SSH võtmepaari tekitamine

helpdesk@emu.ee

1. Tõmba <u>Putty</u> kodulehelt **PuTTYgen** programm. Salvesta see näiteks omale tööauale.

Binaries				
The latest releat	se version (b	Ava lin <u>k</u> uuel kaardil		hink is t
version, it might b	oe worth tryi	Ava link uues aknas		w) to se
		Open Link in <u>F</u> oreground	i Tab	
For Windows o	n Intel x86	Open Link in Backgr <u>o</u> und	d Window	
PuTTY:	putty.exe -	Open Link <u>H</u> ere		- (RSA :
D. TTVA-1		Pa <u>n</u> e see link järjehoidja	itesse	DCA.
Pulliter.	puttyter.e	Salvesta lin <u>k</u> kui		(KSA :
PSCP:	pscp.exe	Saa <u>d</u> a link		<u>(RSA :</u>
PSFTP:	psftp.exe	K <u>o</u> peeri lingi aadress		(RSA :
Plink:	plink.exe –	<u>K</u> opeeri		- (RSA :
Pageant:	pageant.e	Otsi mootoriga Google fi Vaata valiku lähtekoodi	raasi "puttygen.exe"	(RSA :
PuTTYgen:	puttygen.ex		(or by FTP)	(RSA :
A .ZIP file cont	taining all the	binaries (except Pu	1TTYtel), and also	o the help
Zip file:	putty.zip		(or by FTP)	(RSA :
A Windows ins	taller for even	ything except PuT	ΓYtel	
Teatollog	a	installor area	(ar her ETD)	ADCA.

2. Käivita: Run

Open Fi	Open File - Security Warning		
The pa run thi	ublisher could not be verified. Are you sure you want to is software?		
	Name: puttygen.exe		
	Publisher: Unknown Publisher		
	Type: Application		
	From: C:\Documents and Settings\Administrator\Desktop		
	Run Cancel	ן	
💌 Alwa	ays ask before opening this file		
8	This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. <u>How can I decide what software to run?</u>		

 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.

😴 PuTTY Key Generator 🛛 🛛 🛛 🛛	PuTTY Key Generator
File Key Conversions Help	File Key Conversions Help
Key No key.	Key Please generate some randomness by moving the mouse over the blank area.
Actions	Actions
Generate a public/private key pair Generate	Generate a public/private key pair Generate
Load an existing private key file Load	Load an existing private key file Load
Save the generated key Save public key Save private key	Save the generated key Save public key Save private key
Parameters Type of key to generate: SSH-2 RSA SSH-2 RSA O SSH-2 DSA	Parameters Type of key to generate: SSH-2 RSA SSH-2 RSA SSH-2 DSA Musher of hit in a constrated key: D0/9

 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 võme genereerija! Ka ei ole see parool seotud EMÜ keskse konto ega selle parooliga.

P	PuTTY Key Gen	erator	×		
File	e Key Conversior	ns Help			
	Key				
	Public key for pasting into OpenSSH authorized_keys file:				
	ssh-dss AAAAB3NzaC1kc3	MAAAEBAKPW/BZ0cJkBINzXNRWw44PA/Yn961nUotQCR1ByW 合			
	HFo00GfzmnZNBK	AJfsw6P5v+rbhpcN7UWjwgqAqyHj4Jsd7SEe4d9dfLFDF5cVp3krB syMloobaKYNVpTroHurxYmzEMw6187c70sKfWk7pbS3rf/WrECaN			
	XJQs149iwcJMISR	FG9qQ7zXr7WxCBTd2U80Ld7EwLEj2VsN0LpRLp+AQfXQsSnxLG			
	Key fingerprint:	ssh-dss 2048 28:82:9f:0d:99:88:b0:02:b3:8c:5a:bb:2e:eb:be:1c			
	Key <u>comment:</u> Minu Nimi				
	Key p <u>a</u> ssphrase:	issphrase: •••••			
	Confirm passphrase:				
	Actions				
	Generate a public/private key pair Generate				
	Load an existing private key file				
	Save the generated	key Save p <u>ublic key</u> Save private key			
	Parameters				
	Type of key to gene				
	Number of bits in a s	0 55H-2 <u>D</u> 5A			
	manuper of bits in a f	2040			

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 kätesse 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).

PuTTY Key (Generator				×	
Save private k	sions Help					
Save in:	ssh-keys		~	G 🖻	• 🗉 🖻	
My Recent Documents						
Desktop						
My Documents						
My Computer						
	File name:	MinuNimi.ppk			~	Save
	Save as type:	PuTTY Private Key Files (*.pp	k)		*	Cancel
My Network						.::

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).

👇 Koostamine: minu avalik võti 📃 🗖 🔀
Eail <u>R</u> edigeerimine <u>V</u> aade Lisamine Vor <u>m</u> indus <u>V</u> alikud <u>T</u> ööriistad <u>A</u> bi
💽 Saada 🛯 🖓 Õigekiri 🔹 🖉 Lisa 🔹 🚔 Turvalisus 🔹 🔚 Salvesta 🔹
Saatja: Minu Nimi <minu.nimi@emu.ee> min 👽 Manused:</minu.nimi@emu.ee>
★ Kellele: A it@emu.ee
Teema: minu avalik võti
Sisutekst 💽 Muutliku laiusega 💽 두 🌊 🜊 🗛 🖉 🗮 📰
Tere, Saadan oma avaliku võtme. Head päeva