CRS/DAC2 LIETOTĀJA AUTENTIFIKĀCIJAS PROCESA INSTRUKCIJA DATU IESNIEDZĒJIEM

Saturs

1.Ievads	3
1.1. Dokumenta nolūks	3
1.2. Izmantotie saīsinājumi	3
2.Kopējais apraksts	4
3.Piekļuves tiesību pieprasīšana	5
4.Autentifikācijas sertifikāta izveidošana	6
4.1. PFX konteinera izveide	6
4.2. Sertifikāta parakstīšanas pieprasījuma datnes (.csr) izveide	. 10
4.3. VID izdoto piekļuves sertifikātu importēšana	.12

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

Saīsinājums	Saīsinājuma skaidrojums
ADFS	<i>Microsoft Active Driectory Federation Services</i> – Microsoft aktīvās direktorijas pakalpojums
CRS	<i>Common Reporting Standard</i> – 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	<i>eXtensible Markup Language</i> – paplašinātā iezīmju valoda, lai definētu datu formātus. XML piedāvā plašas iespējas definēt un aprakstīt sarežģītus dokumentus un datu struktūras.
PFX	<i>Personal Information Exchange</i> – privātās atslēgas un publiskā sertifikāta datne/konteiners
PKCS	Public Key Cryptography Standards – publiskās atslēgas šifrēšanas standarti
TSL	<i>Transport Layer Security</i> – transporta līmeņa drošības protokols, kuru izmanto datu šifrēšanai, servera autentificēšanai un neobligātai klienta autentificēšanai

Tabula 1

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 <u>CRSNilSample.xml</u> – nulles ziņojumiem; <u>CRSInitialSample.xml</u> – 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:

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"

Т	ab	ul	a	2
		-		

* 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 <u>ip piekluves@vid.gov.lv</u>, cc norādot e-pasta adresi<u>ip dac@vid.gov.lv</u>. 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 <u>ip piekluves@vid.gov.lv</u>, Cc norādot e-pasta adresi <u>ip dac@vid.gov.lv</u> 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* (<u>https://sourceforge.net/projects/keystore-explorer/</u>). Var izmantot arī citus rīkus, piemēram, *OpenSSL*.

4.1. PFX konteinera izveide

1) Rīkā KeyStore Explorer veido jaunu privāto atslēgu:

							H	11128 212				
<u>م</u>	File	Edit Viev	v Tools	Examine	Help		mykey -	KeyStore Ex	plorer 5.5.3		-	×
		New	Ctrl+	N	8 %	£ 7	 0]	1 🚊 🧕	2			
mv		Open	Ctrl+	0								
		Open Special	I	>							1	
I	•	Close Close All	Ctrl+ Ctrl+Shift+	w			,	Algorithm	Key Size	Certificate Expiry	Last Modified	
		Save Save As Save All	Ctrl+ Ctrl+Alt+ Ctrl+Shift+	+S +S +S								
	ē	Recent Files		>								
		Exit	Alt+	F4								
Create	e a n	ew KeyStore										

Att. 2

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

Select the type of the new KeyStore:
PKCS #12
◯ JCEKS
⊖ jks
⊖ BKS
OUBER
OBCFKS
OK Cancel

Att. 3

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



Att. 4

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

🍌 Generat	te Key Pair		×
Algorithm S	Selection		
RSA	Key Size:	2,048	\diamond
	Key Size:	1,024	\diamond
OEC	Set:	ANSI X9.62	\sim
Ν	amed Curve:	prime256v1	\sim
	0	OK Cance	ł



🍌 Generate Key Pair	Certificate X
Version:	○ Version 1
Signature Algorithm:	SHA-256 with RSA V
Validity Start:	2024-08-12 13:42:30 EEST
Validity Period:	1 > Year(s) > Apply
Validity End:	2025-08-12 13:42:30 EEST
Serial Number:	0x725C1EBEFDBE8B0AD64DB974B9FA0191462EB05E
Name:	
	Transfer Name and Extensions Add Extense Edit nam
	OK Cancel
-	

Att. 6

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

🍌 Name					×
Common	Name (CN):	~	ESL	+ -	
Organizat	tion Unit (OU):	~		+ -	
Organizat	tion Name (O):	~		+ -	
Locality N	lame (L):	~		+ -	
State Nar	ne (ST):	~		+ -	
Country (C):	~		+ -	
				Reset	
			ОК	Cancel	

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):

The New Key	Pair Entry Alias	~
Enter Allas:	<u>E51</u>	
	ОК	Cancel

7) Jāievada parole:



Att. 9

渀 File Edit View Tools Examine Help	mykeys * - K	KeyStore Explorer 5.5.3	- 🗆 X
🗅 🖴 📾 i 📥 🥔 🗶 🖿 🖆 🎇 🐁 🞗	📆 📼 📵 🖻 🙆		
mykeys * 🕱			
1 🖻 🖻 Entry Name	Algorithm Key	Size Certificate Expiry	Last Modified
🃅 🚅 🥝 esl	RSA 2048	3 2025-08-21 13:01:24 E	EST -
Gen	erate Key Pair Key Pair Generation Succ	× essful. ОК	



8) Izvēlas *File* un *Save*:

a Upen Special > a Upen Special > Algorithm Key Size Certificate Expiny Last Modified Close All Ctrl+Shift+W RSA 2048 2025-12-12 08:47:58 EET - Save As Ctrl+All+S Save AsII Ctrl+Shift+S - - - - Save AsII Ctrl+Shift+S - - - - - - Recent Files > - - - - - - -	a Uppen Special > a Uppen Special > a Uppen Special > a Uppen Special > b Close Ctrl+W a Save All Ctrl+Shift+W a Save As Ctrl+Alt+S a Save All Ctrl+Shift+S b Recent Files > b Exit Alt+F4	1 nt	New Open	Ctrl+N Ctrl+O) 178 1	L A 11	== 🕕 💆 🛄	0		
Save Ctrl+S Save As Ctrl+Alt+S Save Ava All Ctrl+Shift+S Recent Files >	Save Ctrl+Sh Save As Ctrl+Aht+S Save All Ctrl+Shift+S Recent Files > Exit Alt+F4		Close Close All	Ctrl+W Ctrl+Shift+W			Algorithm RSA	Key Size 2048	Certificate Expiry 2025-12-12 08:47:58 EET	Last Modified
Recent Files			Save Save As Save All	Ctrl+S Ctrl+Alt+S Ctrl+Shift+S						
E Exit Alt+F4		0	Recent Files Exit	> Alt+F4						

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

 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.

	O	
Format:	PKCS #10 SPKAC	
Signature Algorithm:	SHA-256 with RSA	
Distinguished Name (DN)	CN=ESL	
Challenge:		
Optional Company Name:		
Extensions:	Add certificate extensions to request	
CSR File:	C:\Users\Documents\DAC2\esl.csr	Brows

Att. 15

3) Informatīvs paziņojums par veiksmīgu .csr datnes izveidi.

Generate CSR					
0	CSR Generation Successful.				
	OK				
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.

Name	Date modified	Туре	Size
asl.csr	12.12.2024 8:57	CSR File	1 KB
ESL_PFX	12.12.2024 8:57	File	3 KB

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.

🍌 File Edit View	Edit View Tools Examine Help mykeys - KeyStore Explorer 5.5.3				- 🗆	\times			
🗋 🚔 📓 [🕤 🥔 [🗙 🗅 🗈 📅 🐒 🕱 🗖 📼	• • • •	100						
mykeys 🕷 Import Trusted Certificate									
🔟 🚊 匡 Entry Nam	2	Algorithm	Key Size	Certificate Expiry	Last Modified				
📅 🔒 🧭 esl		RSA	2048	2025-08-21 14:02:39 EEST					
Import a Trusted	usted Cettificate Look In: VIDISS_CR5_USER_TEST_KKS VIDISS_CR5_USER_TEST_KKS VIDISSTISB.cer File Name: VIDISSTISB.cer Files of Type: All Files	v E 🌣 E	X) 000 111 Cancel						



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).

🚴 File Edit View Tools Examine Help	mykey	/s * - KeyStor	e Explorer 5.5.3	_		×	
🗋 🖴 📾 🤝 🥔 🖾 🛍 📅 🐍 🕱 🐨	0 🖻 🕻	1 Q 0					
mykey 🕷							
T 🔳 🗉 Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified	ł		
Image: Constraint of the second se	RSA RSA RSA File Clipboard	2048 4096 4096	2025-08-21 14:02:39 EEST 2041-02-02 16:00:33 EET 2026-02-09 15:00:58 EET		-		
KeyStore Type: PKCS #12, Size: 5 entries, selected. 1 entry, Path: 'C:\Users\VID01568\Documents\DAC2\mykeys'							

Att. 26

🍌 Import CA R	eply						\times
(<u>e</u>	Look In: 📜	VIDISST158	~	r 6	÷	00	:=
Recent Items	VID Root	CA Issuing CA					
Desktop		00					
Documents							
Computer (File Name:	VIDISST158.cer					
I	Files of Type:	All Files					~
Network				Import		Cance	əl

Att. 27

Informācija par darbības veiksmīgu izpildi:



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.