2.2 Sertifikāta izveidošana

Ja iestādei nav CA, tad testēšanas nolūkiem VRAA var nodrošināt sertifikāta izveidošanu, izmantojot VISS CA.

Lūgums nepārkopēt dotās komandas no parauga, bet gan rakstīt tās ar rokām, jo pārkopējot tas var nestrādāt.

VRAA CA sertifikātu sagatavo, izmantojot openssl bibliotēku:

Sagatavošanas solī nepieciešams uzlikt openssl un palaist to no komandrindas

openssl>

Jāuzģenerē privātā atslēga, kur xxxxx ir izdomāts kodēts nosaukums katram klientam unikāls

>genrsa -out c:\temp\xxxxx.key 2048

Jāuzģenerē sertifkāta pieprasījums

>req -new -subj '/C=LV/ST=Riga/L=Riga/O=Organizacijas nosaukums/OU=IT/CN=xxxxx/emailAddress=it@kllients.lv' -key c:\temp\xxxxx.key -out c:\temp\xxxxx.req -days 1800

Uzģenerētais fails xxxxx.req jānosūta VRAA. VRAA pēc šī pieprasījuma uzģenerē xxxxx.cer failu un nosūta to klientam.

Kad klients saņem .cer failu, tas jāiekopē blakus .key failam, jāatver openssl un jāizpilda komanda:

>pkcs12 -export -in c:\temp\xxxxx.cer -inkey c:\temp\xxxxx.key -out c:\temp\xxxxx.pfx

Iegūto .pfx failu var izmantot pēc vajadzības.

Linux sertifikāta apstrāde:

openssl pkcs7 –print_certs –in iestade.p7b –out certificate.cer

Kur iestade.p7b ir VRAA atsūtītais .p7b fails

openssl pkcs12 –export –in xxxxx.cer –inkey/opt/certi/iestade.key –certfile iestade.cer –out iestade.pfx

Kur certificate.cer ir iepriekšējās komandas uzģenerētais fails; iestade.key ir Jūsu key fails, iestade.cer ir VRAA atsūtītais. Šī komanda prasīs ievadīt paroli – Jūsu izdomāta parole, kuru vajadzēs app.config failam.

openssl pkcs12 –info –in iestade.pfx

Šī komanda izdrukā uzģenerētā .pfx faila info – no kā var iegūt nepieciešamos datus, prasti tas ir thumbprint (tas ir localKeyID) - ciparu un burtu kombinācija ar visām atstarpēm.