Manual Document – MyTrustID Desktop

Project Name:	MyTrustID API		
Date:	24 Jan 2020	Release:	~~Draft~~/Final
Author:	Zulkifle Muhammad		
Owner:	Zulkifle Muhammad		
Client:	Federal Court of Malaysia		
Document Number:	1.2		

Note: This document is only valid on final version.

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
17-09-2019	N/A	Release draft version 1.0	1.0
08-01-2020	17-09-2019	Release version 1.1	1.1
24-01-2020	08-01-2020	Release version 1.2 with some changes in user interface	1.2

Approvals

This document does not require any approvals.

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

Contents

Figures

1. Introduction
1.1. Purpose

This document describes the detail user guide for users on using MyTrustID Desktop for User Authentication

1.2. Scope

This document describes the following scope and functions:

   i.   Installations
   ii.   Using The Application

2. Installations

This section describes installations procedures of MyTrustID Desktop Software:

2.1. Installation Steps

   1)   Run the software installer : MyTrustID.msi
   2)   Click **Next** on the following
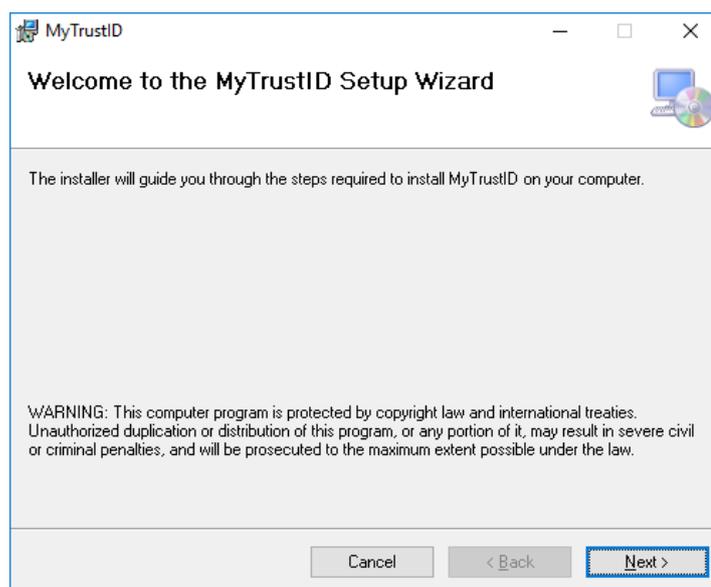
Figure 1: Installation

3) Select Installation folder
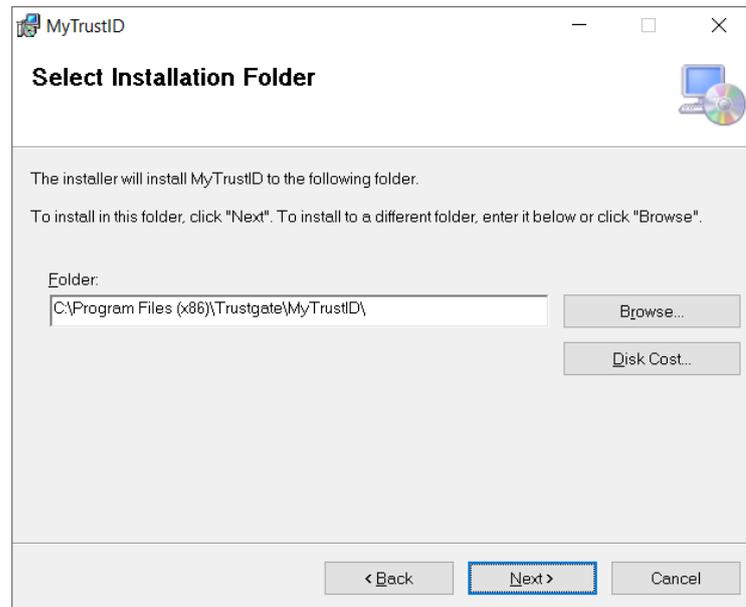
Figure 2: Select Folder

4) Click **Next** to Confirm an installation
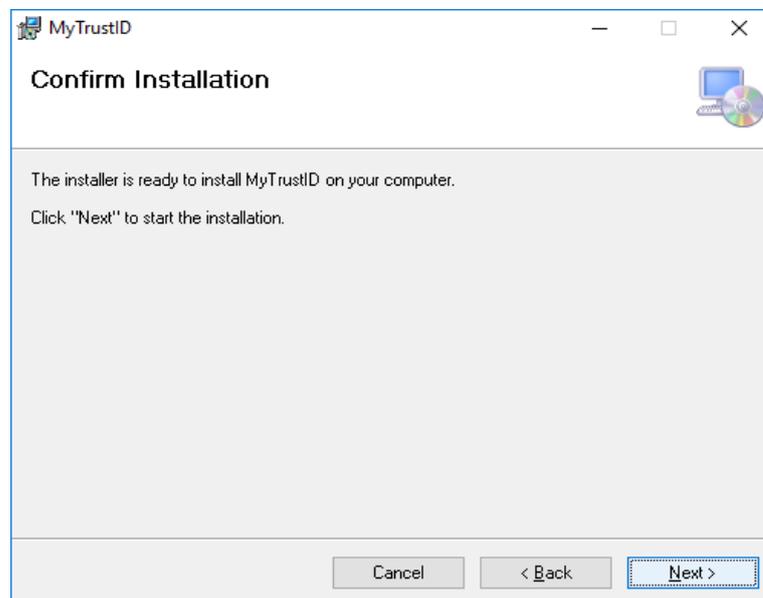
Figure 3: Confirm

5) Wait until the installation process being completed
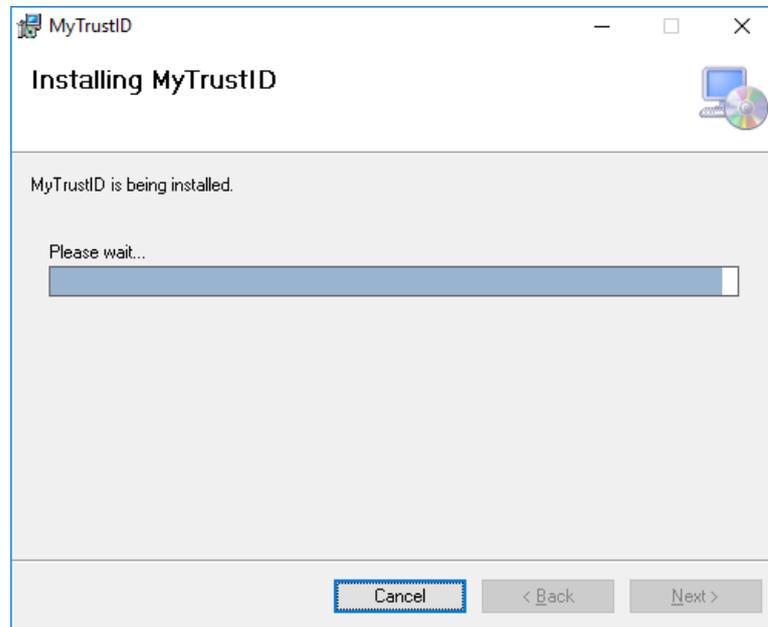
Figure 4: Installation process

6) MyTrustID has been successfully installed
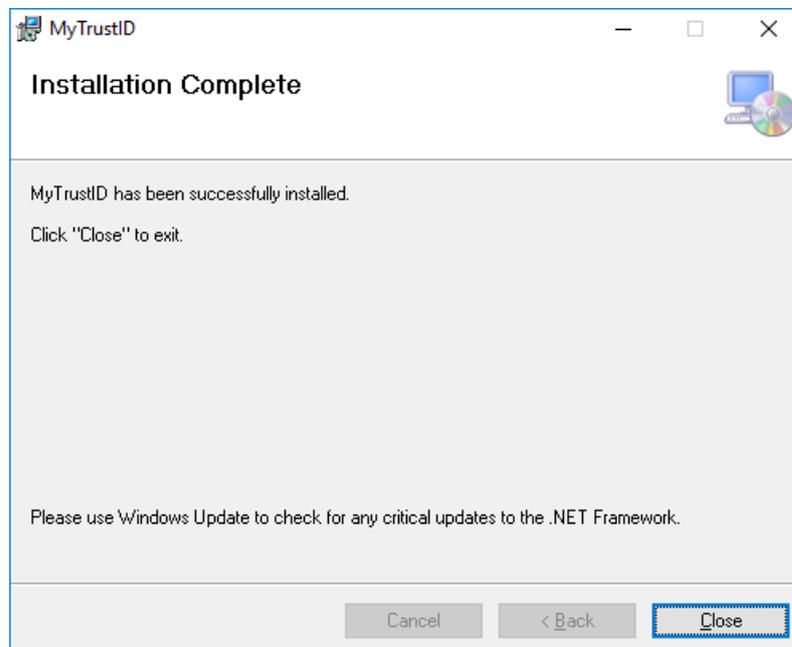
Figure 5: Installation complete

2.2. Running the Application

1) Run shortcut icon at the desktop

Figure 6: MyTrustID icon at desktop

2) MytrustID icon will automatically added into the system tray
3) By right click at the icon, it will show the menu item such show window, hide window and exit
4) Select Exit to close the application
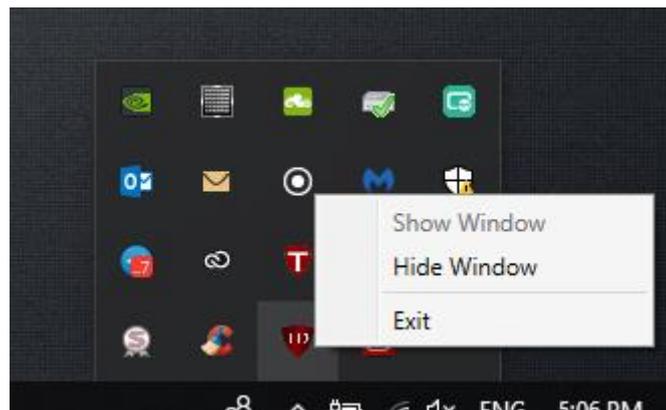
Figure 7: MyTrustID Icon at taskbar

2.3. Post-Installation : Setting My Certificate

1) Select **USB Token** as certificate type and click *Continue* button
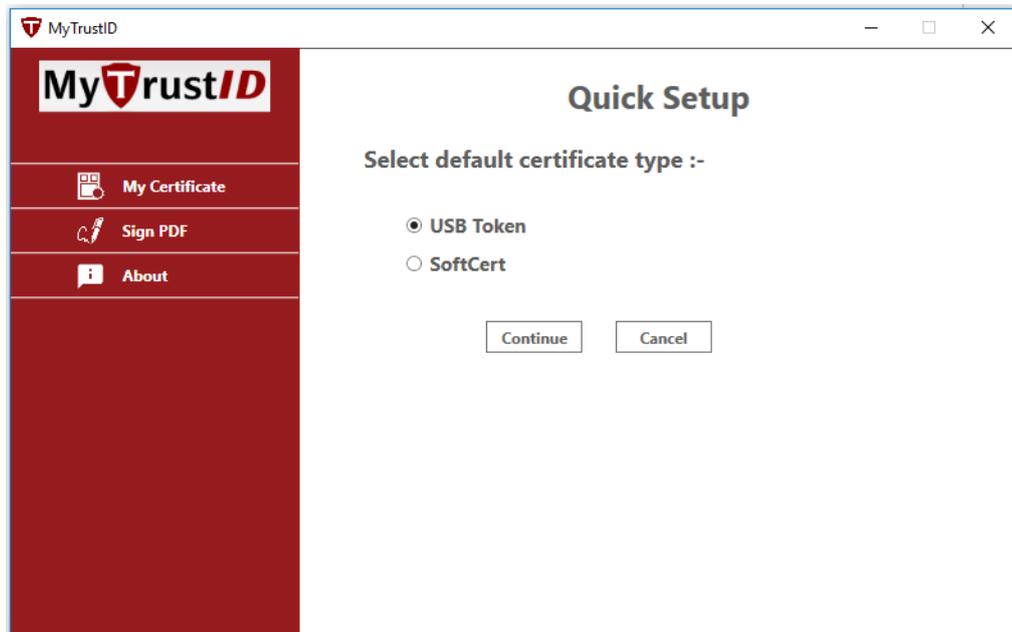
Figure 8: Select USB Token

2) Application will automatically detect an inserted token
3) Enter PIN number and click *Login* button
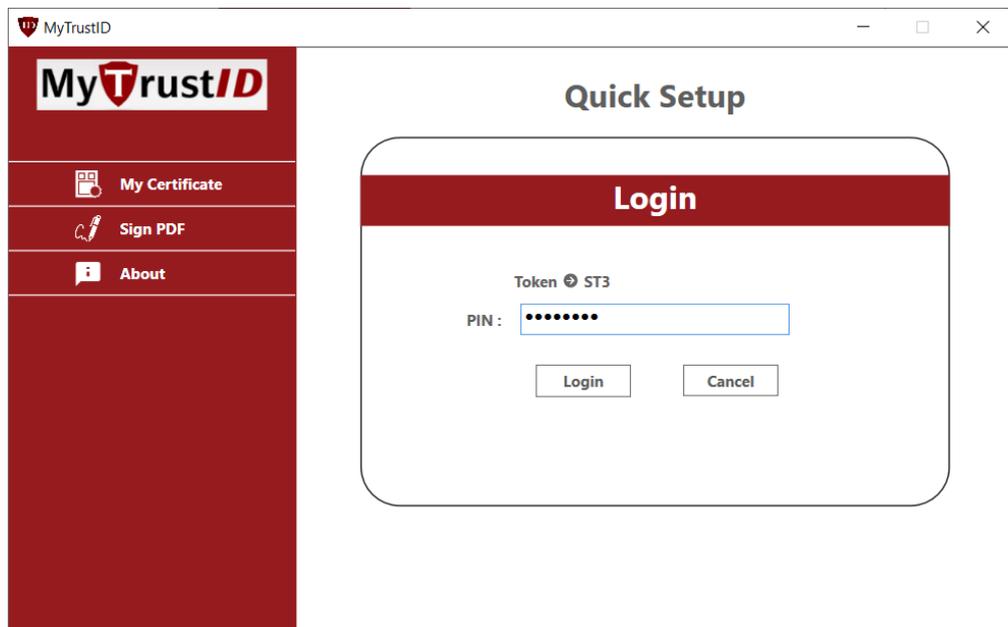
Figure 9: Enter Token PIN number

4) When read token is success, it will navigate to certificate detail page that shows important information of user.

5) Once user have setup the default certificate, anytime the *MyCertificate* button is clicked it will redirect to certificate detail page.
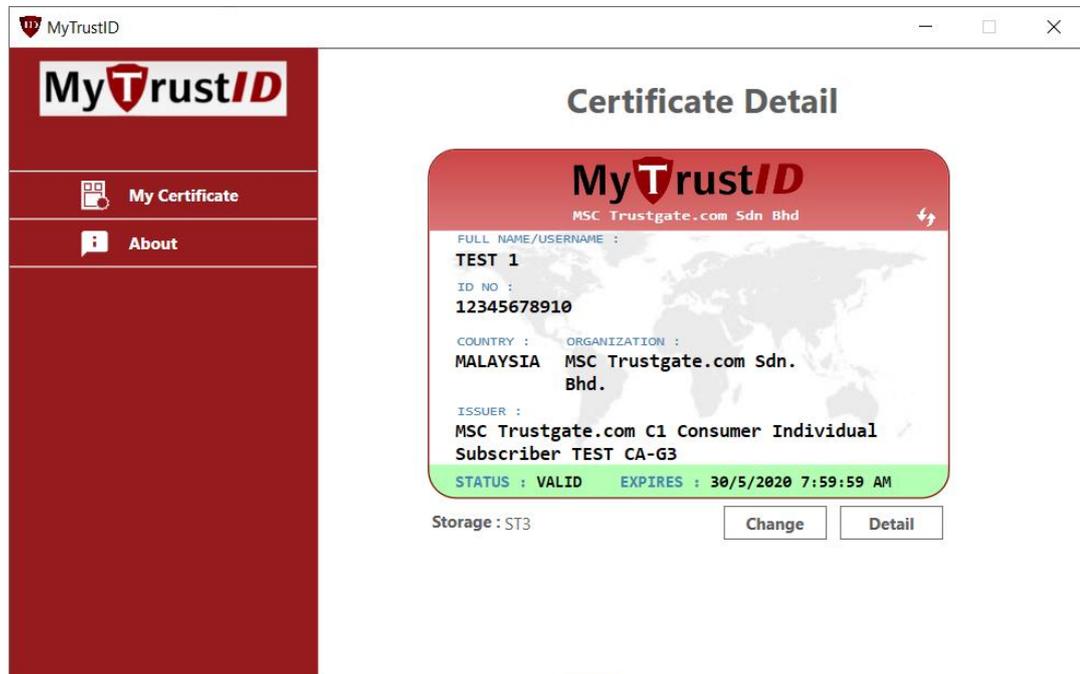
Figure 10: Certificate detail page

6) By clicking the *Detail* button, it will shows more detail of user information
7) By clicking the *Change* button, it allowed user to change the default certificate/Storage type by do quick setup again.
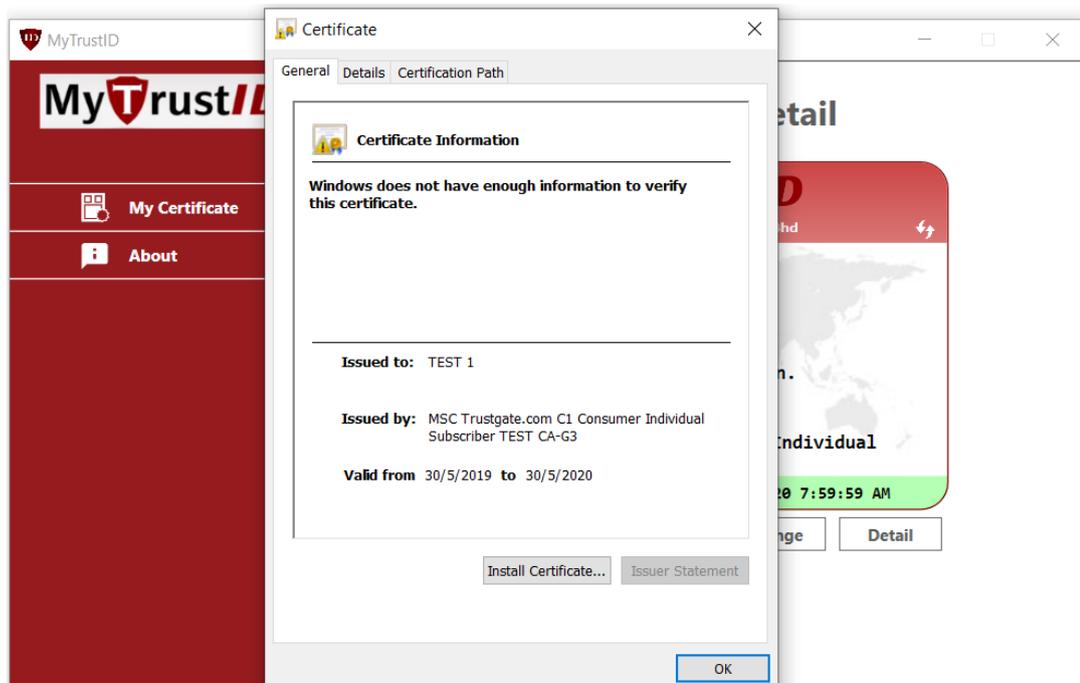
Figure 11: Certificate information in dialog box

3. Using the Application

3.1. Signing PDF using Token with MyTrustID Desktop API

3.1.1. UserID not same as configured certificate

1) MyTrustID Desktop app will show up with Select Storage message box if request userID is not same as configured certificate
2) Insert the USB Token into a USB port on your computer
3) Select Token and Click *Ok*
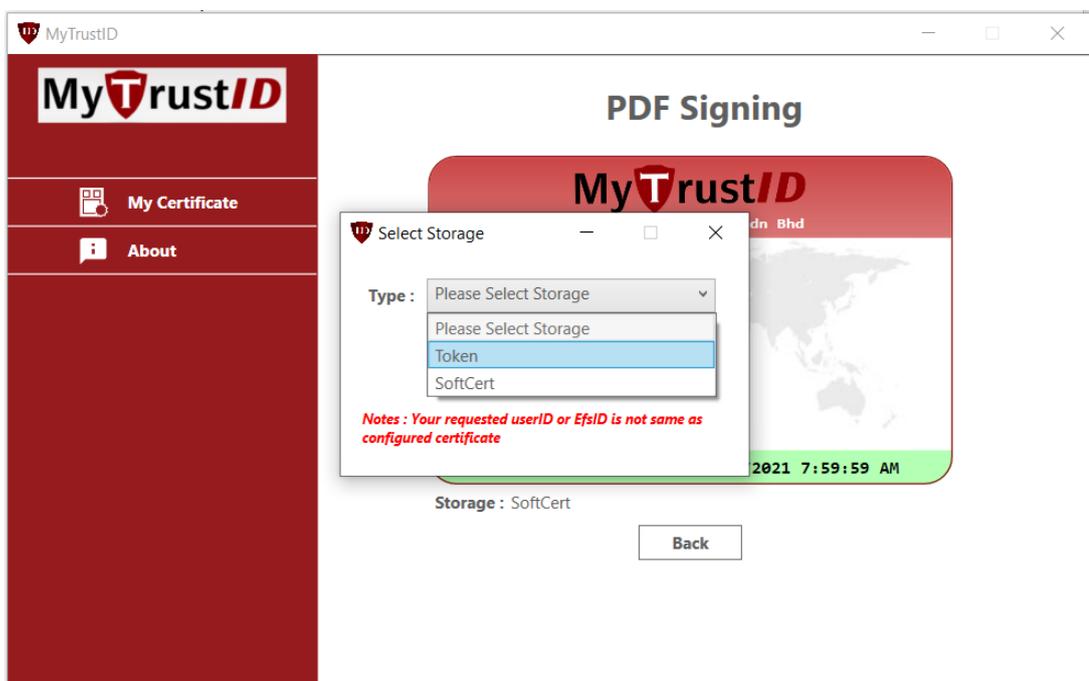
Figure 12: Select Storage Type

4) Application will automatically detect inserted token, enter token PIN and tick remember me with selected timeout for subsequent signing

Figure 13: Select Token Type and insert PIN
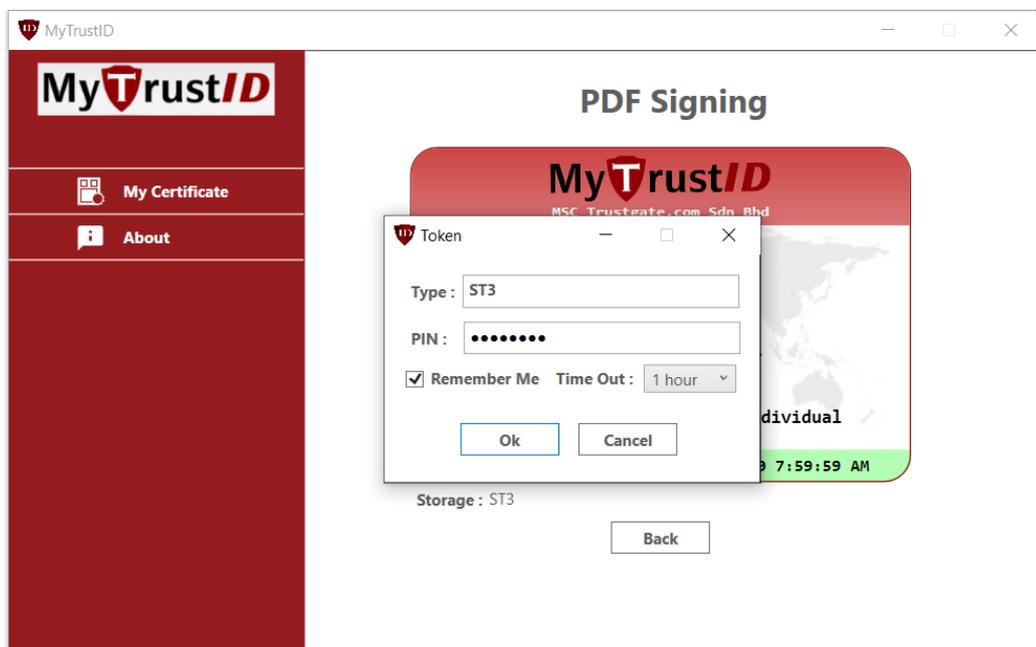
Figure 14: Click remember me and select time out

5) The Application will read token and show another pop up for signing
6) Click **Sign** button to proceed with signing

Figure 15: Message for signing using token

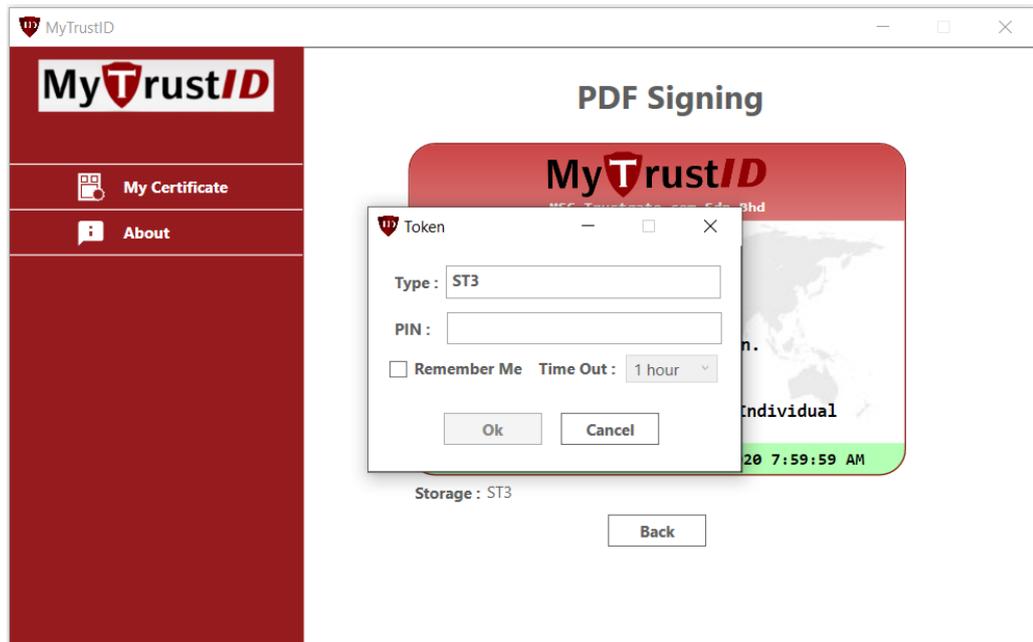7) It will close automatically after signing process is complete

3.1.2. UserID same as configured certificate

1) MyTrustID Desktop app will show up with insert token PIN message box if request userID is same as configured certificate

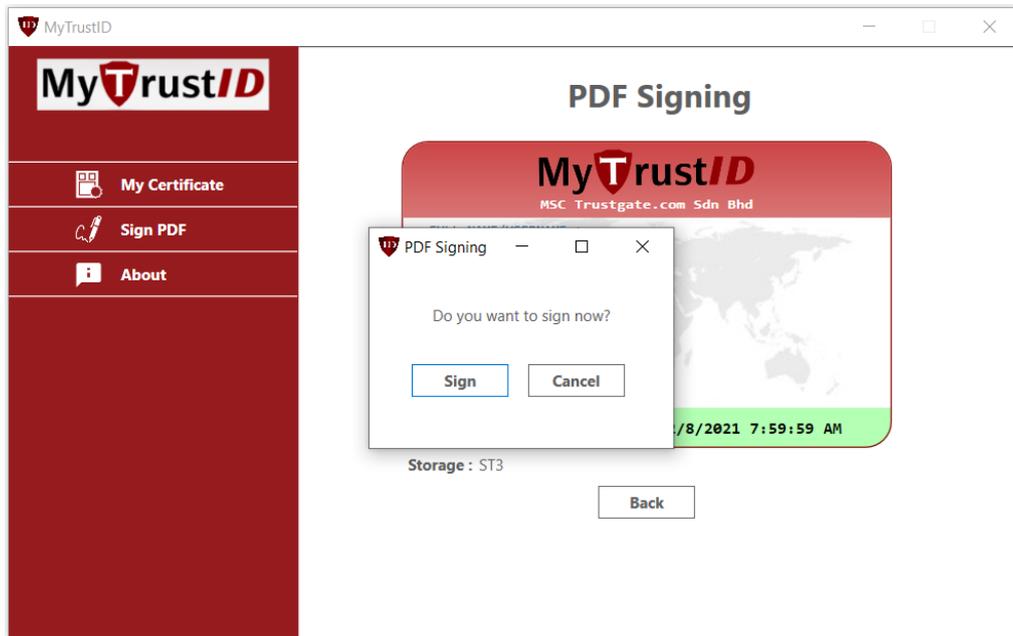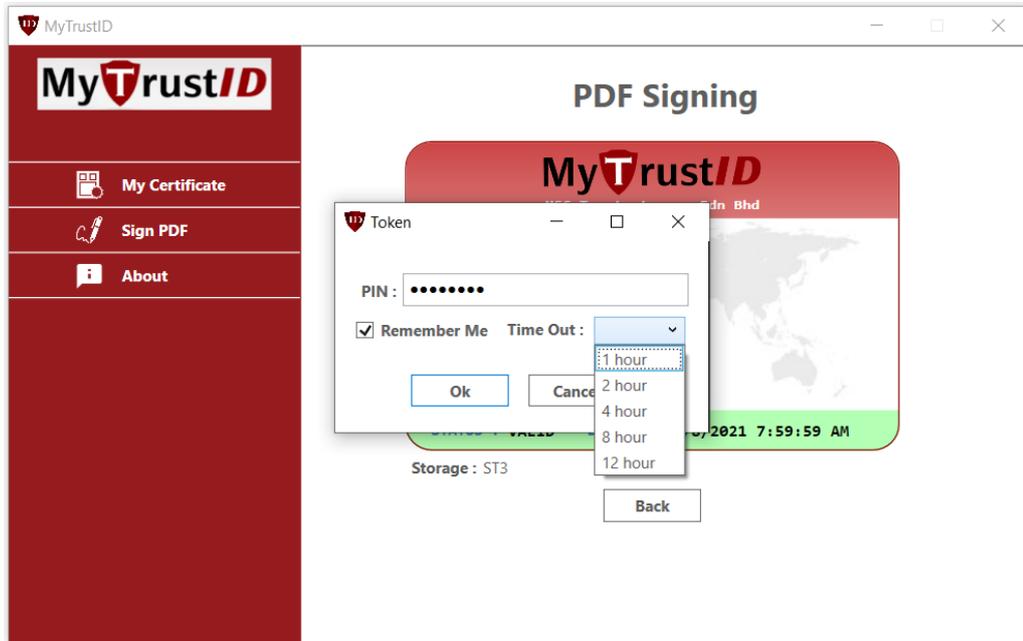2) Enter token PIN and tick remember me with selected timeout for subsequent signing

Figure 16: Dialog box for signing using token

3) The Application will read token and show another pop up for signing
4) Click **Sign** button to proceed with signing

Figure 17: Message for signing using token

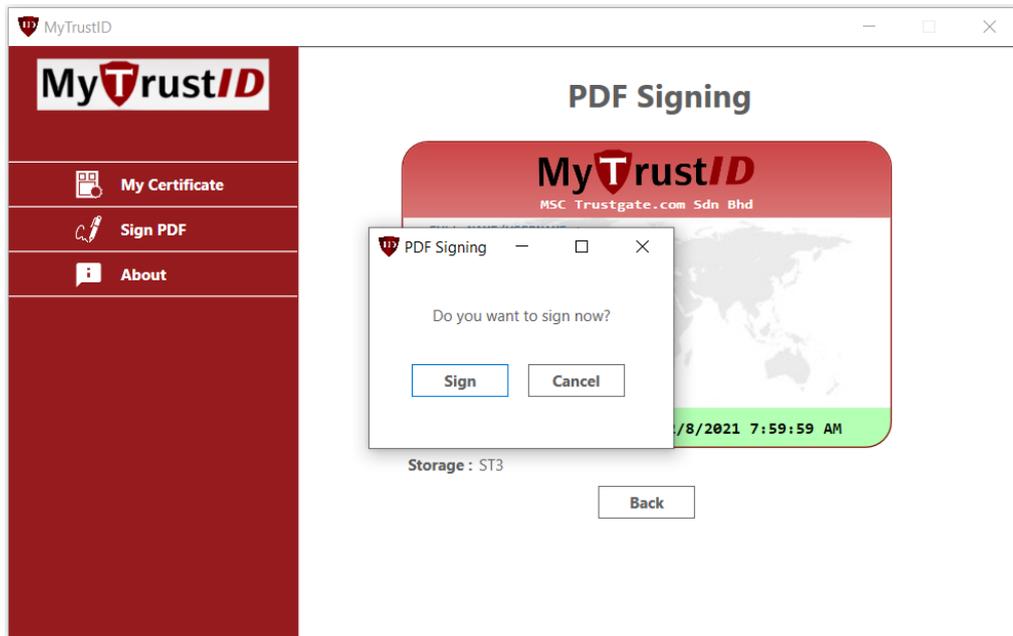5) It will close automatically after signing process is complete

3.2.   Signing hash using SoftCert with MyTrustID Desktop API

3.2.1. UserID not same as configured certificate

1)   Client system should integrate with MyTrustSignerServer
2)   MyTrustID Desktop app will show up with Select Storage message box if request userID is not same as configured certificate
3)   Select Softcert and Click **Ok**

Figure 18: Select Storage Type

4) Enter Token PIN and tick remember me with selected timeout for subsequent signing
5) Click button **Browse** to select softcert file from your directory
6) Enter SoftCert PIN and tick remember me with selected timeout for subsequent signing

Figure 19: Dialog box for signing using softcert

7) The Application will softcert and show another pop up for signing
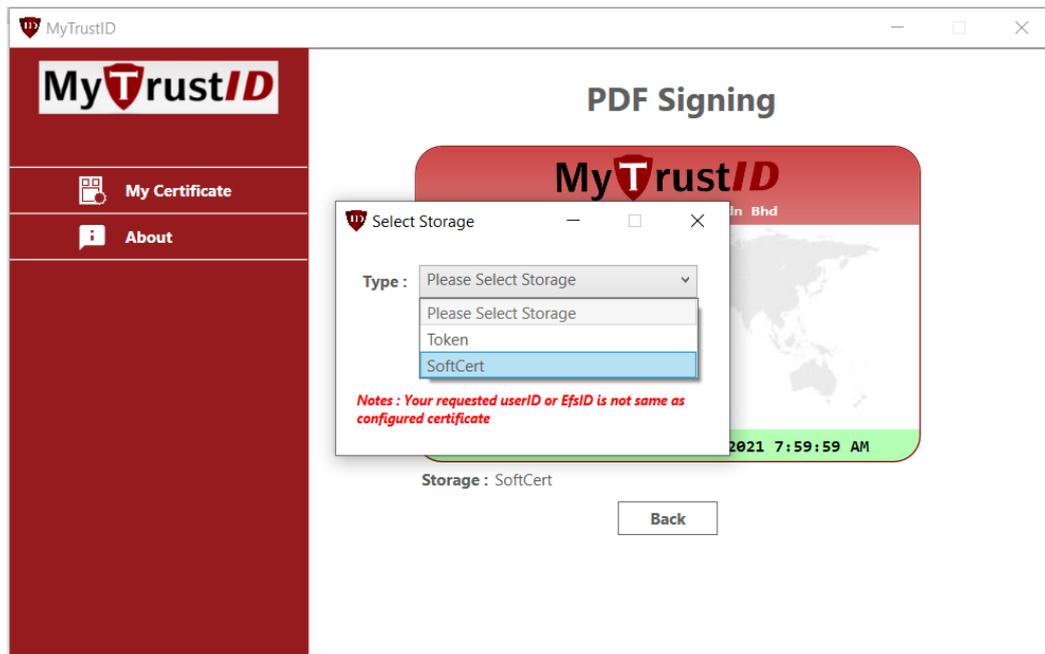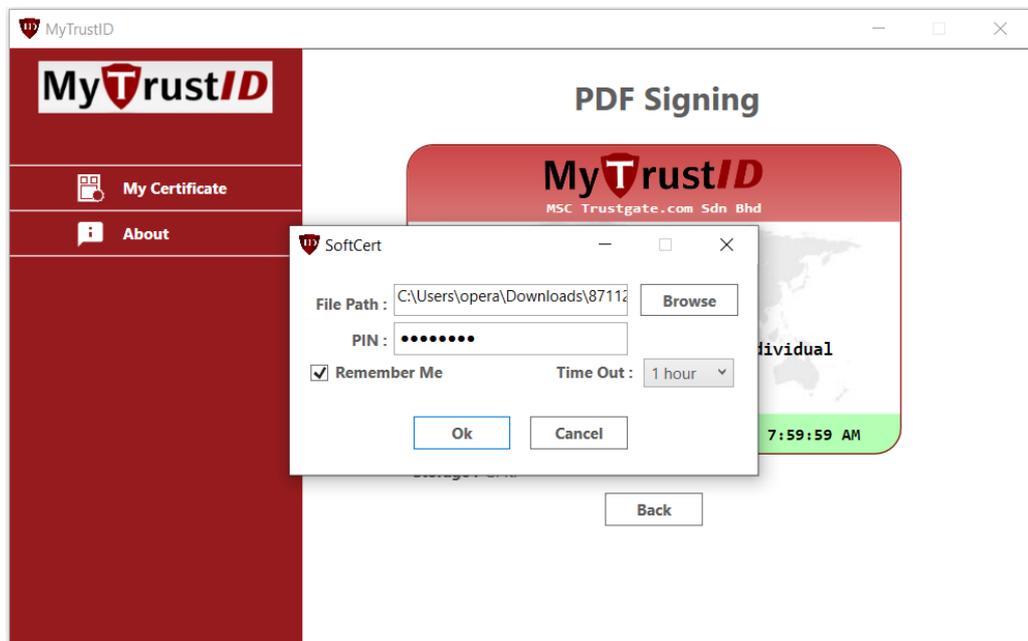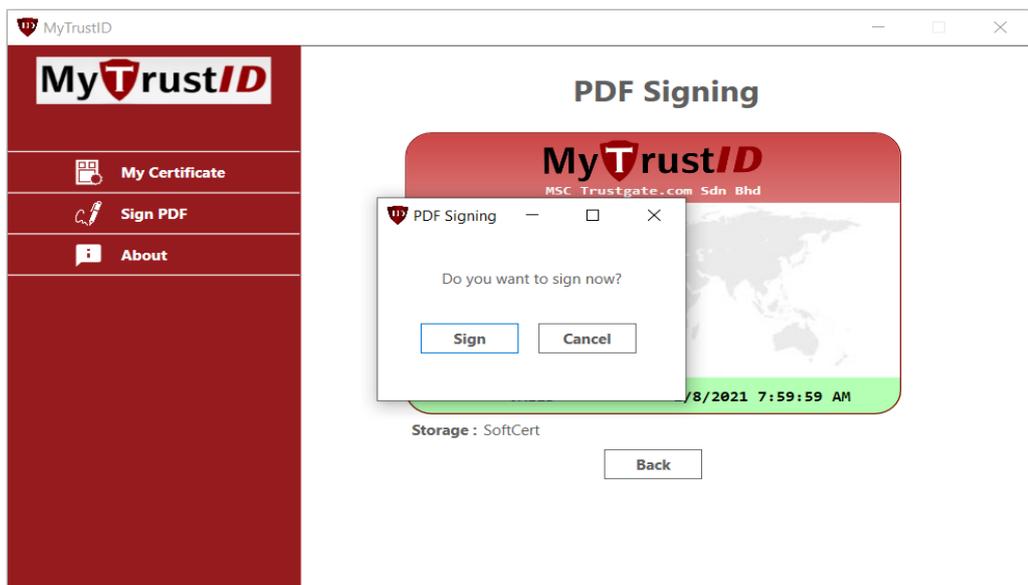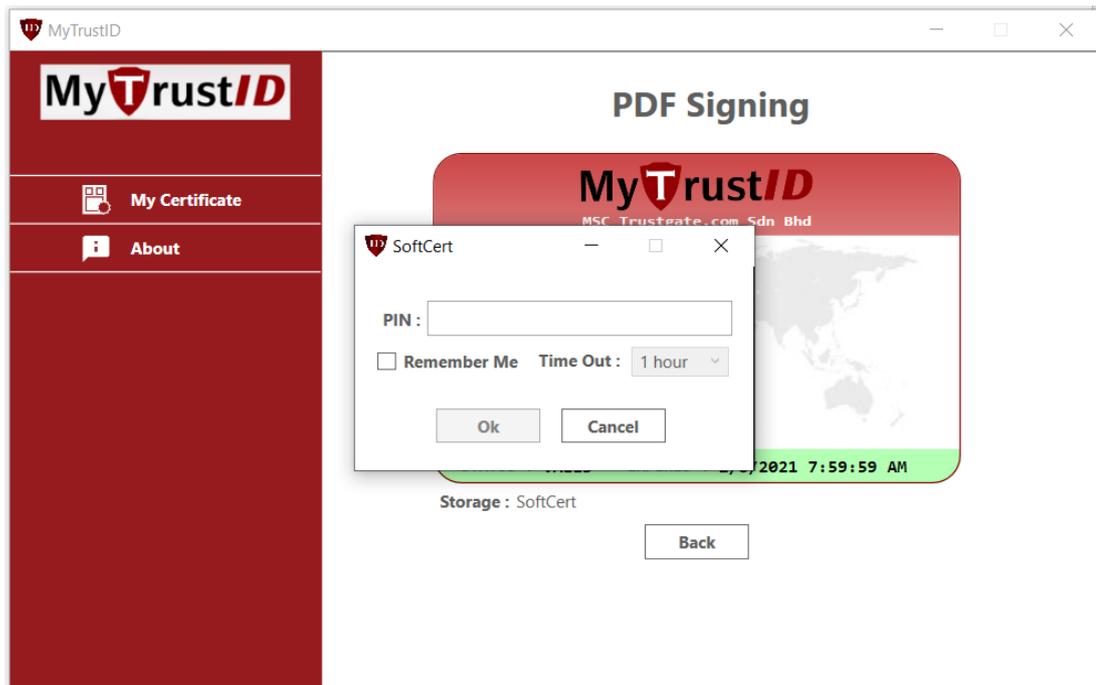8) Click **Sign** button to proceed with signing

Figure 20: Message for signing using softcert

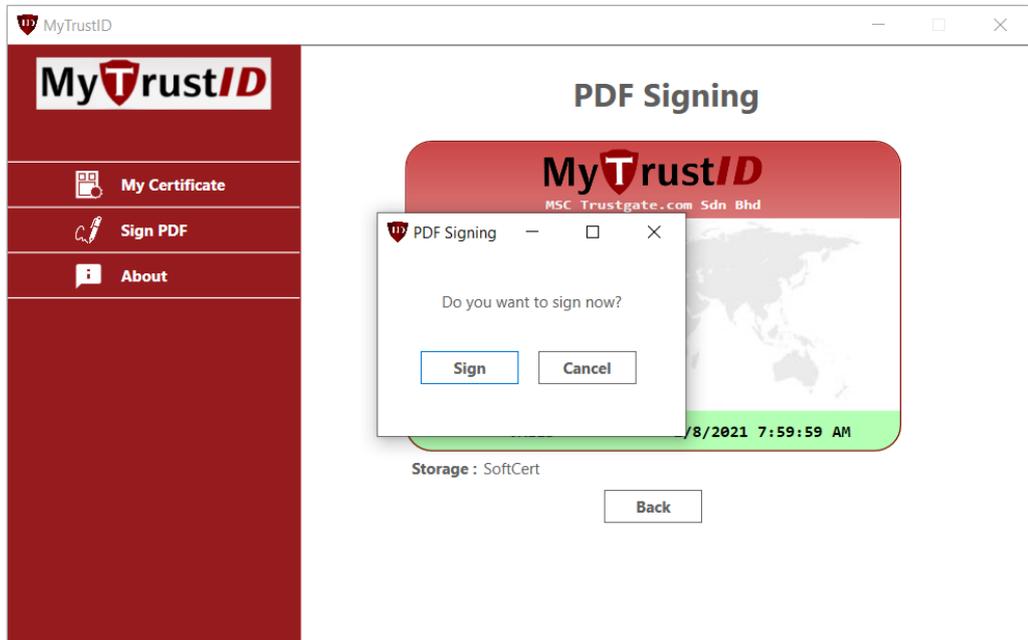9) It will close automatically after signing process is complete

3.2.2. UserID same as configured certificate

1) MyTrustID Desktop app will show up with insert Softcert PIN message box if request userID is same as configured certificate
2) Enter Softcert PIN and tick remember me with selected timeout for subsequent signing

Figure 21: Dialog box for signing using softcert

3) The Application will softcert and show another pop up for signing
4) Click **Sign** button to proceed with signing

Figure 22: Message for signing using softcert

5) It will close automatically after signing process is complete