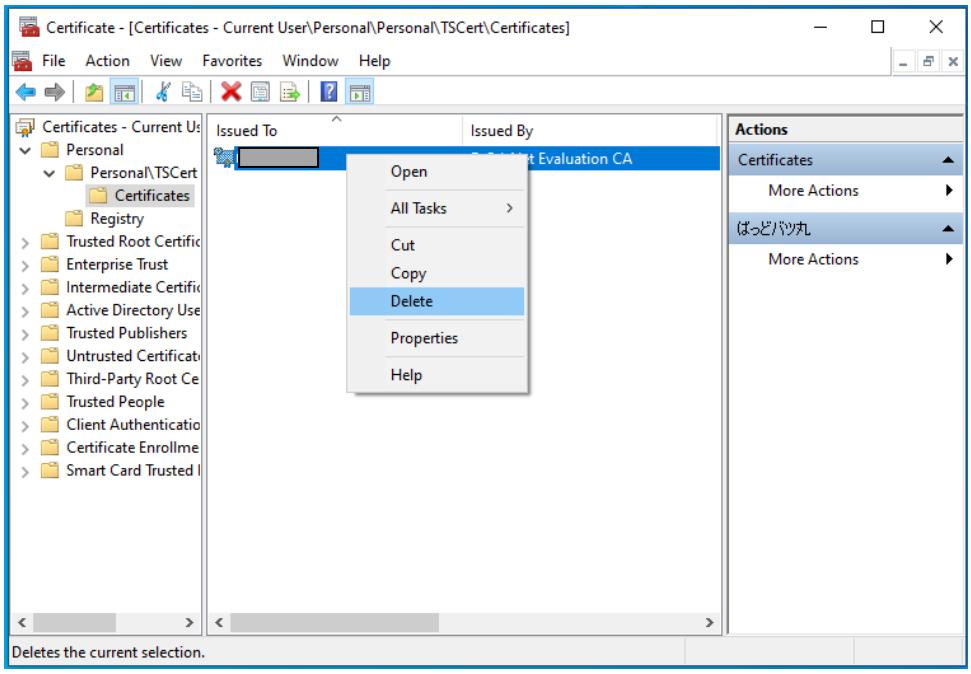


Figure 134 Delete Certificate

7. When the certificate deletion confirmation screen is displayed, carefully confirm that there is no data encrypted using the certificate to be deleted, and click the "Yes" button only if there is no data.

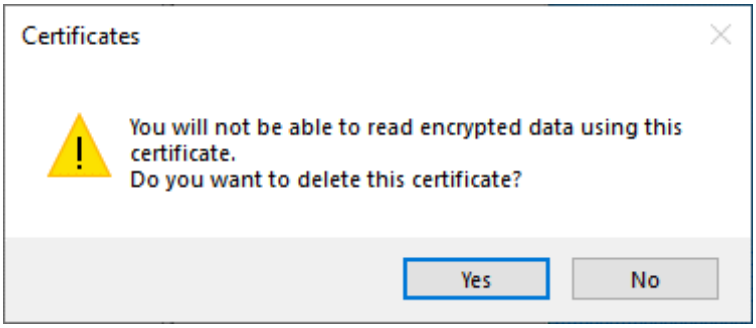


Figure 135 Delete Certificate Confirmation

8. When you have finished deleting the certificate, right-click "TSCert" in the left pane of the certificate console to display the pop-up menu, and click "Refresh" to confirm that no certificates are displayed in the right pane.

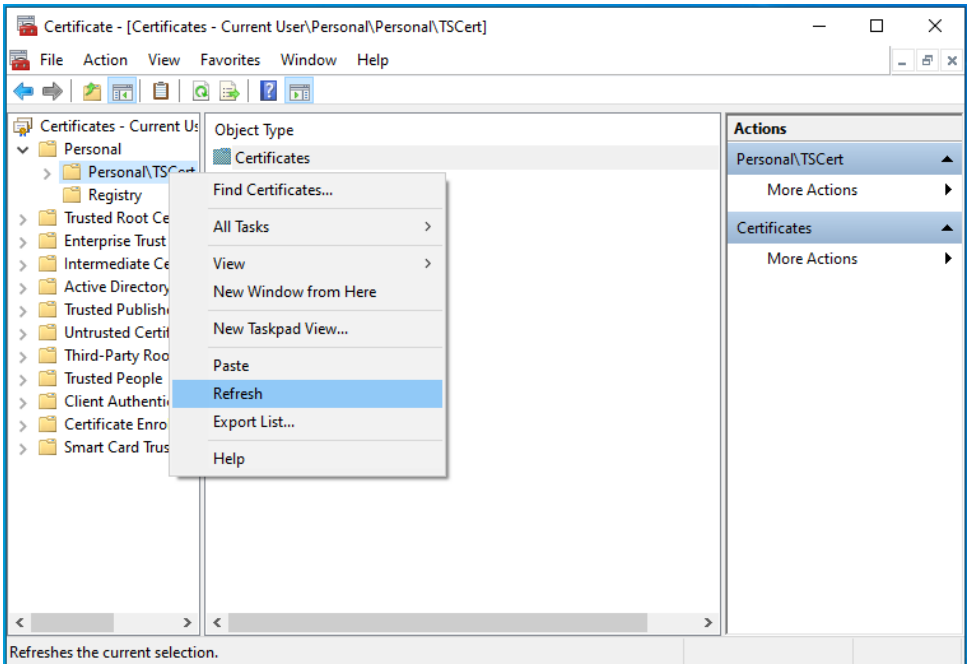


Figure 136 Refresh Certificate console

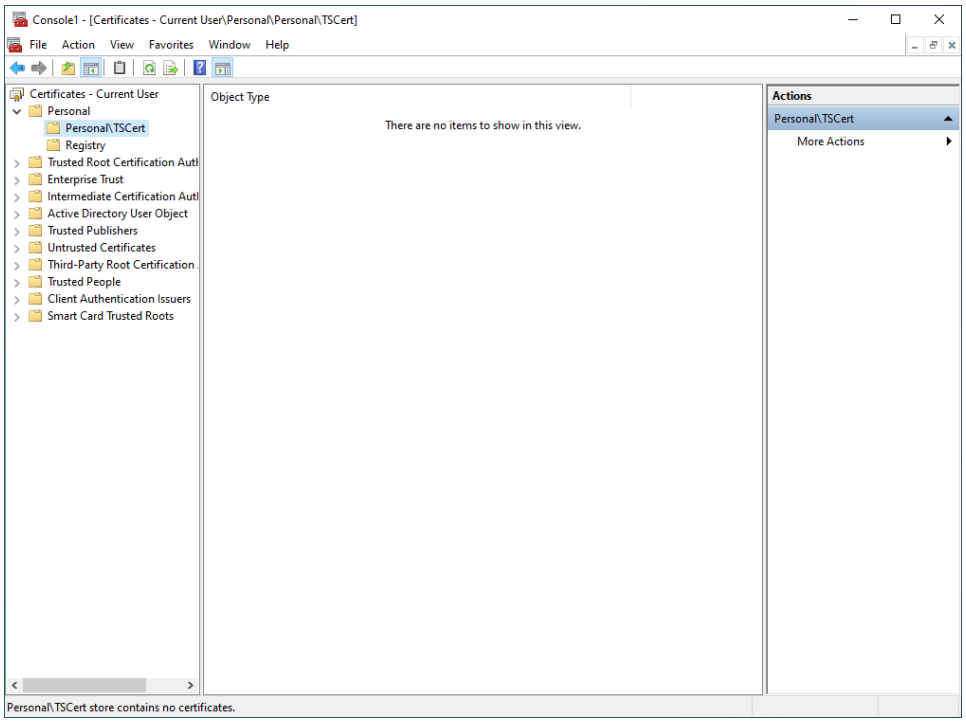


Figure 137 Certificate console – Certificate Deleted

9. Once confirmed, select "File" - "Exit" from the certificate console screen to exit.

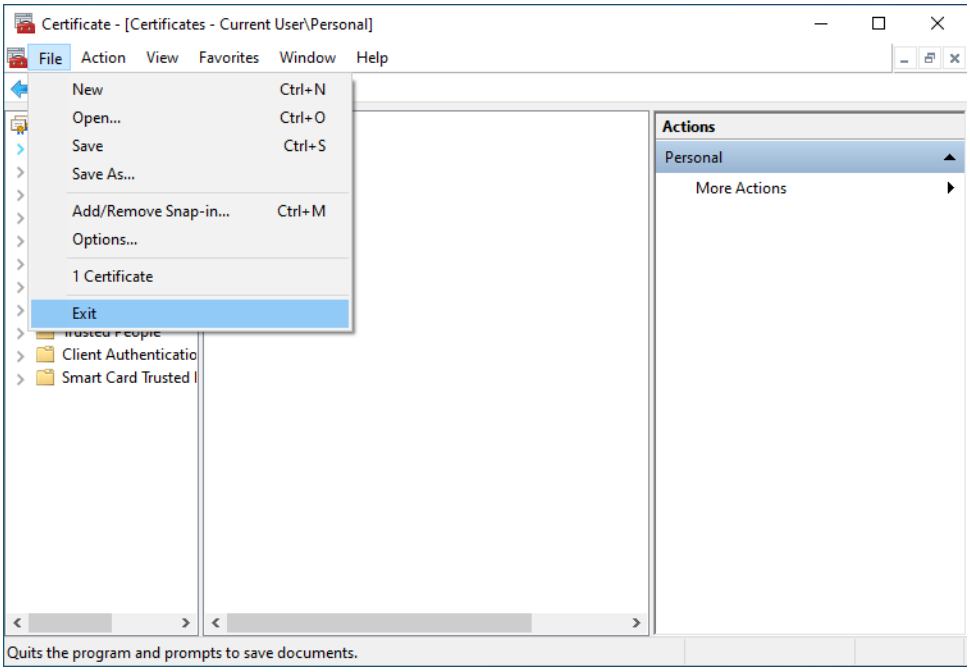


Figure 138 Exit Certificate console

g. About authentication with TruCSP

If you specify TruStack Cryptographic Provider as the CSP type and specify strong private key protection when obtaining a certificate, the first time that certificate is used in an application, device authentication screen will be displayed depending on each authentication device.

If the device authentication screen is displayed, please authenticate your device.

Once device authentication is successful, the certificate can be used. If device authentication fails, the certificate will not be available.

Note: If you log on to Windows using a user name (Well Known Users) reserved in advance for the OS such as Administrator, the authentication screen will not be displayed. Also, depending on the authentication device used, the device authentication screen may not be displayed.

h. What to do when a certificate request error/import error occurs

If an error message is displayed when requesting or importing a certificate, close the message screen, cancel the certificate request or import process, initialize the data according to the steps below, and then reset the certificate. After that, please try the request or import again.

For instructions on how to use each utility, please refer to the TruGate user's guide.

1. Launch the client configuration utility included with TruGate.
2. Execute unregistration of the user who encountered the error.
3. Register the template again.
4. Reset your password.
5. Exit the client configuration utility.

If you are using TruGate Management Utility, please use TruGate Management Utility instead of the above utility.

For instructions on how to use the utility, please refer to the TruGate Management Utility User's Guide.

i. Product Registration

i. Launch Registration Utility

Note: To operate the product registration utility, log on to the local computer with administrator privileges.

Click "Start" - "All Apps" - "TruStack" - "TruCSP License Registration".

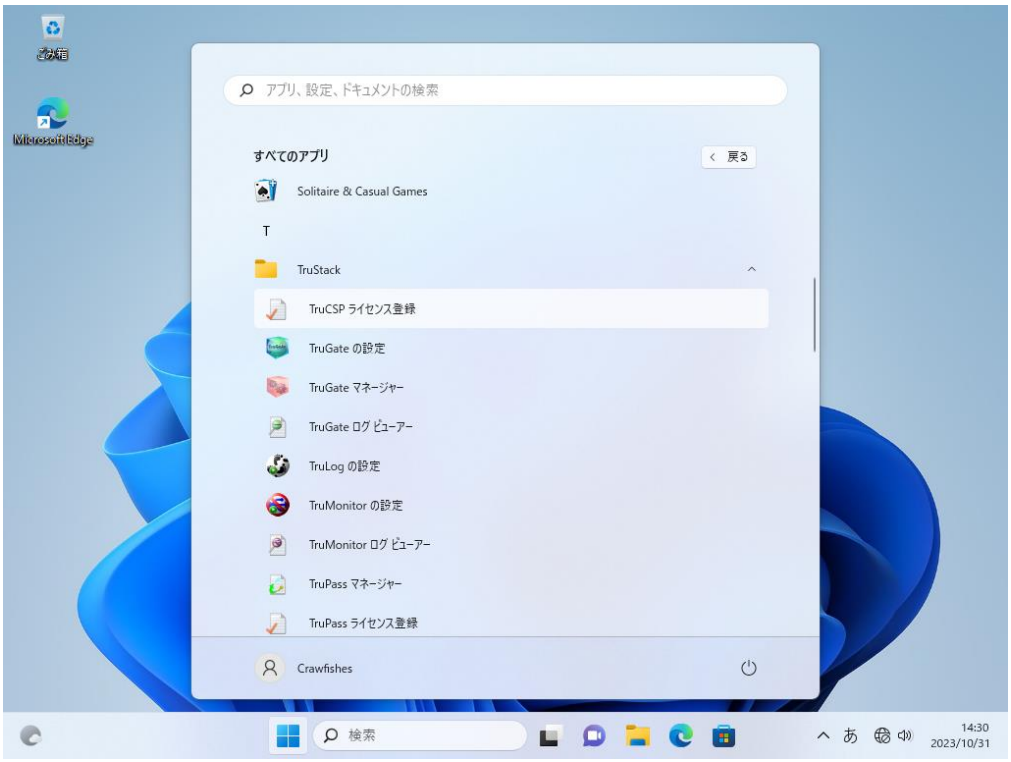


Figure 139 Launch License Registration Utility

When the "TruCSP License Registration" dialog is displayed, enter the separately obtained product key in the edit box, and then click the "OK" button. Clicking the "Cancel" button will cancel product registration.

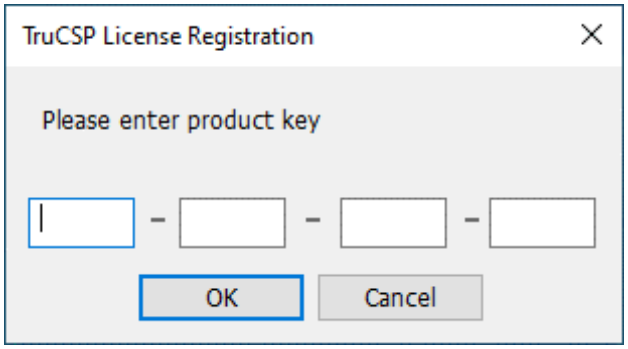


Figure 140 Product License Registration

When product registration is successfully completed, the screen shown below will be

displayed.

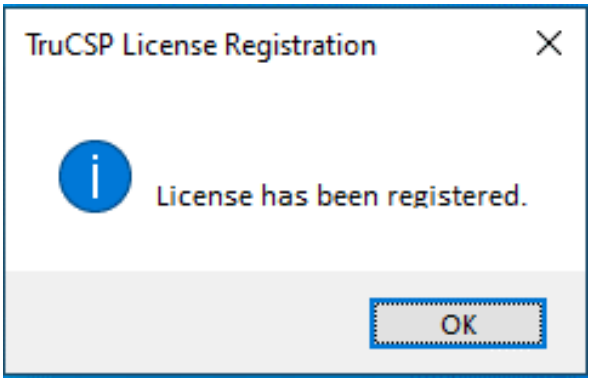


Figure 141 Product License Registration Successful

End of Document

Questions to Trusted Stackware series product
D.O.I-Net Co., Ltd.
Zip Code: 190-0011
2-25-23 Takamatsu, Tachikawa, Tokyo JAPAN
E-Mail: info@doi-net.com
URL: https://www.doi-net.com/