

CRS/DAC2 LIETOTĀJA AUTENTIFIKĀCIJAS PROCESS

Informācijas iesniegšana tiks tehniski realizēta, izmantojot web servisu tehnoloģiju. Finanšu iestādes, kurām ir jāiesniedz CRS/DAC2 dati, tiek pierēģistrētas VID. Tiek izveidots un izsniegts autentifikācijas sertifikāts, atvērta piekļuve VID datortīkla ugunsmūrī. Visa datu apmaiņa starp Finanšu iestādi un VID serveri tiek nodrošināta izmantojot ar TLS (*Transport Layer Security*) protokolu šifrētu datu kanālu.

Datu apmaiņai starp Finanšu iestādi un VID jānotiek automatizēto sistēmu līmenī (*system to system*).

Latvijas finanšu iestādes CRS/DAC2 datus iesniedz izmantojot VID Informācijas sistēmu savietotājā (VID ISS) izmitinātu servisu.

Finanšu iestādes autentifikācijai un autorizācijai tiek izmantots SSL (*Secure Sockets Layer*) sertifikāts.

Zemāk ir aprakstītas veicamās darbības piekļuves sertifikāta saņemšanai:

1. Jāizveido CSR (*certificate signing request*) datne (aprakstīts sadaļā “VID WEB servisa sertifikāta izveide”);
2. Jāsagatavo piekļuves tiesību pieprasījums, kurš satur zemāk tabulā aprakstīto informāciju:

NMR numurs	Nosaukums	IP adrese/ adrese.*	Kontaktpersona (vārds/uzvārds, tālruna numurs, e-pasta adrese)	Sistēmas/servisa nosaukums kurai nepieciešama piekļuve	Pamatojums (šajā gadījumā, normatīvais akts uz kura pamata nepieciešams saņemt piekļuves tiesības)
				CRS/DAC2	

* - Jābūt norādītām precīzām publiskajām IP adresēm. Tīkla apgabalu adrese netiks pieņemtas.

3. 1. un 2. punktā sagatavotās datnes, e-parakstītā formātā, elektroniski jānosūta VID uz e-pasta adresi ip_piekluves@vid.gov.lv, Cc nosūtot uz e-pasta adresi ip_dac@vid.gov.lv un vēstules tekstā norādot kurai videi (testa vai produkcijas) tiek pieprasītas tiesības;
4. Piekļuves tiesību pieprasījumus VID sāks pieņemt un apstrādāt pēc 01.01.2017.;
5. VID, pēc piekļuves tiesību pieprasījuma un CSR datnes saņemšanas, izveidos piekļuves sertifikātu;
6. Pēc piekļuves sertifikāta izveidošanas, tas tiks nosūtīts uz pieteikumā norādītās Finanšu iestādes kontaktpersonas e-pasta

adresi, kopā ar papildus nepieciešamo informāciju veiksmīgi
servisa izmantošanai.

VID WEB servisa sertifikāta izveide

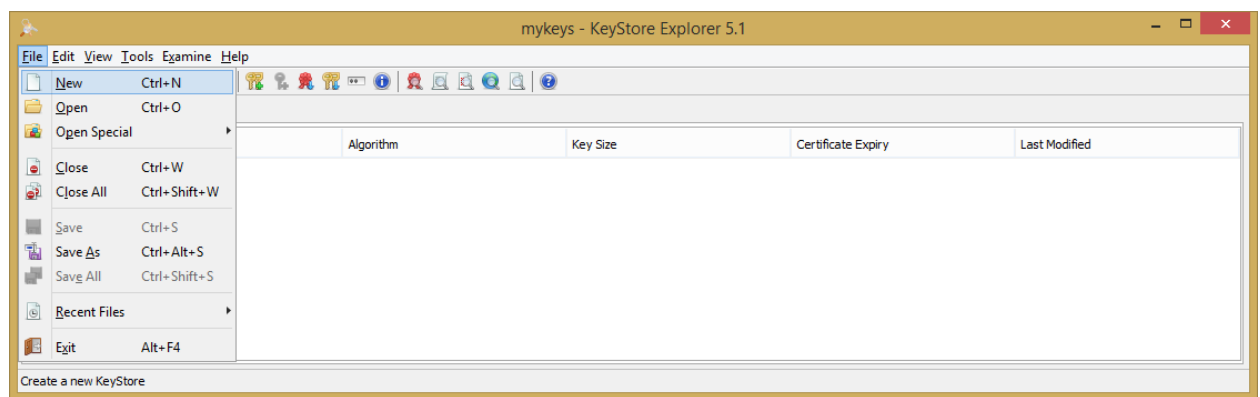
Piemērs veidots ar KSE 5.1 (<https://sourceforge.net/projects/keystore-explorer/>). Var izmantot arī citus rīkus kā piemēram OpenSSL.

Lai sagatavotu sertifikātu datni, ko izmantot WS autentifikācijai ir jāveic šādas darbības:

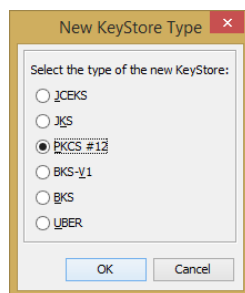
1. Jāsagatavo PFX datne ar privāto atslēgu;
2. Jāizveido un jānosūta CSR (certificate signing request) datne VID;
3. PFX datnē jāieimportē VID izdotie root sertifikāti;
4. PFX datnē jāieimportē VID izdotā CSR CA atbilde.

1. PFX datnes ar privāto atslēgu sagatavošana

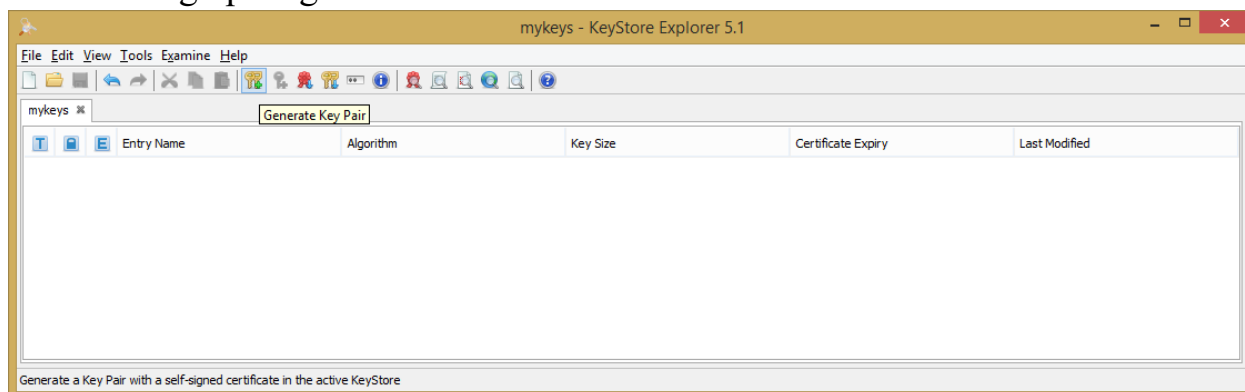
Jāizveido tukša PFX datne (PKCS12 konteineris):



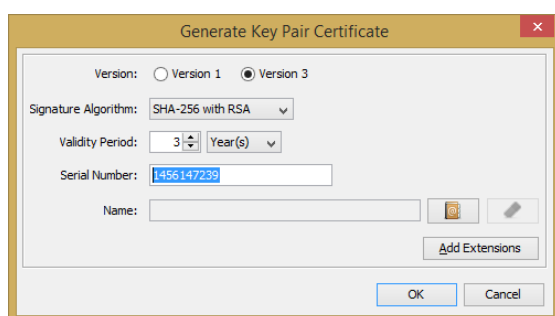
Veidojot datni jānorāda tips – PKCS#12:



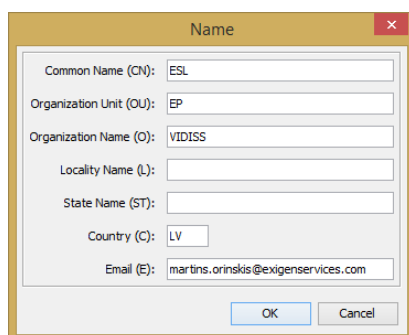
Jāveic atslēgu pāra ģenerēšana:



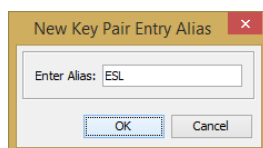
Jānorāda algoritms un derīguma termiņš:



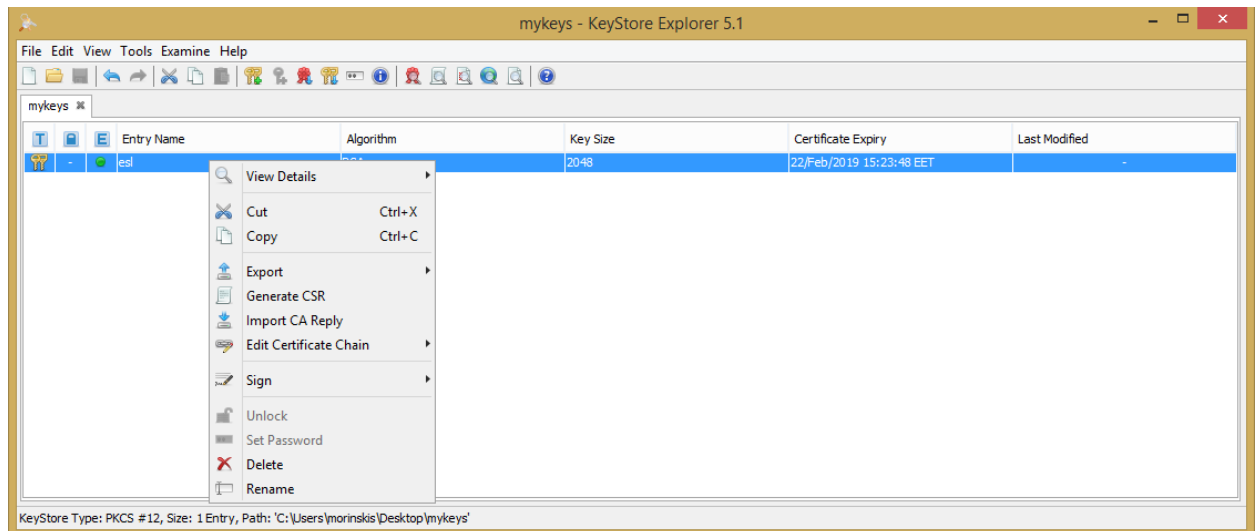
Jānorāda sertifikāta detaļas, obligāti norādot Common Name (CN) un e-pasta adresi (E):



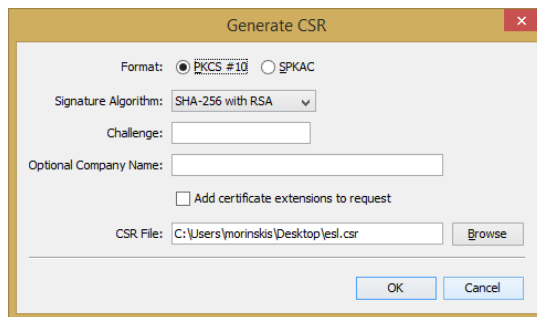
Jānorāda ieraksta loģiskais nosaukums, kas tiek izmantots lietojumprogrammās, lai nolasītu sertifikātu:



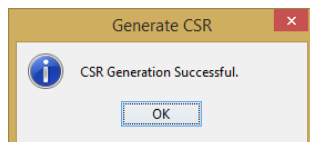
2. Jāizveido un jānosūta CSR (certificate signing request) datne VID Sertifikāta parakstīšanas pieprasījuma izveide jāveic norādītajam ierakstam izmantojot Generate CSR:



Jānorāda algoritms un formāts:



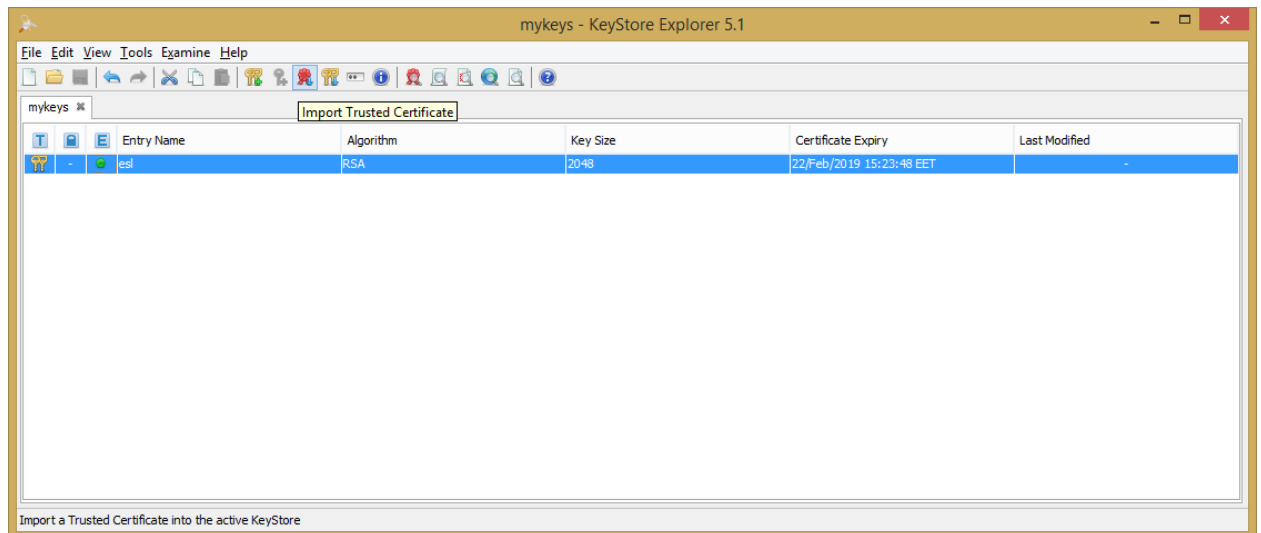
Informatīvs paziņojums par veiksmīgu CSR datnes izveidi:



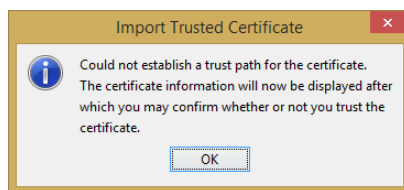
Izveidoto datni jānodod VID tālākai apstrādei. Šinī piemērā esl.csr tiek nodots VID.

3. PFX datnē jāieimportē VID izdotie root sertifikāti

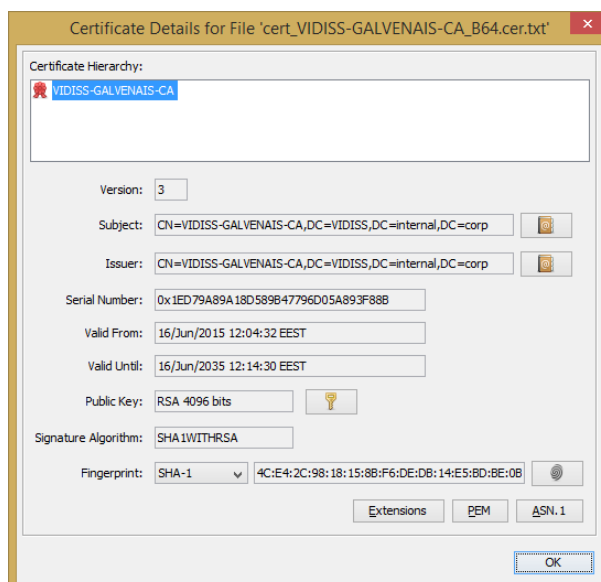
Pirms importēt CSR atbildi ir nepieciešams importēt VID CA root sertifikātus (visu root sertifikātu ķēdi). Šos sertifikātus piegādā VID. Jāveic *Import Trusted Certificate*, izvēloties datni, kura satur root sertifikātu (root sertifikātu datnes piegādā VID). Root sertifikāta imports jāveic katram sertifikātam atsevišķi (šīs darbības jāatkārto katram sertifikātam atsevišķi):



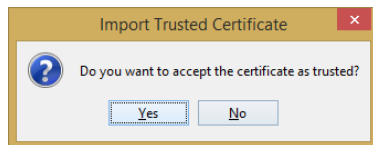
Sagaidāms paziņojums, ka nav zināms root sertifikāta izdevējs:



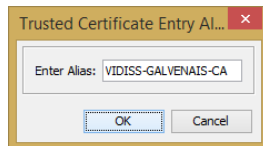
Informācija par importējamo root sertifikātu:



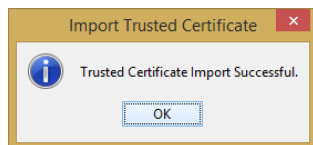
Apstiprinām, ka izmantosim šo sertifikātu [Yes]:



Norādām sertifikāta loģisko nosaukumu:



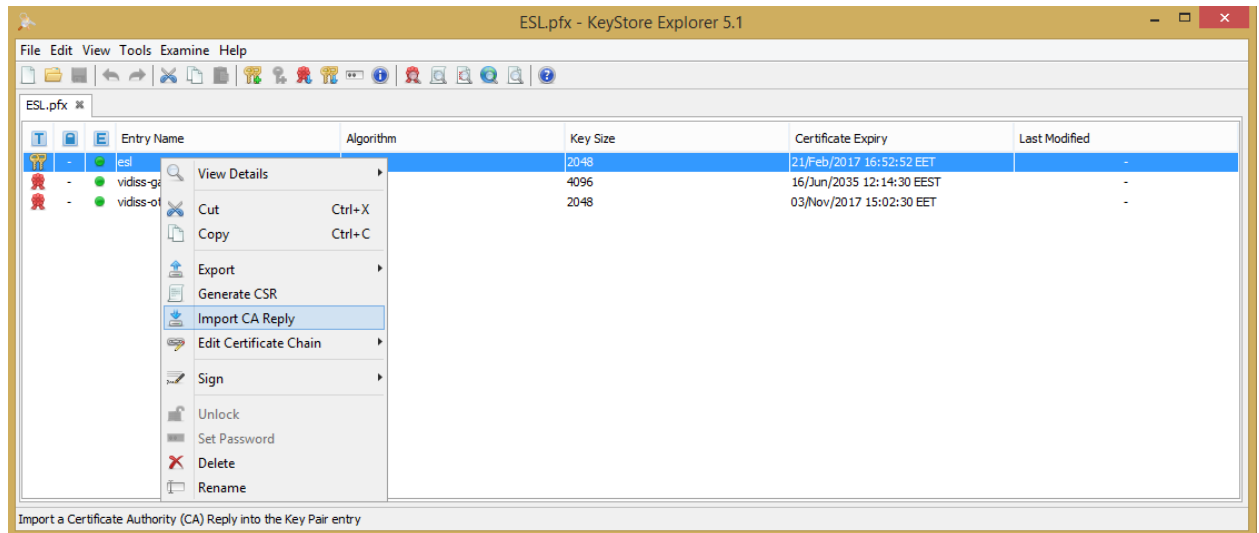
Informācija par darbības veiksmīgu izpildi:



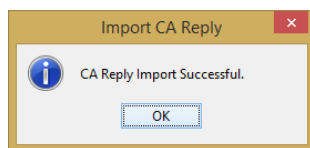
4. PFX datnē jāieimportē VID izdotā CSR CA atbilde

Importējam CSR apstiprinājumu. Šo apstiprinājumu sagatavo un piegādā VID pēc CSR pieprasījuma nosūtīšanas (sk. 2. punktu).

Atbilstošajam ierakstam jāizvēlas *Import CA Replay*, norādot saņemto apstiprinājuma datni:



Paziņojums par veiksmīgu darbību:



Pēc šīm darbībām PFX datne veiksmīgi sagatavota un ir izmantojama lietojumprogrammās (.NET, Java), lai veiktu autentifikāciju un izgūtu SAM