CRS/DAC2 LIETOTĀJA AUTENTIFIKĀCIJAS PROCESA INSTRUKCIJA DATU IESNIEDZĒJIEM

Saturs

1. Ievads

1.1. Dokumenta nolūks

Dokumenta nolūks ir sniegt instrukciju Latvijas finanšu iestādēm (turpmāk – FI) kā sagatavot datu iesniegšanai nepieciešamo autentifikācijas sertifikātu. Process sastāv no trīs etapiem:

1) privātās atslēgas izveidošana jeb PFX konteiners;

2) sertifikāta parakstīšanas pieprasījuma datnes izveidošana jeb datne .csr;

3) atbildes sertifikātu importēšana, kā rezultātā iegūst datu apmaiņai derīgu autentifikācijas sertifikātu.

1.2. Izmantotie saīsinājumi

Tabula 1

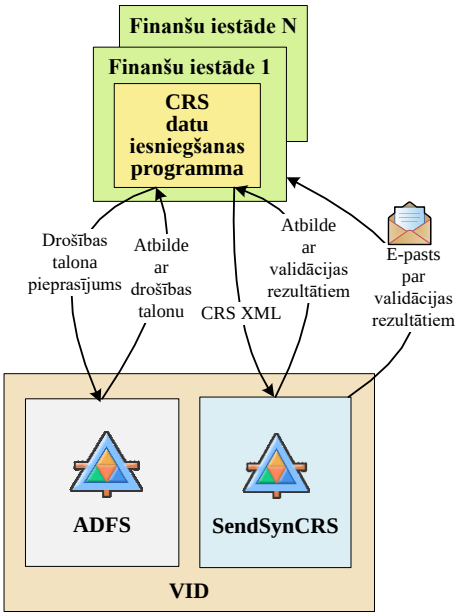
Saīsinājums	Saīsinājuma skaidrojums
ADFS	*Microsoft Active Driectory Federation Services* – Microsoft aktīvās direktorijas pakalpojums
CRS	*Common Reporting Standard* – starptautisks standarts, kas nosaka kārtību, kādā notiek automātiskā informācijas apmaiņa par finanšu kontiem
CSR	*Certificate Signing Request* – sertifikāta parakstīšanas pieprasījuma datne .csr
DAC2	Direktīva 2014/107/ES attiecībā uz obligāto automātisko informācijas apmaiņu nodokļu jomā
XML	*eXtensible Markup Language* – paplašinātā iezīmju valoda, lai definētu datu formātus. XML piedāvā plašas iespējas definēt un aprakstīt sarežģītus dokumentus un datu struktūras.
PFX	*Personal Information Exchange* – privātās atslēgas un publiskā sertifikāta datne/konteiners
PKCS	*Public Key Cryptography Standards* – publiskās atslēgas šifrēšanas standarti
TSL	*Transport Layer Security* – transporta līmeņa drošības protokols, kuru izmanto datu šifrēšanai, servera autentificēšanai un neobligātai klienta autentificēšanai

2. Kopējais apraksts

CRS iekšzemes ziņojumu iesniegšana tehniski realizēta, izmantojot web servisu tehnoloģiju un autentifikāciju ar sertifikātiem VID sistēmā. Datu apmaiņa starp FI programmatūru un VID serveriem notiek izmantojot ar TLS protokolu šifrētu datu kanālu.

FI sagatavo CRS iekšzemes ziņojuma XML datni (pēc parauga saitē https://www.vid.gov.lv/lv/starptautiskie-ligumi-un-administrativa-sadarbiba#crs CRSNilSample.xml – nulles ziņojumiem; CRSInitialSample.xml – iekšzemes datu ziņojumus par nerezidentu finanšu kontiem).

FI datu iesniegšanas programmatūra (piemēram, SoapUI) autentificējas ADFS pakalpojumā, no tā saņem drošības talonu un, izmantojot to, ar sinhronu pieprasījumu nosūta CRS ziņojumu uz web servisa *SendSynCRS* adresi VID. Servisa pusē tiek veikta ziņojuma validācija atbilstoši XML shēmai un nosūtīta atbilde uz FI datu iesniegšanas programmatūru par validācijas rezultātiem sinhronajā atbildē, kā arī uz FI reģistrēto e-pastu tiek nosūtīts paziņojums par CRS ziņojuma saņemšanu un veiksmīgu validēšanu, vai arī par ziņojumā esošajām kļūdām un lūgumu tās novērst un ziņojumu iesniegt atkārtoti.



Att. 1 CRS ziņojuma sūtīšana

3. Piekļuves tiesību pieprasīšana

Pirmreizējā datu sūtīšana vienmēr tiek veikta testa vidē. Pēc veiksmīgas datu iesniegšanas testa vidē veic datu iesniegšanu produkcijas jeb darba vidē. Katrai videi nepieciešami atsevišķi piekļuves sertifikāti. Zemāk ir aprakstītas veicamās darbības autentifikācijas sertifikāta iegūšanai:

1. Jāsagatavo elektroniski parakstīts iesniegums par piekļuves tiesību pieprasījumu, kurš satur zemāk tabulā aprakstīto informāciju:

Tabula 2

Nodokļu maksātāja reģistrācijas numurs	
Nosaukums	
IP adrese/adreses*	
Testa/Produkcijas vide**	
Kontaktpersonas vārds uzvārds	
Kontaktpersonas tālruņa numurs	
Kontaktpersonas e-pasta adrese	
Sistēmas/servisa nosaukums	CRS/DAC2
Pamatojums***	Likums Par nodokļiem un nodevām un Ministru kabineta 2016. Gada 5. janvāra noteikumi Nr. 20 "Kārtība, kādā finanšu iestāde izpilda finanšu kontu pienācīgas pārbaudes procedūras un sniedz VID informāciju par finanšu kontiem"

** Jābūt norādītām precīzām statiskām publiskajām IP adresēm. Tīkla apgabalu adreses netiks pieņemtas. Informāciju par savu IP adresi var precizēt pie interneta pakalpojuma sniedzēja.*
*** Var vienā iesniegumā norādīt abas vides, ja sakrīt pārējā informācija.*
**** Normatīvais akts, uz kura pamata nepieciešams saņemt piekļuves tiesības.*

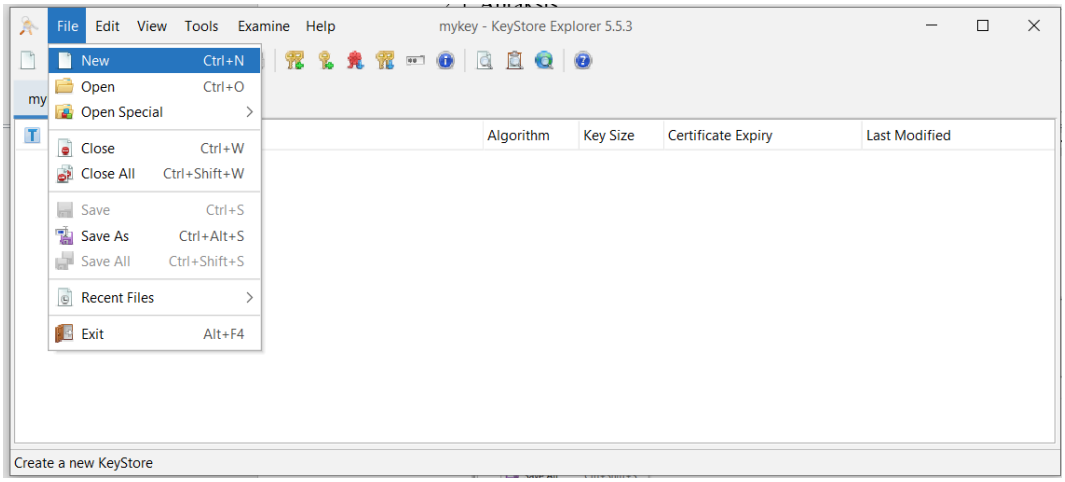
2. Jāizveido privātās atslēgas konteiners (PFX) un sertifikāta parakstīšanas pieprasījums (.csr) – (apraksts punktā 4.1. un 4.2.);
3. 1. un 2. punktā sagatavotās datnes (iesniegums un .csr) jānosūta VID uz e-pasta adresi ip_piekluves@vid.gov.lv, cc norādot e-pasta adresi ip_dac@vid.gov.lv. Vēstules nosaukumā tēmas (*subject)* laukā jānorāda tematu "Par CRS/DAC2 datu iesniegšanu no *Finanšu Iestāde*" *Finanšu Iestāde* vietā norādot FI nosaukumu. Datnes var sūtīt gan atsevišķi, gan vienā e-pastā;
4. Pieprasījums par informācijas atjaunošanu vai izmaiņām kontaktpersonu informācijā, kā arī piekļuves tiesībās CRS/DAC2 ziņošanas prasību izpildei, ir iesniedzams elektroniski parakstītā iesniegumā nosūtot uz VID uz e-pasta adresi ip_piekluves@vid.gov.lv, Cc norādot e-pasta adresi ip_dac@vid.gov.lv līdz pēctaksācijas gada **31. maijam**;
5. Pēc 1. un 2. punktā sagatavoto datņu saņemšanas, VID izveidos piekļuves sertifikātu, un tas tiks nosūtīts uz pieteikumā norādītās FI kontaktpersonas e-pasta adresi, kopā ar papildu instrukciju datu nosūtīšanas vides sagatavošanai un datu nosūtīšanas uzsākšanai;
6. VID aicina gan testēšanu, gan ziņojuma iesniegšanu uzsākt savlaicīgi, vēlams vismaz **3 nedēļas** pirms noteiktā termiņa (31.jūlijs), lai konstatējot problēmas, tās operatīvi var atrisināt gan FI, gan VID.

4. Autentifikācijas sertifikāta izveidošana

Piemērs veidots ar publiski pieejamu bezmaksas rīku *KeyStoreExplorer* (https://sourceforge.net/projects/keystore-explorer/). Var izmantot arī citus rīkus, piemēram, *OpenSSL*.

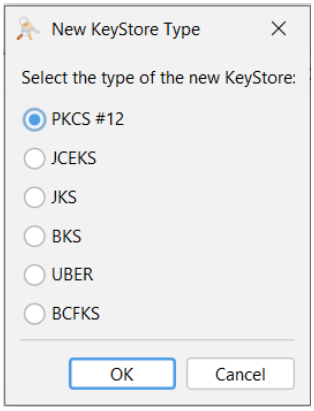
4.1. PFX konteinera izveide

1) Rīkā *KeyStore Explorer* veido jaunu privāto atslēgu:



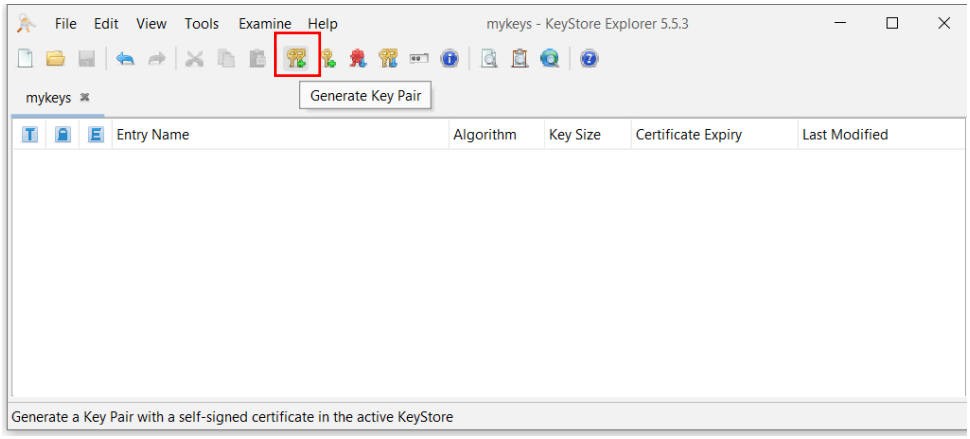
Att. 2

2) Veidojot datni, jānorāda tips – "PKCS#12":



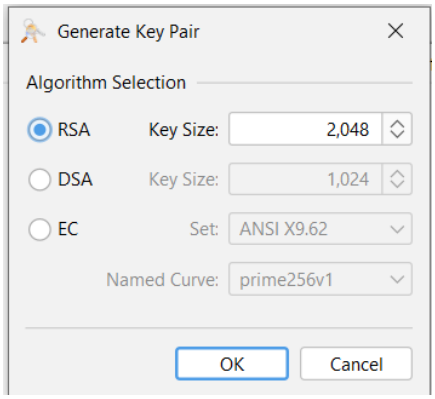
Att. 3

3) Jāveic atslēgu pāra ģenerēšana no izvēlnes ar pogu *Generate Key Pair:*

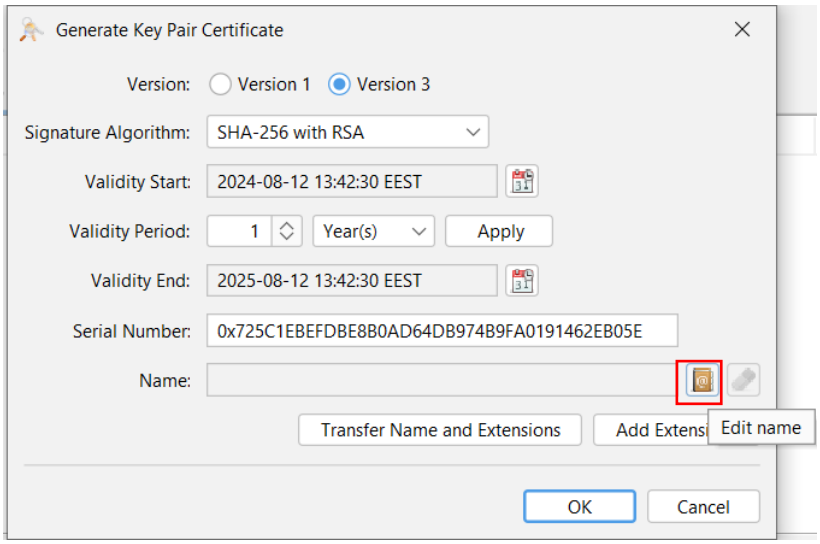


Att. 4

4) Jānorāda algoritms RSA un jānospiež "*Edit name*":

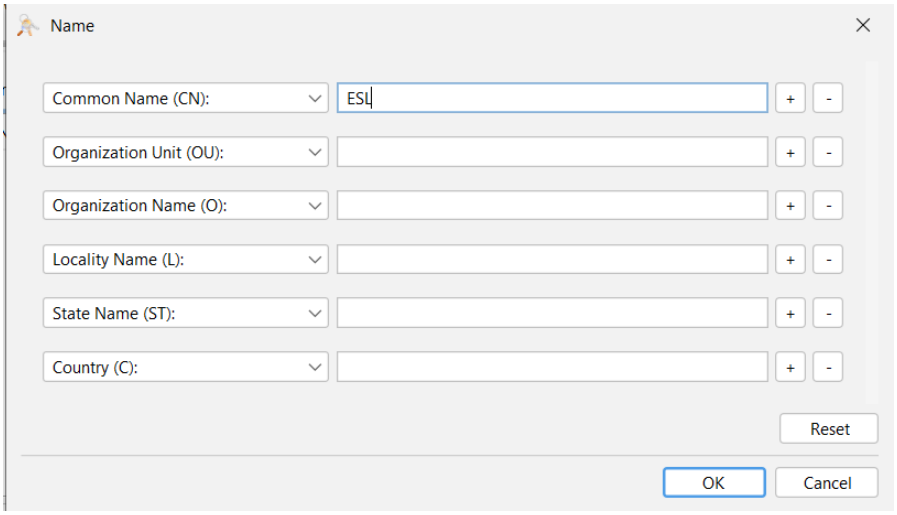


Att. 5



Att. 6

5) Jānorāda informācija par sertifikātu, obligāti norādot "*Common Name (CN)*":

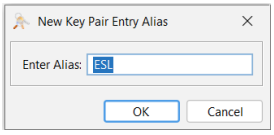


Att. 7

Citi lauki ir norādāmi pēc izvēles un aizpildot tos ir ieteicams ievērot šādus norādījumus (drīkst lietot tikai latīņu burtus un ciparus):

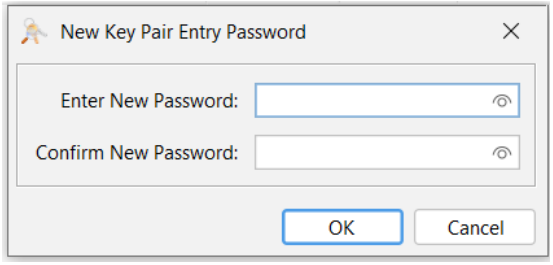
- *Common Name (CN)* – datora raksturojums, kur tiek veidots konkrētais PKCS #12 konteiners. Tas var būt vai nu tikai datora vārds (piemēram, *SERVER1*), vai arī datora FQDN (piemēram, *SERVER1.DOM.ORGANIZACIJA.LV*);
- *Organisation Unit (OU)* – organizācijas apakšvienības (departamenta, nodaļas vai cita veida struktūrvienības nosaukums), piemēram, IT;
- *Organisation Name (O)* – pilns vai saīsināts organizācijas nosaukums, piemēram, FI KKS;
- *Locality Name (L)* – pilsēta, kurā atrodas konkrētais dators, piemēram, *Riga*;
- *State Name (ST)* –Latvijas gadījumā var norādīt pilsētu vai novadu;
- *Country (C)* – valsts kods, kurā atrodas dators. Latvijas gadījumā tas ir LV.
- *Email (E)* – konkrētās personas (lietotāja) e-pasta adrese (drīkst lietot latīņu burtus, ciparus un simbolus, kas ir atļauti e-pasta adresēs).

6) Jānorāda nosaukums, kas tiks izmantots, lai nolasītu sertifikātu (tas var sakrist ar iepriekš norādīto *Common Name* vērtību):

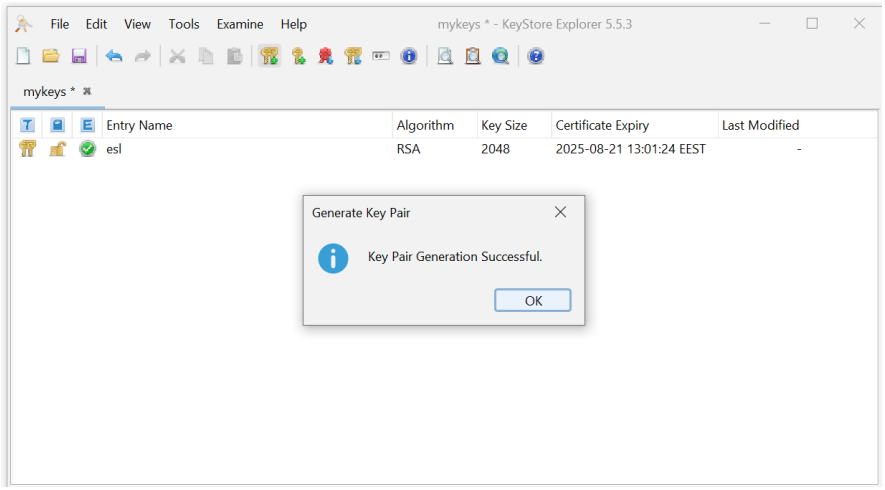


Att. 8

7) Jāievada parole:

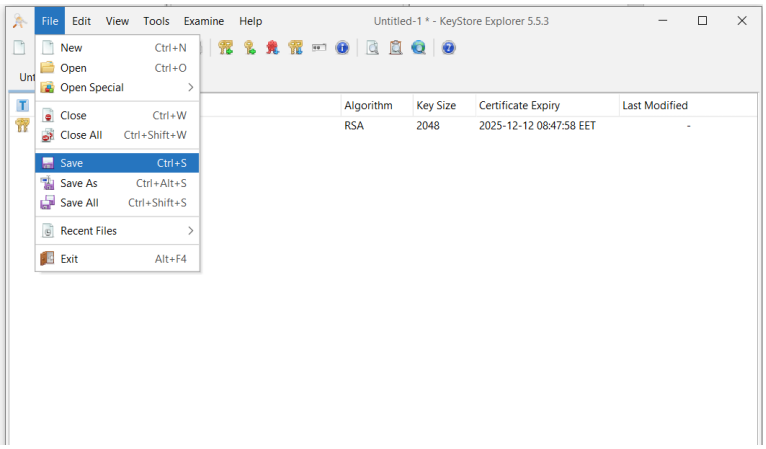


Att. 9



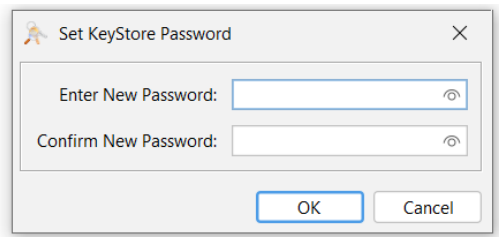
Att. 10

8) Izvēlas *File* un *Save*:



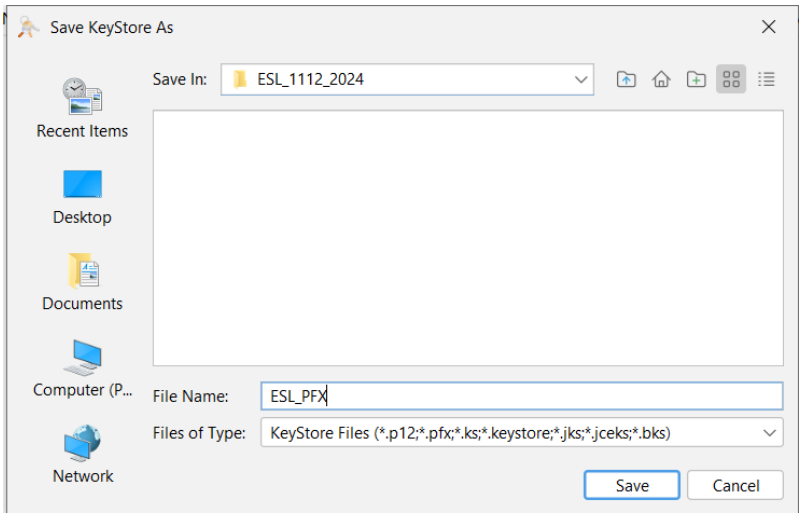
Att. 11

9) Pirms saglabāšanas, tiks piedāvāts ievadīt paroli (var norādīt vēlreiz to pašu, ko izmantoja 7. punktā)



Att. 12

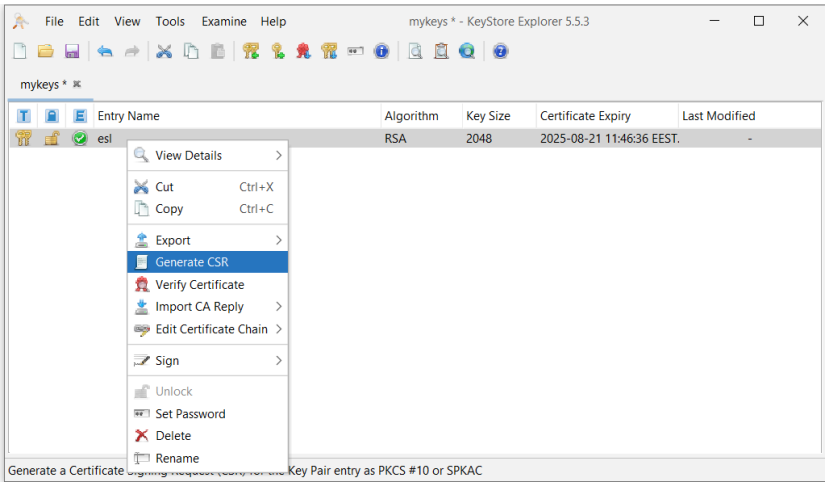
10) Tālāk turpināsies faila saglabāšana. Ieteicams izveidot atsevišķu jaunu mapi testa videi un atsevišķu produkcijas videi, un testa un produkcijai domātās datnes glabāt nodalīti katrai videi atsevišķi. Ievada datnes nosaukumu un nosaukuma beigās ieteicams pierakstīt *_PFX*, kas turpmākajās darbībās ar sertifikātu atvieglotu datnes sameklēšanu un norādīšanu:



Att. 13

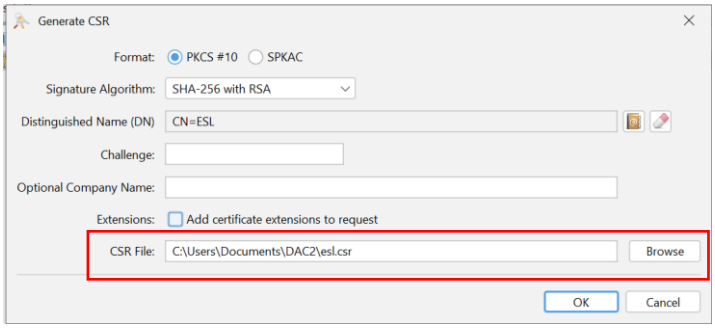
4.2. Sertifikāta parakstīšanas pieprasījuma datnes (.csr) izveide rīkā *KeyStoreExplorer*

1) Sertifikāta parakstīšanas pieprasījuma izveide rīkā *KeyStoreExplorer* jāveic izvēloties ierakstu un no izvēlnes izvēloties – *Generate CSR*.



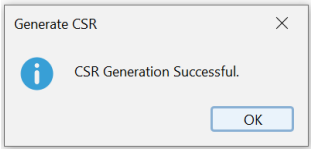
Att. 14

2) Jānorāda formāts "PKCS#10", algoritms "SHA-256 with RSA" un jānorāda datnes saglabāšanas vieta datorā – iepriekš izveidotā mape (testa vai produkcijas videi, turpat, kur tika saglabāts PFX). Datne izveidojas ar paplašinājumu .csr.



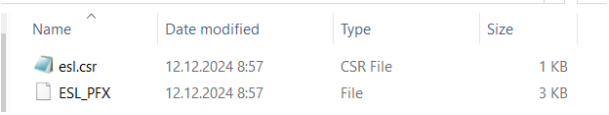
Att. 15

3) Informatīvs paziņojums par veiksmīgu .csr datnes izveidi.



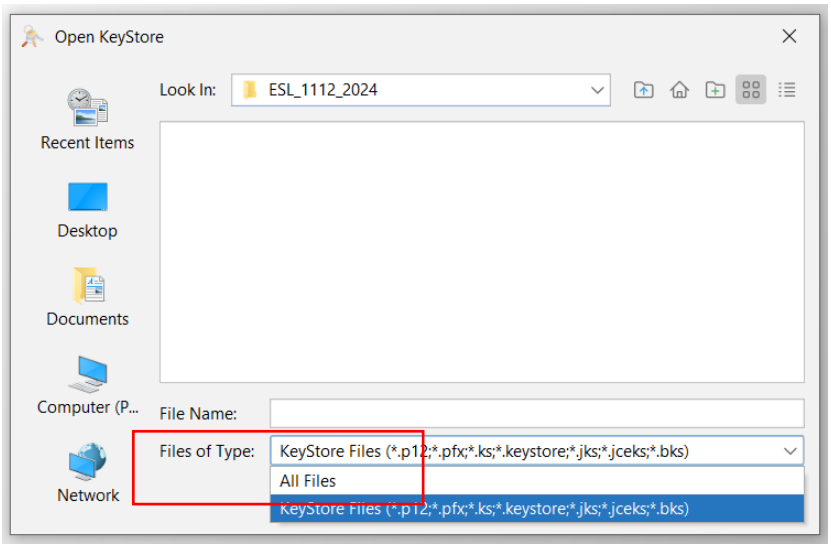
Att. 16

4) Izveidotā .csr datne jānosūta VID uz e-pastu ip_piekluves@vid.gov.lv, cc norādot e-pasta adresi ip_dac@vid.gov.lv. Vēstules nosaukumā tēmas (*subject*) laukā aprakstā lūgums norādīt tekstu tematu "Par CRS/DAC2 datu iesniegšanu no *Finanšu Iestāde*" un *Finanšu Iestāde* vietā norādot FI iestādes nosaukumu. Datnes var sūtīt gan atsevišķi, gan vienā e-pastā tālākai apstrādei. Šajā piemērā izveidotā esl.csr tiek sūtīta VID.



Att. 17

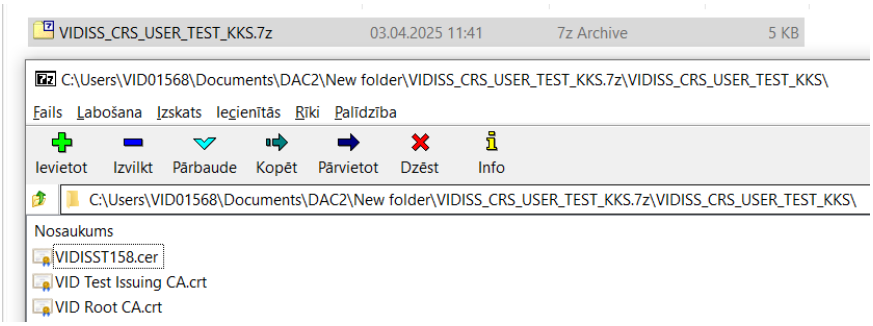
Ja turpmāk rodas problēma ar *KeyStore Explorer* un neredz iepriekš saglabātajā mapē failus, tad jāpāriet *Files of Type* uz *All Files*!



Att. 18

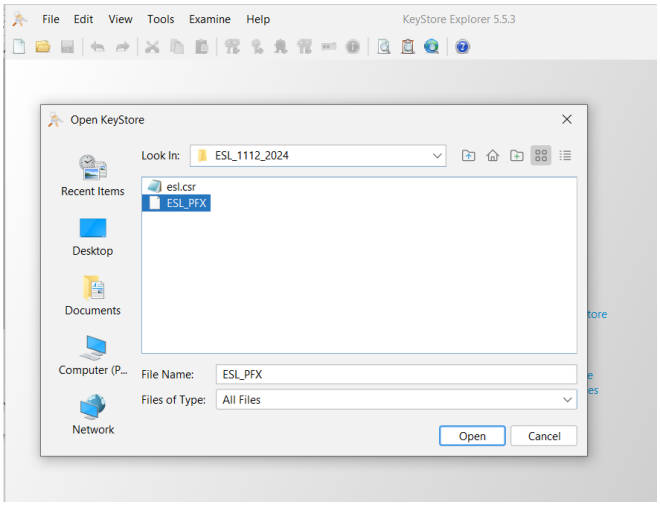
4.3. VID izdoto piekļuves sertifikātu importēšana

No VID tiek saņemtas arhīvā 3 datnes (nosaukumi attēlā var atšķirties no saņemtajiem datņu nosaukumiem). Lejupielādē datorā un saglabā attiecīgajā testa vai produkcijas mapē. Arhīvu nepieciešams atarhivēt (uzklikšķinot uz saņemtās arhīva datnes ar labo peles taustiņu un nospiežot uz 7-zip un pēc tam uz izvilkt "arhīva datnes nosaukums" mapē).



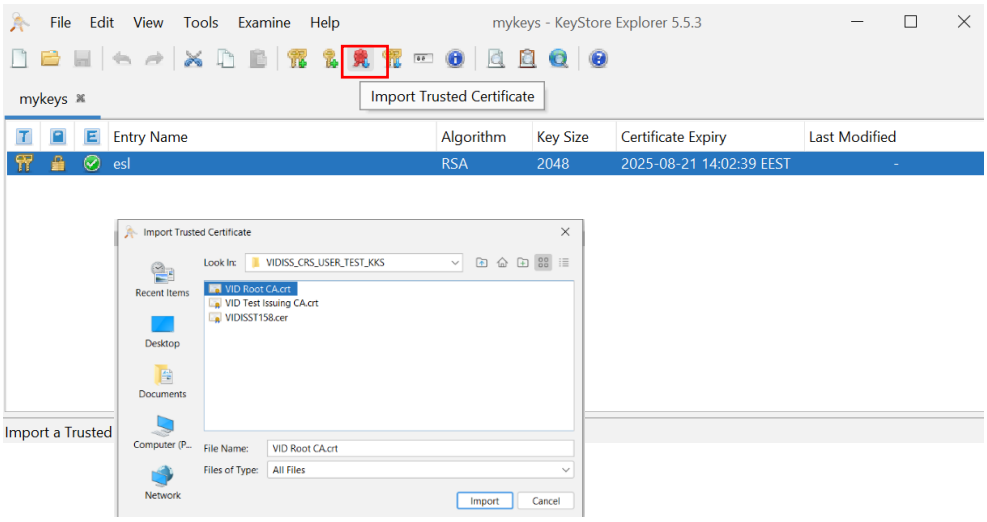
Att. 19

1) Atver *KeyStore Explorer* un atver ar *File->Open* iepriekš izveidoto un saglabāto PFX konteinera datni.



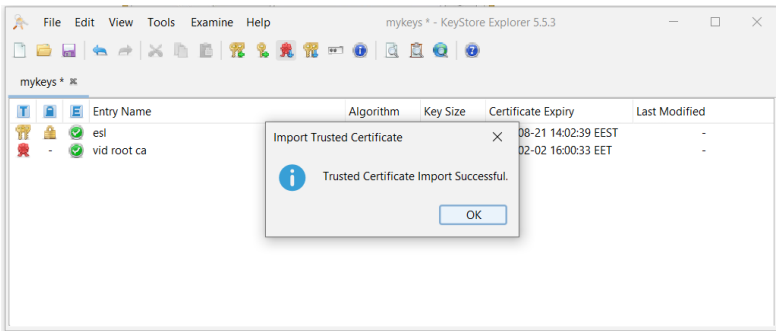
Att. 20

2) Veic *Import Trusted Certificate* ar datni *VID Root CA*.



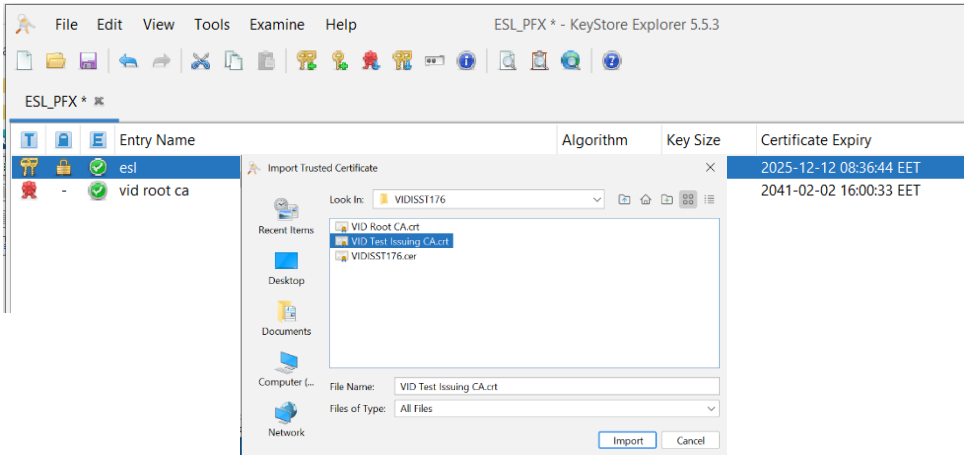
Att. 21

Informācija par darbības veiksmīgu izpildi:



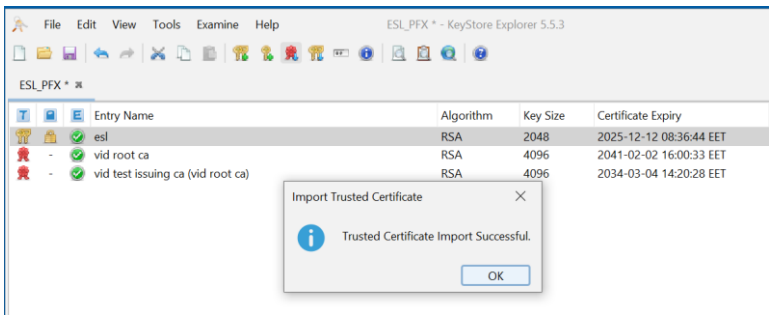
Att. 22

3) Veic *Import Trusted Certificate* ar datni *VID Test Issuing CA* (vai produkcijas videi ar *VID Issuing CA*).



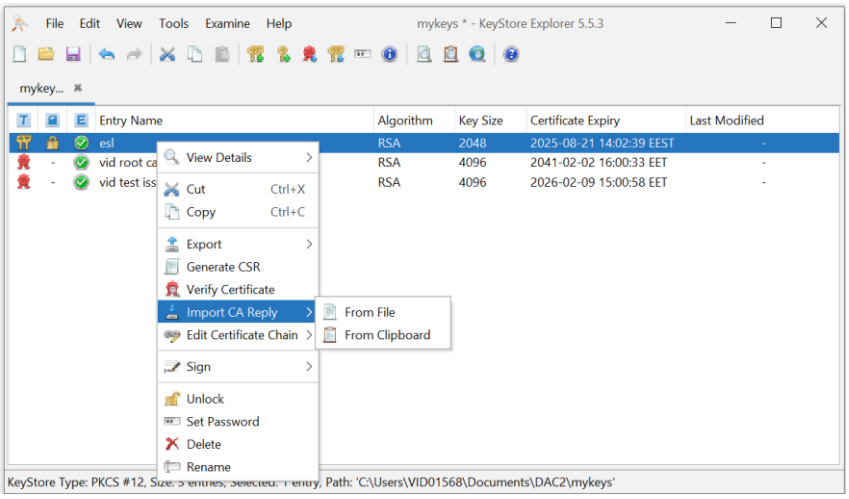
Att. 23

Informācija par darbības veiksmīgu izpildi:

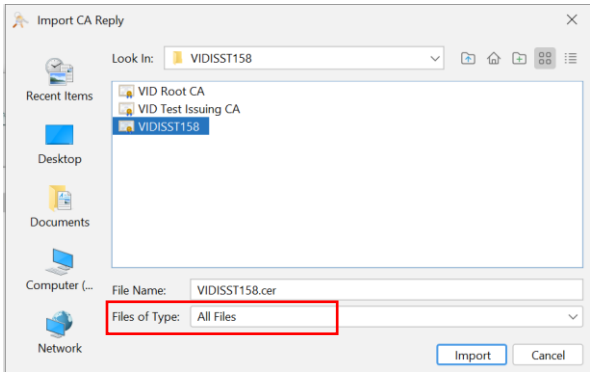


Att. 25

4) Veic ar peles labo pogu *Import CA Replay -> From file, ->Files of Type:All Files->* norāda saņemto apstiprinājuma datni (parasti ar nosaukuma šablonu VIDISSxxxx.cer).

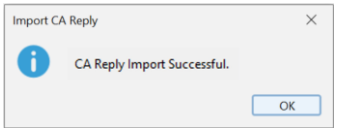


Att. 26



Att. 27

Informācija par darbības veiksmīgu izpildi:



Att. 28

Pēc šim darbībām piekļuves sertifikāts ir veiksmīgi sagatavots un tas būs jāizmanto datu iesniegšanas risinājumā, piemēram, uz .NET, Java bāzētā vai publiski pieejamā bezmaksas rīkā *SoapUI* (https://www.soapui.org/). Detalizēta instrukcija par datu iesniegšanas risinājumu tiks nosūtīta vienā e-pastā ar VID izdoto piekļuves sertifikātu arhīvu.