

Andmete krüpteerimine OpenPGP-ga

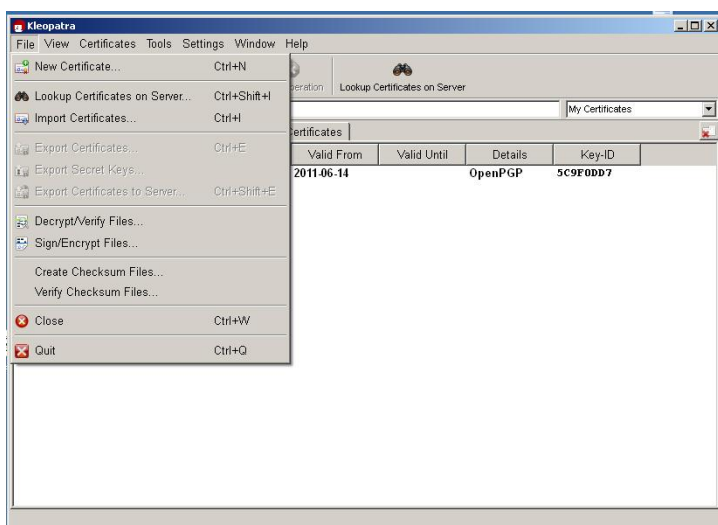
Laadiga alla ja installeerige programm Gpg4win aadressilt www.gnupg.org

Peal e installeerimist avage start menüüst Gpg4win->Kleopatra

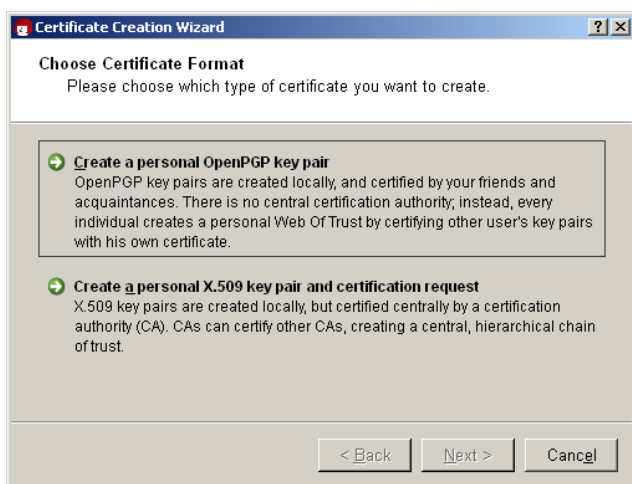
Uue võtme loomine

Selleks, et andmeid krüpteerida, tuleb teha endale võti. Eksisteerib kaks võtit: avalik ja salajane. Salajast võtit teab ja omab ainult selle looja, avalikku võib aga jagada ka teistele. Antud juhul anname meie, Finantsinspeksioon, teile oma avaliku võtme ja Teie annate meile oma avaliku võtme, et me saaksime hakata krüpteeritult andmeid vahetama.

File menüüst valige **New Certificate**



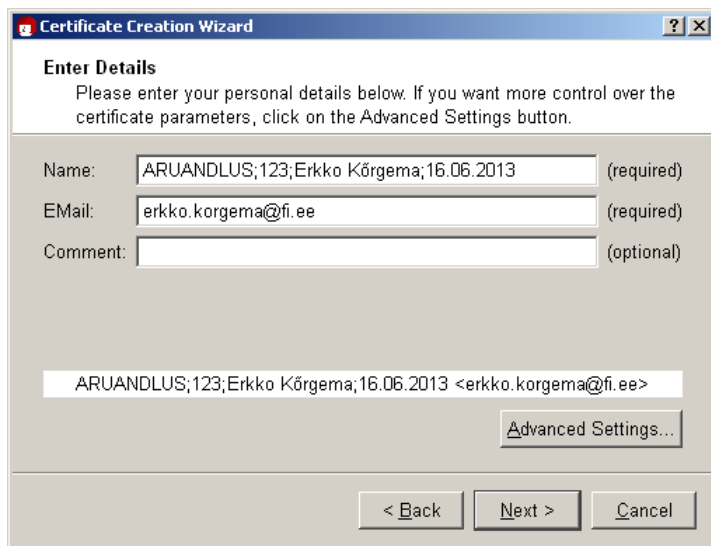
Avanevas aknas valige **Create a personal OpenPGP key pair**



Nime väljale tuleb kirjutada sõna “ARUANDLUS”, oma asutuse kood, vastutava isiku nimi ja võtmepaari kehtivuse lõpptähtaeg (vahele tuleks kirjutada semikoolon). Nt kui teie asutuse kood (koodi saate meie käest) on 2222, siis nime väli võib välja näha järgmine

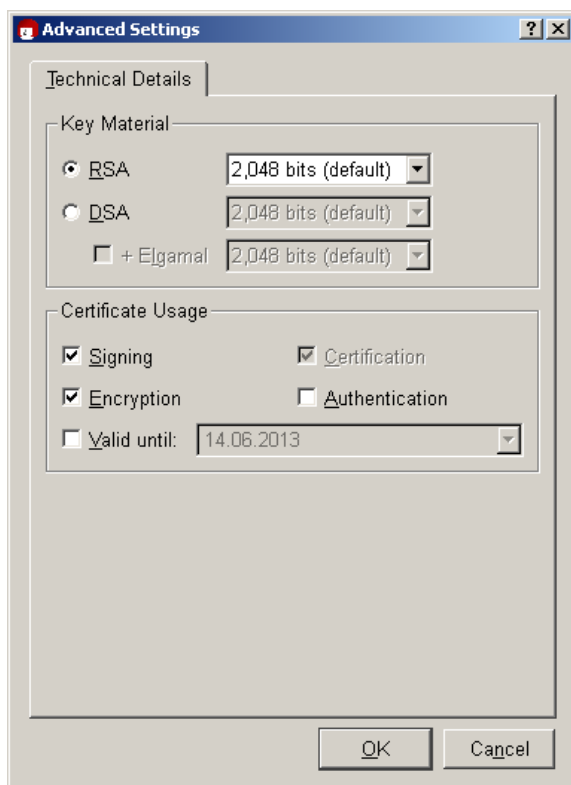
ARUANDLUS;123;PEETER KUUSK;07.05.2013

Võtmepaarid kuuluvad vahetamisele vähemalt üks kord kahe aasta jooksul. Vastavalt sellele tuleb valida ka lõpptähtaeg.



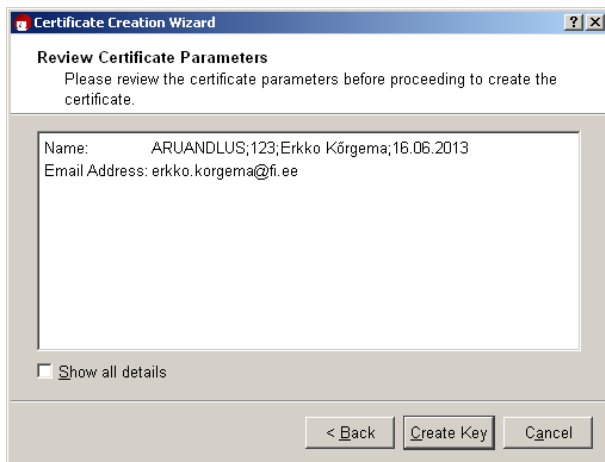
The 'Certificate Creation Wizard' dialog box has a title bar with a question mark and close button. The main area is titled 'Enter Details' and contains instructions: 'Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button.' There are three input fields: 'Name:' with the value 'ARUANDLUS;123;Erkko Kõrgema;16.06.2013' (required), 'EMail:' with the value 'erkko.korgema@fi.ee' (required), and 'Comment:' (optional). Below these fields is a summary line: 'ARUANDLUS;123;Erkko Kõrgema;16.06.2013 <erkko.korgema@fi.ee>'. At the bottom right is an 'Advanced Settings...' button. At the very bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Advanced Settings nupu alt kontrollige, et võtme tüüp oleks RSA ja pikkus vähemalt 2048



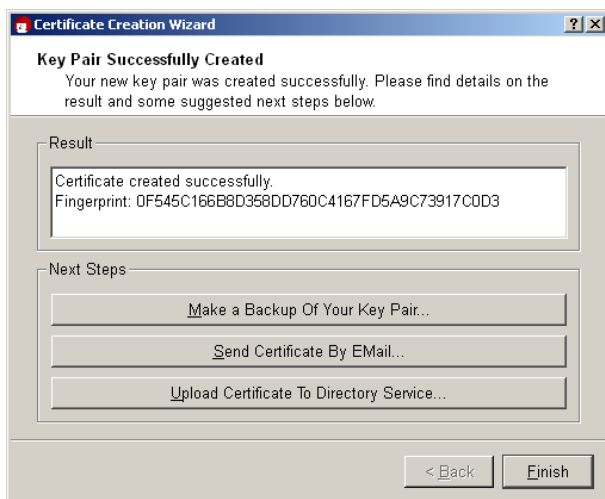
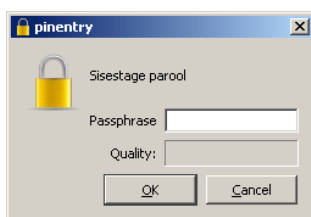
The 'Advanced Settings' dialog box has a title bar with a question mark and close button. It features a 'Technical Details' tab. Under 'Key Material', there are three radio buttons: 'RSA' (selected), 'DSA', and '+ Elgamal'. Each has a dropdown menu set to '2,048 bits (default)'. Under 'Certificate Usage', there are four checkboxes: 'Signing' (checked), 'Encryption' (checked), 'Certification' (checked), and 'Authentication' (unchecked). There is also a 'Valid until:' field with a date selector set to '14.06.2013'. At the bottom are 'OK' and 'Cancel' buttons.

OK-> NEXT



Create Key

Sisestage oma salajase võtme aktiveerimiseks vajalik salasõna, mis peab olema vähemalt 8 sümbolit pikk ja soovitatav sisaldama lisaks tähemärkidele ka erisümboleid. (NB Parooli ei tohi unustada, sest selle ununemisel ei ole enam võimalik krüpteeritud faile lahti krüpteerida. Samuti peab salasõna hoidma ainult enda teada, sest selle teadasaamisel kõrvaliste isikute poolt on võimalik nendel aktiveerida salajane võti ja lahti krüpteerida Teie salajane informatsioon.)

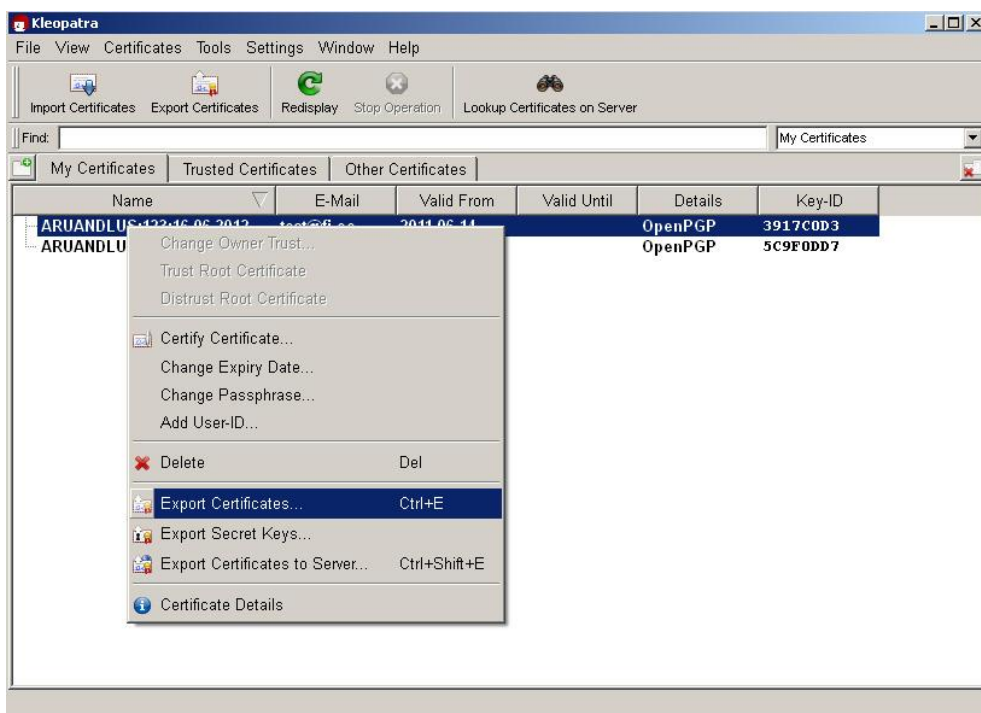


Võti edukalt genereeritud.

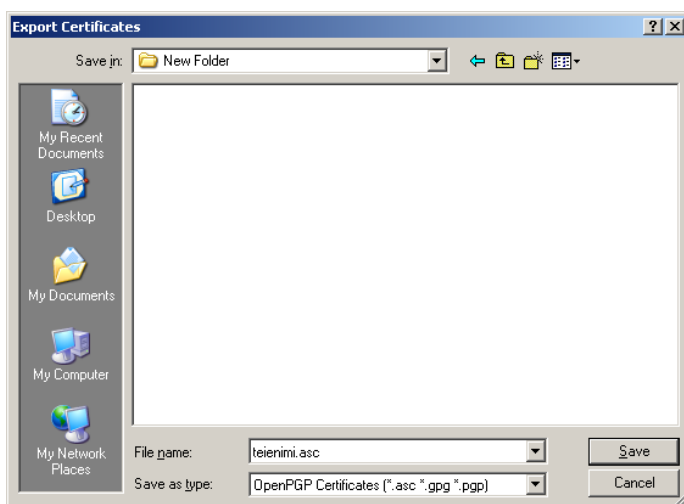
Võtmete vahetamine

Valige oma võti ja **File** menüüst **Export Certificates**.



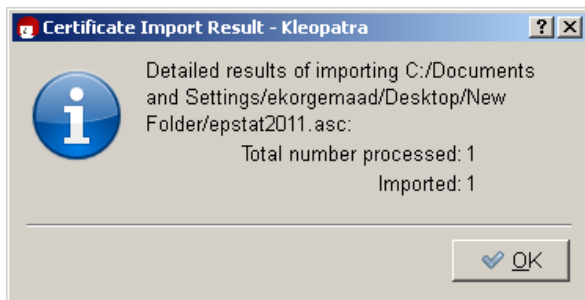


Selle faili (avaliku võtme) peate toimetama meile.



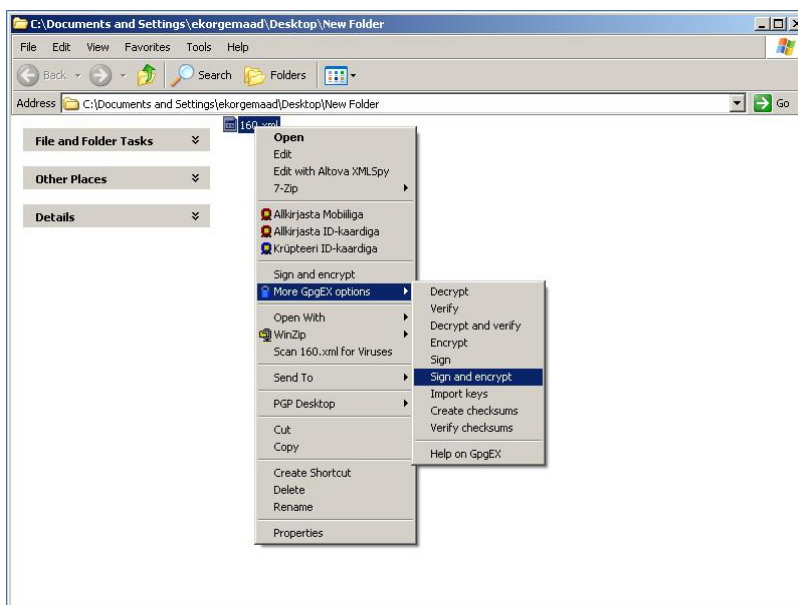
Finantsinspektsiooni võtme saate alla laadida aadressilt www.fi.ee/schemas (*.asc laiendiga fail, milles hulgast tuleks valida kõige uuem)

Salvestage fail enda arvutisse ja failil hiire parema klahviga klikkides valige **More GpgEX options->Import Keys**.



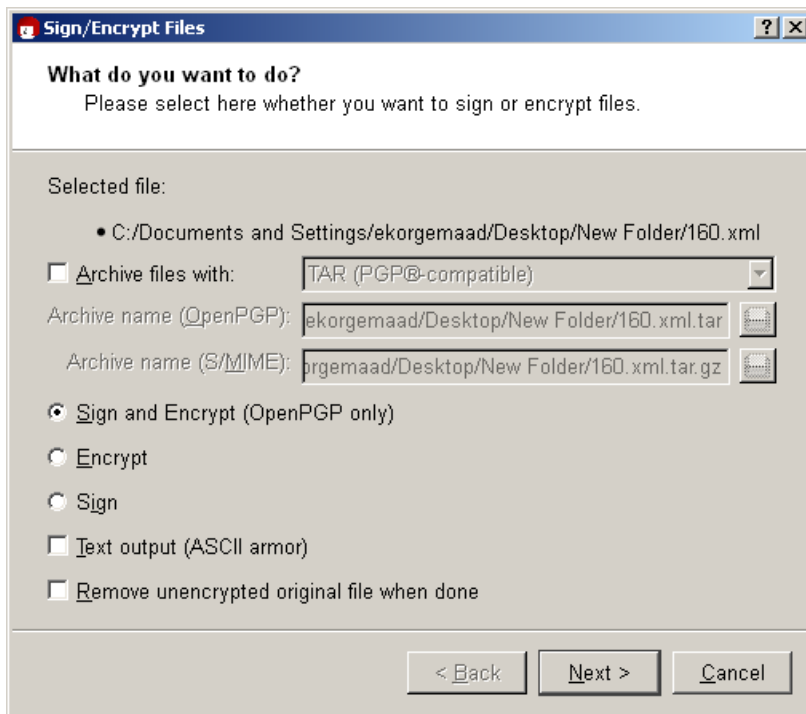
Andmete allkirjastamine ja krüpteerimine

Valige fail, mida soovite krüpteerida ja hiire parema klahvi alt avanevast menüüst valige **More GpgEX options-> Sign and encrypt**

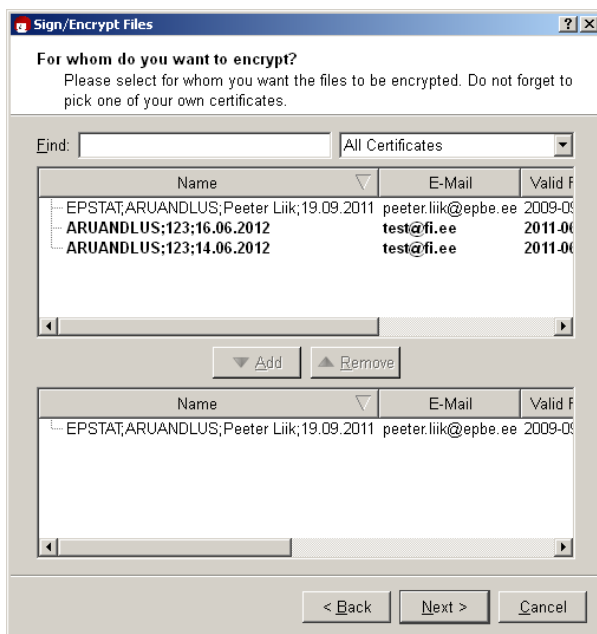


Avanevas aknas tuleb järgida, et valitud oleks **Sign and Encrypt (OpenPGP only)**.



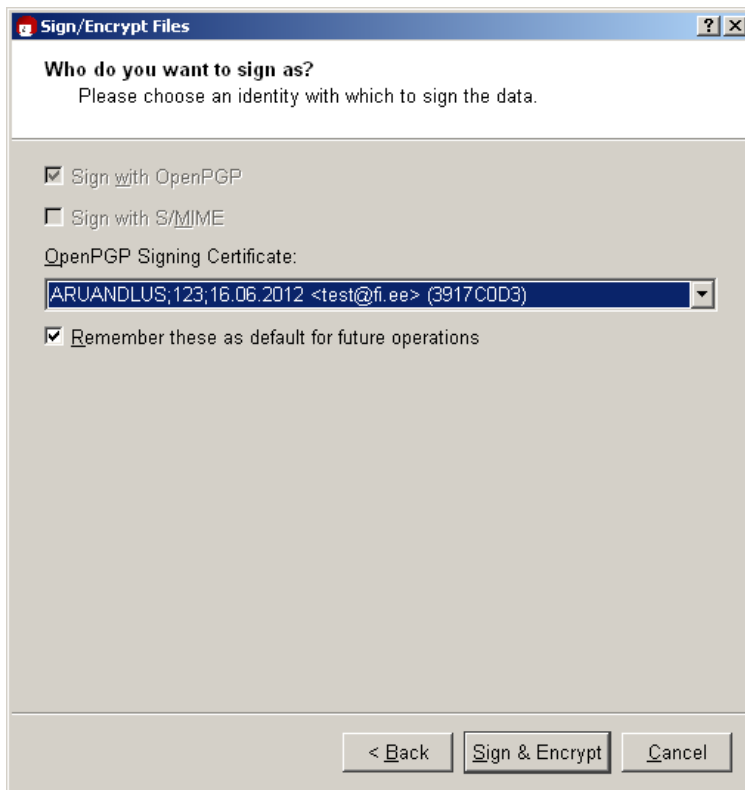


Lisage ülemisest kastist alumisse võti, millele soovite andmeid krüpteerida. Finantsinspeksioonile edastatavates andmetes peaks alumisse kasti kindlasti jõudma Finantsinspeksiooni avalik võti.



Andmete allkirjastamiseks valige oma võti ja sisestage parool.





Andmed edukalt krüpteeritud. Samasse kataloogi krüpteeritava failiga, loodi uus krüpteeritud fail, mis tuleb edastada Finantsinspektsioonile.

