3. september 2021

Pangalingi võtmete genereerimise juhend

Pangalingi rakenduse tarvis on soovitatav luua eraldi võtmepaar, millel ei tohiks www serveri sertifikaadiga midagi ühist olla.

Soovitame kasutada **OpenSSL'i** (http://www.openssl.org) ja genereerida pangalingi jaoks eraldi salajane võti ning siis teha sellele võtmele sertifikaadipäring (certificate request).

Kliendi poolt genereeritud salajase võtme pikkusena toetame vähemalt 2048 bitti.

Salajase võtme saab genereerida järgmise käsureaga:
openssl genrsa -out private_key.pem 2048

Olemasolevale salajasele võtmele saab sertifikaati pärida järgnevalt:
openssl req -new -key private_key.pem -out certrequest.pem

Sertifikaadipäringu DN (distinguished name) kuju peaks olema järgmine:

E (e-maili aadress) = partneri sertifikaadi haldaja kontakt emaili aadress (xxx@xxx.ee)

CN (Common Name) = FQDN kus pangalinki kasutama hakatakse (www.puukool.ee)

OU (Organizational Unit Name) = banklink

O (Organization Name) = asutuse registreeritud nimi (näiteks: Puukool OÜ)

C (Country Name) = EE

Käsu tulemusena tekib 2 faili: "private_key.pem", mis sisaldab salajast võtit ja "certrequest.pem", mis sisaldab sertifikaadipäringut. Salajane võti jääb kaupmehele ja see tuleb sisestada veebipoe seadistusse. Sertifikaadipäring tuleb edastada pangale.

NB! Palun hoidke oma salajast võtit turvaliselt ja ärge edastage seda kolmandatele isikutele (sh pangale)! Kui saadate oma salajase võtme pangale, keeldub pank selle võtmepaari kasutamisest ja palub teil genereerida uus võtmepaar.

Lepingu sõlmimiseks ja teenuse aktiveerimiseks kasutab pank kaupmehe **avalikku võtit**, mis võetakse välja kaupmehe saadetud sertifikaadipäringust. Kui soovite veenduda, et lepingusse sai kaupmehe salajasele võtmele vastav avalik võti, saab avaliku võtme ise salajasest võtmest teisendada käsuga:

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

Kaupmehe salajane võti ei tohi lekkida, sest sellega on võimalik kolmandatel isikutel teie asemel allkirjastada panka minevaid maksepäringuid ja seeläbi tekitada Teile kahju.

Kliendil on vaja pangalingi kasutamiseks ka **panga avalikku võtit**, mille leiab lepingust ja mille saab alla laadida panga kodulehelt. Selle abil valideerib kliendi veebipoe rakendus panga poolt saadetud vastuse, et selle alusel lugeda tehing teostatuks.

Juhul kui Teil puudub võimalus genereerida pangalingi võtmeid OpenSSL-ga, siis alternatiivina soovitame Zone.ee veebilehel olevat blogi https://blog.zone.ee/2006/12/12/pangalink/ ja võtmete generaatorit https://blog.zone.ee/pangalingid/.

Pank eelistab käsitsi OpenSSL-ga genereeritud sertifikaadipäringut, sest seal on kaupmees ise saanud enda andmed sisestada, kuid võtame vastu ka Zone.ee veebilehel genereeritud sertifikaadipäringuid.