User Manual

How to start using a certificate issued on a Gemalto IDPrime PKI token?

Version: 4.2

Date: 02.02.2022

103.18

KIBS AD Skopje

http://www.kibstrust.com/

Table of Contents

1. Purpose of use

This user manual is strictly intended for the users of Qualified certificates for qualified electronic signature: **Verba Sign PKI token and Verba Sign Pro PKI token.**

Those users who have obtained Gemalto IDPrime PKI token, with a generated pair of keys and a certificate, in a Local Registration Authority (LRA) of Certificate Authority KIBS (CA KIBS), and need to access the certificate trough Microsoft Internet Explorer, Google Chrome or Mozilla Firefox.

Definitions:

QSCD = Qualified Signature Creation Device

Gemalto IDPrime PKI token can refer to:

- Gemalto IDPrime MD 840 token (QSCD)
- Gemalto IDPrime MD 940 token (QSCD)
- Gemalto IDPrime .NET token (non QSCD, used in legacy certificates profiles)

The same software is used for all types of tokens.

The certificate is installed on Gemalto IDPrime PKI token, in the presence of the user, using a software for secure certificate management. This software guarantees that the private key is solely stored on the Gemalto IDPrime PKI token, which is delivered to the user.

NOTICE: The Gemalto Classic Client software is not applicable for Gemalto IDPrime token!

2. How to install the middleware software used for the Gemalto IDPrime PKI token?

2.1 Intro

In most of the cases, without additional middleware software installation, only with plugging the Gemalto IDPrime PKI token in your computer with Windows operating system, Plug&Play installation is initialized, and the certificate is loaded in your Internet Explorer web browser.

However, for better support for most recent versions of Windows 11 and Windows 10, our recommendation is to install the special package **SafeNet Authentication client (SAC Client)** from the following links:

For x86-based PC, for 32-bit operating system:
https://www.kibstrust.com/Storage/Support/Software/KIBSTrust-SAC-x32-10.8-R6.msi
For x64-based PC, for 64-bit operating system:
https://www.kibstrust.com/Storage/Support/Software/KIBSTrust-SAC-x64-10.8-R6.msi

Notes:

This software package replaces the need for separate installation of minidriver and PKCS#11 library. For Legacy, those packages are still available on our web site https://www.kibstrust.com/en-GB/Home/Support/:

1. You can download the older version of minidiver from the section “Software & Drivers”, part “**Minidrivers for Gemalto ID Prime (.NET & MD) PKI tokens**”

2. You can download the older version of PKCS#11 library, from the section “Software & Drivers”, part “**PKCS#11 Library for Gemalto ID Prime (.NET & MD) PKI tokens**”

IMPORTANT: Before installation of SAC Client, you need to uninstall minidriver and PKCS#11 library!

To make a right choice of the middleware packet (32 or 64-bits), check the type of your computer’s operating system by following the next procedure:

Click Start->Programs->Accessories->System Tools->System Information.

In the part: **OS name** is the information about the operating system version.

In the part: System Type, there is one of the following information:

- x86-based PC, for a 32-bit operating system
- x64-based PC, for a 64-bit operating system

Note: If you are our customer, you can obtain middleware software for Gemalto IDPrime PKI tokens for MAC and Linux Operation systems, after request via e-mail message to helpdesk@kibstrust.com.

2.2 Installation of middleware software on Windows operating system

Supported Windows operation systems for **SafeNet Authentication client** version 10.8 R6 are:

- Windows 11 (64-bit), Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit);
- Windows Server 2019 (64 bit), Windows Server 2016 (64 bit), Windows Server 2012 and 2012 R2 (64-bit), Windows Server 2008 R2 SP1 (32-bit, 64-bit), Windows Server 2008 SP2 (32-bit, 64-bit)

The installation process is very simple, following the screens and predefined values. The installation starts with double click of proper installation file (32-bit or 64-bit), and proceeds by clicking the **Next** button (Figure 1).

Figure 1

On next window, leave the predefined interface language – English, do not select “Use the existing configuration settings” and then click **Next** (Figure 2):

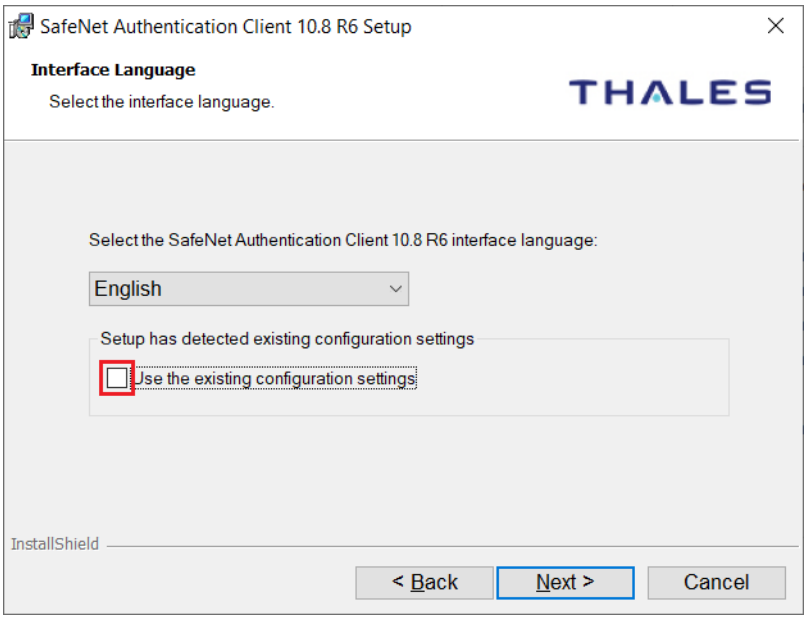

Figure 2

On the next window, select “I accept the terms in the license agreement”, and then click **Next** (Figure 3):

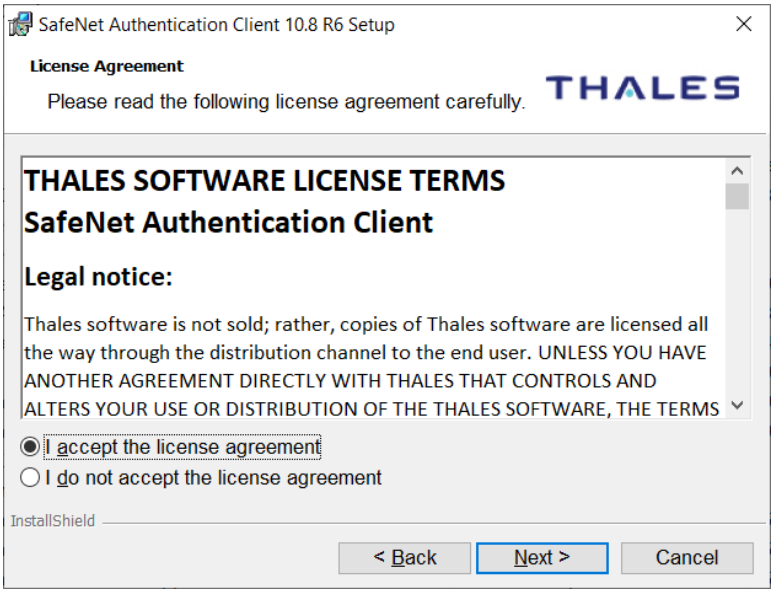

Figure 3

Leave the predefined installation path and choose **Next** (Figure 4):

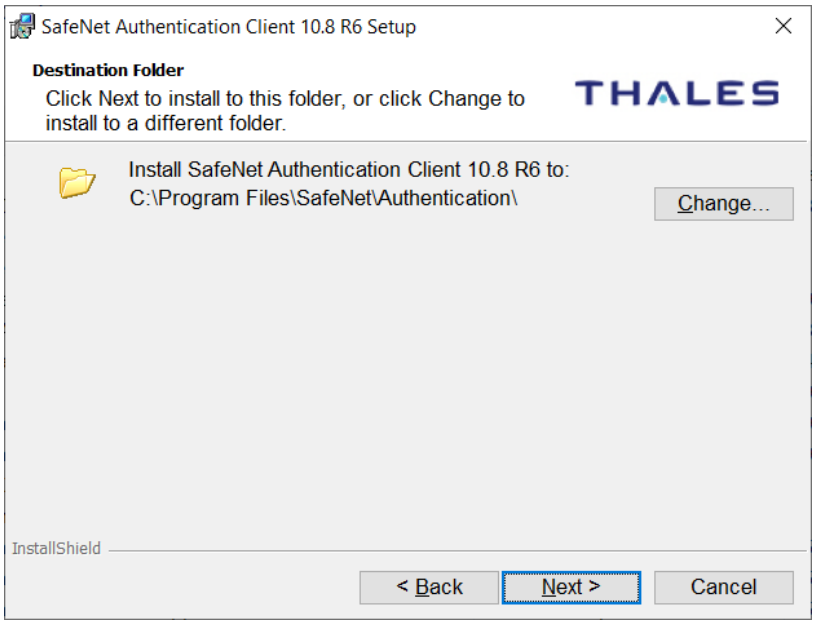

Figure 4

On next window (Figure 5), click **Install**:

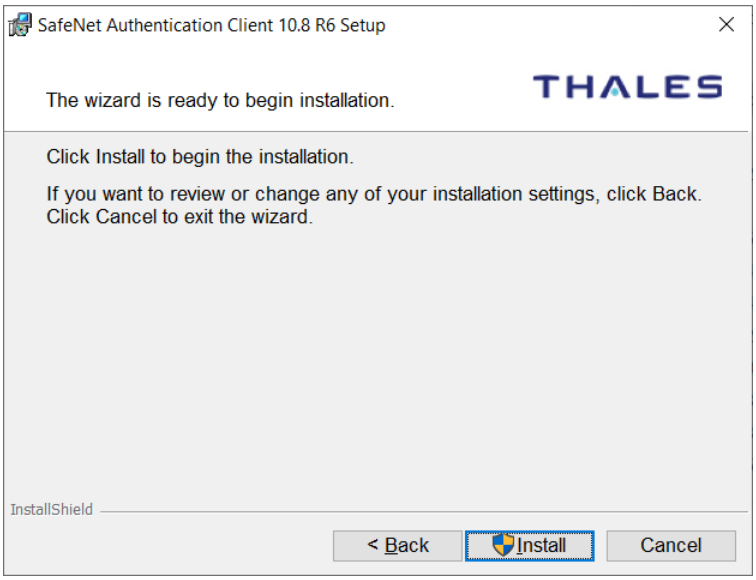

Figure 5

Wait for installation process (

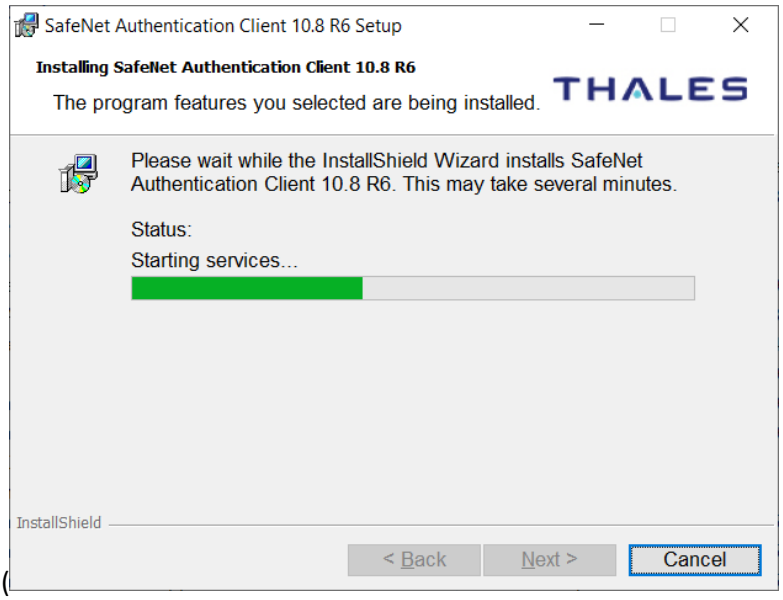

Figure 6):

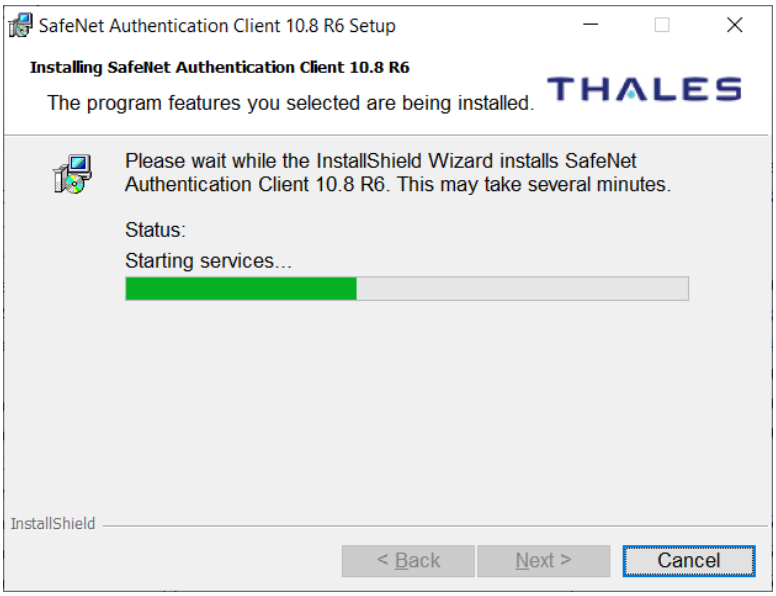

Figure 6

When the installation is finished, chose **Finish** (Figure 7):

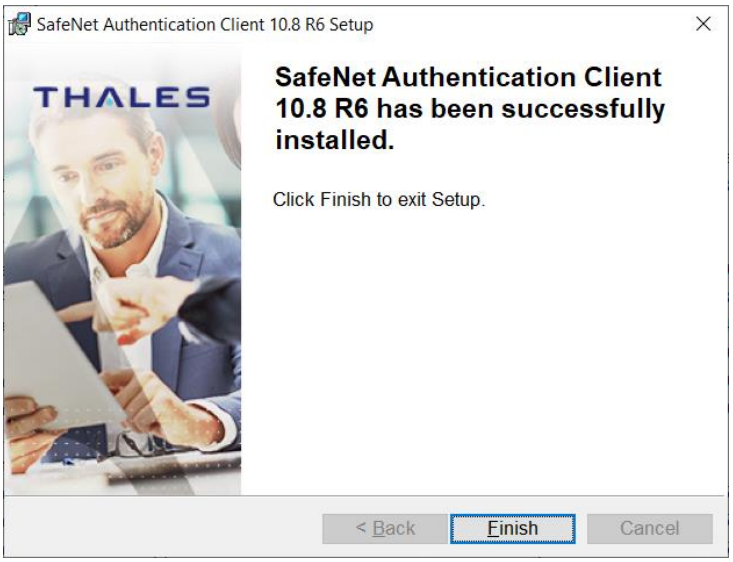

Figure 7

If you get the message like in Figure 8, restart the computer!

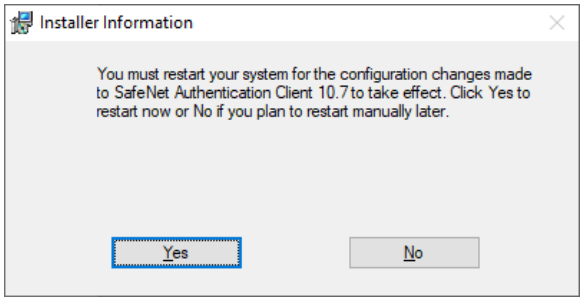

Figure 8

IMPORTANT: The procedure of installing the middleware software described in part 2.2 should be repeated on each PC on which you intend to use the Gemalto IDPrime PKI token.

3. Check the content of the Gemalto IDPrime PKI token

After the installation of middleware software SAC, you will notice icon in the right down corner of your screen. When you plug in your PKI token, the icon gets fulfilled red color: . When you right click on the icon, you can see the following information about Your PKI token, like in Figure 9:

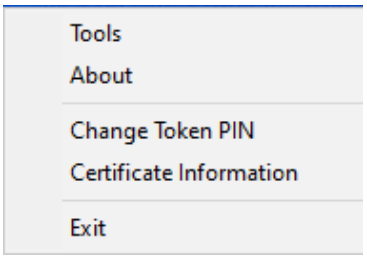

Figure 9

If You choose “Certificate Information“, You should get the Figure 10.

Under “User” type, the user certificate is shown.

Under “CA” type, the intermediate certificates are shown.

You can open certificates by double click and check their characteristics.

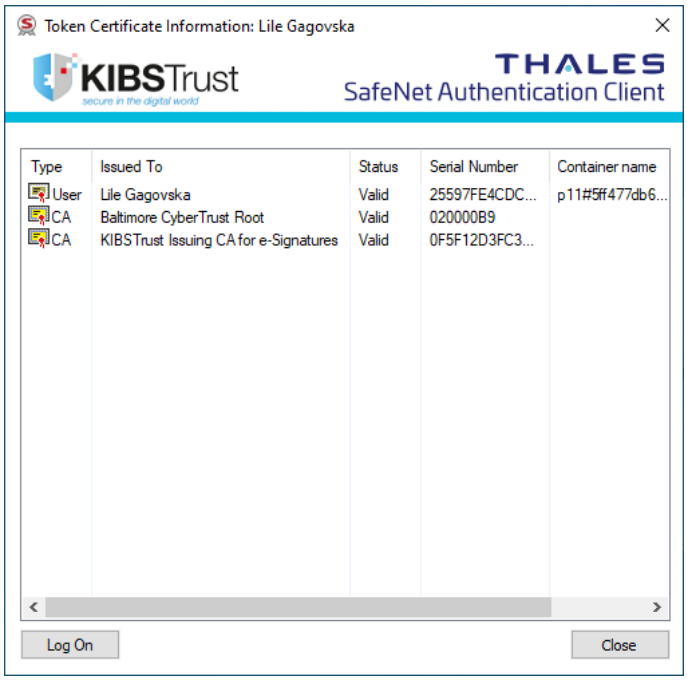

Figure 10

4. Change of user PIN

You can change Your current PIN with right click on the icon , where you can choose “Change Token PIN“ and you can set new PIN, by entering current PIN, see Figure 11:

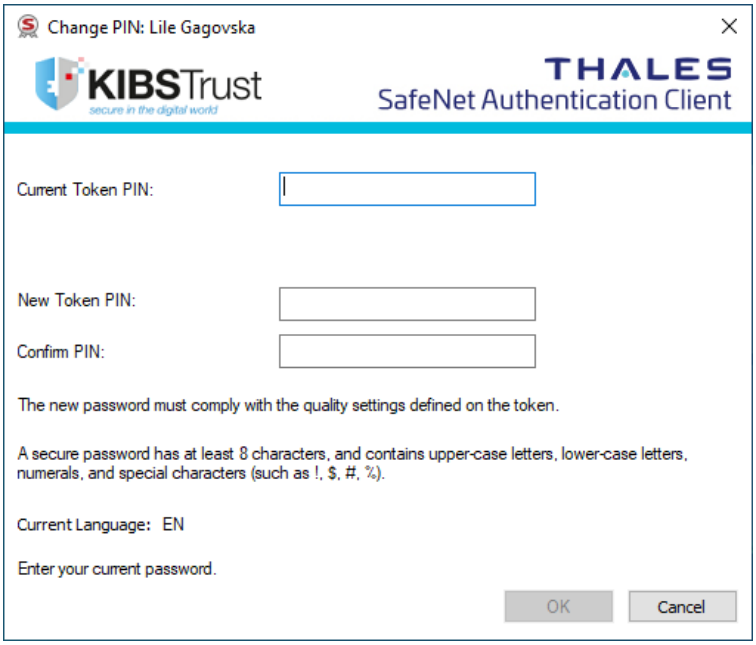

Figure 11

You can reach the same “Change Token PIN” menu (Figure 11) trough right click on icon then choose Tools, and (Figure 12**Error! Reference source not found.**) choose „Change Token PIN“.

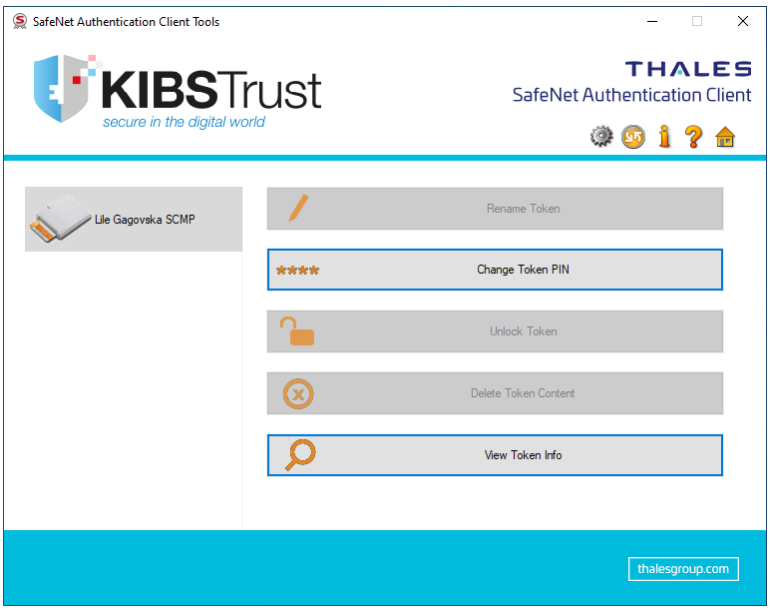

Figure 12

5. Token information

With right click on icon we choose „Tools“(Figure 11**Error! Reference source not found.**) then „View Token Info” and you will get your PKI token information, as shown on Figure 13 .

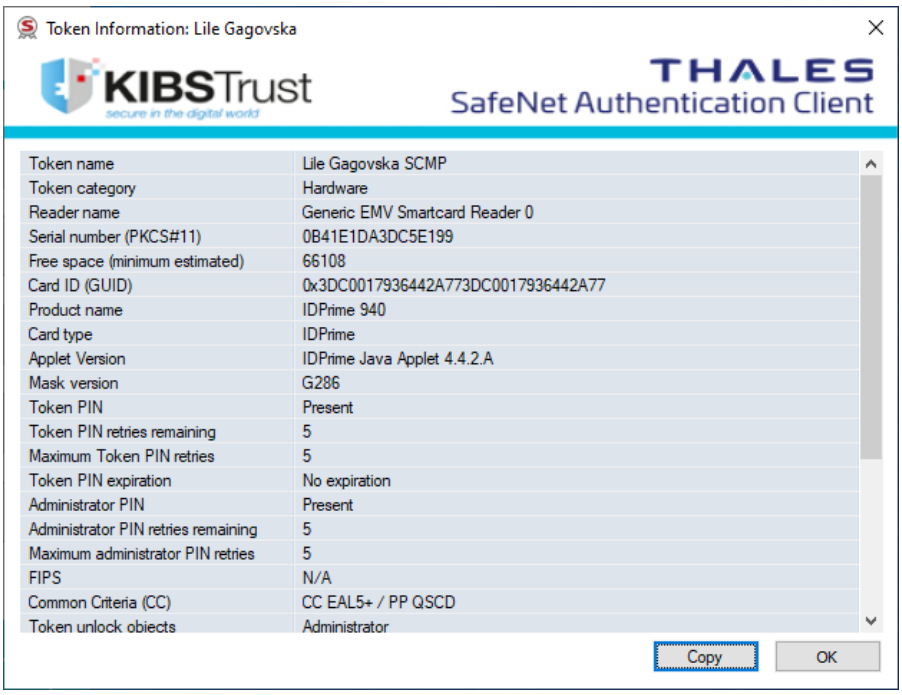

Figure 13

6. How to check if the certificate from my Gemalto IDPrime PKI token is shown in Internet Explorer?

6.1 How to check if the certificate is shown in Internet Explorer

You need to insert the Gemalto IDPrime PKI token in the PC, which has the SAC middleware software installed, according to part 2.2 of this user manual.

Open the web browser Internet Explorer and from the menu, choose **Tools** ->**Internet Options** (Figure 14)

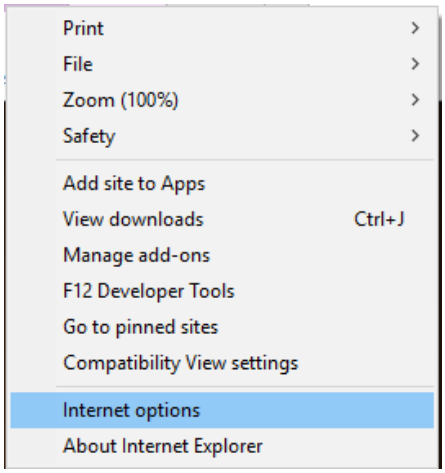

Figure 14

In the new window, choose the **Content** tab and click on **Certificates** (Figure 15).

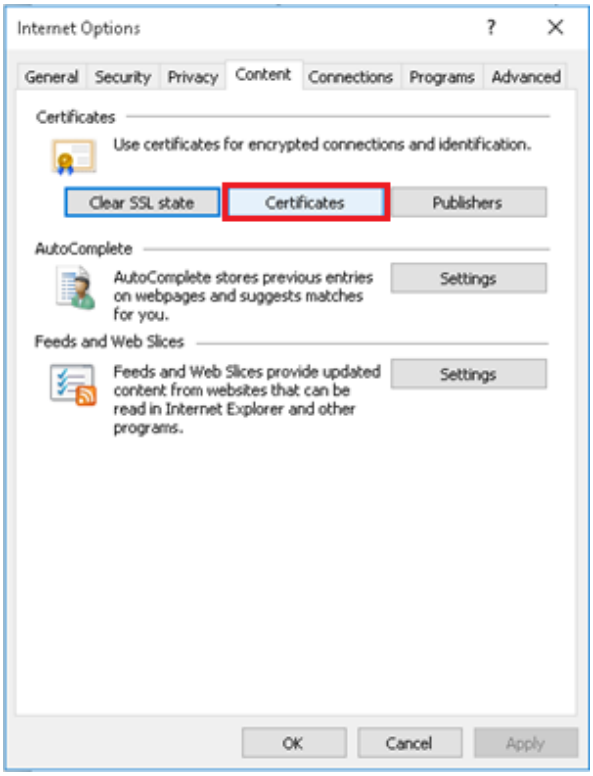

Figure 15

Your certificate should be in **Personal** tab (Figure 16).

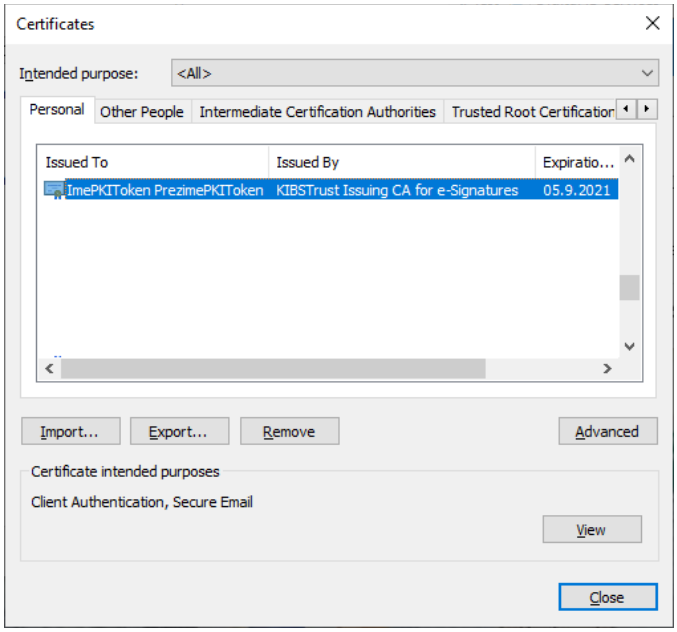

Figure 16

When double-click on the certificate you should get a preview like on Figure 17, which shows information regarding the certificate.

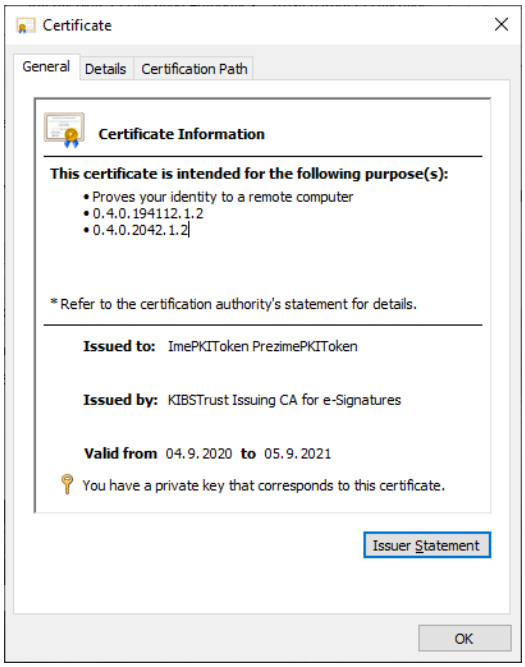

Figure 17

After that, check the **Certification Path**. There are two possible previews:

1. If the preview is like on Figure 18 all the settings for the certificate are OK and it is ready for use.

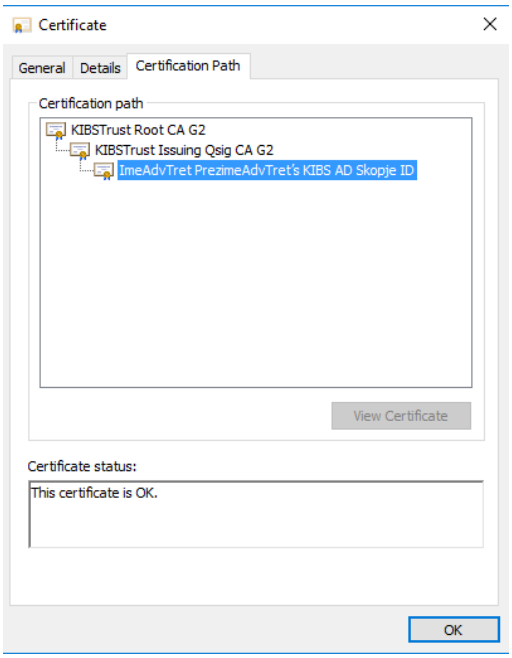

Figure 18

2. If the preview is like on Figure 19 (only the name and surname are shown) or only one root certificates is shown, **you must continue with part 6.2.**

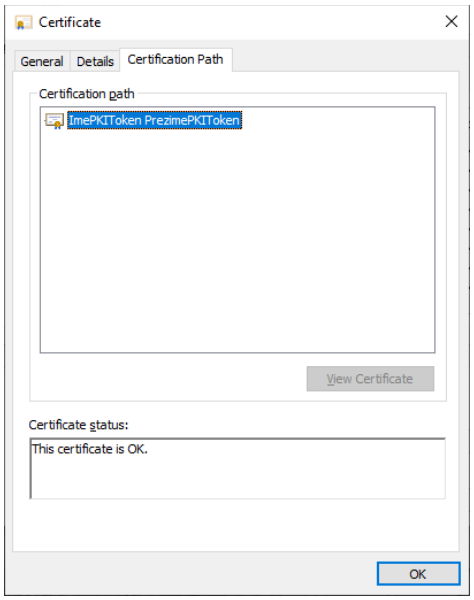

Figure 19

6.2 Installation of root certificates in Internet Explorer

If some of KIBSTrust root certificates is missing in the certificate chain, you can download them from section **Root certificates** from https://www.kibstrust.com/en-GB/Home/Support/ and please install them:

KIBSTrust Root CA G2 (install in Trusted Root Certficate Authorities)
KIBSTrust Issuing Qsig CA G2 (install in Intermediate Certificate Authorities)

After importing the two root certificates, make sure you get a preview as in one of the pictures in Figure 18!

The installation is described in one of the FAQ on the following link: https://www.kibstrust.com/en-GB/Home/Support "How to install root certificates in Internet Explorer".

7. Does my certificate from the Gemalto IDPrime PKI token is shown in Google Chrome?

7.1 Check if the certificate is shown in Google Chrome

Gemalto IDPrime PKI should be inserted in the computer where the middleware software is installed, according 2.2 from this manual.

Open Google Chrome, then Settings, Privacy and Security, Security, Manage Certificates. Open User Certificate store, as is open in Internet Explorer.

8. How to check if the certificate from my Gemalto IDPrime PKI token is shown in Mozilla Firefox?

8.1 Adding a Gemalto IDPrime PKI token as a security device

To access the certificate issued on Gemalto IDPrime PKI token, in Mozilla Firefox, beside the installation of middleware software, you need to add proper security device.

From the browser menu click on the right upper button and select **Options** (**Error! Reference source not found.**Figure 20):

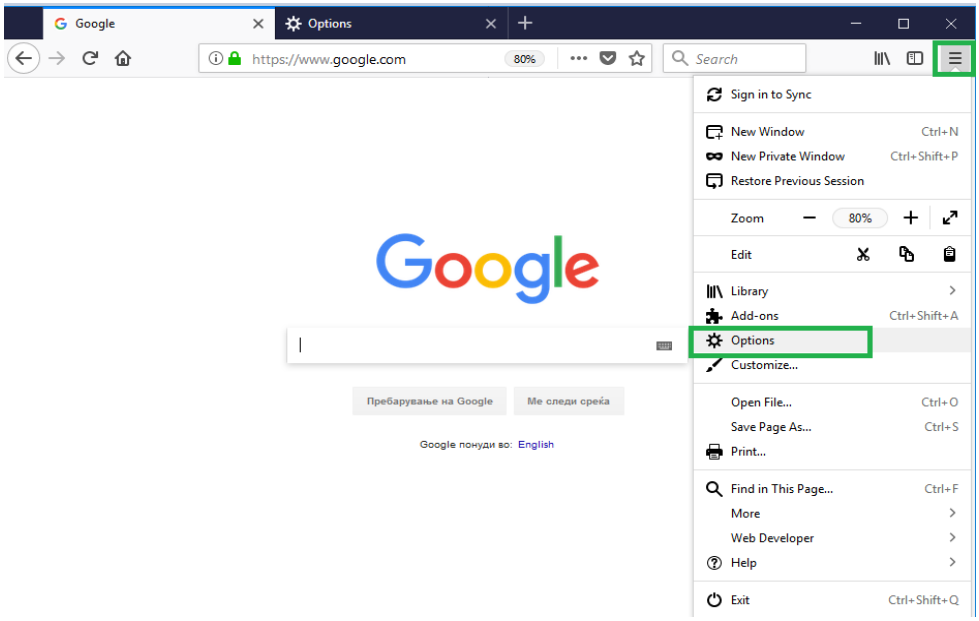

Figure 20

In the new tab select the **Privacy & Security** option from the menu on the left side, go down and click on the **Security Devices** button (Figure 21)

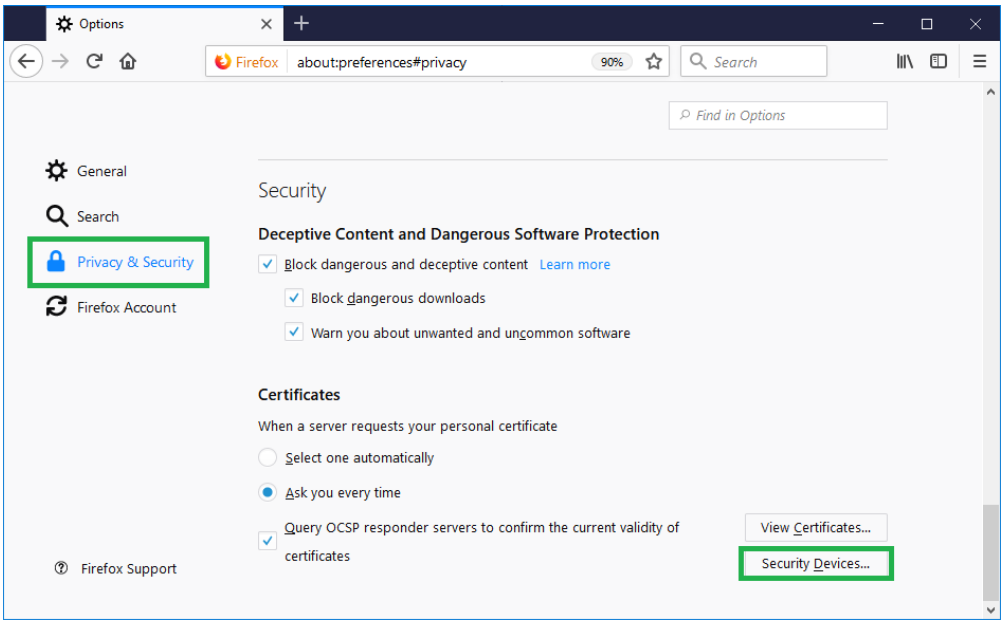

Figure 21

In the next window click **Load** (Figure 22)

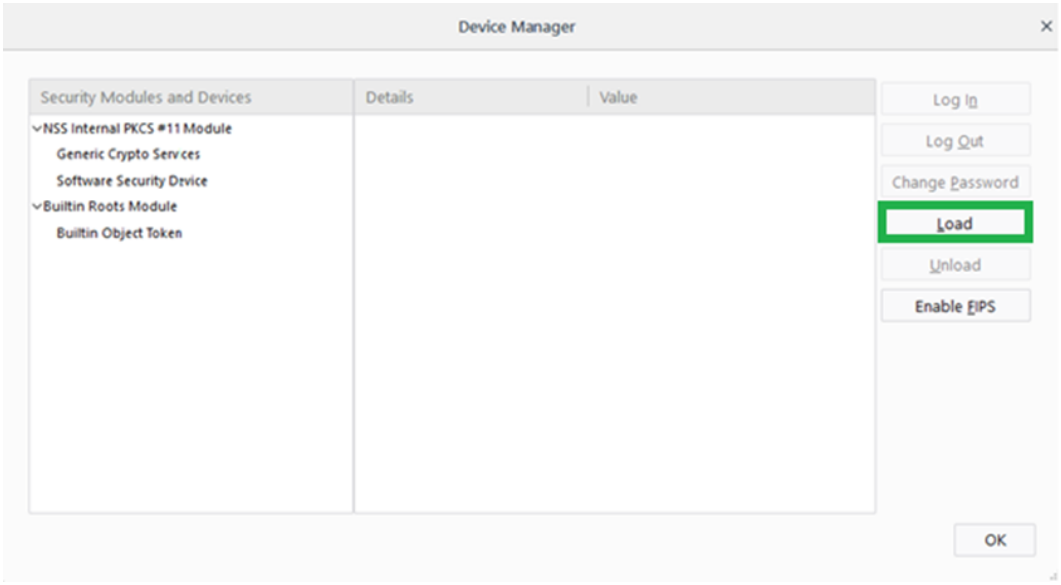

Figure 22

In the new window, in the field **Module Name** enter „Gemalto IDPrime“ and click **Browse** (Figure 23) in order to find the required file.

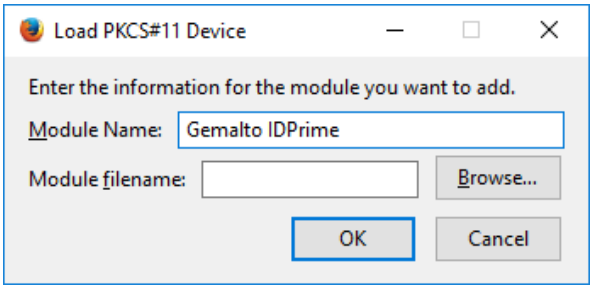

Figure 23

The file is located in:

- C:\Program Files (x86)\Gemalto\IDGo 800 PKCS#11 (for 64-bit OS), or
- C:\Program Files\Gemalto\IDGo 800 PKCS#11 (for 64-bit OS).

Select the file **IDPrimePKCS11.dll** for 32-bit version of Mozilla Firefox (or IDPrimePKCS1164.dll for 64-bit version) and click **Open** (Figure 24) and then click **OK** (Figure 25).

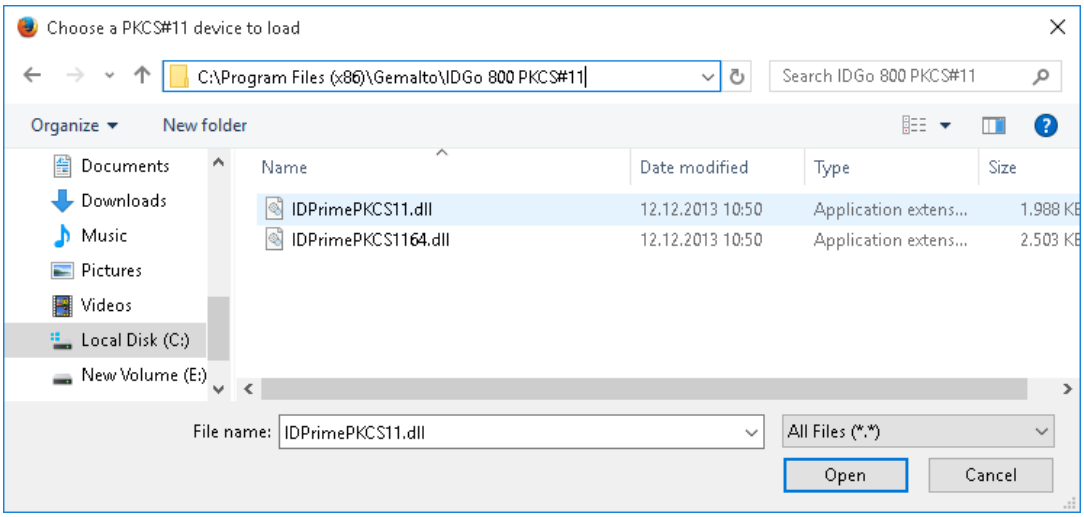

Figure 24

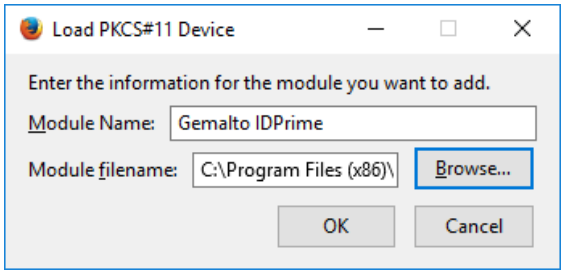

Figure 25

Your PKI token Gemalto IDPrime is now shown in the list on the left side of the window (Figure 26)

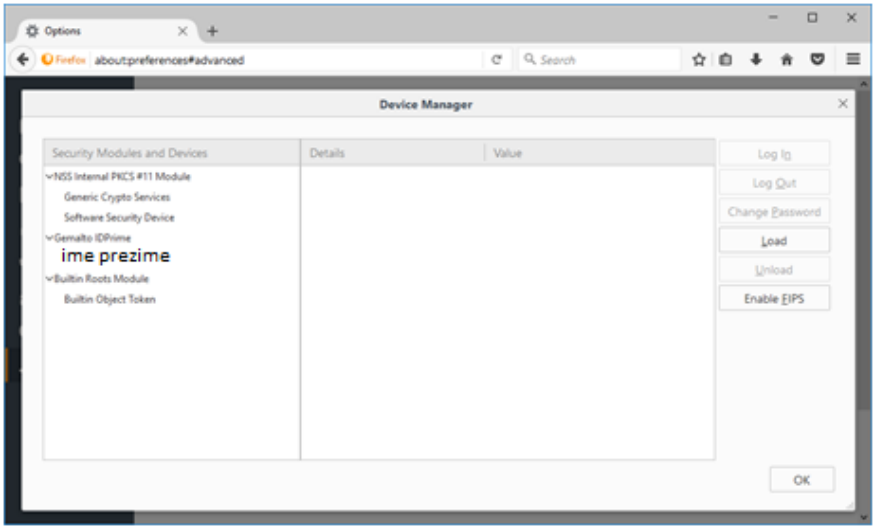

Figure 26

Click **OK** two times to close the window.

8.2 How to check if the certificate from the Gemalto IDPrime PKI token is shown in Mozilla Firefox?

The Gemalto IDPrime PKI token should be inserted in the PC. Open the web browser Mozilla Firefox, click on the right upper button, and select **Options,** select the **Privacy & Security** option from the menu on the left side, then click on the button **View Certificates** (Figure 27).

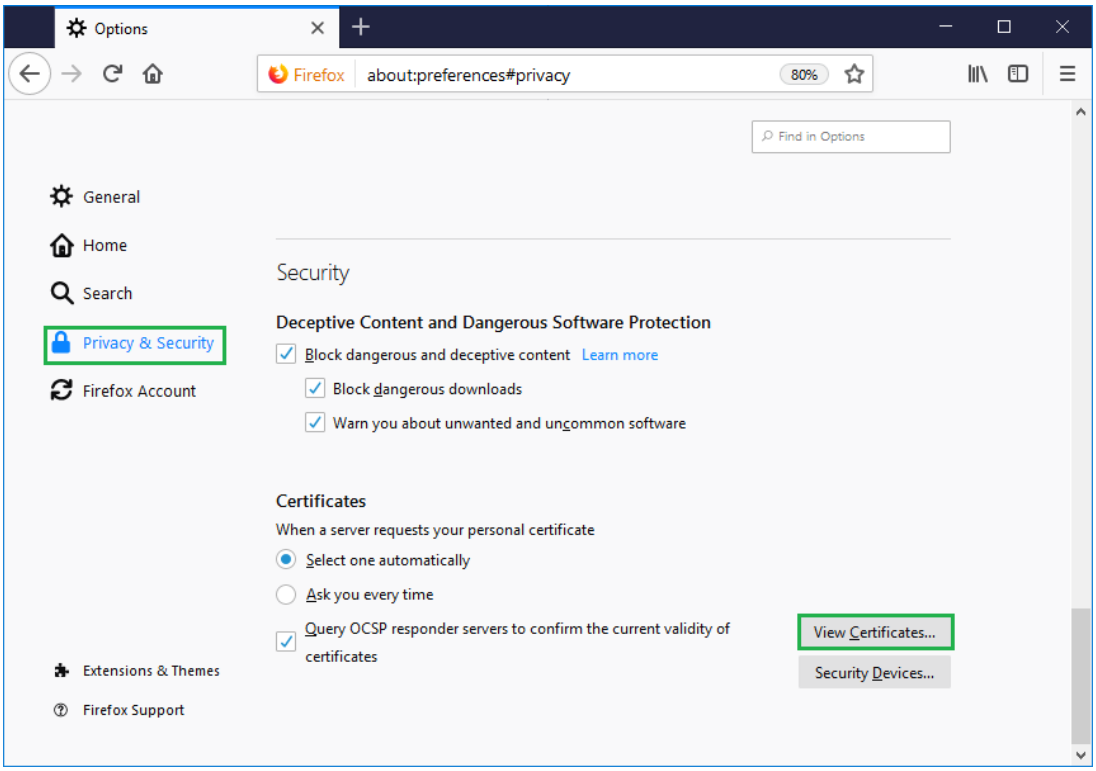

Figure 27

In the next window (Figure 28) a password is required, **DO NOT ENTER ANYNOTHING,** just click OK or Cancel:

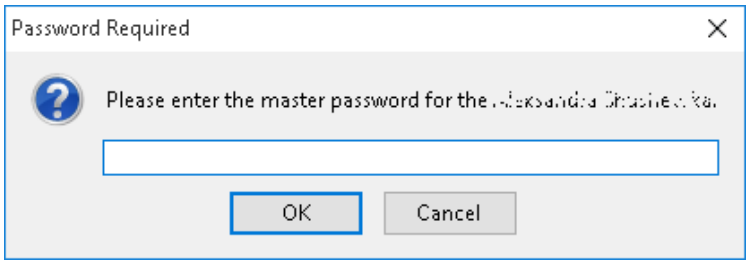

Figure 28

Your personal certificate is located in **Your Certificates** (Figure 29)

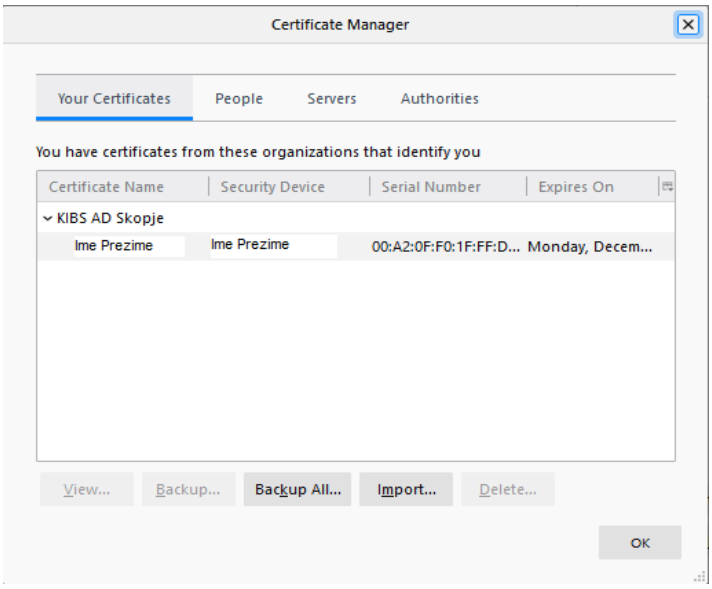

Figure 29

8.3 How to install root certificates in Mozilla Firefox?

Save locally root certificate's files from:

KIBSTrust Root CA G2

KIBSTrust Issuing Qsig CA G2,

Than you can go to Options, Privacy & Security, View Certificates, Authorities chose Import and browse to local path where you have saved the certificates and import them one by one.

The installation of root certificates more detailed is described in one of the FAQ on the following link https://www.kibstrust.com/en-GB/Home/Support "How to install root certificates in Mozilla Firefox?"

***