

User Guide For PKI Token

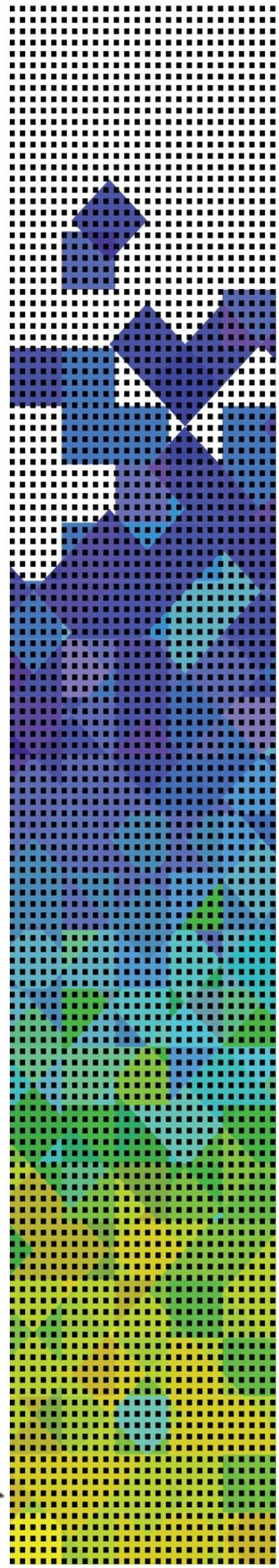
Oman National PKI

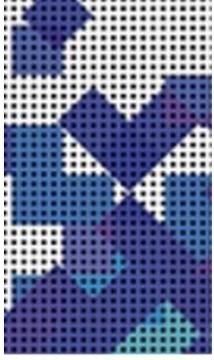
Version 2.0

May 2023



سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and
Information Technology





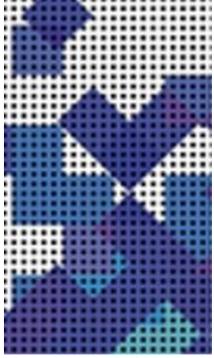
Contents

| | |
|---|----|
| 1. Document terminology | 3 |
| 2. Recommended Acrobat configuration to perform digital signature according to the best practices:..... | 4 |
| 2.1 First Step is to configure Adobe Reader DC as explained below:..... | 4 |
| 2.2 Second step is to install Oman ROOT Certificate in windows store:..... | 9 |
| 3. How to digitally sign a PDF document using the token..... | 12 |
| 3.1 What is PKI token?..... | 12 |
| 3.2 Token Type Description | 12 |
| 3.3 Token fees | 12 |
| 3.4 Who can request for PKI Token? | 12 |
| 3.5 How to request for PKI Token?..... | 13 |
| 3.6 Digital Signature using PKI Token | 13 |
| 4. Digital Signature Validation in Adobe..... | 17 |
| 5. Token Cases and how to resolve issue through self care portal | 21 |



1. Document terminology

| | |
|--------------|--|
| MTCIT | Ministry of Transport, Communications and Information Technology |
| PKI | Public key infrastructure |
| OCSP | Online certificate status protocol |
| CRL | Certificate revocation list |
| CA | Certificate Authority |
| TSA | Time Stamp Authority |

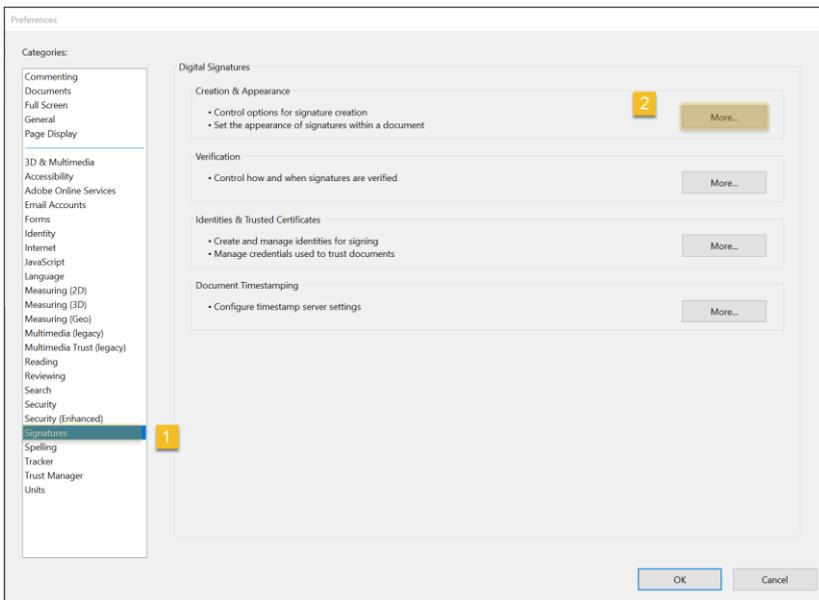


2. Recommended Acrobat configuration to perform digital signature according to the best practices:

2.1 First Step is to configure Adobe Reader DC as explained below:

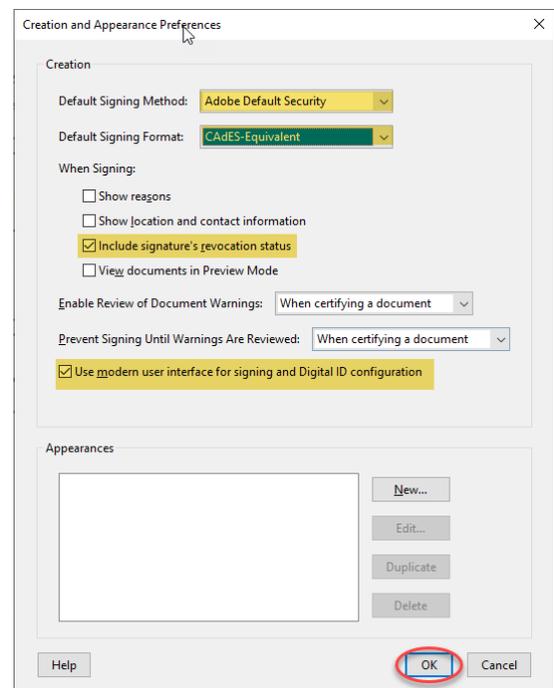
- Procedures are based on the 2020.009 versions of Adobe Reader DC. While previous versions are similar, the procedures are not identical. For instructions involving older product versions, see the Adobe documentation.

1. Open Adobe Reader and select **Edit > Preferences**. The Acrobat *Preferences* dialog box appears.



2. Select the *Signatures* option
3. In the **Creation & Appearance** area, Click on the button labelled 'More...'

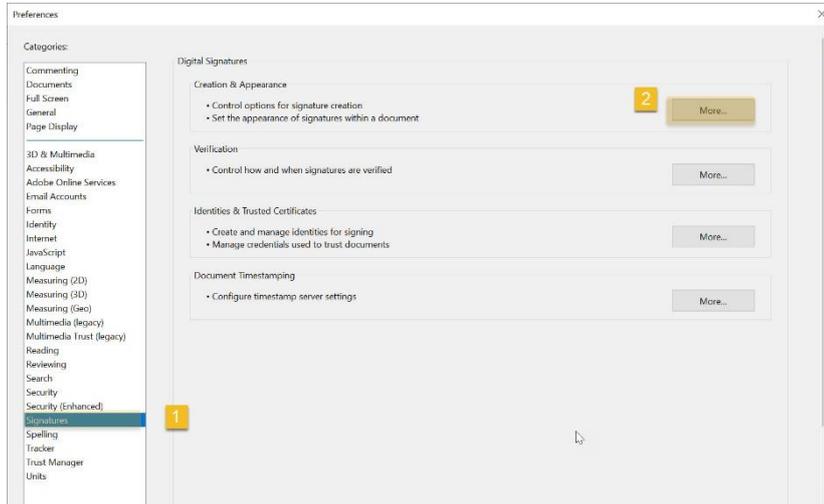
4. The *Creation and Appearance* Preferences box will appear.
5. Choose *Default* Signature Signing Method and Format
6. The option to '*Include signature's revocation status when signing*' should be checked.
7. The option to '*use modern user interface...*' should be unchecked.
8. Click **OK** to return to the *Preferences* dialog box.





9. In the **Verification** area, click on the button labelled 'More...'

10. The **Signature Verification** Preferences box will appear.



11. In **Verification Behavior**, The option to 'Require certificate revocation checking...' should be **checked**.

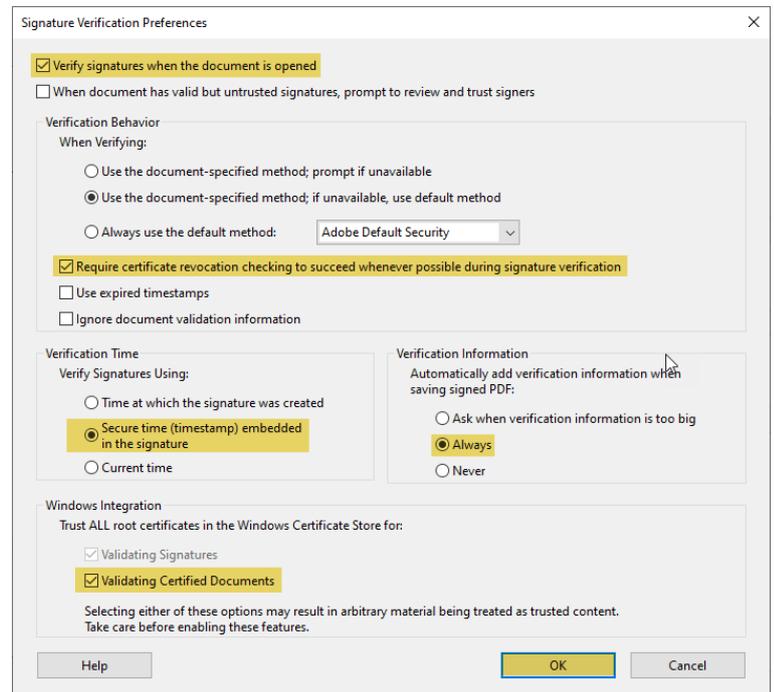
12. The option to 'Use expired timestamp' should be **unchecked**.

13. In **Verification Time** area, Choose 'Secure time (timestamp) embedded in the signature'

14. In **Verification Information** area, set 'Automatically add verification information when saving signed PDF' to **Always**.

15. In the **Windows Integration** area, both of the options should be selected.

16. Click **OK** to return to the **Preferences** dialog box.

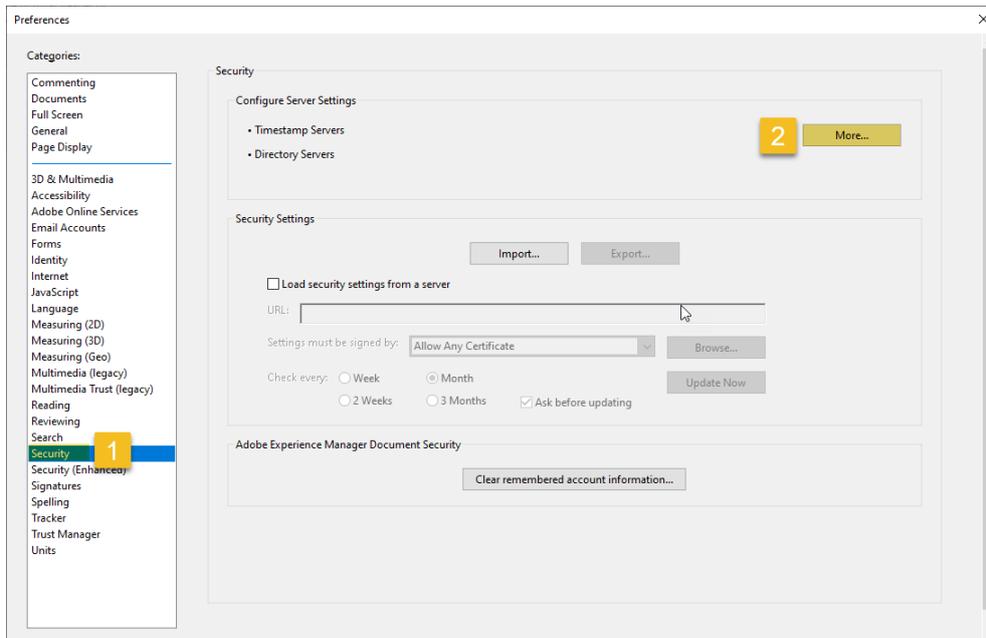


Note: Setting the **Verify signatures when document is opened** option automatically activates a validation procedure for all of the document's digital signatures when the document is opened. The default is that digital signatures are not validated automatically when a document is opened. For optimum workflow, it is best to check this option.



17. Select the **Security** option

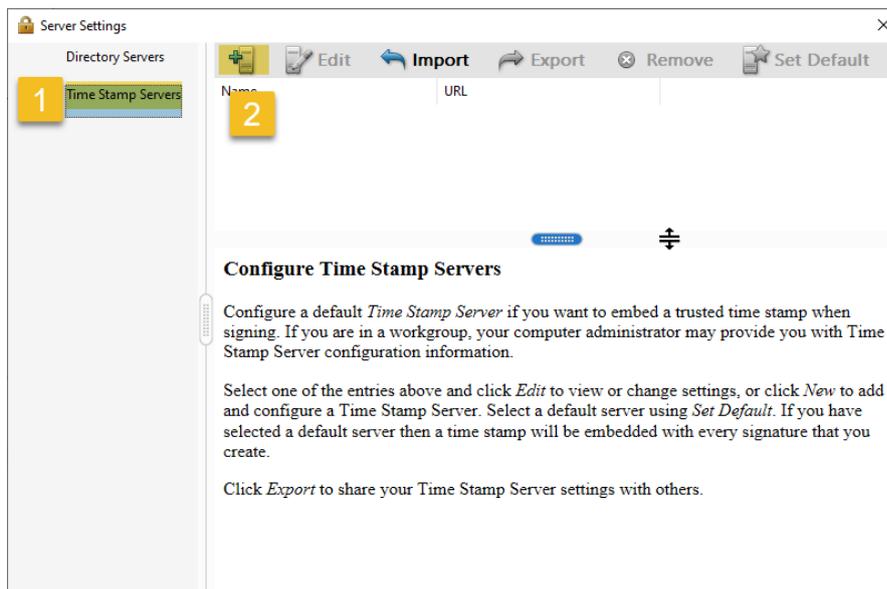
18. In the **Security** area, click on the button labelled 'More...'



19. **Server Settings** box will appear.

20. Choose '**Time Stamp Server**'. Then **New** to add a new Time Stamp Server.

21. New Tim Stamp Server box will appear.





22. Set configuration as below:

Name: **Oman Public TSA**

Server URL: <https://tsa.pki.ita.gov.om/ds-server-ita/process?workspace=ITA-TSA>

New Time Stamp Server

1 Name: Oman Public TSA

Server Settings

2 Server URL: pv.om/ds-server-ita/process?workspace=ITA-TSA

This server requires me to log on

User name:

Password:

OK Cancel

23. The new Server will be add.

24. Choose **Oman public TSA Server**, the click **Set Default**.

25. Will be marked as a Star.

Server Settings

Directory Servers

Time Stamp Servers

Edit Import Export Remove Set Default

| Name | URL |
|-----------------|--|
| Oman Public TSA | https://tsa.pki.gov.om/ds-server-it... |

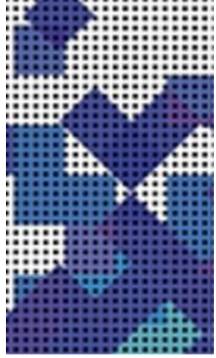
1

Configure Time Stamp Servers

Configure a default *Time Stamp Server* if you want to embed a trusted time stamp when signing. If you are in a workgroup, your computer administrator may provide you with Time Stamp Server configuration information.

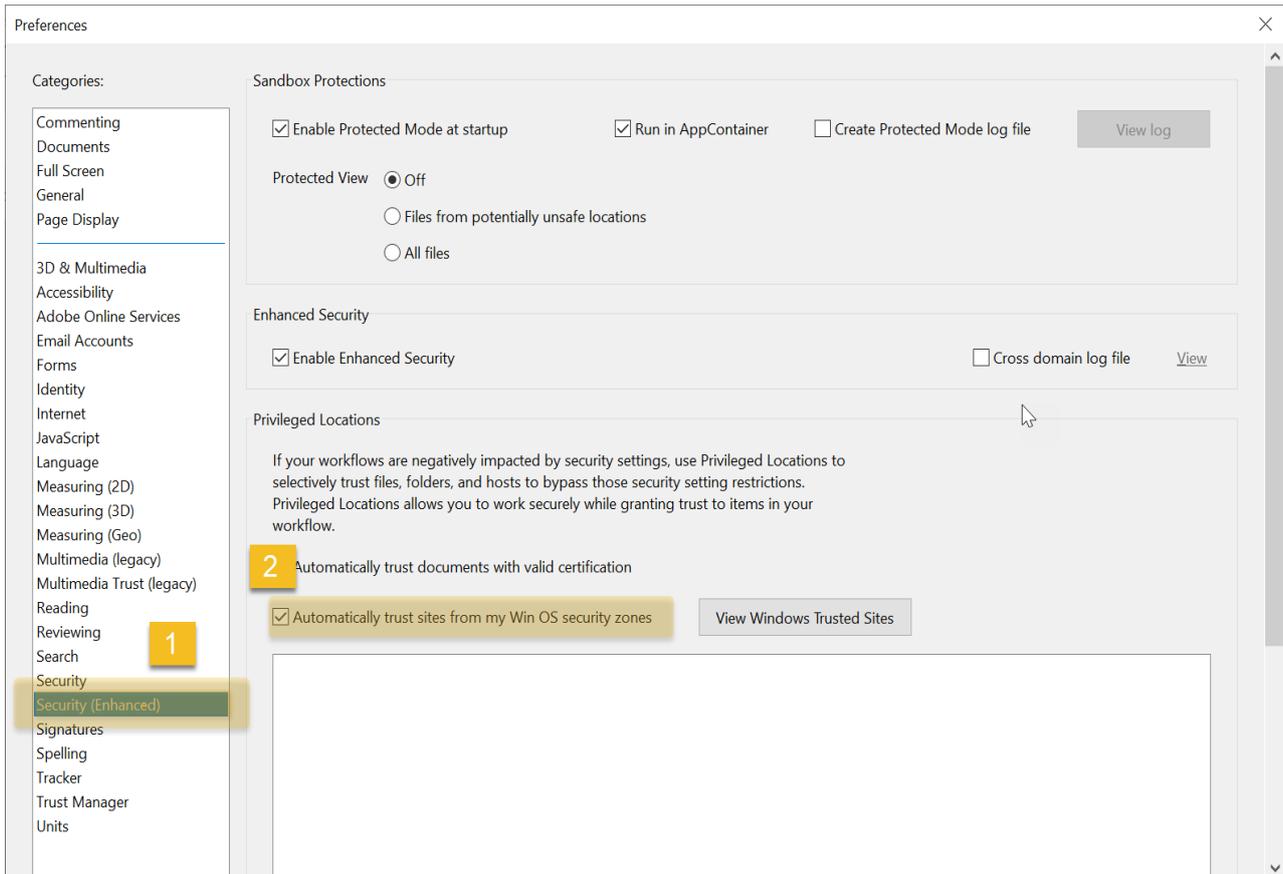
Select one of the entries above and click *Edit* to view or change settings, or click *New* to add and configure a Time Stamp Server. Select a default server using *Set Default*. If you have selected a default server then a time stamp will be embedded with every signature that you create.

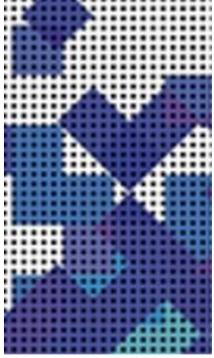
Click *Export* to share your Time Stamp Server settings with others.



26. Select the *Security (Enhanced)* option

27. In the *Privileged Locations* area, the option to 'Automatically trust sites Win OS security zones box' should be *checked*.





2.2 Second step is to install Oman ROOT Certificate in windows store:

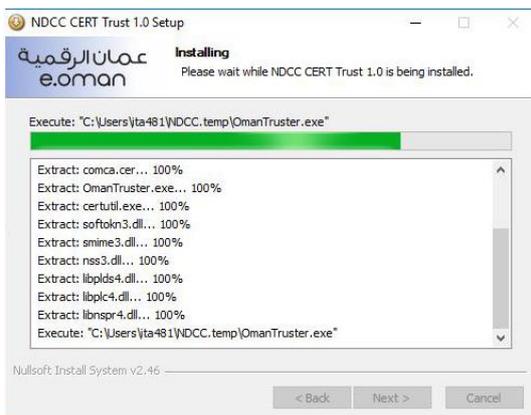
There are two different methods to download and install Oman ROOT Certificate to your machine. These methods explained below:

2.2.1 Method 1. NDCC-CERT_Trust-1.0.exe program

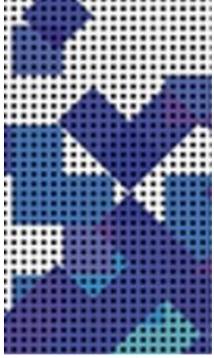
1.1. download NDCC-CERT_trust tool from the below link:

<https://oman.om/tam/downloads/NDCC-CERT-Trust-1.0.exe>

1.2. Once you run the program, the Setup Wizard will appear.



1.3. Once you complete all the steps, **Oman ROOT Certificate** successfully installed in your machine.



2.2.2 Method 2. Oman Root CA file

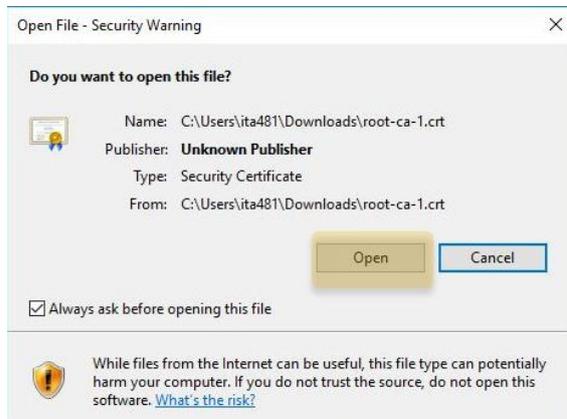
1.1. Download Oman root ca from the following link:
<http://pki.ita.gov.om/CACerts/root-ca-1.crt>

1.2. double click on the certificate to open it

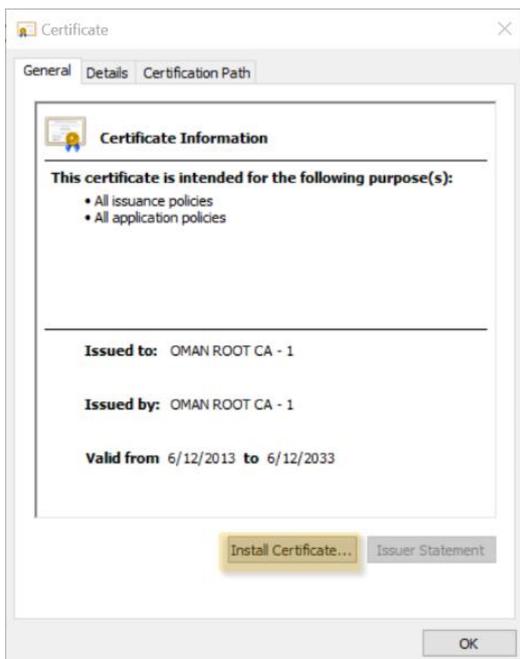
1.3. Choose to **open** it.



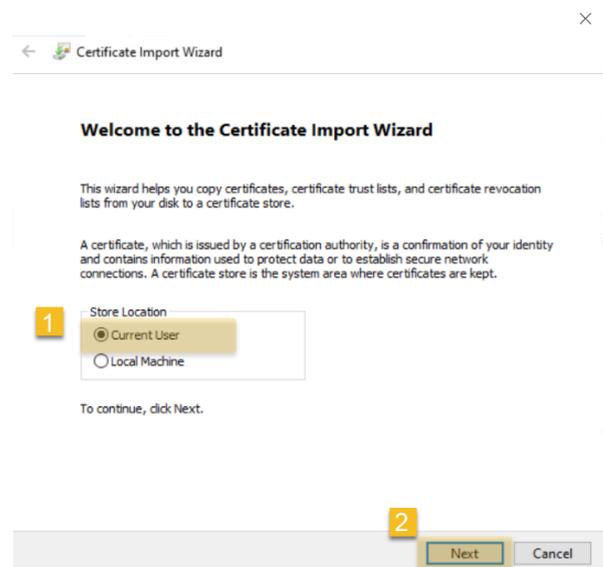
root-ca-1



1.4. Click on **Install Certificate**

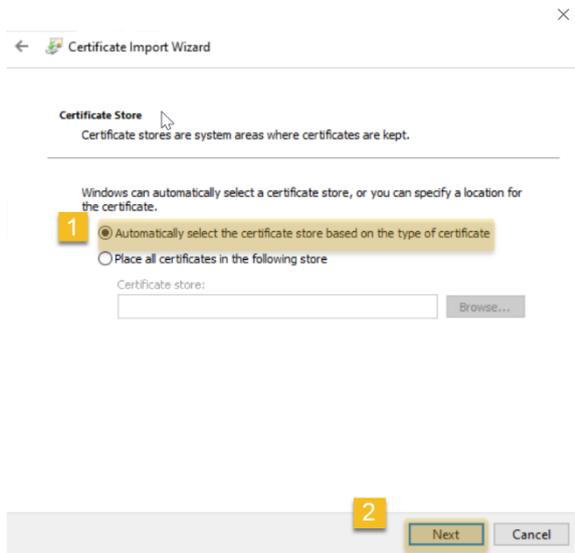


1.5. Choose **current user**, then click **Next**

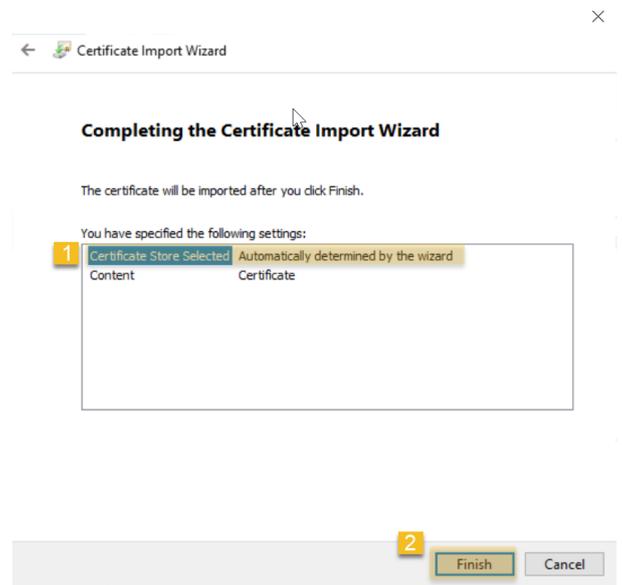




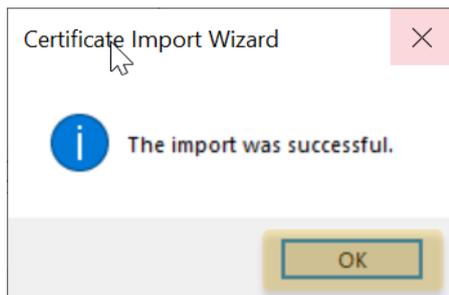
1.6. Choose **Automatically select the certificate store**, then click **Next**

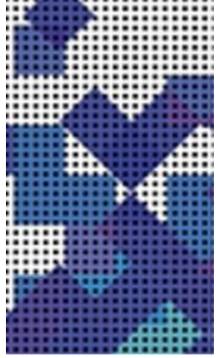


1.7. Click **Finish**



1.8. Now it is successfully imported, Click **OK**





3. How to digitally sign a PDF document using the token

3.1 What is PKI token?

PKI token are hardware device that store digital certificates and private keys securely¹. When you need to encrypt, decrypt or sign something, the token does this internally in a secure chip meaning the keys are never at risk of being stolen.



3.2 Token Type Description

MTC provides three types of certificates: Digital Signature Certificate, Secure Authentication Certificate, and Encryption Certificate. The certificates are issued inside a smart card device called Token. There are five types of Token issued by NDCC depending on the number of certificates:

- **Token Classic:** includes **signature** certificate only, which is used to sign documents and emails.
- **Token Encryption:** includes **encryption** certificate only, which is used to encrypt documents and emails.
- **Token Advanced:** includes **signature and Encryption** certificates, which are used to sign documents and emails, and to encrypt documents and emails.
- **Token Premium:** includes **authentication, signature, and encryption** certificates, which are used for secure authentication, to sign documents and emails, and to encrypt documents and emails.
- **Token Pro:** includes **authentication and signature** certificates, which are used for secure authentication and to sign documents and emails.

3.3 Token fees

Please contact us by email on pki@mtcit.gov.om to get the update price of token.

3.4 Who can request for PKI Token?

The corporate token is intended to be generated for corporate use. Government and private sector's employees are eligible to get token.

¹ <https://www.microcosm.com/products/pki-tokens>



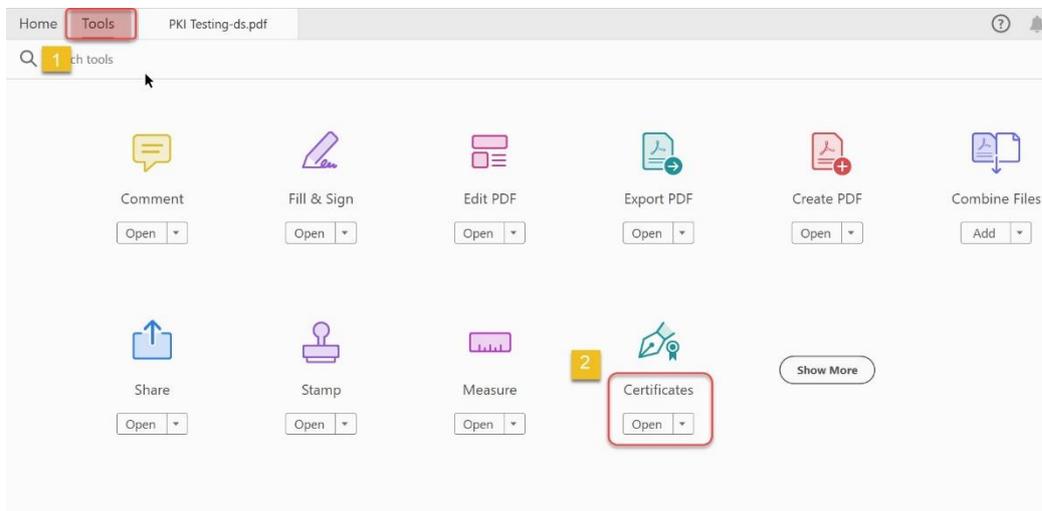
3.5 How to request for PKI Token?

- Send official Email for Technical team on pki@mtcit.gov.om
- Specify your requirements on Email, and objectives of your request
- Technical team will study your requirement and will be in follow up with you.

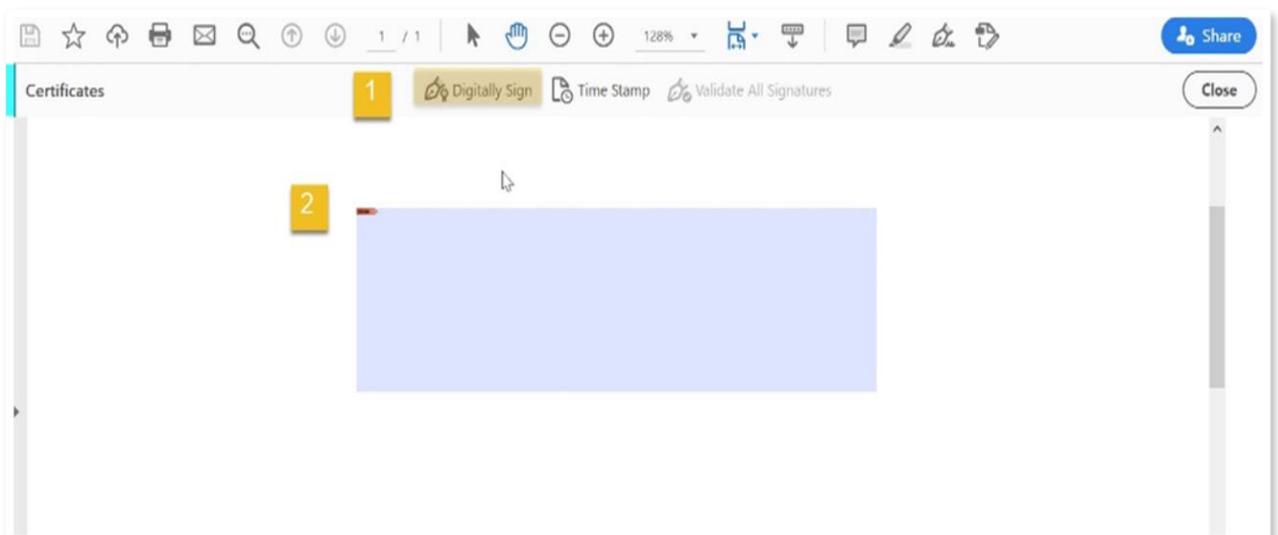
3.6 Digital Signature using PKI Token

3.6.1 To Sign a PDF document, follow the below steps:

- **Open** PDF File.
- Select **Tools**, and then choose **Certificates** as shown below.

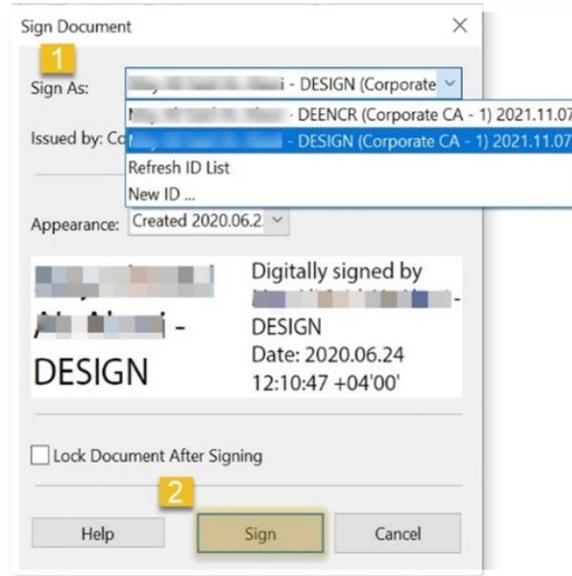


- Select **Digitally Sign**.
- Choose the place where you suppose to sign, then draw a label for the signature as showing below





- The following box will appear. You have to choose (*your-name-DESIGN*), then click *sign*

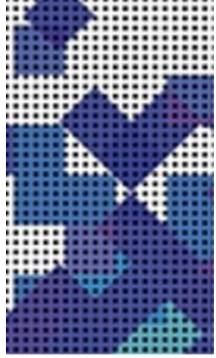


- Save your Document, and then enter your *TOKEN PIN*.



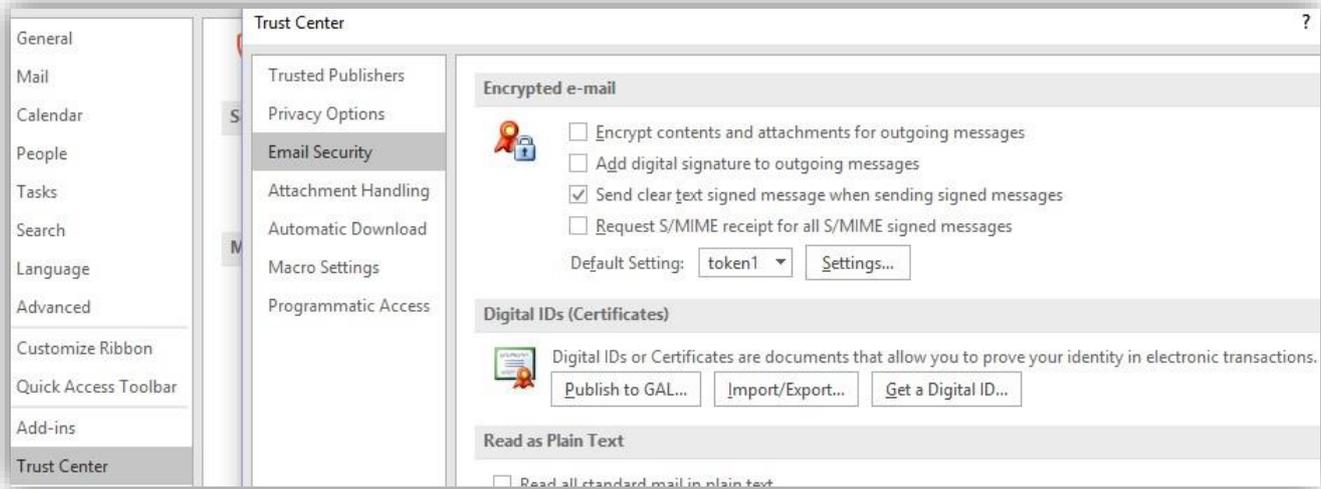
- Finally, your document is digitally *signed*.





3.6.2 Email Signing

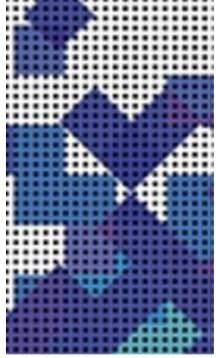
- Go to **File**, then select **Trust center**, then choose **center setting**.
- From the menu, choose **Email Security**, then **Default Setting**, click on **settings**.



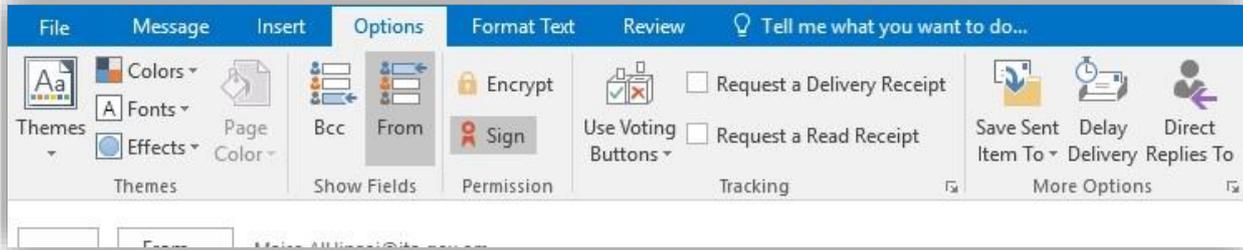
- Ensure to include signing certificate. On Certificates and algorithms section → Go to Signing Certificate → Press Choose → Token Certificates will be appeared, choose (DESIGN).



*Hint: This is for first time only.



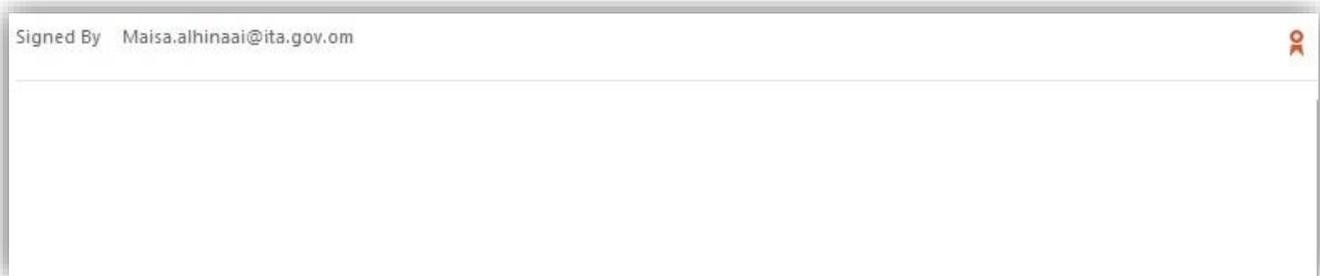
- Go to new email, on option press Sign



- Add recipients of Email
- Press send, and system will ask user for Token PIN code



- Your email will be signed , and will appear as below

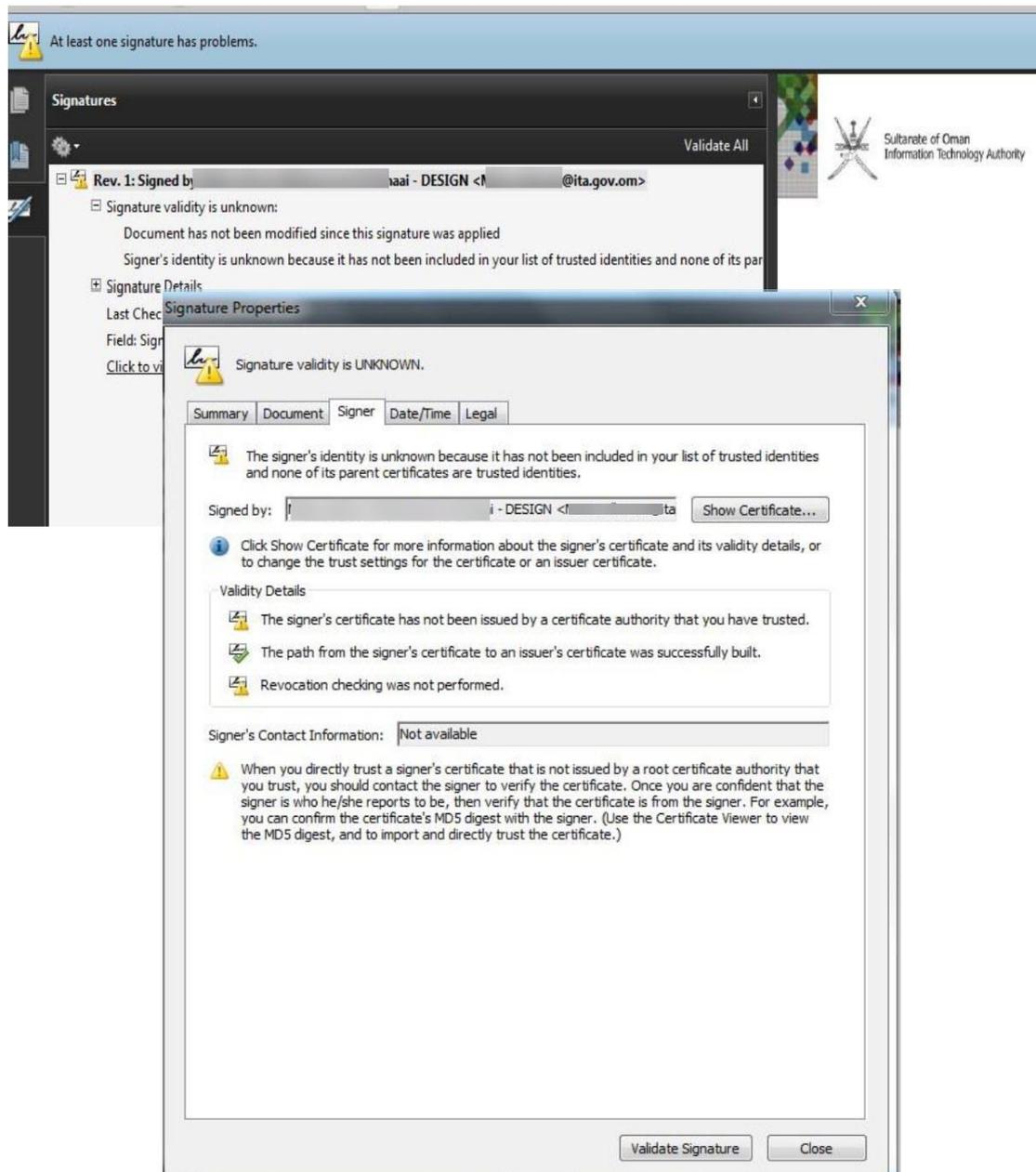




4. Digital Signature Validation in Adobe

Some of the Root CA's are included by default in Windows Certificate Store (Trusted Root Certification Authorities) and only a few are included in Adobe Trusted Identities.

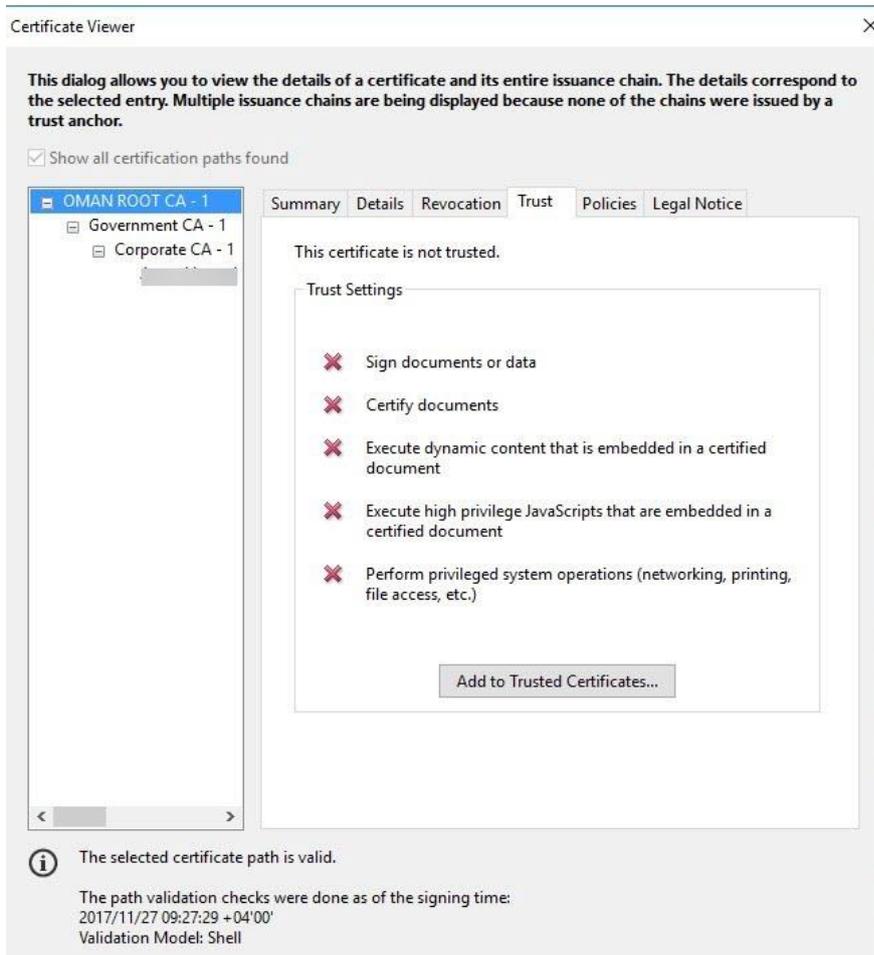
Because the Oman Root CA of the signing certificate is not included on Adobe Trusted Identities, the Signature is considered “not trusted” (but NOT invalid) as below





To manually add Oman Root CA Certificate on the Adobe Trusted Identities, open the signature properties and Signature is not trusted:

- Click Show Certificate and select Trust tab.
- Be sure that you have selected the topmost Root Certificate.





- Press Add to Trusted Identities tab and be sure you have checked all checkboxes, as below.

Import Contact Settings ×

Certificate Details

Subject: OMAN ROOT CA - 1
Issuer: OMAN ROOT CA - 1
Usage: Sign Certificate (CA), Sign CRL
Expiration: 6/12/2033 12:00:00 AM

Trust

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

Signed documents or data
 Certified documents
 Dynamic content
 Embedded high privilege JavaScript
 Privileged system operations (networking, printing, file access, etc.)

Help OK Cancel



- After all dialog boxes are closed and the document is re-opened, the signature considered **Valid**.
- The Root Certificate is now Trusted and all signatures generated with this Root Certificate will be also trusted.

Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

OMAN ROOT CA - 1

- Government CA - 1
- Corporate CA - 1

Summary Details Revocation Trust Policies Legal Notice

This certificate is directly trusted in your trusted certificates list.

Trust Settings

This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to:

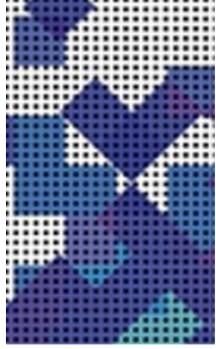
- ✓ Sign documents or data
- ✓ Certify documents
- ✓ Execute dynamic content that is embedded in a certified document
- ✓ Execute high privilege JavaScripts that are embedded in a certified document
- ✓ Perform privileged system operations (networking, printing, file access, etc.)

Revocation checking is not performed for this certificate because it is directly trusted as a trust anchor.

Add to Trusted Certificates...

i The selected certificate path is valid.

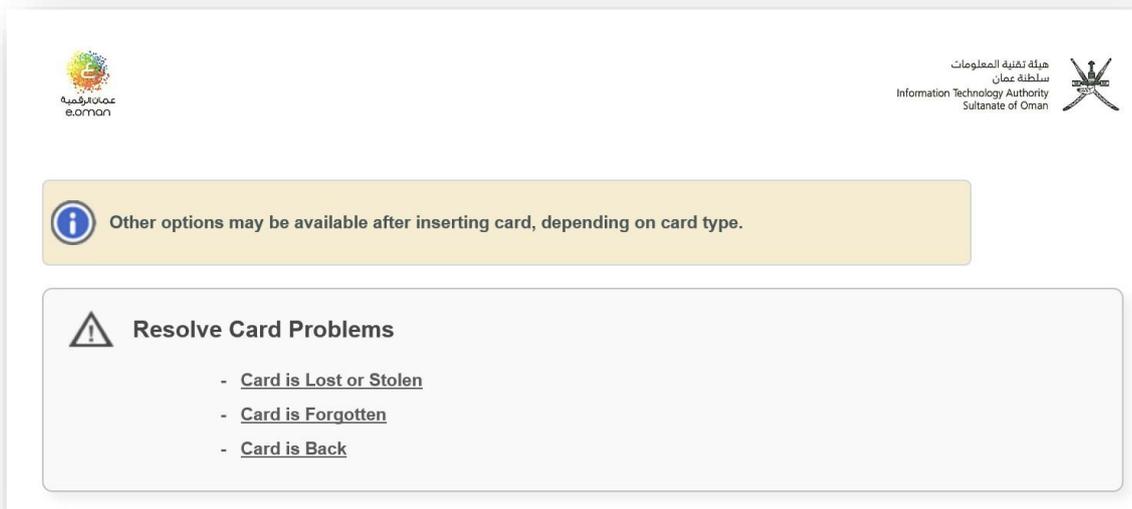
The path validation checks were done as of the signing time:
2017/11/27 09:27:29 +04'00'
Validation Model: Shell



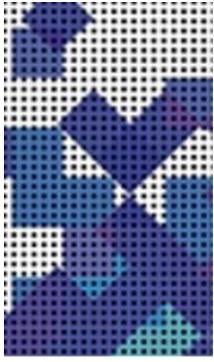
5. Token Cases and how to resolve issue through self care portal

Case 1: if you lost your PKI Token and you couldn't find it, or Token has been stolen (If you think you will not find/get the token back or you don't want to use the token anymore, then you need to revoke it to deny any online use of the token, then you can request for a new token later -if needed- following the request process.)

- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Choose the option, (Card is lost or Stolen) as below



- ✓ System will ask you to enter your civil ID number as below



Register Self-Revocation Request

[Back to main screen](#)

Please fill at least one of the following fields to identify the card you wish to revoke.

i Only cards belonging to a profile in which self-revocation is activated can be revoked.

Note: the fields below are not case sensitive.

| | |
|--|----------------------|
| ID Civil Number (الرقم المدني) | <input type="text"/> |
| Name Of Entity (جهة العمل) | <input type="text"/> |
| Token Number (رقم الحاوية الذكية للشهادات) | <input type="text"/> |
| Role (الدور الوظيفي) | <input type="text"/> |
| Customer (العميل) | <input type="text"/> |

- ✓ Card(Token) serial number will be appear to you, choose card(Token) you want to disabled
- ✓ Then, system will ask you to answer your security question that you chooses during token Activation.
- ✓ If you can't remember the answer for the security questions then you need to contact PKI team on telephone number: **24166440** or email: pki@mtcit.gov.om



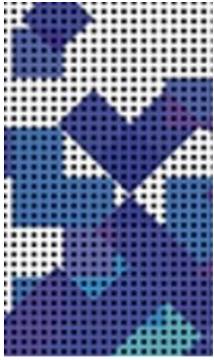
Case 2: if you lost your token in somewhere, and you are worry if someone find it and can use it if PIN code shared with other. (if you think you can find the token, but you want to suspend any online use of the token until you find/get the token.)

- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Choose the option, (Card is Forgotten) as below

**** This option will help users to disabled card for temporary (Suspension).**

The screenshot shows the self-care portal interface. At the top left is the e.oman logo. At the top right is the logo of the Information Technology Authority, Sultanate of Oman. Below the logos is a yellow information box with a blue 'i' icon and the text: "Other options may be available after inserting card, depending on card type." Below this is a white box with a warning icon and the heading "Resolve Card Problems". Underneath the heading are three bullet points: "- Card is Lost or Stolen", "- Card is Forgotten", and "- Card is Back".

- ✓ System will ask user to enter Civil ID number.



Register Self-Revocation Request

[Back to main screen](#)

Please fill at least one of the following fields to identify the card you wish to revoke.

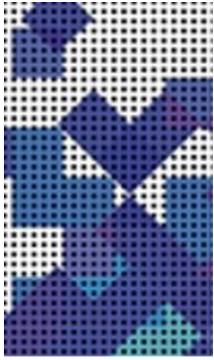


Only cards belonging to a profile in which self-revocation is activated can be revoked.

Note: the fields below are not case sensitive.

| | |
|--|----------------------|
| ID Civil Number (الرقم المدني) | <input type="text"/> |
| Name Of Entity (جهة العمل) | <input type="text"/> |
| Token Number (رقم الحاوية الذكية للشهادات) | <input type="text"/> |
| Role (الدور الوظيفي) | <input type="text"/> |
| Customer (العميل) | <input type="text"/> |
| <input type="button" value="OK"/> | |

- ✓ Card(Token) serial number will be appear to you, choose card(Token) serial number you want to disabled.
- ✓ System will ask user to answer security questions that you choose them during Token Activation.
- ✓ If you can't remember the answer for the security questions then you need to contact PKI team on telephone number: 24166440 or email: pki@mtcit.gov.om



Case 3: To resume your suspended Card (Token) to be able to use it online again.

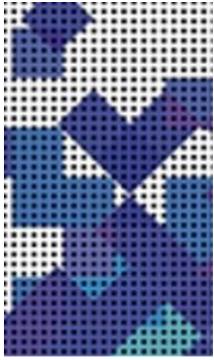
- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Choose the option, (Card is back) as below

The screenshot shows the self-care portal interface. At the top left is the 'e.oman' logo. At the top right is the logo of the Information Technology Authority, Sultanate of Oman. Below the logos is a yellow information box with an 'i' icon and the text: 'Other options may be available after inserting card, depending on card type.' Below this is a white box with a warning icon and the title 'Resolve Card Problems'. Underneath the title are three bullet points: '- Card is Lost or Stolen', '- Card is Forgotten', and '- Card is Back'.

- ✓ System will ask you to enter your Civil ID number

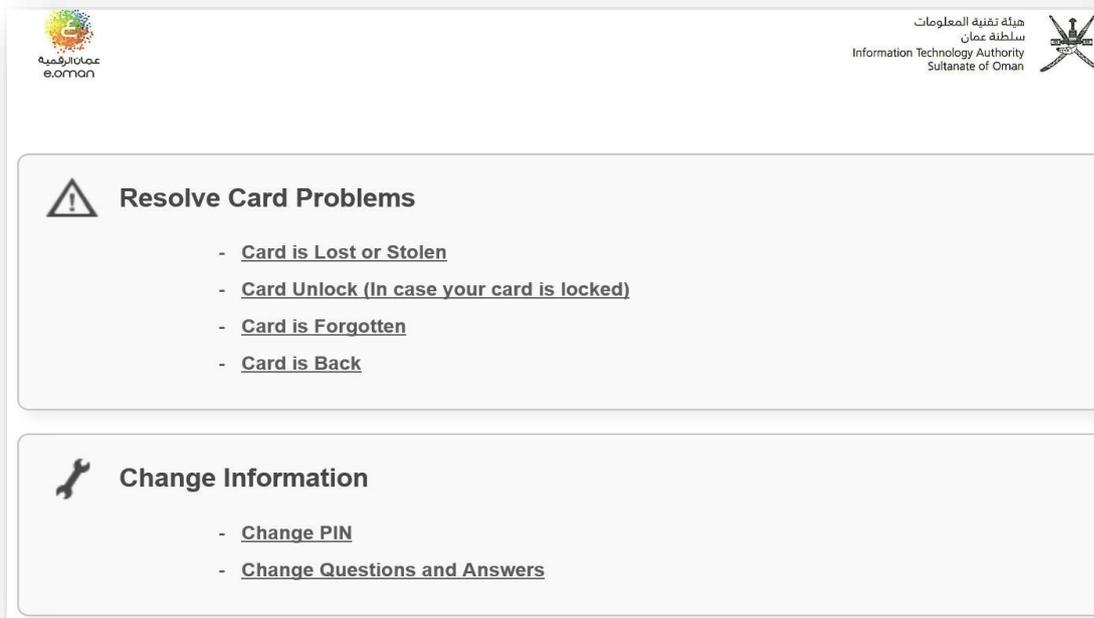
The screenshot shows the 'Register Self-Revocation Request' form. At the top left is the 'e.oman' logo. At the top right is the logo of the Information Technology Authority, Sultanate of Oman. Below the logos is a yellow information box with an 'i' icon and the text: 'Please fill at least one of the following fields to identify the card you wish to revoke. Only cards belonging to a profile in which self-revocation is activated can be revoked. Note: the fields below are not case sensitive.' Below this is a form with five input fields: 'ID Civil Number (الرقم المدني)', 'Name Of Entity (جهة العمل)', 'Token Number (رقم البطاقة المكية للشهادات)', 'Role (الدور الوظيفي)', and 'Customer (العميل)'. There is an 'OK' button at the bottom right of the form.

- ✓ Result will be appear, if you request before to disable card or not.



Case 4: if you enter PIN code for Token three time wrongly, and token is blocked.

- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Insert your token in laptop
- ✓ Choose Card Unlock (In case your card is locked)



- ✓ System will ask user to answer security questions that you choose them during Token Activation.



Case 5: if you Want to change your Token PIN code.

- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Insert your token in laptop.
- ✓ Go to change information section.
- ✓ Choose, change PIN

The screenshot shows the self-care portal interface. At the top, there are logos for the Sultanate of Oman and the Information Technology Authority. The main content area is divided into two sections: 'Resolve Card Problems' and 'Change Information'. The 'Change Information' section is highlighted and contains two options: 'Change PIN' and 'Change Questions and Answers'.

- ✓ System will ask you to enter your Current PIN code, and New PIN code

The screenshot shows the 'PIN Change' form. It includes a 'Back to main screen' link, a warning message, and a list of rules for the new PIN. The form fields are: 'Current PIN', 'New PIN', and 'PIN confirmation', followed by an 'OK' button.

PIN Change

[Back to main screen](#)

You are about to modify the PIN of your card. This PIN should respect the security policy of your organization.

Please enter your current PIN and the new PIN according to the following rules:

- Minimum Length: 6
- Maximum Length: 6
- Minimum Number of Unique Characters: 3
- Only Allow Numeric Characters
- Forbid Sequences

PIN Change

Current PIN

New PIN

PIN confirmation

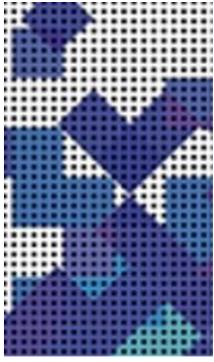


Case 6: if you Want to change your Security questions.

- ✓ Open self-care portal (<https://selfcare.pki.mtcit.gov.om>)
- ✓ Insert your token in laptop.
- ✓ Go to change information section, and choose change security questions

The screenshot shows the self-care portal interface. At the top left is the e.oman logo. At the top right is the logo of the Information Technology Authority, Sultanate of Oman. The main content area is divided into two sections:

- Resolve Card Problems** (indicated by a warning triangle icon):
 - [Card is Lost or Stolen](#)
 - [Card Unlock \(In case your card is locked\)](#)
 - [Card is Forgotten](#)
 - [Card is Back](#)
- Change Information** (indicated by a wrench icon):
 - [Change PIN](#)
 - [Change Questions and Answers](#)



Thank You for Using
PKI Services