15. February 2022

Instructions for generation of banklink key

It's recommended to create a separate key pair for the banklink application, which shouldn't have anything in common with the server certificate.

We recommend using **OpenSS**L (http://www.openssl.org) and generating a separate secret key for the banklink, and then making a certificate request for that key.

The length of the secret keys generated by clients that we support is at least 4096 bit.

A secret key can be generated with the following command line:
openssl genrsa -out private_key.pem 4096

A certificate for an existing secret key can be requested as follows:
openssl req -new -key private_key.pem -out certrequest.pem

The DN (distinguished name) format of the certificate request should be as follows:

E (email address) = contact email address of the administrator of the partner's certificate (xxx@xxx.ee)

CN (Common Name) = the FQDN where banklink will be used (www.puukool.ee)

OU (Organisational Unit Name) = banklink

O (Organisation Name) = registered name of the organisation (e.g.: Puukool OÜ)

C (Country Name) = EE

Two files are generated as a result of the command: "private_key.pem", which includes the secret key and "certrequest.pem", which includes the certificate request. The secret key remains with the merchant and it must be entered in the settings of the online store. The certificate request must be sent to the bank.

Please note: Please keep your secret key securely and do not pass it on to third parties (incl. the bank)! If you send your secret key to the bank, the bank will refuse to use the key pair and asks you to generate a new key pair.

To activate the service, the bank uses the merchant's **public key**, which will be taken from the certificate request sent by the merchant. It is convert the public key from the secret key with the following command:

openssl rsa -in private_key.pem -outform PEM -pubout -out public.pem

The merchant's secret key may not leak, because third parties can use it to sign the payment requests going to the bank on your behalf and thereby cause you damage.

The client also needs the **public key of the bank** for using the banklink, which can be downloaded from the bank's website. The client's online store uses this to validate the response sent by the bank and consider the transaction completed.