

Dokumendi informatsioon	
Loomise kuupäev	04.06.2009
Teema	Asutuse sertifikaadid
Viide	
Kellele	Asutuse sertifikaatide kasutajad
Koostaja(d)	Urmo Keskel
Versioon	1.1

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 Aladini 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.



## 2 Dokumendi eesmärk

Käesoleva dokumendi eesmärk on kirjeldada Aladdin krüptopulgale eToken Pro asutuse sertifikaatide kandmise protseduur ja sellega seotud toimingud. Protseduuri sisaldab krüptopulga initsialiseerimise, PIN koodide vahetamise, võtmete ja sertifikaaditaotluse genereerimist ning sertifikaadi laadimist kiipkaardile. Juhend on koostatud Aladdin eToken Pro pulka kasutades, kuid peaks kehtima kõikidele Aladdin eToken pulkadele, mis on Aladdini tarkvaraga PKI Client ühilduvad (nt. eToken Pro Anywhere, eToken NGFlash)

## 3 Tegevuste kirjeldus

### 3.1 Tarkvara paigaldamine

Paigalda tokeni kasutamiseks vajalik tarkvara Aladdin PKI Client, mille saab alla laadida 32 bitisele operatsioonisüsteemile aadressilt

<http://demo.digidoc.ee/download/aladdin/PKIClient-x32-5.1-SP1.msi>

ja 64 bitisele operatsioonisüsteemile aadressilt:

<http://demo.digidoc.ee/download/aladdin/PKIClient-x64-5.1-SP1.msi>.

**NB! Antud tarkvara kasutamise õigus kaasneb ainult SK-st Aladdin krüptopulga ostmisega.**

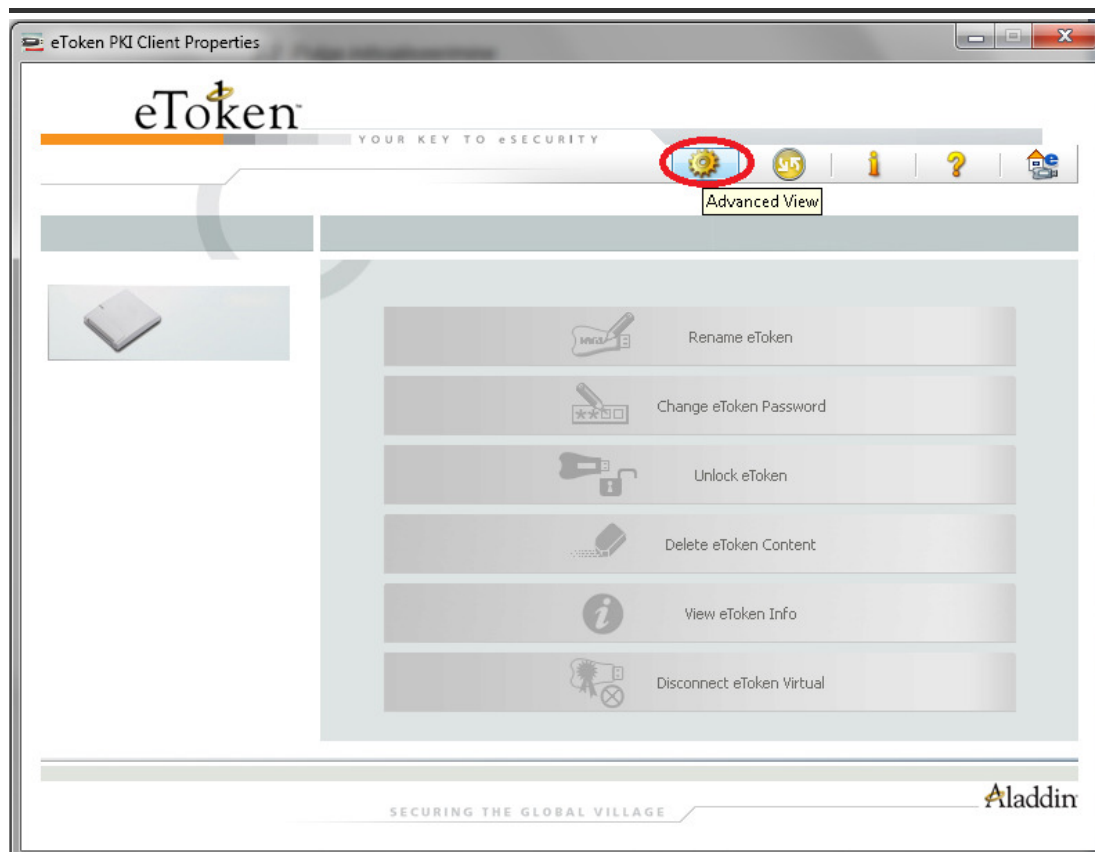
Tarkvara paigaldamiseks vajalik kasutajanimi on „aladdin“ ja parool „SKasutuseToken“ Tarkvara paigaldada vaikeseadetes.

Tarkvara paigaldamise järgselt tekib Start menüüsse „All Programs->EToken->EToken PKI Client“ menüüjaotusse „eToken properties“ programm. Sama programmi on võimalik käivitada ka Taskbarilt (ikoon eToken PKI Client).

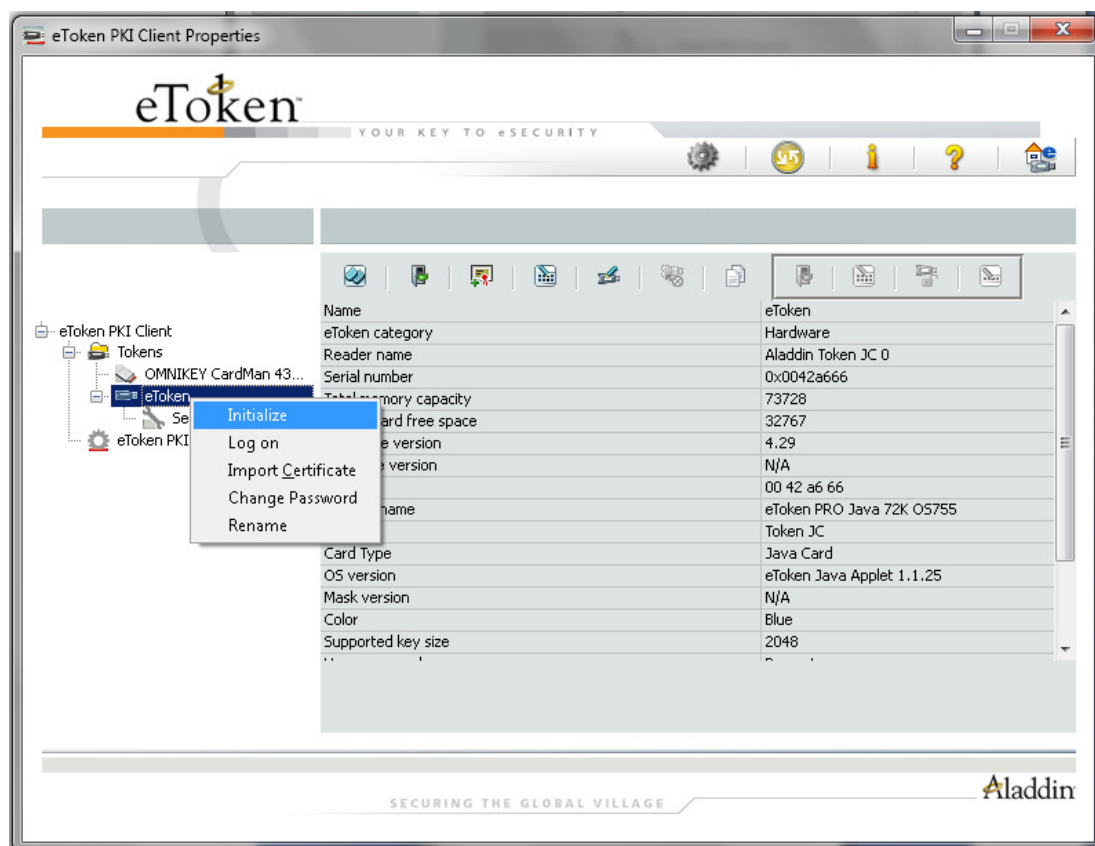
### 3.2 Pulga initsialiseerimine

**HOIATUS! Pulga initsialiseerimise järgselt 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 tuleks INITSIALISEERIMIST MITTE TEHA ja jätkata punktits juhendi punktist 3.3 (Sertifikaaditaotluse genereerimine).**

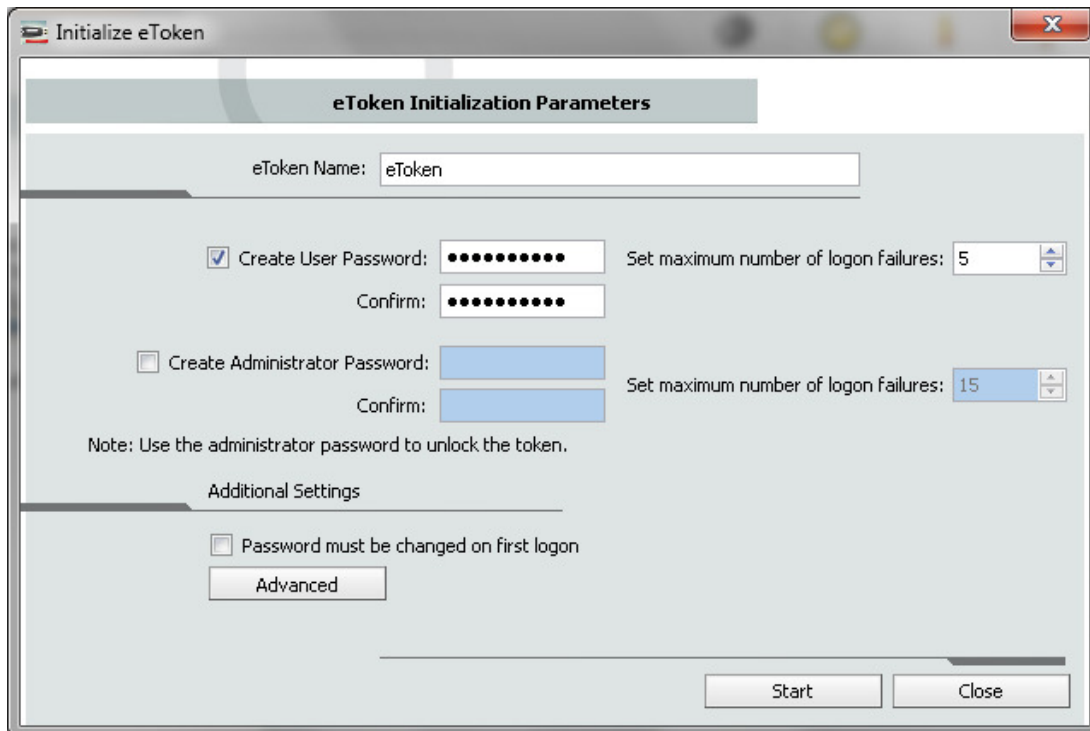
Pulga initsialiseerimiseks käivita eToken PKI Client (vajutades taskbaril ikoonil eTokeni ikoonil või valides start menüüst All Programs->EToken->EToken PKI Client->EToken properties.



Avanenud vaatest vali eToken ja vajuta paremat hiire nuppu, mille järgselt avaneb kontekstmenüü, kust vali „Initialize“:



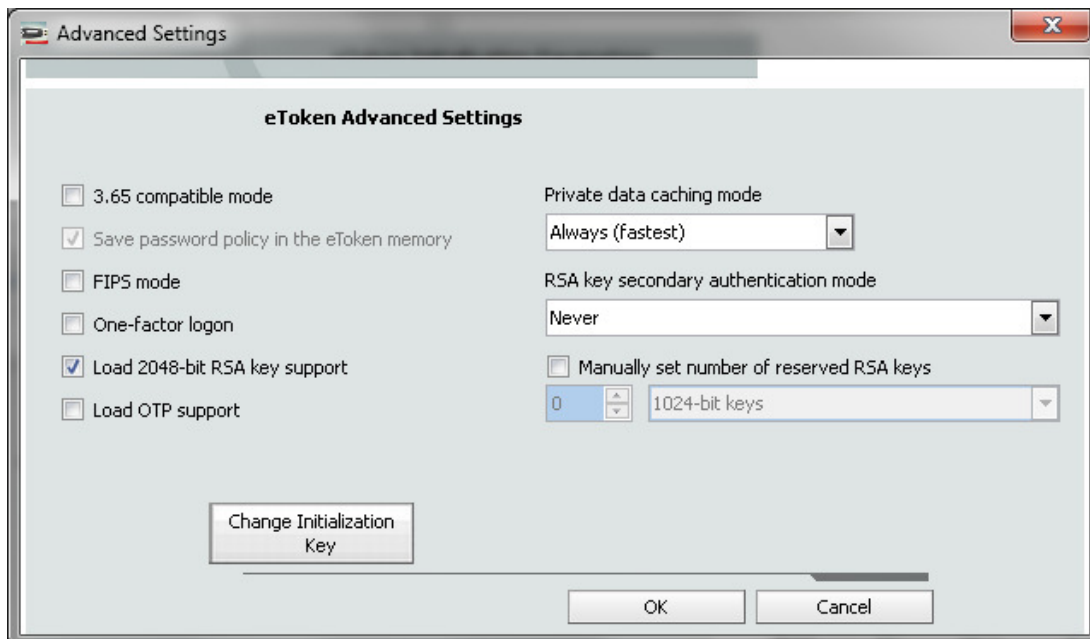
Määra Tokenile parool (UserPassword), Admin passwordi võib jätta määratamata. Soovitav valeparoolide sisestamise arv võiks olla 5.



The dialog box is titled "Initialize eToken" and contains the following fields and options:

- eToken Name:** A text field containing "eToken".
- Create User Password:** A checked checkbox. Next to it are two password fields (one for the password, one for confirmation) both containing eight dots. To the right is a spinner box for "Set maximum number of logon failures" set to 5.
- Create Administrator Password:** An unchecked checkbox. Next to it are two empty password fields. To the right is a spinner box for "Set maximum number of logon failures" set to 15.
- Note:** "Use the administrator password to unlock the token."
- Additional Settings:** A section containing an unchecked checkbox for "Password must be changed on first logon" and a button labeled "Advanced".
- Buttons:** "Start" and "Close" buttons at the bottom right.

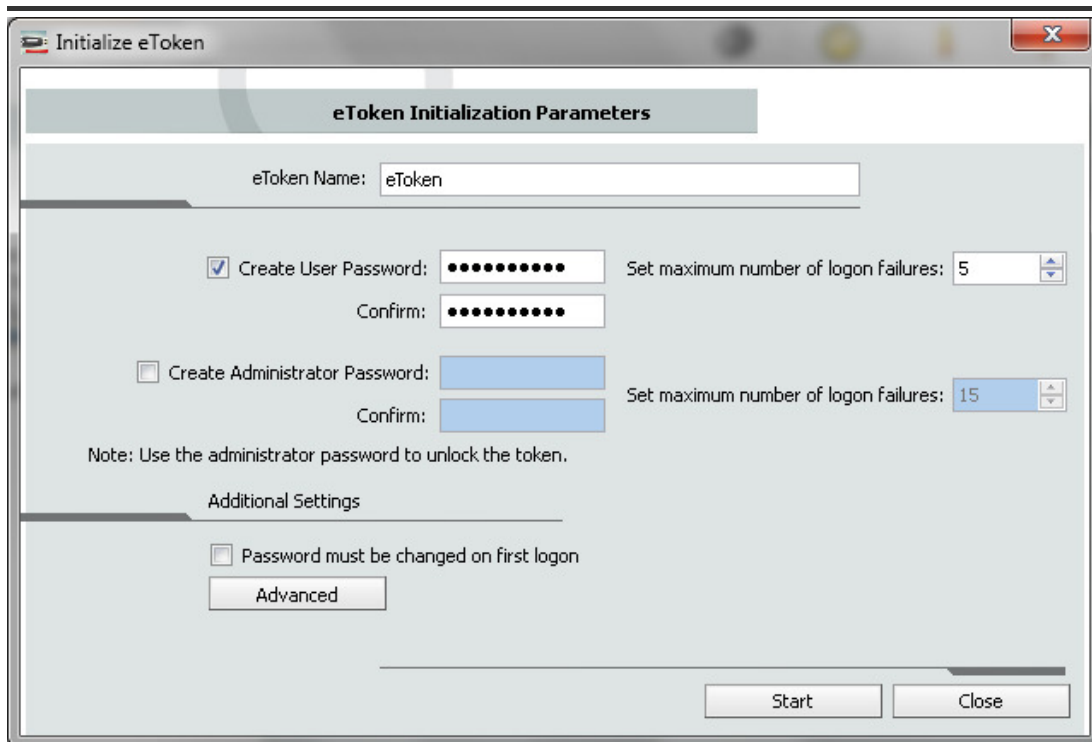
Vali „Advanced“



The dialog box is titled "Advanced Settings" and contains the following fields and options:

- 3.65 compatible mode:** An unchecked checkbox.
- Save password policy in the eToken memory:** A checked checkbox.
- FIPS mode:** An unchecked checkbox.
- One-factor logon:** An unchecked checkbox.
- Load 2048-bit RSA key support:** A checked checkbox.
- Load OTP support:** An unchecked checkbox.
- Private data caching mode:** A dropdown menu set to "Always (fastest)".
- RSA key secondary authentication mode:** A dropdown menu set to "Never".
- Manually set number of reserved RSA keys:** An unchecked checkbox. Below it is a spinner box set to 0 and a dropdown menu set to "1024-bit keys".
- Buttons:** "Change Initialization Key", "OK", and "Cancel" buttons at the bottom.

Avanened dialogis määra valituks „Load 2048-bit RSA key support“ ning vajuta OK.



The dialog box is titled "Initialize eToken". It contains a section "eToken Initialization Parameters" with the following fields and options:

- eToken Name: eToken
- ☒ Create User Password: [password field] Set maximum number of logon failures: 5
- Confirm: [password field]
- ☐ Create Administrator Password: [password field] Set maximum number of logon failures: 15
- Confirm: [password field]
- Note: Use the administrator password to unlock the token.
- Additional Settings
- ☐ Password must be changed on first logon
- Advanced
- Start
- Close

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

Valiku järgselt kuvatakse hoiatust, millega tuleb nõustuda:

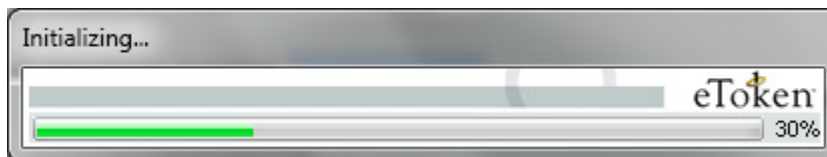


The dialog box is titled "About to Initialize eToken". It contains the following text:

This operation will reset all the eToken parameters and delete all eToken content.

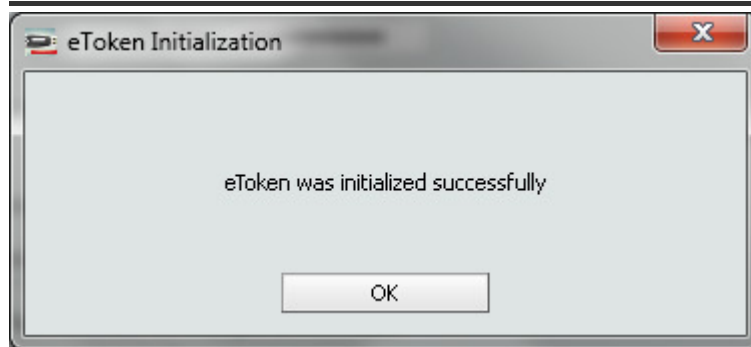
OK Cancel

„OK“ valiku järgselt kuvatakse ülevaadet initsialiseerimisprotsessist:



The progress bar is titled "Initializing...". It shows a green progress bar at 30% completion. The eToken logo is visible on the right side of the bar.

ning teadet toimingute eduka soorituse kohta:

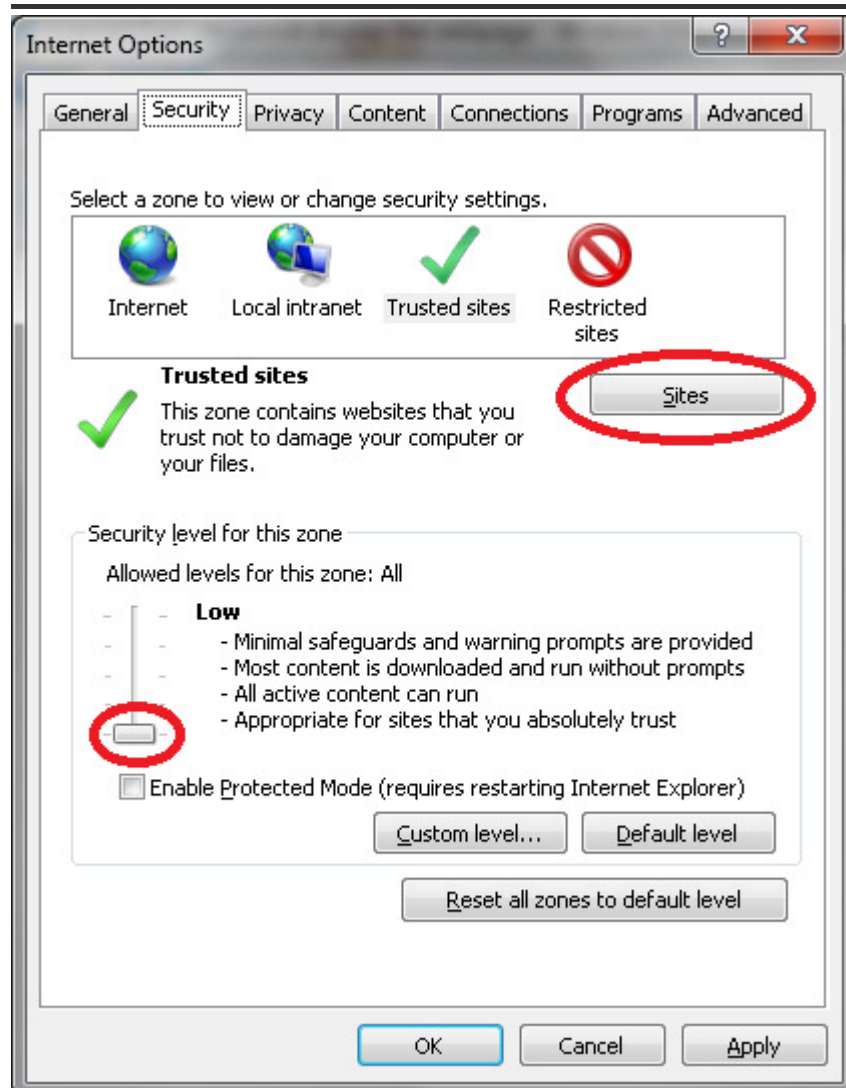


### 3.3 Sertifikaaditaotluse genereerimine

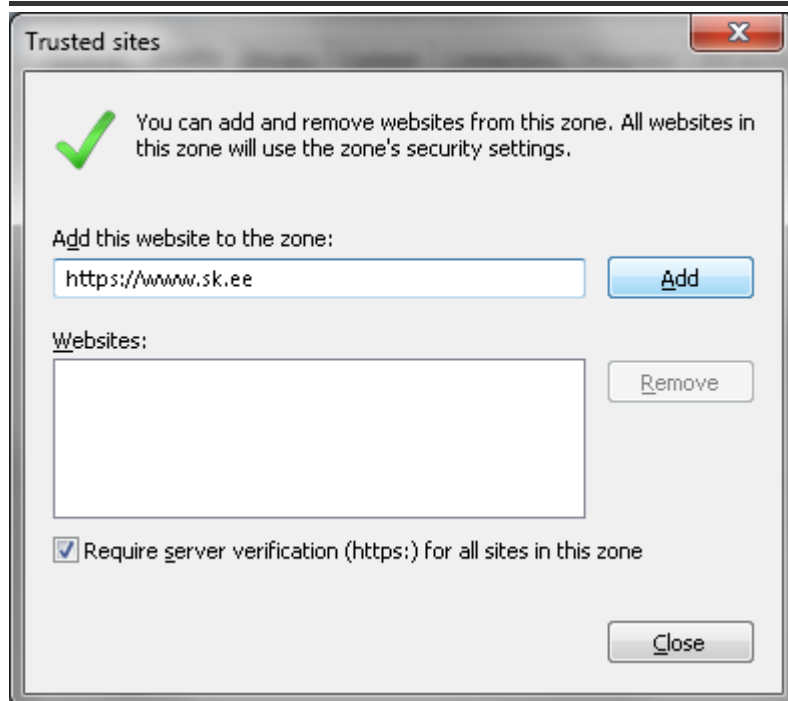
Sertifikaaditaotluse genereerimise jaoks tuleks kasutada veebilehte [https://www.sk.ee/util/csr\\_genereerimine/](https://www.sk.ee/util/csr_genereerimine/) (NB! Antud veebilehe kasutamiseks on vajalik Windowsi ja Internet Explorer veebilehitseja kasutamine),

**NB! Windows Vista ja Windows 7 operatsioonisüsteemi korral tuleb enne võtme genereerimist <https://www.sk.ee/> lisada Internet Exploreri „Trusted Site“-ide hulka ning määrata „Trusted Site“-idele turvasemeks „Low“.**

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



„Sites“ nupu vajutamise järgselt lisa usaldatud lehekülgede hulka <https://www.sk.ee/>.



Vajuta „Add“ ning sulge aadresside lisamise aken.  
Määrangute tegemise järselt sulge IE seaded vajutades „OK“.

Ava veebiaadress [https://www.sk.ee/util/csr\\_genereerimine/](https://www.sk.ee/util/csr_genereerimine/)

CSR genereerimine

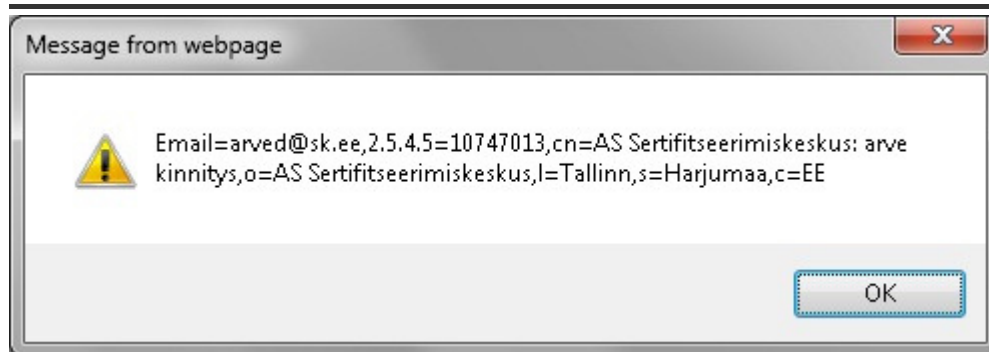
<b>Sertifikaadi nimi (CN)</b>	AS Sertifitseerimiskeskus: arve kinnitys
<b>Organisatsiooni allüksuse nimi (OU)</b>	
<b>Organisatsiooni nimi (O)</b>	AS Sertifitseerimiskeskus
<b>Organisatsiooni registrikood (SN)</b>	10747013
<b>Asukoht (L)</b>	Tallinn
<b>Riik/Maakond (ST)</b>	Harjumaa
<b>E-post</b>	arved@sk.ee
<b>Kiipkaardi valik:</b>	eToken Base Cryptographic Provider
<b>Võtme asukoht</b>	<div> <div>Signeerimisvõti</div> <div>Võtme pikkus: 2048</div> </div> <div> Gemplus kaardi puhul: Autentimine, krüptimine, allkirjastamine: Tuvastamise võti  Setec kaardi puhul: Autentimine, krüptimine: Tuvastamise võti // Allkirjastamine: Signeerimise võti </div>

Genereeri CSR

Antud veebivormil tuleks määrata sertifikaadi atribuudid, võtme asukohaks määrata „Signeerimisvõti“ ning kiipkaardi valikuks „eToken Base Cryptographic provider“.

„Genereeri CSR“ nupu vajutamise järgselt kuvatakse sertifikaadi atribuudid





Antud teatele tuleks vajutada „OK“, mille järgselt palutakse sisestada PIN kood:



ja kuvatakse võtme genereerimise teadet.

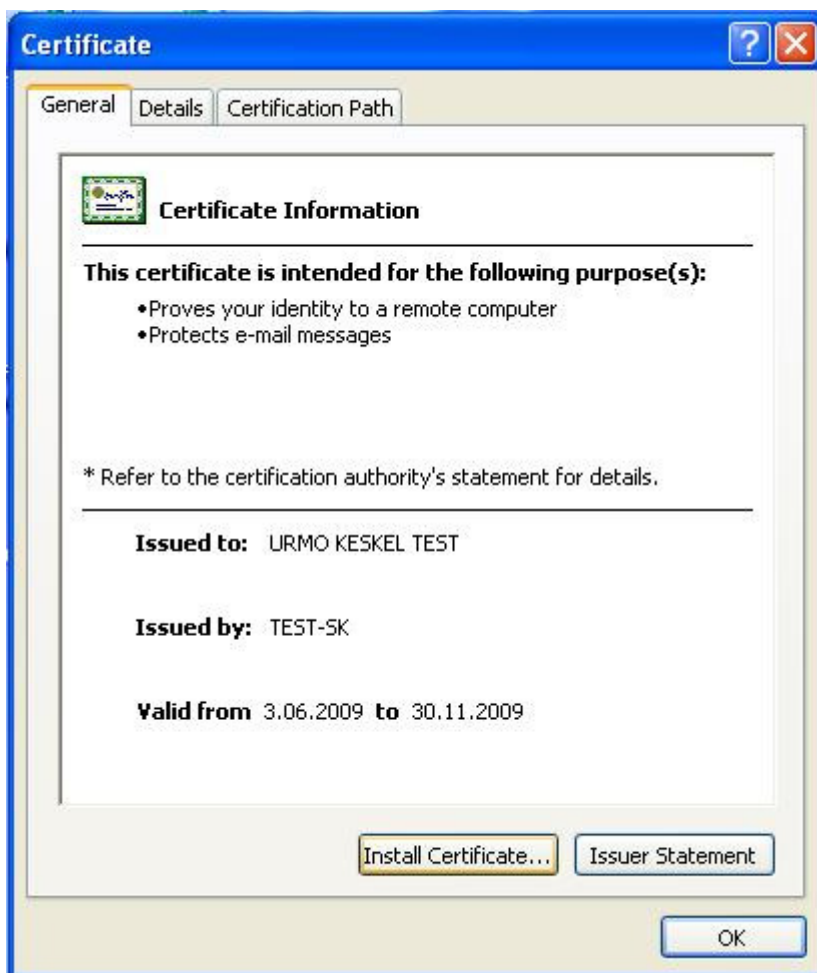
Võtme genereerimise järgselt ilmub samasse HTML aknasse sertifikaaditaotluse (CSR-i) sisu. See tuleks sertifikaadi tellimusel esitada E-teeninduses CSR-i väljal.

## 3.4 Sertifikaadi laadimine kiip kaardile

Sertifikaadi laadimiseks kiipkaardile tuleks sertifikaadifail (pärast selle allalaadimist e-teenindusest salvestada oma arvutisse ning topeltkõlpsuga sertifikaadi faili ikoonil avada.



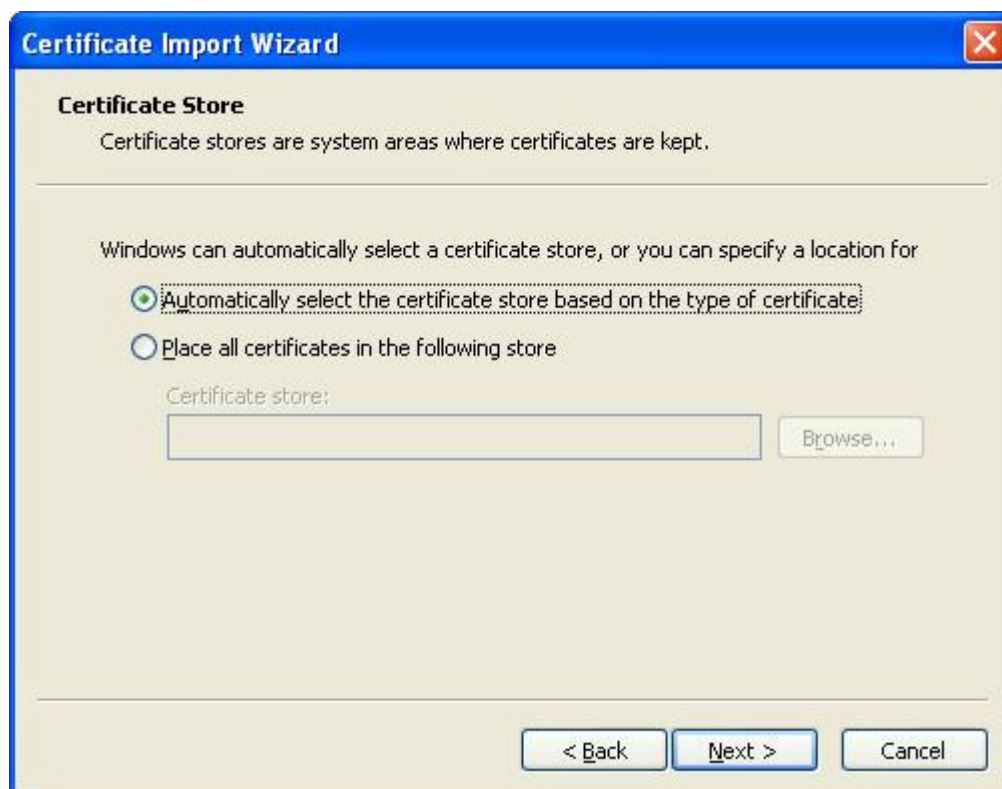
Avanenud sertifikaadiinfo aknast tuleks valida „Install Certificate“



Sertifikaadi importimise viisardist vajutada „Next“



Alljärgnevalt palutakse täpsustada sertifikaadi hoidla, määrata, et sertifikaadihoidla valitakse automaatselt:



„Nex >“ vajutamise järgselt tuleb anda veelkordne kinnitus sertifikaadi importimise kohta.



Mille järgselt küsitakse PIN koodi:



Nüüd kuvatakse kinnitus sertifikaadi eduka importimise kohta:



**Krütopulk on kasutamiseks valmis!**

Kui ühele pulgale soovitakse laadida mitut sertifikaati tuleks samme 3.3 (CSR-i genereerimine) ja 3.4 (sertifikaadi laadimine pulgale) korrata iga sertifikaadi jaoks eraldi.