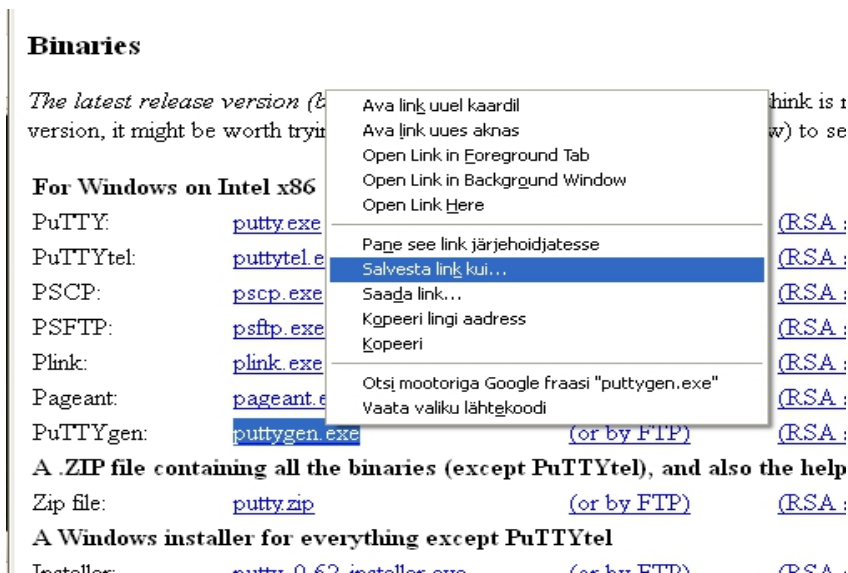


SSH võtmepaari tekitamine

helpdesk@emu.ee

1. Tõmba [Putty](#) kodulehelt **PuTTYgen** programm. Salvesta see näiteks omale tööauale.



Binaries

The latest release version (0.62) is available for download. If you are using an older version, it might be worth trying the latest version.

For Windows on Intel x86

PuTTY:	putty.exe		
PuTTYtel:	puttytel.exe		(RSA : ...)
PSCP:	pscp.exe		(RSA : ...)
PSFTP:	psftp.exe		(RSA : ...)
Plink:	plink.exe		(RSA : ...)
Pageant:	pageant.exe		(RSA : ...)
PuTTYgen:	puttygen.exe	(or by FTP)	(RSA : ...)

A .ZIP file containing all the binaries (except PuTTYtel), and also the help files

Zip file:	putty.zip	(or by FTP)	(RSA : ...)
-----------	---------------------------	-----------------------------	-----------------------------

A Windows installer for everything except PuTTYtel

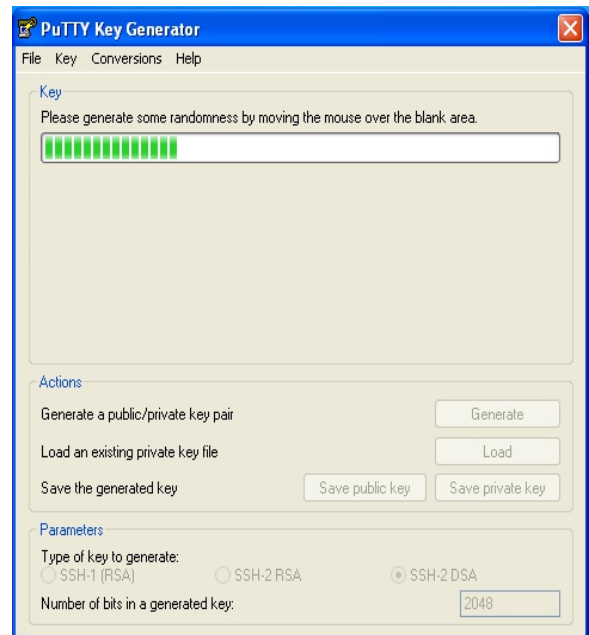
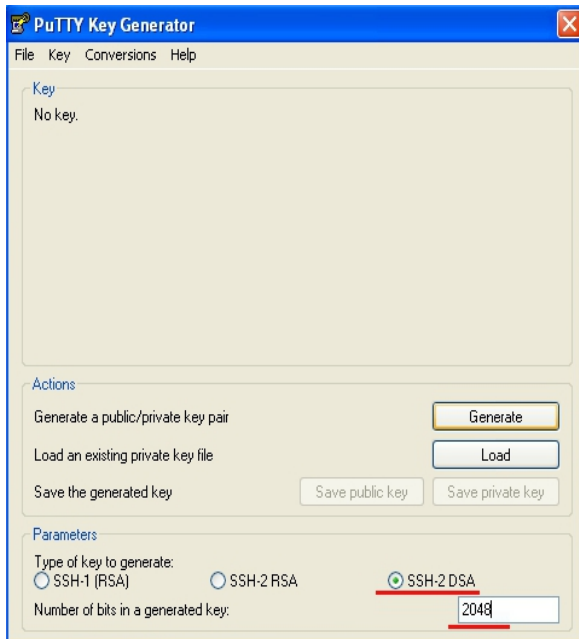
Installer:	putty-0.62-installer.exe	(or by FTP)	(RSA : ...)
------------	--	-----------------------------	-----------------------------

2. Käivita: **Run**



3. Määra genereeritava võtme tüübiks **SSH-2 RSA** ning soovituslikult määra ka võtme suuruseks **2048** (vaikimisi 1024). Seejärel vajuta nuppu **Generate**.

Liiguta hiirt programmi tühjal alal tekitamaks juhuslikkust, mida kasutatakse võtme genereerimiseks, kuni roheline riba on jõudnud lõppu.



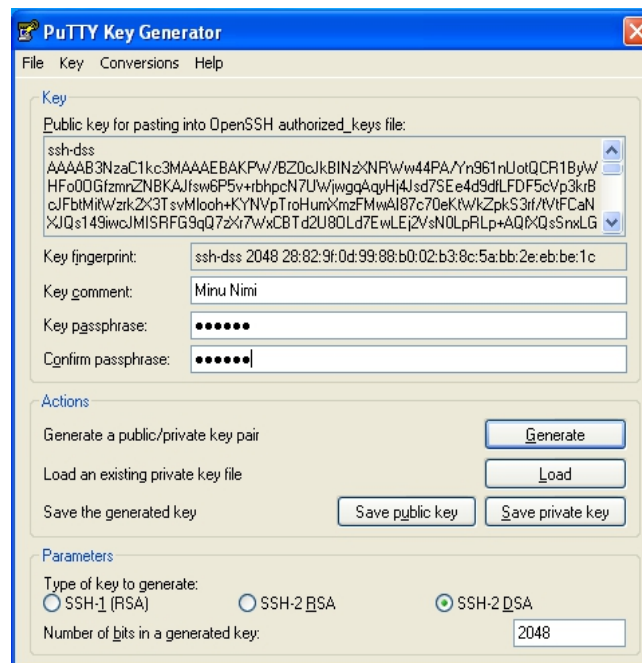
4. Kui võti on genereeritud, siis täida lahtrid:

Key comment: <siia kirjuta oma nimi>

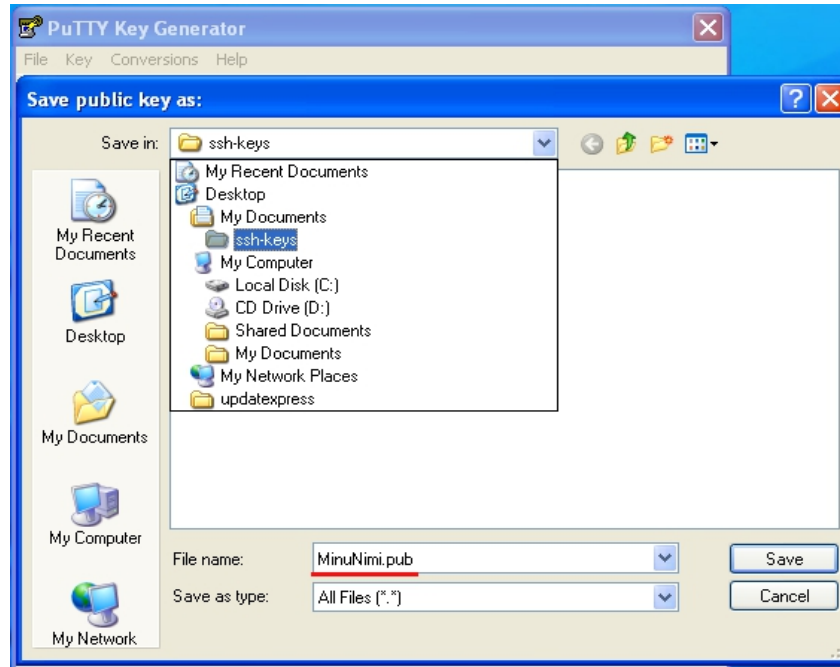
Key passphrase/Confirm: <VägaHeaParool>

Seda parooli hakatakse kasutama võtme avamiseks.

NB! Seda parooli tohib teada ainult võtme genereerija! Ka ei ole see parool seotud EMÜ keskse konto ega selle parooliga.



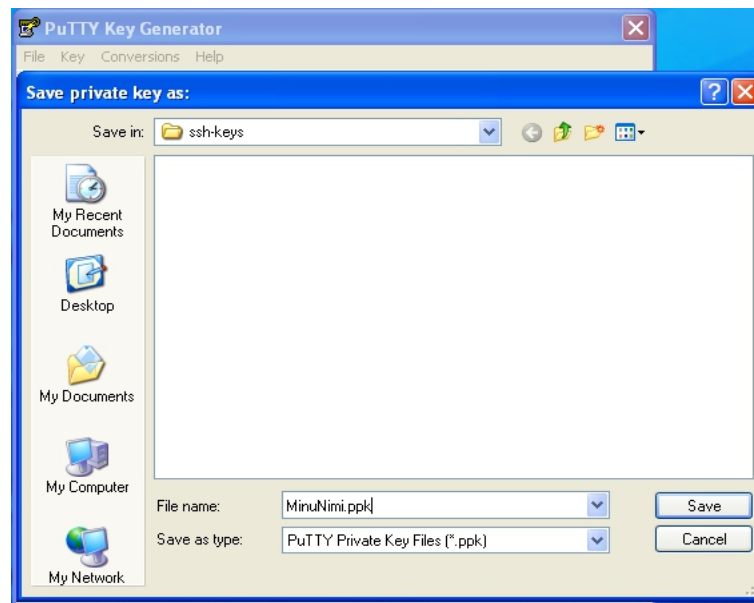
5. Salvesta genereeritud võtme AVALIK pool näteks ssh-keys kataloogi: **Save public key**
 Faili nimeks pane oma nimi ja määra ka faili laiend. Näiteks **.pub** (sõnast **public**). Programm ise laiendit ei paku. Salvesta: **Save**



6. Salvesta võtme **PRIVAATNE** pool: **Save private key**

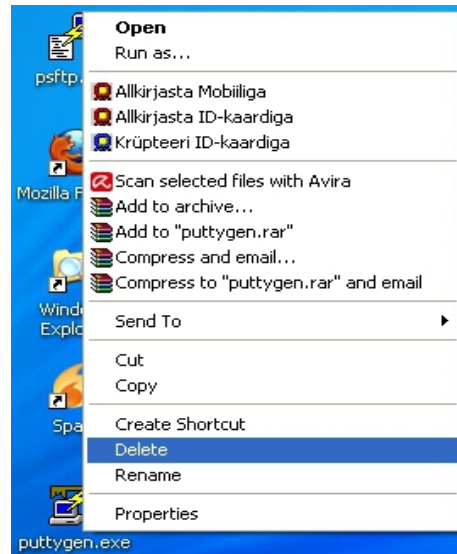
Seekord pakub programm ise laiendi: .ppk. Faili nimeks pane jällegi oma nimi ning salvesta: **Save**.

NB! Võtme privaatset poolt tuleb hoolega hoida võõrastesse kättesse sattumise eest, seda ei tohi ära kaotada ega ka unustada parooli, millega selle võtme lahti saab. Kui võti on kompromiteeritud, siis tuleb sellest koheselt teavitada IKT osakonda ja võti kasutusest eemaldada (sh serverites asuvad avalikud pooled).



7. Sellega on võti genereeritud ja võib PuTTYgen programmi sulgeda. Soovi korral kustuta ka

töölaualt.



8. Serverile ligipääsu saamiseks saada võtme **avalik** pool serveri haldajale. Võti tuleb saata manusena (attachment).

