Dokumendi informatsioon	
Loomise kuupäev	04.06.2009
Teema	Asutuse sertifikaadid
Viide	
Kellele	Asutuse sertifikaatide kasutajad
Koostaja(d)	Urmo Keskel
Versioon	1.2

Versiooni info		
Kuupäev	**Versioon**	**Muudatused**
04.06.2009	0.1	Esialgne versioon
09.06.2009	0.2	Lisatud õige CSR-i genereerimise veebilehe link ja kirjeldatud nõuded CSR-i genereerimise veebilehele.
07.05.2010	0.3	Tehtud juhend ümber Aladdini jaoks, võetud aluseks 2009 aastal IKey tarbeks kirjutatud juhend.
08.07.2010	0.4	Lisatud Alladini softi URL, eemaldatud Vistal ja 7-l kasutamise jutt (kuna antud täiendus ei ole veel toodangus), eemaldatud tokeni initsialiseerimisel lisaseadete määramine.
16.12.2010	1.0	Uuendatud CSR-i genereerimise aadressi, lisatud Vista ja Windows 7 selgitus. Lisatud 2048 bitiste võtmete ja FIPS toe seadistamine.
07.02.2011	1.1	Pulga initsialiseerimisel FIPS seadeid muudetud, lisatud hoiatus pulga initsialiseerimisega kaasnevate tagajärgede kohta, lehekülg 8 oli jäänud CSR genereerimise aadress vale.
13.11.2012	1.2	Juhend viidud kooskõlla Authentication Client 8.1 SP1 tarkvara kasutamisega.

2 Dokumendi eesmärk

Käesoleva dokumendi eesmärk on kirjeldada eToken Pro krüptopulgale asutuse sertifikaatide kandmise protseduur ja sellega seotud toimingud. Protseduur sisaldab krüptopulga initsialiseerimist, PIN-koodide vahetamist, võtmete ja sertifikaaditaotluse genereerimist ning sertifikaadi laadimist kiipkaardile. Juhend on koostatud SafeNet eToken Pro pulka kasutades, kuid peaks kehtima kõikidele SafeNet eToken pulkadele, mis on SafeNet Authentication Client 8.1 tarkvaraga (nt. eToken Pro Anywhere, eToken NGFlash)

3 Tegevuste kirjeldus

3.1 Tarkvara paigaldamine

Paigalda Tokeni kasutamiseks vajalik tarkvara SafeNet Authentication Client.

Tarkvara saab alla laadida: https://installer.id.ee/media/etoken/

ZIP pakis sisalduvad järgmised failid:

Failinimi	**Kirjeldus**
SafeNetAuthenticationClient-eToken-x32-8.1-SP1.msi	Tarkvara paigalduspakett Windowsi 32-bitistele operatsioonisüsteemidele
SafeNetAuthenticationClient-eToken-x64-8.1-SP1.msi	Tarkvara paigalduspakett Windowsi 64-bitistele operatsioonisüsteemidele
SAC_8.1_SP1_User_Guide_Rev_A.pdf	SafeNet Authentication Client tarkvara kasutusjuhend
SafeNetAuthenticationClient_8_1_SP1Windows key.txt	Tarkvara litsentsivõti. **NB! Antud võtme kasutamise õigust omavad ainult kasutajad, kes on ostnud SK-st krüptopulga.**

SafeNet Authentication Client 8.1 tarkvara poolt toetatud operatsioonisüsteemid on:
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)

Juhul, kui eelnevalt on arvutisse paigaldatud SK poolt levitatud eToken PKI Client 5.1 tarkvara, siis seda eraldi eemaldada vaja ei ole.

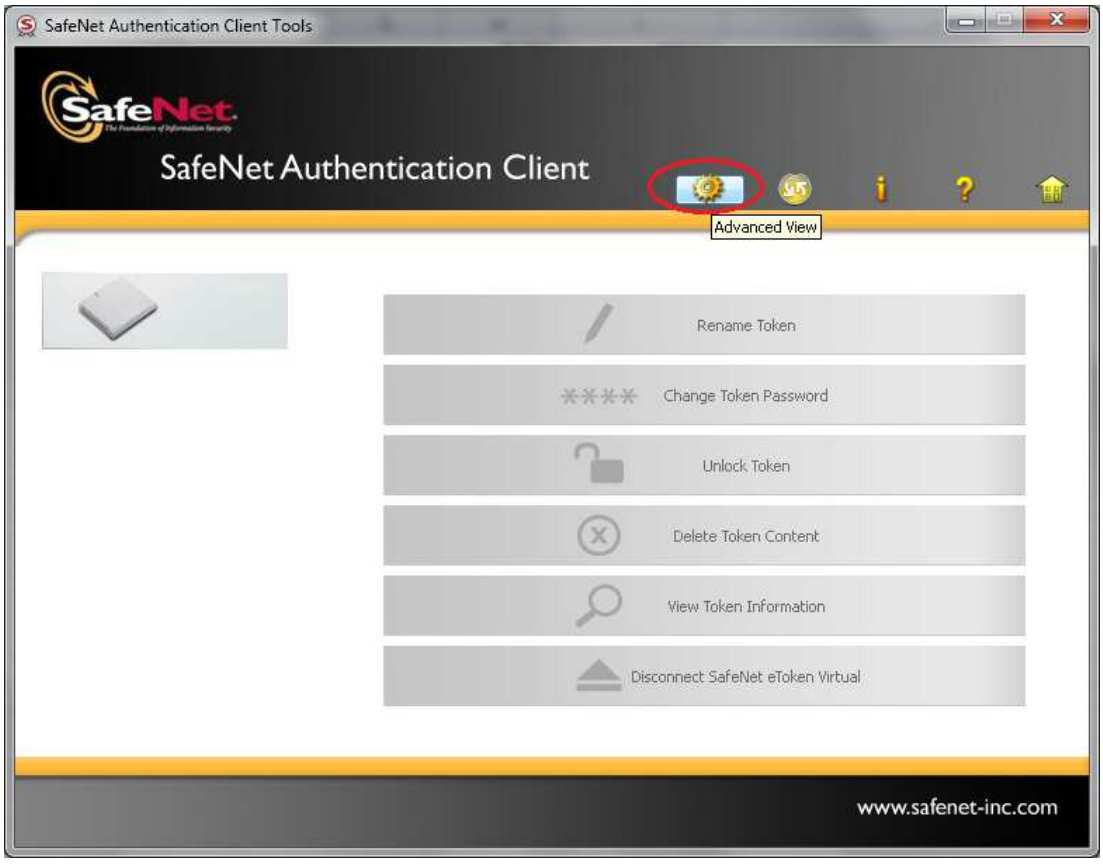
Pärast tarkvara paigaldamist tekib Start menüüsse „All Programs->SafeNet-> SafeNet Authentication Client" menüüjaotusse „SafeNet Authentication Client Tools" programm. Sama programmi on võimalik käivitada ka Taskbarilt (ikoon Safenet Authentication Client).

Tarkvara paigaldamise järel tuleb importida litsentsifail SafeNet Authentication Client Tools tarkvara abil. Selleks valida menüüst „About"

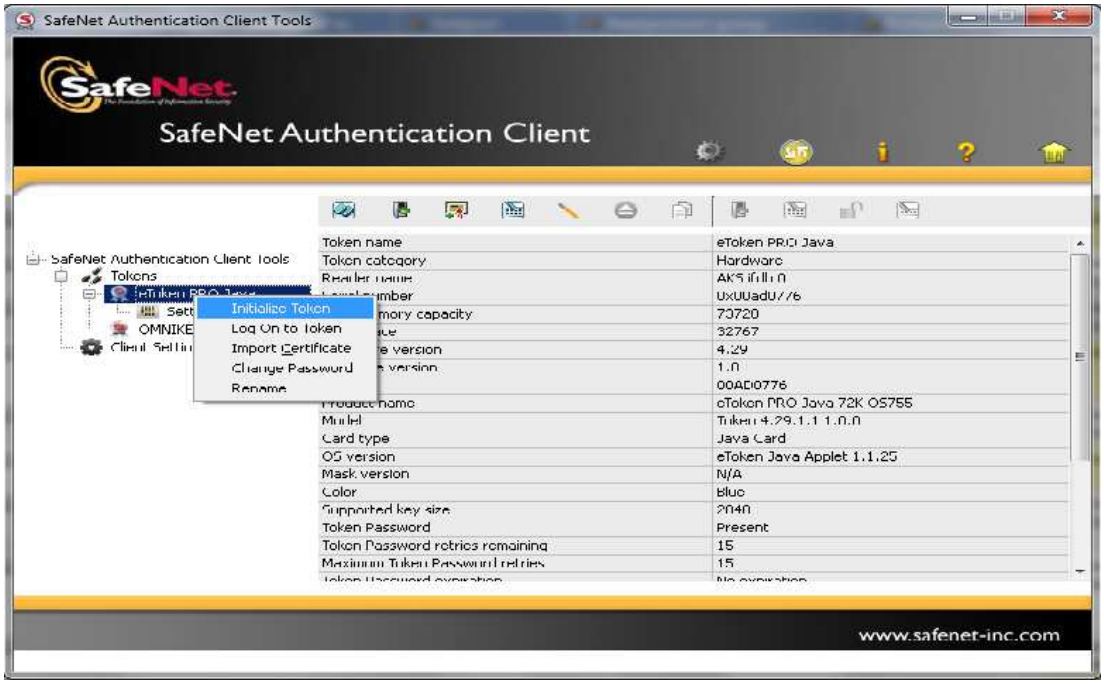
3.2 Pulga initsialiseerimine

HOIATUS! Pulga initsialiseerimise järel kustutatakse kõik krüptopulgal olevad sertifikaadid ja võtmed. Antud toimingut tasub teha vaid juhul, kui pulgale ei ole veel sertifikaate väljastatud või kui kõik väljastatud sertifikaadid on aegunud. Ühele pulgale mitme sertifikaadi taotlemiseks nii, et varasemad sertifikaadid ära ei kustuks, tuleb INITSIALISEERIMIST MITTE TEHA ja jätkata juhendi punktist 3.3 (Sertifikaaditaotluse genereerimine).

Pulga initsialiseerimiseks käivita eToken PKI Client. Seda saab teha vajutades taskbari ikoonil Safenet Authentication Client ( ) või valides start menüüst All Programs->SafeNet-> SafeNet Authentication Client -> SafeNet Authentication Client Tools.



Avanenud vaatest vali Token ja vajuta paremat hiire nuppu, avanenud alammenüüst vali „Initialize“:

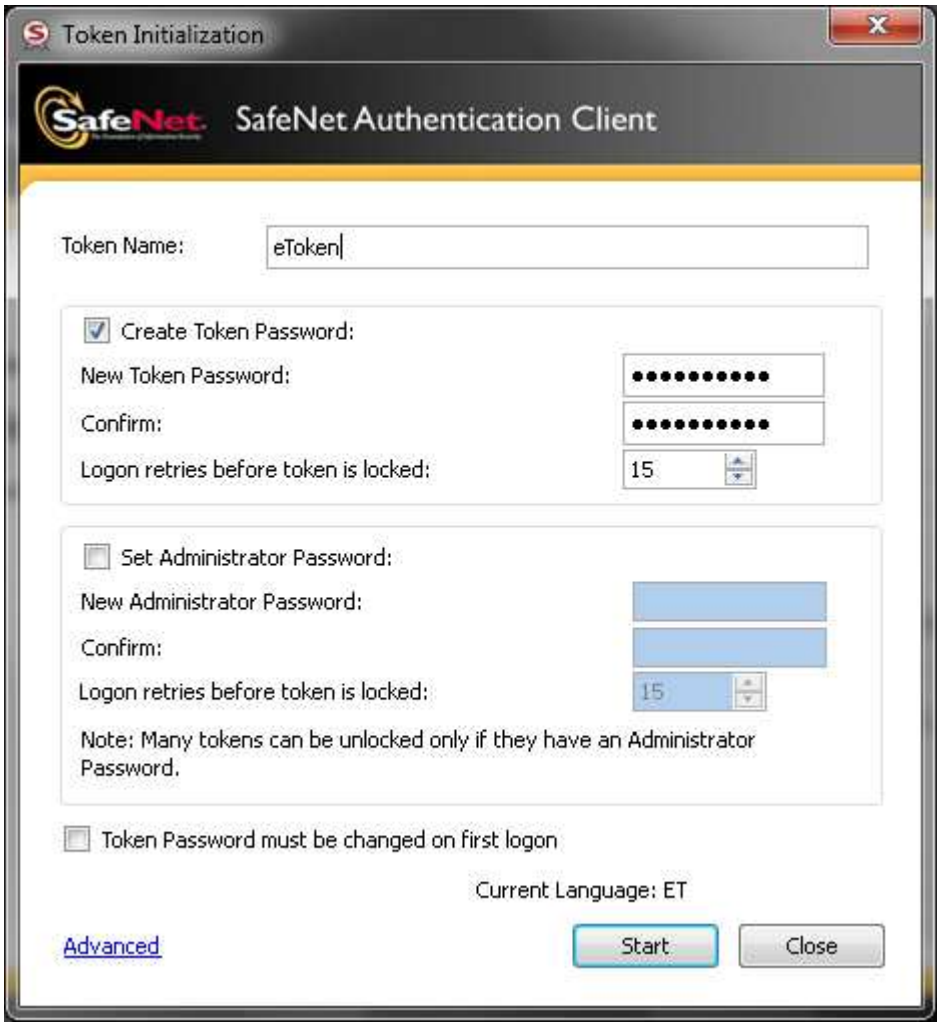


Esimese sammuna määra Tokenile nimetus (asutuse nimi, allüksuse nimi vms.), mille järgi seda hiljem ära tunda.

See on oluline kui ühes süsteemis kasutatakse paralleelselt mitut Tokenit.Järgmiseks määra Tokenile parool (Create Token Password).

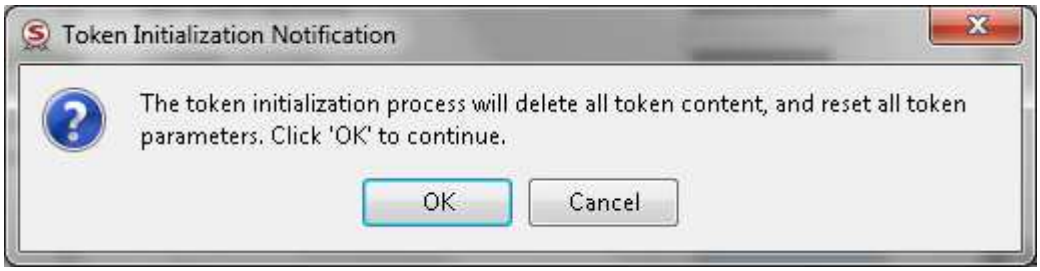
Soovituslik on määrata lisaks Admin password (selle abil lukustatakse lahti Token Password). Valeparoolide sisestamise arv võiks olla 5.

Administrator passwordi määramata jätmisel tuleb arvestada, et Token passwordi lukustamisel tuleb Token initsialiseerida ja tellida uued sertifikaadid!



Nüüd käivita tokeni initsialiseerimine valides „Start“ (vaata eelmist ekraanipilti).

Seejärel kuvatakse hoiatust:



NB! Nõustuge hoiatuse ja käivitage initsialiseerimisprotsess ainult juhul kui krüptopulgale ei ole juba kantud võtmeid/sertifikaate, mida soovite jätkuvalt kasutada. Valides „OK“ kuvatakse ülevaade initsialiseerimisprotsessist:

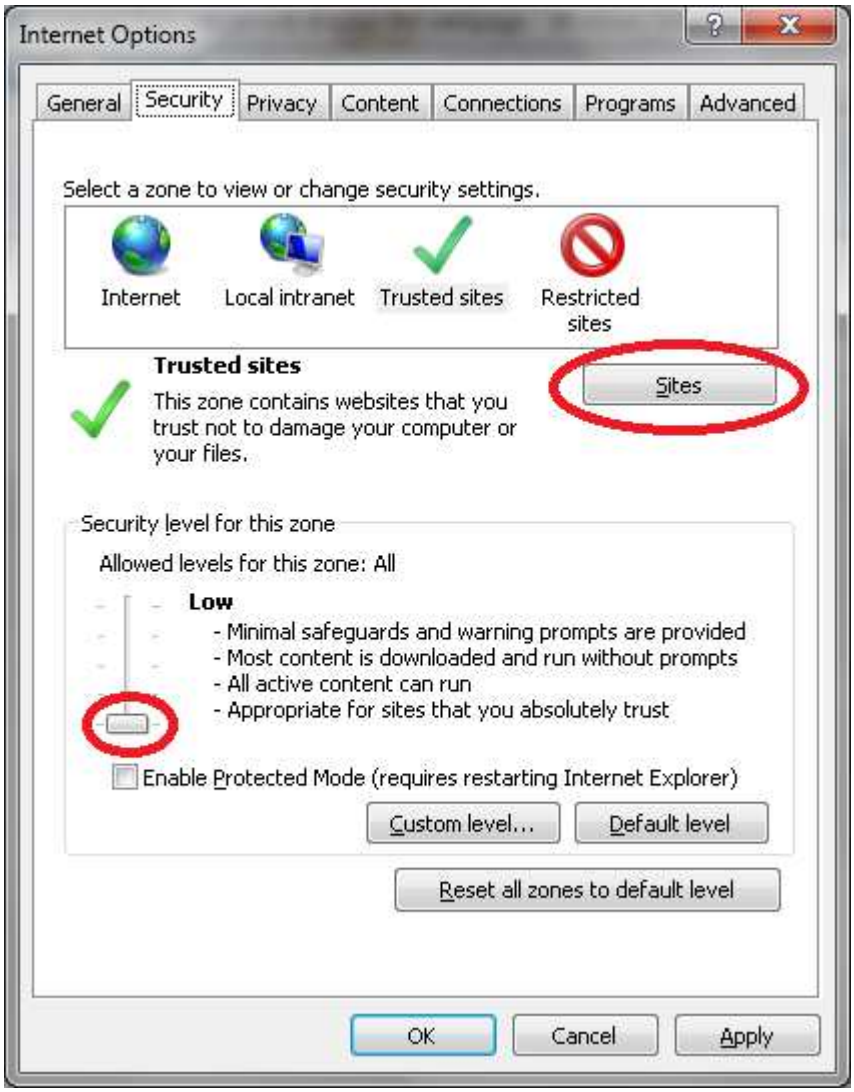
ning teade toimingu eduka soorituse kohta:

3.3 Sertifikaaditaotluse genereerimine

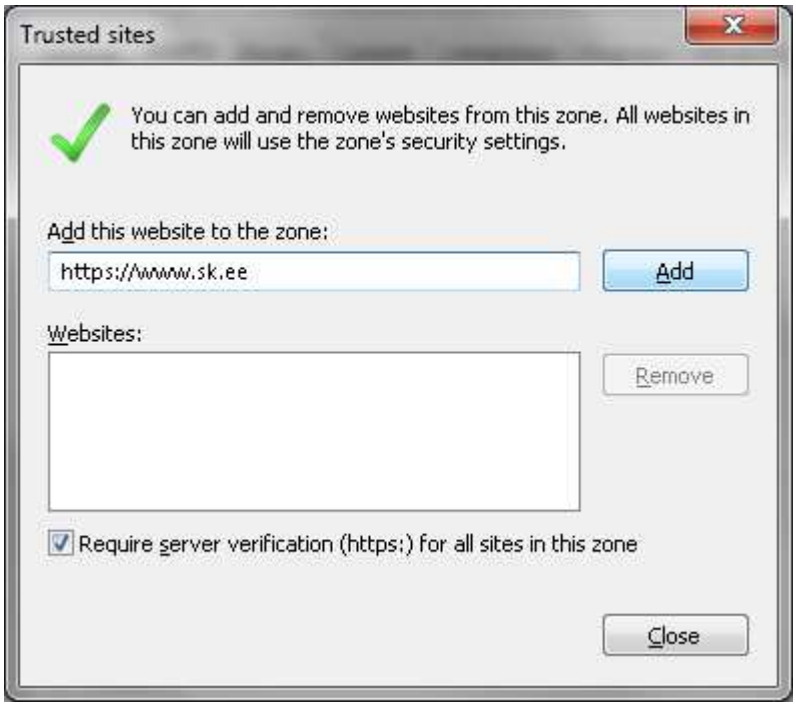
Sertifikaaditaotluse geneereerimise jaoks tuleb kasutada veebilehte https://www.sk.ee/util/csr_genereerimine/ (NB! Antud veebilehe kasutamiseks on vajalik Windowsi ja veebilehitseja Internet Explorer kasutamine).

NB! Windows Vista ja Windows 7 operatsioonisüsteemi korral tuleb enne võtme genereerimist lisada Internet Exploreri *„Trusted Site"-ide hulka ning määrata „Trusted Site"-idele turvatasemeks „Low".*

Seadete muutmiseks vali Internet Exploreri „Tools" menüüst „Internet Options". Avanenud aknas vali „Security" sektsioon ja sealt „Trusted Sites"



Seejärel lisa usaldatud lehekülgede hulka https://www.sk.ee



Vajuta „Add“ ning sulge aadresside lisamise aken.
Lõpuks sulge IE seaded vajutades „OK“.

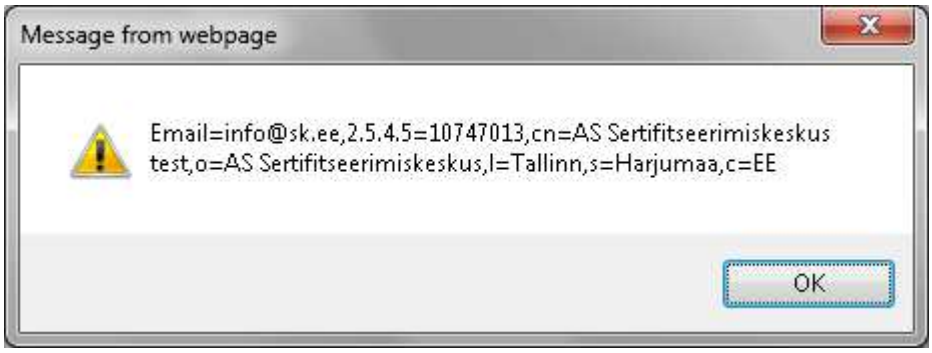
Ava veebiaadress https://www.sk.ee/util/csr_genereerimine/

Antud veebivormil tuleb määrata sertifikaadi atribuudid. Võtme asukohaks määra „Signeerimisvõti“ või „Tuvastusvõti“ (mõlemad valikud kui genereeritakse taotlust digitembeldamiseks ja krüpteerimiseks). Kiipkaardi valikuks SK-st saadud seadme puhul määra „eToken Base Cryptographic provider“.

OU välja täidab SK esindaja sertifikaadi genereerimisel!

Seejärel vajuta „Genereeri CSR“.

„Genereeri CSR“ nupu vajutamise järel kuvatakse sertifikaadi atribuudid



Antud teatele tuleb vajutada „OK“ ja sisestada Tokeni PIN-kood:

Võtme genereerimise järel ilmub samasse HTML aknasse sertifikaaditaotluse (CSR-i) sisu. Sisu soovitame kopeerida näiteks tekstfaili ja nimetada vastavalt sisule kas signeerimis- või tuvastusvõti. Fail(id) tuleb lisada tellimusele, mida saab esitada SK kodulehelt oranžist nupust „Telli“ http://sk.ee/teenused/digitempli-teenus/

3.4 Sertifikaadi laadimine Tokenile

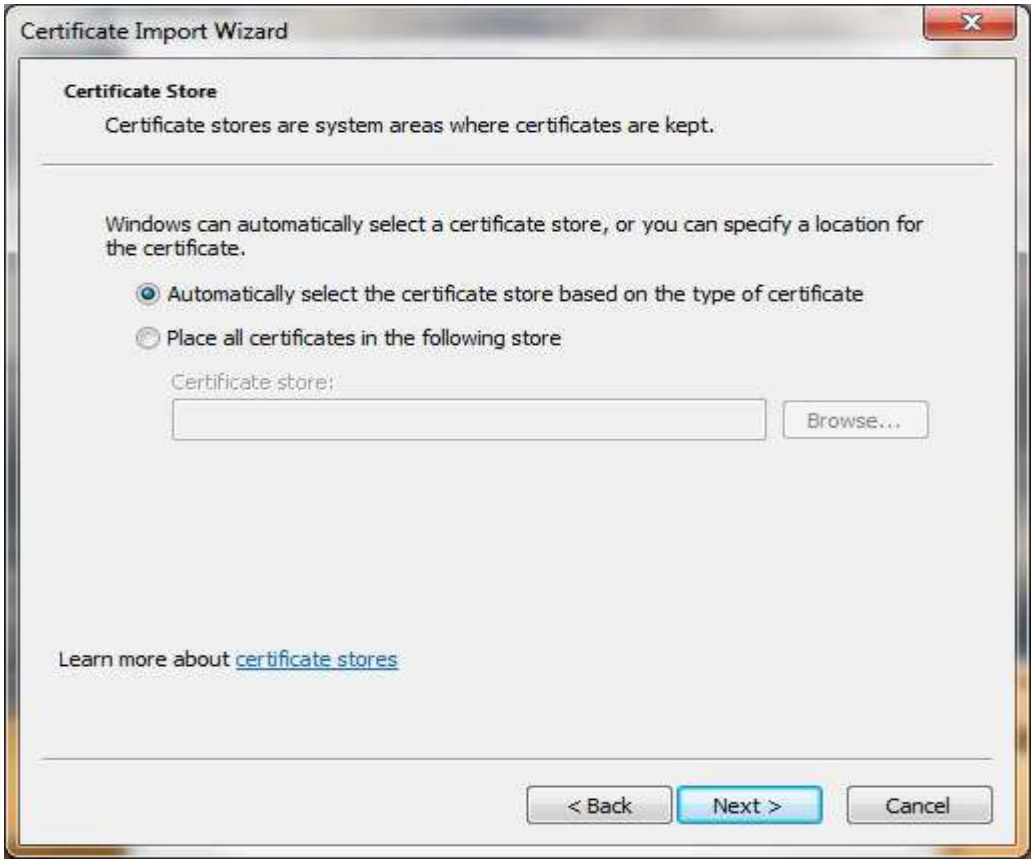
Esitatud tellimusele saab klienditeenindusest vastu sertifikaadi(id).

Sertifikaadi laadimiseks Tokenile salvesta esmalt fail oma arvutisse ja kui faililaiend on määratud .crt, siis ava sertifikaat topelt hiireklõpsuga.

Avanenud sertifikaadiinfo aknas vali „Install Certificate“

Sertifikaadi importimise viisardis vajuta „Next“

Alljärgnevalt palutakse täpsustada sertifikaadihoidla. Tuleb määrata, et sertifikaadihoidla valitakse automaatselt.

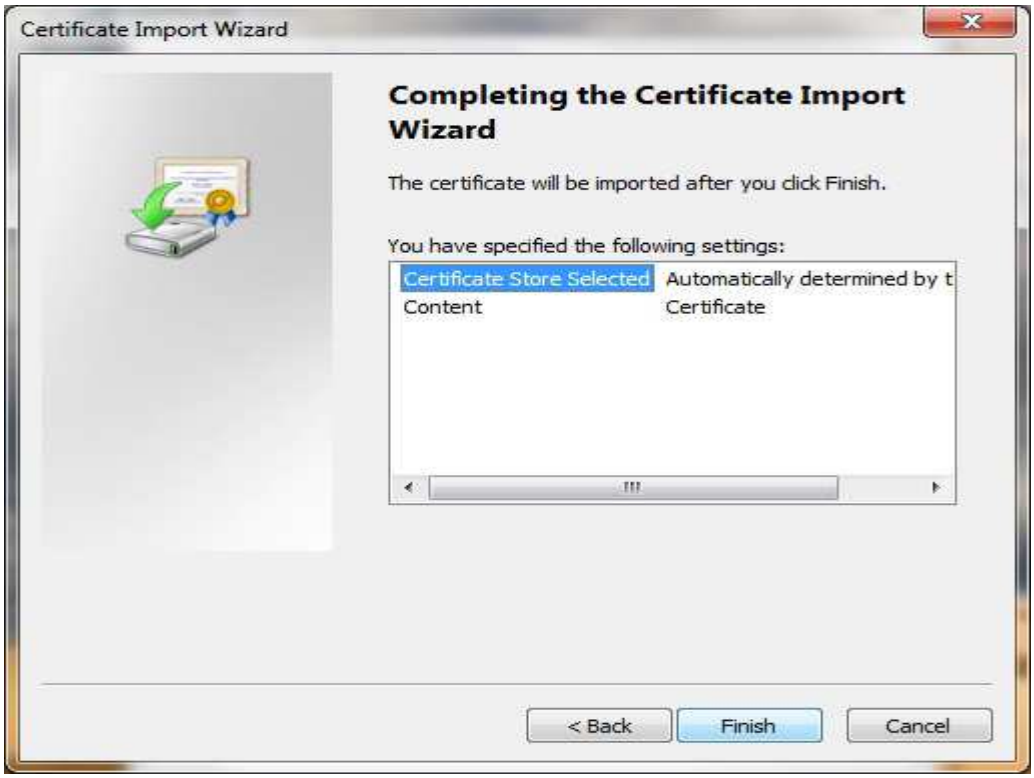


Seejärel vali „Next“ ning anna veelkord kinnitus sertifikaadi importimise kohta.

Küsitakse ka PIN-koodi:

Nüüd kuvatakse kinnitus sertifikaadi eduka importimise kohta:

Sulge sertifikaadi paigaldusviisard nupust „Finish“



Krüptopulk on kasutamiseks valmis!

Kui ühele pulgale on soov laadida mitu sertifikaati, tuleb samme 3.3 (CSR-i genereerimine) ja 3.4 (sertifikaadi laadimine pulgale) korrata iga sertifikaadi jaoks eraldi.

Küsimuste korral pöördu support@sk.ee