1 Table of contents

Information about the document	
Date of creation	04.06.2009
Topic	Institution's certificates
Reference	
Recipient	Users of the institution's certificates
Prepared by	Urmo Keskel
Version	1.2

Version information		
Date	**Version**	**Changes**
04.06.2009	0.1	Initial version
09.06.2009	0.2	Added the correct CSR generation website link and the requirements for CSR generation website are described.
07.05.2010	0.3	The manual for Aladdin is redone, using the manual written for IKey in 2009 as the base.
08.07.2010	0.4	Added Aladdin software URL, instructions regarding Windows Vista and Windows 7 are removed (since the respective update is not yet ready), description of additional devices during initialization of a token is removed.
16.12.2010	1.0	The CSR generation address is updated, explanations regarding Windows Vista and Windows 7 are added. Support for 2048-bit keys and FIPS is added.
07.02.2011	1.1	FIPS settings during the token initialization are changed, warning during the initialization is added, there was a wrong CSR generation address on page 8.
13.11.2012	1.2	The manual is updated to describe use of Authentication Client 8.1 SP1 software.

2 The aim of this document

The purpose of this document is to describe the procedure of installing the institution's certificates to eToken Pro encryption token and other actions in relation to this procedure. The procedure involves initialization of the encryption token, changing PIN codes, generation of keys and certificates as well as uploading the certificate on a smartcard. The manual is prepared for SafeNet eToken Pro encryption token, but should also be applicable to all SafeNet eToken tokens with SafeNet Authentication Client 8.1 software (e.g. eToken Pro Anywhere, eToken NGFlash)

3 Description of actions

3.1 Software installation

Install SafeNet Authentication Client software necessary for use of Token.

Download software here: https://installer.id.ee/media/etoken/

The ZIP archive contains the following files:

File name	**Description**
SafeNetAuthenticationClient-eToken-x32-8.1-SP1.msi	Software installation package for 32-bit Windows operating systems
SafeNetAuthenticationClient-eToken-x64-8.1-SP1.msi	Software installation package for 64-bit Windows operating systems
SAC_8.1_SP1_User_Guide_Rev_A.pdf	SafeNet Authentication Client user manual
SafeNetAuthenticationClient_8_1_SP1Windows key.txt	Software license key. **Attention! Only the users who purchase an authorization token from SK have the right to use the key.**

Operating systems supported by SafeNet Authentication Client 8.1:
Windows XP SP2, SP3 (32-bit, 64-bit)
- Windows Server 2003 SP2 (32-bit, 64-bit)
- Windows Server 2003 R2 (32-bit, 64-bit)
- Windows Vista SP2 (32-bit, 64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2008 SP1 R2 (64-bit)

Where the computer already has eToken PKI Client 5.1 distributed by SK, there is no need to uninstall it separately.

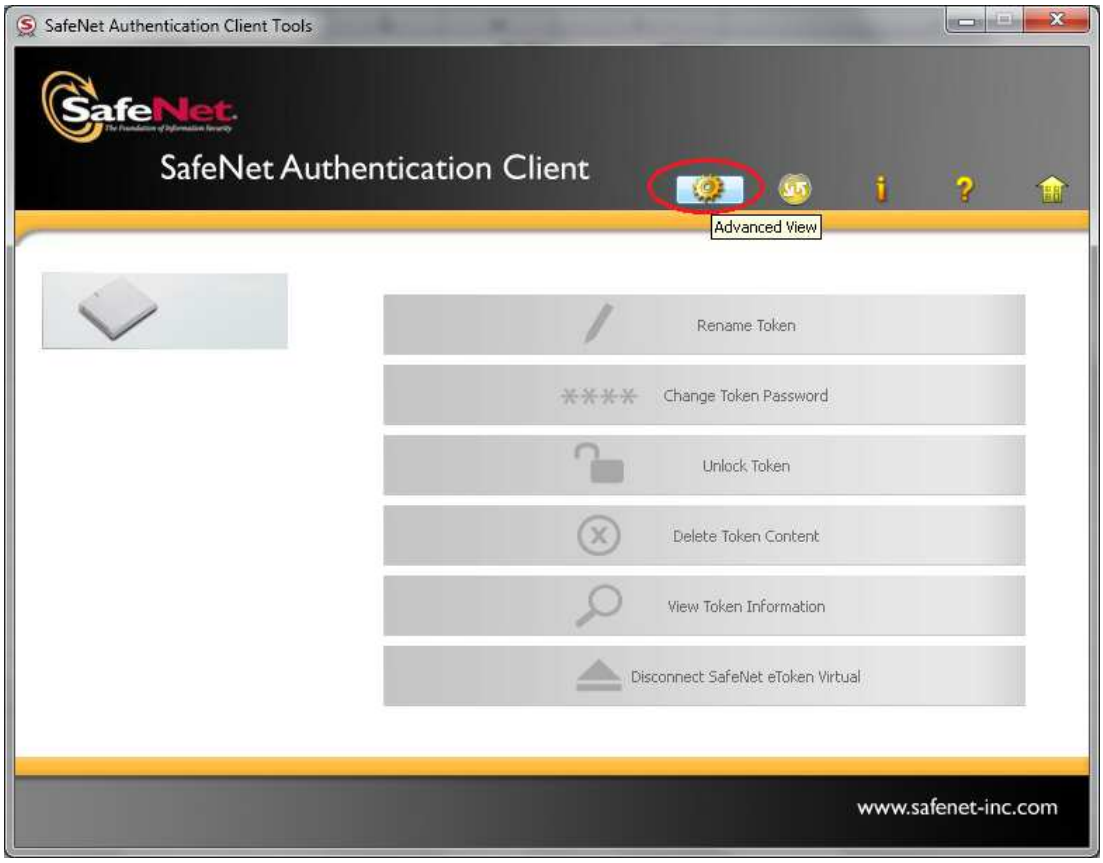
After installation "SafeNet Authentication Client Tools" will appear in Start menu under "All Programs->SafeNet->SafeNet Authentication Client". You may also launch the program from the Taskbar (Safenet Authentication Client icon).

After installation of the program it is necessary to import the license file using SafeNet Authentication Client Tools. It is done through "About" menu.

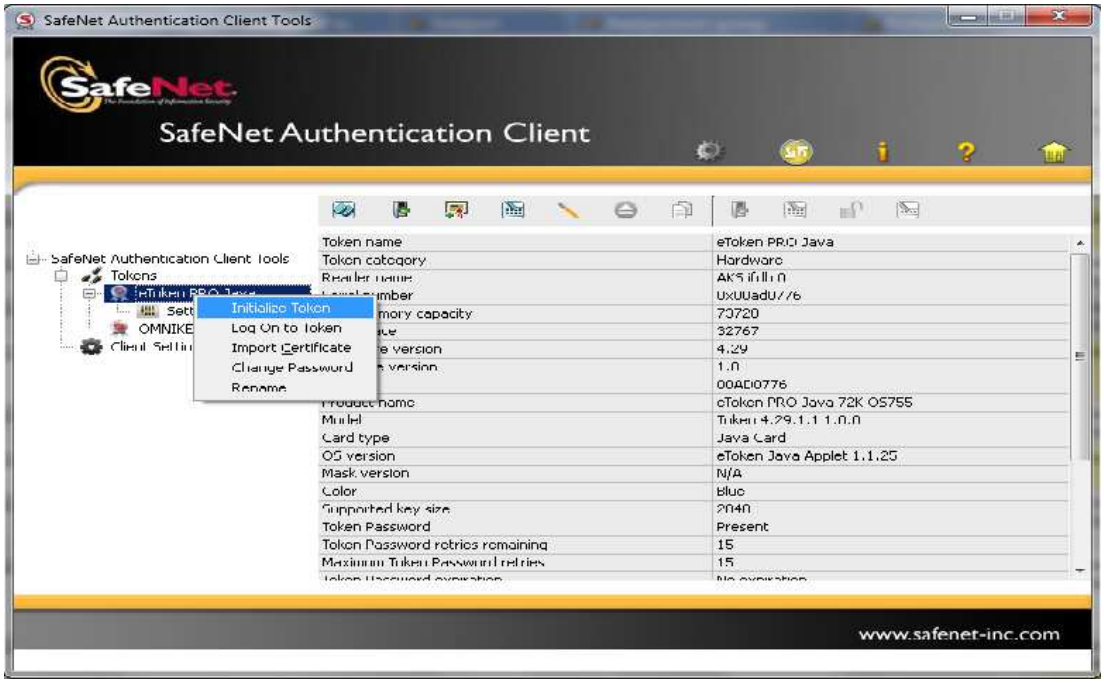
3.2 Initialization of a token

WARNING! After initialization of a token any certificates and keys it contains will be deleted. This action is to be performed only where no certificates have yet been installed to the token, or where all issued certificates are out of date. If you wish to apply several certificates to a single token so that earlier certificates are not deleted, you SHOULD NOT PERFORM INITIALIZATION and should skip to Section 3.3 of this manual (Generation of the certificate application).

In order to initialize the token launch eToken PKI Client by clicking Safenet Authentication Client ( ) icon on the Taskbar or by selecting All Programs->SafeNet-> SafeNet Authentication Client -> SafeNet Authentication Client Tools from the Start menu.



In the opened view select the Token with the right mouse button and choose "Initialize" from the context menu.

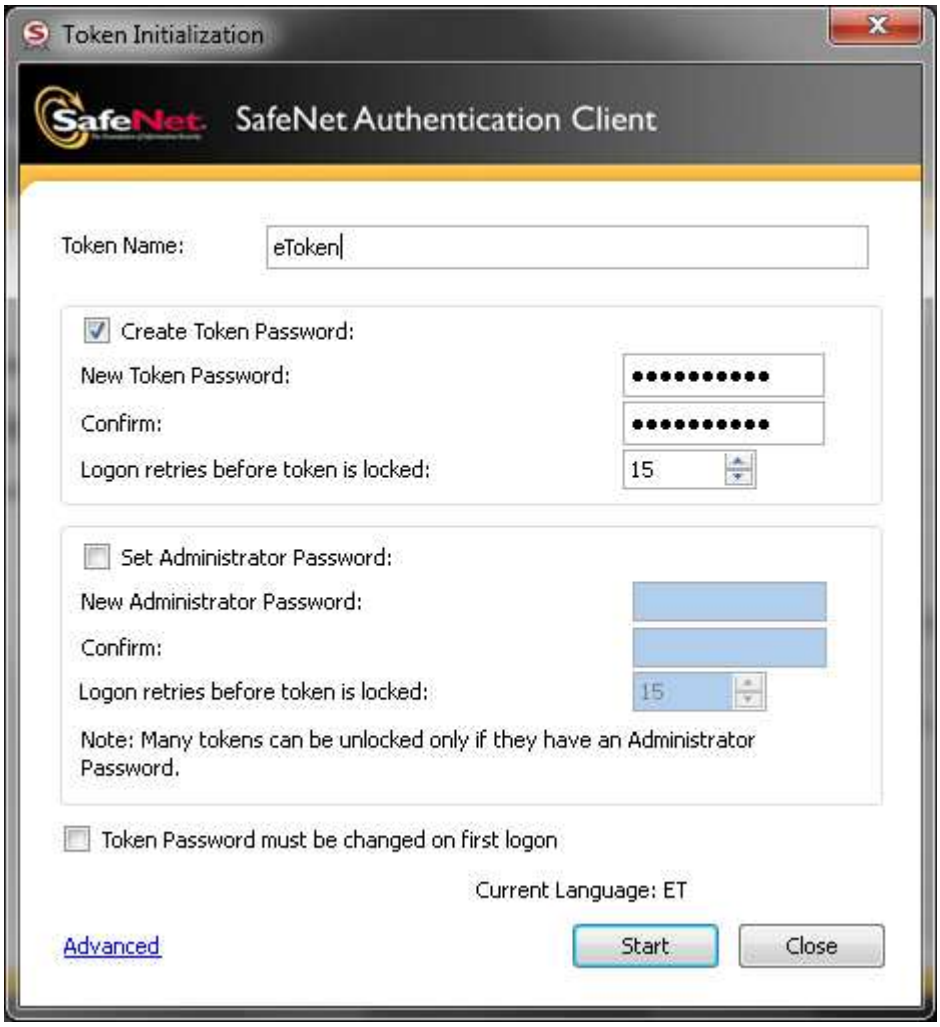


First provide the Token name (name of the institution, division etc.) so that you can easily recognize it later.

It is important if several Tokens are used in the same system. Then create the Token Password.

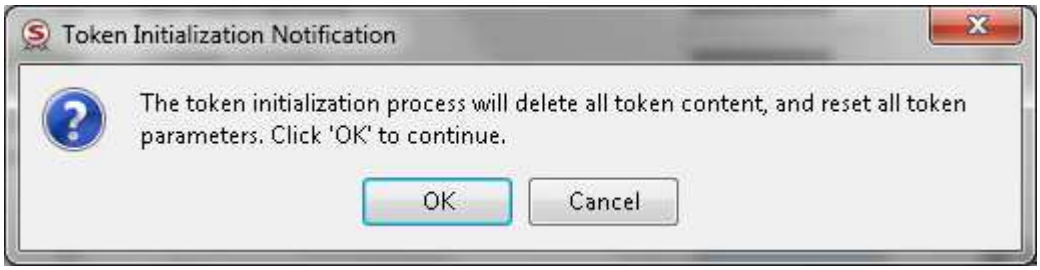
It is also recommended to set the Admin password (it is used to unlock the Token Password). 5 logon retries are allowed.

If you choose not to indicate the Administrator password, keep in mind that in case your Token password gets locked, you will have to initialize the Token and order new certificates!



Now launch Token initialization by clicking "Start" (see the previous screenshot).

The following warning will be displayed:



Attention! Agree with the warning and launch the initialization process only if the token does not have any keys/certificates on it that you want to use. After clicking OK you will see an overview of the initialization process:

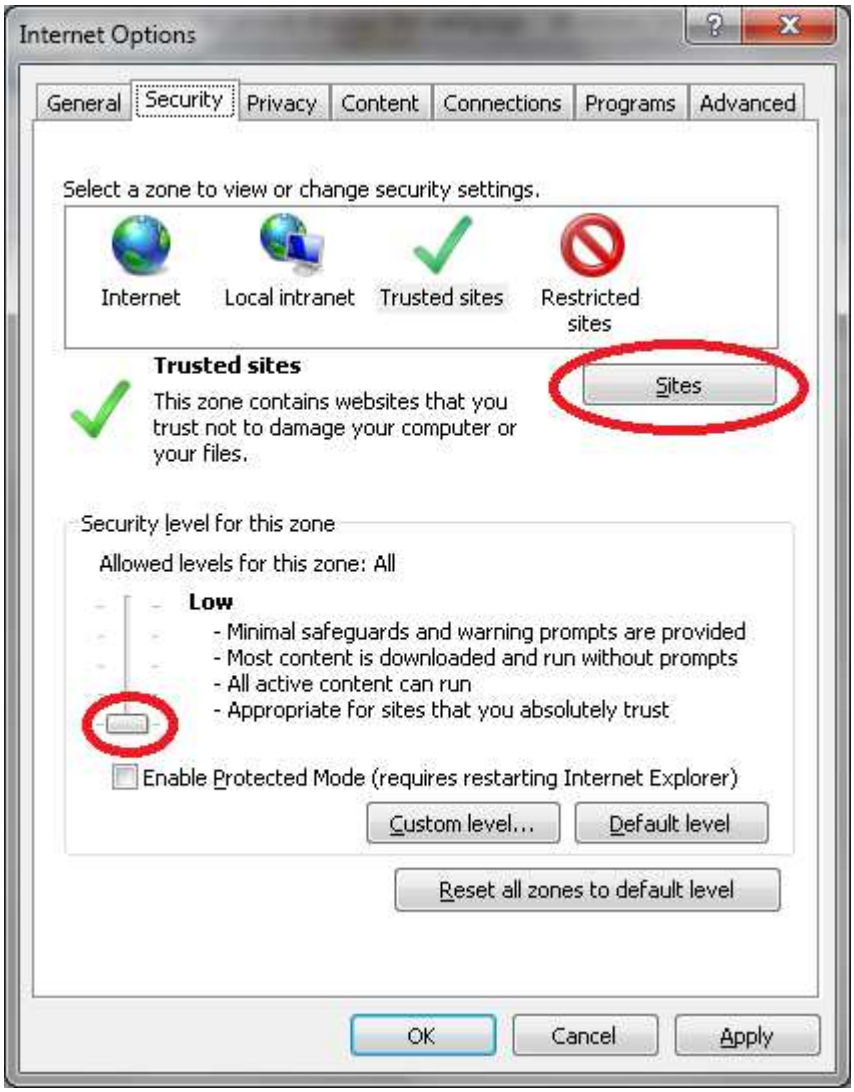
and will be informed about successful completion of initialization:

3.3 Generation of the certificate application

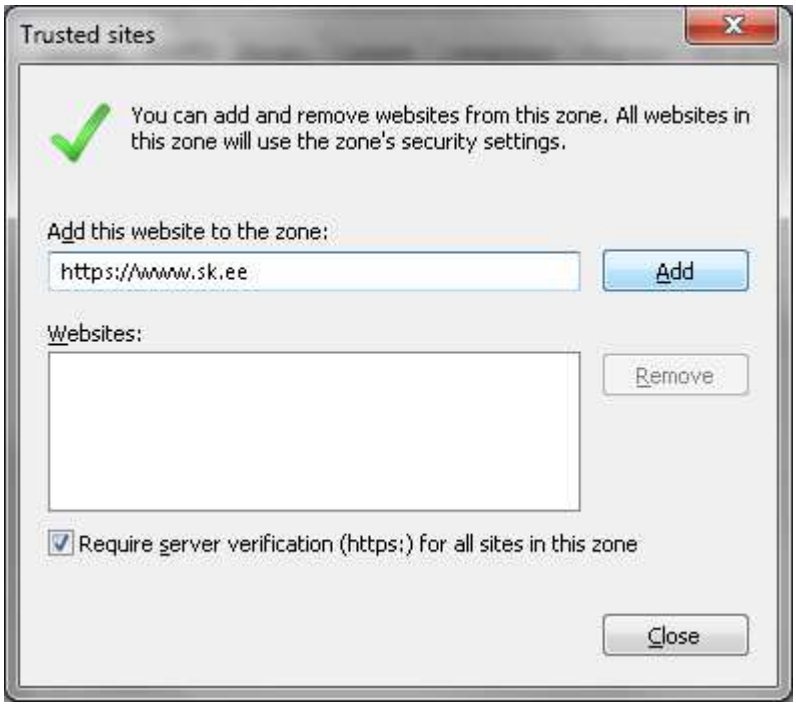
Use the following website to generate a certificate application https://www.sk.ee/util/csr_genereerimine/ (Attention! This page can be accessed with Windows and the Internet Explorer).

Attention! Before generating a key users of Windows Vista and Windows 7 should add the above page to the list of Trusted Sites in the Internet Explorer and set the security level for trusted sites to Low.

To change settings select "Internet Options" from "Tools" menu in the Internet Explorer. In the window that opens slick on "Security" tab and select "Trusted Sites".



Add https://www.sk.ee to the list of trusted websites



Click "Add" and close the window.
Finally, close the IE settings by clicking OK.

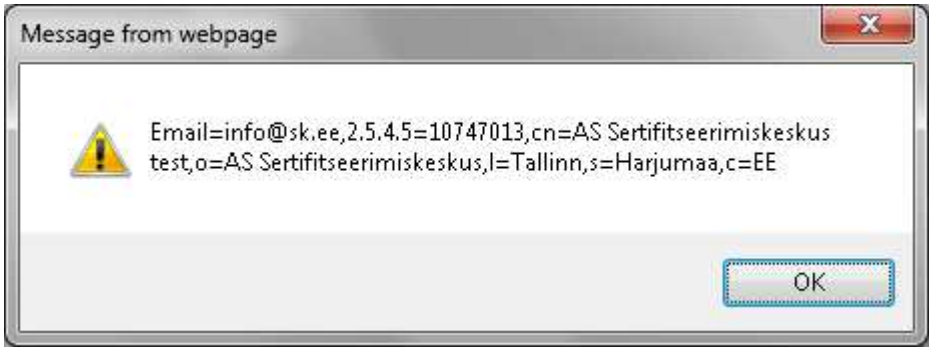
Go to website https://www.sk.ee/util/csr_genereerimine/

In the provided form you should indicate attributes of the certificate. Select "Signeerimisvõti" ("Signature key") or "Tuvastusvõti" ("Recognition key") (both choices apply if you generate an application for digital stamping or encrypting). As a smartcard selection for a device issued by SK select "eToken Base Cryptographic provider".

OU field is filled in by a representative of SK upon generation of the certificate!

After that click on "Genereeri CSR" ("Generate CSR").

After you click on "Genereeri CSR" ("Generate CSR"), attributes of the certificate are displayed.



Click OK to dismiss this notification and input Token PIN code:

After generation of the key the content of the certificate application (CSR) will appear in the same HTML window. We recommend copying the content of the window, for instance, into a text file and naming it appropriately (either Signature or Recognition key). The file(s) should be added to the order that can be submitted on SK website under the orange button "Telli" ("Order") http://sk.ee/teenused/digitempli-teenus/

3.4 Installation of a certificate to the Token

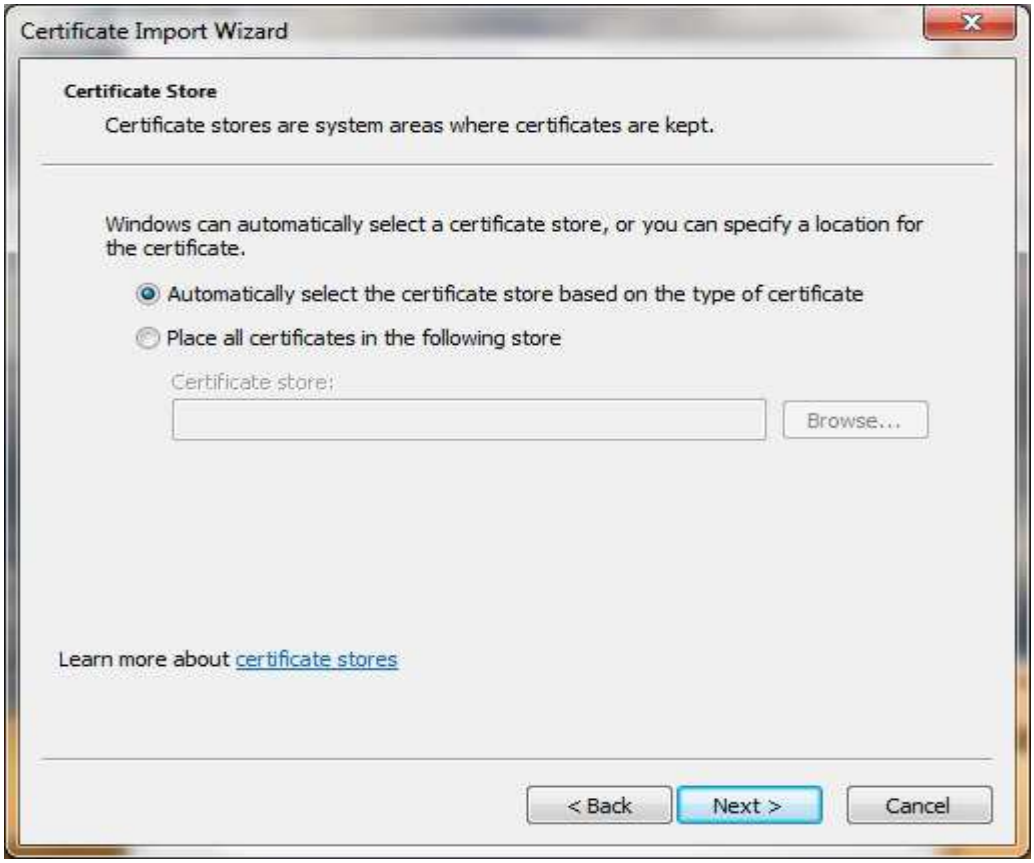
Having submitted an order you will receive your certificate(s) from the customer support.

In order to install a certificate to the Token you must first save the file to your computer and if the file's extension is .crt, open the certificate by double-clicking on it.

In the certificate information window select "Install Certificate"

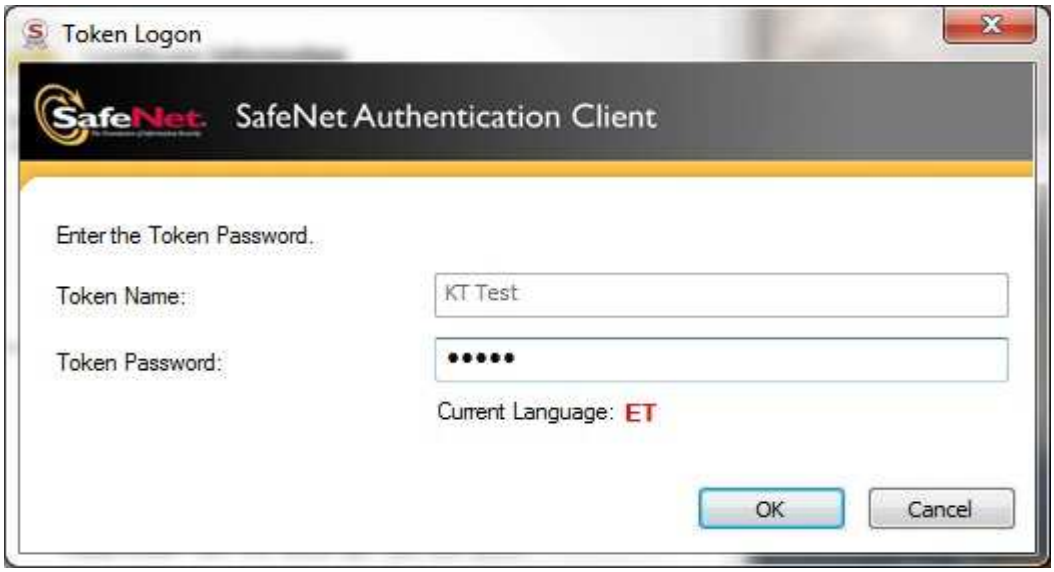
In the Certificate Import Wizard select "Next".

Then you are asked to specify the certificate store. Choose to automatically select the certificate store.



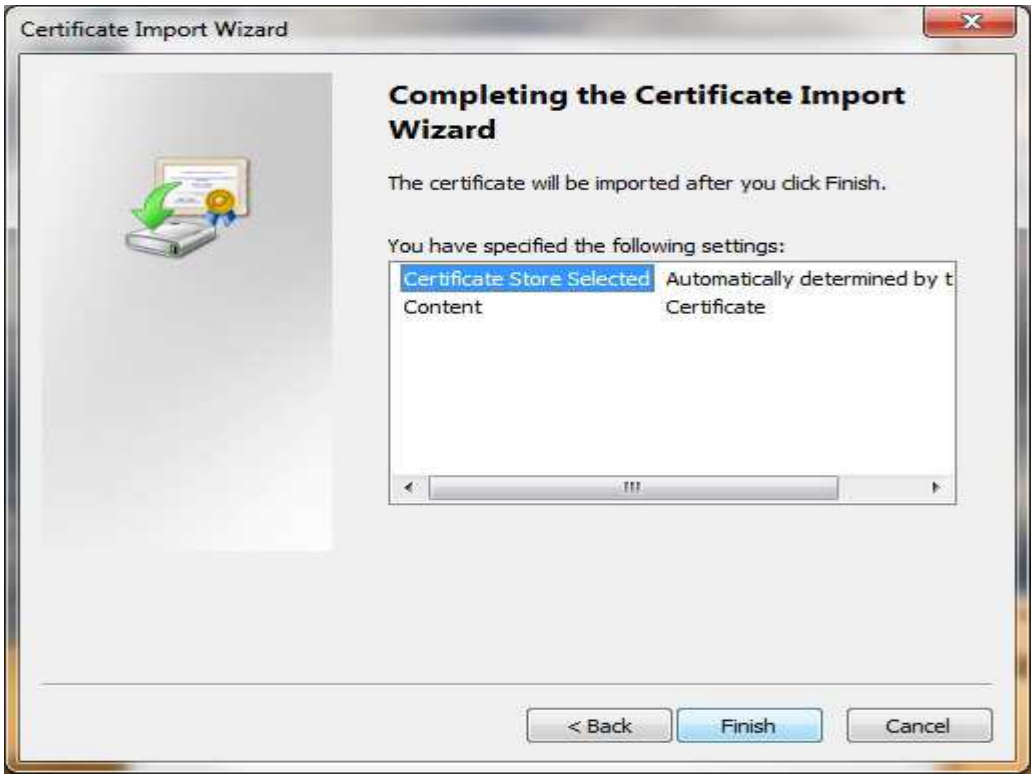
Click "Next" and confirm certificate import once again.

You will be asked your PIN code:



Now you must see the notification saying that the import was successful:

Close the wizard by clicking "Finish".



Your authorization token is ready!

If you wish to load several certificates on a single token, please repeat steps 3.3 (Generation of the certificate application) and 3.4 (Installation of the certificate to a Token) for each required certificate.

If you have any questions, please turn to support@sk.ee