# Зміст

1
2
4
5
10
14
16

## Інструкція по підключенню SSL-сертифіката

В мережевому варіанті FREDO для шифрування каналу зв'язку між серверною частиною і станцією передбачено можливість підключити SSL-сертифікат.

Досвідчені користувачі, які усвідомлюють ризики самопідписаних сертифікатів, можуть використати самопідписаний SSL-сертифікат.

Користувачам, що ще не мають досвіду в області ІТ безпеки, для отримання SSL-сертифіката рекомендується звернутися до кваліфікованого надавача електронних довірчих послуг (КНЕДП).

У інструкції описані наступні варіанти отримання SSL-сертифіката з подальшим його підключенням:

- 1. Створення самопідписаного сертифіката з параметрами вашого сервера за допомогою утиліти ConnectionSetup в складі FREDO.
- 2. Створення самопідписаного сертифіката за допомогою безкоштовної утиліти OpenSSL з відкритим кодом.
- 3. Створення сертифіката і ключа у КНЕДП за допомогою запиту на сертифікат.

Для створення та підключення SSL-сертифіката необхідно виконати кроки:

- 1. <u>Створити самопідписаний SSL-сертифікат</u> або замовити SSL-сертифікат у КНЕДП (для замовлення сертифіката необхідно <u>створити запит на сертифікат</u>).
- 2. <u>Імпортувати сертифікат у сховище</u>. У разі потреби, (якщо видавець передав сертифікат в форматі \*.cer, \*.crt) перед імпортом у сховище необхідно <u>експортувати сертифікат в форматі \*.pfx</u>.
- 3. <u>Підключити сертифікат</u> за допомогою утиліти ConnectionSetup.exe.

### Важливо

- Самопідписані сертифікати не є визнаними довіреними сертифікатами і не можуть бути відкликані КНЕДП. Якщо ви не впевнені в своїх діях, рекомендовано отримати сертифікат від КНЕДП.
- Для підключення SSL-сертифікат повинен бути наданий у вигляді контейнера \*.pfx, який містить секретний ключ та сертифікат.
- Сертифікат створюється для сервера.
- Сертифікат необхідно додати в сховище довірених кореневих сертифікатів сервера і всіх станцій.
- Назва сервера і домена в сертифікаті мають співпадати.
- Звернення до сервера зі станції відбувається по імені сервера, <u>не допускається</u> використання тільки ІР-адреси сервера.
- В сертифікаті мають бути вказані:
  - о в якості (альтернативних) доменних імен DNS: повне ім'я пристрою сервера, localhost, 127.0.0.1, IP адреса сервера;
  - о призначення сертифіката: для шифрування даних, авторизації сервера і клієнта.

## Створення самопідписаного сертифіката за допомогою утиліти

## ConnectionSetup

В утиліті **ConnectionSetup** реалізовано функцію створення самопідписаного сертифіката з параметрами, необхідними для коректної роботи.

- 1. Відкрийте утиліту **ConnectionSetup**.
- 2. Натисніть кнопку Створити сертифікат.

🍪 Налаштування з'єдна	іння	_	
			Довідка
Основні Налаштування Fi	rebird		
Сервер			
Служба сервера:	FREDOService16		
Адреса:			
Порт:	10016 🜩		
🗌 Змінити налаштуван	ня Клієнта		
📃 Виконувати запуск т	ермінального клієнта без копін	овання файлів п	рограми
🗹 Використовувати SS	iL		
Сертифікат:			
Пароль:		Створити с	ертифікат
палаштування рівня прото За допомогою повзунка в програми	жолювання системних поди/ экажіть рівень деталізації для	запису до log-q	райлів
-			
📄 - Помил	ки та попередження		
-			
Робоча станція			
Адреса:	10.380.67.62		
Порт:	10016 🜩		
		Зберегти	Відмінити

3. Перевірте і, у разі потреби, відкоригуйте поле **Ім'я сервера**. Поле повинно містити ім'я ПК, на якому встановлено сервер.

Якщо сертифікат створюється на сервері, ім'я сервера співпадає з іменем ПК та заповнюється у полі за замовчуванням.

Якщо сертифікат створюється для сервера, що розташований на іншому ПК, у полі **Ім'я сервера** введіть ім'я ПК, на якому встановлено сервер.

4. Введіть секретний пароль довжиною до 32 символів.

Параметри			_		$\times$
Ім'я сервера:	testFredoPC				
Пароль:	*****				
		Зген	ерувати 😡	Відм	іінити

- 5. Натисніть кнопку Згенерувати.
- 6. Для збереження файлів сертифіката вкажіть папку розташування.

Огляд папок	×
🔜 Робочий стіл	^
> 🜰 OneDrive - Personal	
> 2 Anatolii Lukianev	
> 💻 Цей ПК	
Бібліотеки	
> 🧮 Відео	
🗸 🚊 Документи	
> 🗮 Документи	
> 三 Збережені зображення	
> 📃 Зображення	
> 🔔 Музика	
🔉 📃 Фотографії з камери	
> 🥏 Мережа	
> 🖭 Панель керування	
🔯 Кошик	~
Створити папку ОК	Скасувати

7. У вказану папку буде збережено сертифікат у форматах \*.crt, \*.pfx.

	Повідомлення ×					
☐   ☑ _ =   Docurr File Home Sha ← → ✓ ▲ □ ×	nents are View This PC > [	Document	5 >	<u>ок</u>	- C ×	•
<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> <li>This PC</li> </ul>		* * *	Name testFredoPC.pfx FredoPC.crt	Date modified 25.05.2022 15:56 25.05.2022 15:56	Type Personal Informati Security Certificate	s

 Якщо в утиліті ConnectionSetup перед створенням сертифіката не були заповнені поля Сертифікат і Пароль, в них копіюється вказаний шлях збереження сертифіката (п. 6), а також пароль, зазначений в генераторі сертифіката (п. 4). За потреби, значення у цих полях можна змінити.

and the second se
Contraction of the second
Створити сертифікат

**Важливо.** Для коректної роботи FREDO з створеним SSL-сертифікатом його необхідно імпортувати в сховище 'Довірені кореневі центри сертифікації\Certificates\' серверу і всіх станцій (див. <u>Імпорт сертифіката в</u> <u>сховище</u>).

#### Приклад створення самопідписаного сертифіката OpenSSL

Для генерації самопідписаного сертифіката можна скористатися ПЗ з відкритим кодом OpenSSL (https://wiki.openssl.org/index.php/Binaries).

Після встановлення OpenSSL, в командному рядку виконайте команду:

"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -x509 -v3 -newkey rsa:2048 -sha256 keyout MedocCert.key -out MedocCert.crt -days 600 -config req.conf

з параметрами:

-keyout MedocCert.key – шлях збереження і ім'я ключа сертифіката;

-out MedocCert.crt – шлях збереження і ім'я сертифіката;

-days 600 – тривалість дії сертифіката;

-config req.conf - шлях збереження і ім'я файлу конфігурації;

Файл конфігурації (req.conf) містить такі рядки:

```
[reg]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
x509 extensions = v3 ca
[req distinguished name]
C = UA
ST = Kyiv
L = Kyiv City
0 = MedocOrganization
CN = MyWorkPC
[v3 req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = XXX.XXX.XXX.XXX
DNS.2 = MyPC
DNS.3 = localhost
DNS.4 = 127.0.0.1
DNS.5 = MyWorkPC.FullName
[v3_ca]
basicConstraints = CA:FALSE
nsCertType = client, server
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
nsComment = "OpenSSL Generated Test Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid, issuer
subjectAltName = @alt_names
```

Важливо. Необхідно вказати:

 у якості альтернативних імен (subjectAltName) DNS повне ім'я пристрою сервера, IP адресу сервера, localhost, 127.0.0.1;

- основне призначення сертифіката для шифрування даних (keyUsage);
- розширене призначення сертифіката для авторизації сервера і клієнта (nsCertType, extendedKeyUsage).

Для експорту сертифіката в форматі pfx виконайте команду:

"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -export -name "MedocCert" -out "MedocCert.pfx" -inkey MedocCert.key -in MedocCert.crt

з такими параметрами:

-name "MedocCert" — зрозуміле ім'я;

-out "MedocCert.pfx" – шлях збереження і ім'я сертифіката в форматі pfx;

-inkey MedocCert.key – шлях до ключа згенерованого сертифіката;

-in MedocCert.crt – шлях до згенерованого сертифіката.

# Створення запиту на сертифікат за допомогою Microsoft Management Console (MMC)

Запит на сертифікат потрібен для генерації сертифіката у КНЕДП.

1. Запустіть mmc.exe в командному рядку Windows:

💷 Викона	ти	$\times$
B II	ведіть ім'я програми, папки, документа або ресурсу ітернету, і Windows відкриє їх.	
<u>В</u> ідкрити:	mmc.exe	$\sim$
	ОК Скасувати О <u>г</u> ляд	

2. В меню Файл оберіть Додати/видалити оснастку:

	Консо	ль1 - [	Коренева	папка консолі	]		
-	Файл	Дія	Вигляд	Уподобання	Вікно	Довідка	
	C	творит	и			Ctrl+N	
	Bi	дкриті	и			Ctrl+0	
	30	берегт	и			Ctrl+S	
	30	берегт	и як				У цьол
	Д	одати/	видалити	оснастку	N	Ctrl+M	
	П	араме	три		6		
	1	C:\WI	DOWS\'	\compmgmt.m	isc		
	В	ийти					

3. Додайте оснастку Сертифікати:

Снастка	Постачальник	^	]	📔 Коренева папка консолі	Змінити розширення
	Microsoft Corp			Certificates - Current User	
Certificates	Microsoft Corp				Видалити
Component Services	Microsoft Corp				
Event Viewer	Microsoft Corp				Brony
IP Security Monitor	Microsoft Corp				ыору
IP Security Policy Ma	Microsoft Corp				Вниз
Local Users and Gro	Microsoft Corp		Додати >		
Performance Monitor	Microsoft Corp				
🖶 Print Management	Microsoft Corp				
Security Configuratio	Microsoft Corp				
Security Templates	Microsoft Corp				
Services	Microsoft Corp				
Shared Folders	Microsoft Corp				
Task Scheduler	Microsoft Corp	~			Додатково
TDM Management	Microsoft Corn				1,11,11,11,11,11,11,11,11,11,11,11,11,1
ис:					

Якщо при інсталяції вимагається вказати користувача – оберіть поточного користувача.

4. Оберіть рядок **Сертифікати – Поточний користувач**, і в контекстному меню виберіть **Усі завдання – Розширені операції – Створити користувацький запит**.

🧧 Консоль1 - [Коренева папка консолл Сайл Дія Вигляд Уподобання Сайл Дія 🗈 🗈 🔹 🖬	\Certificates - Curre Вікно Довідка	ent User]				
📔 Коренева папка консолі	Logical Store Nan	ne				Дії
<ul> <li>Q Certificates - Current User</li> <li>Ocoбисті</li> </ul>	Особист Довірені	Find Certificates				Certificates - Curren
<ul> <li>Довірені кореневі центри серт</li> <li>Довірені підприємства</li> </ul>	📔 Довірені	Усі завдання	Find Certificates			додаткові дл
<ul> <li>Э доврені підприємства</li> <li>Э Проміжні центри сертифікації</li> </ul>	Проміжн три сертифікації увача Active Direc вці отифікати Проміжн Об'єкт ко Довірені Недовірє	Відкрити нове вікно звідси	о звідси Request New Certificate			Особисті
<ul> <li>&gt; Об'єкт користувача Active Direction     <li>Довірені видавці     </li> </li></ul>		Оновити	Import			Додаткові дії
Недовірені сертифікати		Довідка	Advanced Operations	>	Create Custom Request	-
<ul> <li>Сторонні кореневі центри сер-</li> <li>Поріодні кореневі центри сер-</li> </ul>	Довірені кори	стувачі			Enroll On Behalf Of	~
<ul> <li>Довірені користувачі</li> <li>Постачальники послуг автенти</li> </ul>	Постачальник	ки послуг автентифікації клієнтів			Manage Enrollment Po	licies
<ul> <li>інші користувачі</li> </ul>	📔 Інші користув	ачі				
Local NonRemovable Certificate	Local NonRem	ovable Certificates				
<ul> <li>Запити заяв на реєстрацію сер</li> <li>Довірені кореневі папки смарт</li> </ul>	Запити заяв н Довірені коре	а реєстрацію сертифікатів еневі папки смарт-карток				

5. В майстрі запиту на сертифікат натисніть Властивості для заповнення властивостей сертифіката

			-		$\times$
🔄 Certificate I	Enrollment				
Certific	ate Information				
Click Ne request,	d to use the options alread and then click Next.	ly selected for this template, or click Details to o	ustomize th	ne certificate	•
🖂 Cu	stom request	(i) STATUS: Available		Details	^
The	<ul> <li>following options describe</li> <li>Key usage:</li> <li>Application policies:</li> </ul>	e the uses and validity period that apply to this	; type of cer	rtificate:	
	Validity period (days):				
				Properties	
					_
			Далі	Скасува	ати

6. У вкладці General (Загальні) заповніть назву і опис сертифіката:

Certificate Properties	×
General Subject Extensions Private Key	
A friendly name and description will make it easier to identify and use a certificate.	
Friendly name:	
FREDO_test	
Description:	
тестовий сертифікат для станції FREDO	
	_
ОК Скасувати Застосу	вати

7. В вкладці **Subject** заповніть:

ertificat	e Propert	ies				×
General	Subject	Extensions	Private Key			
The sub can ente can be u	ject of a c er informa used in a c	certificate is t ation about certificate.	the user or co the types of s	mputer to whi subject name a	ich the certificate is iss ind alternative name v	ued. You values that
Subject	of certific	ate				
The use	r or comp	outer that is i	eceiving the	certificate		
Subject	name:					
Type:					CN= FredoTest	
Localit				Add >	C=Ukraine	
Locality	у				O=MedocOrg	
Value:			<	Remove	L=Kviv Citv	
					2	
Alternat	ive name	2:				
Туре:					DNS	
DNS					MyPC MyPC local	
Value					localhost	
l				Add >	127.0.0.1	
L				nuu >	123.123.12.654	
			<	Remove		
				OK	Cupana	20070000000
				OK	Скасувати	застосувати

- Країна Country C = Ukraine;
- Основне ім'я ПК Common names CN;
- Додайте у розділі альтернативних імен параметри DNS-імен (тип DNS), в яких також вкажіть ім'я комп'ютера (Common names, так само, як вказали параметри CN вище), IP-адресу сервера, localhost, "127.0.0.1".

За потреби вкажіть інші параметри.

Ім'я ПК можна перевірити у розділі Налаштування Windows – Система – Про програму – Ім'я пристрою:

Настройки		
🟠 Домашня сторінка	Про програму	/
Знайти настройку	Ваш ПК відстежуєт	ься та
Система	Переглянути відомості на Windows"	екрані "Безпека у
💭 Сповіщення й дії		
Д Планувальник сповіщень	Специфікації прис	трою
( <sup>1</sup> ) Живлення та режим сну	ім я пристрою Повне ім'я пристрою	EPW06 MEDOC local
🗆 Сховише	Процесор	Intel®) Core(TM) 6-7400 CPU @ 3.00GHz 3.00 GHz
	ОЗП	Н.О.Г.Б. (достугно) для використания. 15,9 ГК)
-0 планшет	Ідентифікатор пристрою	3340F908-0018-458F-9009-595255043C3
🛱 Багатозадачність	Код продукту	00125-10438-49748-44317
Проєктування на цей ПК	Тип системи	64-розрядна операційна система, процесор на базі архітектури зб4
🛠 Спільні можливості	Перо та дотики	Пдериниа пера за сдиодотикового велау
🛍 Буфер обміну	Копіювати	
> Віддалений робочий стіл	Перейменувати ПК	
D Про програму	Специфікації Wind	ows

8. У вкладці **Extensions** (**Розширення**) переконайтеся, що в розділі використання ключа вказано шифрування ключів, шифрування даних, цифровий підпис:

Certificate Properties		×
General Subject Extensions Private Key		
The following are the certificate extensions for this certificate type.		^
Key usage	^	
The key usage extension describes the purpose of a certificate.          Available options:       Selected options:         CRL signing       Data encipherment         Decipher only       Add >         Key agreement       Add >         Key certificate signing          ✓ Make these key usages critical		
Extended Key Usage (application policies)	*	
Basic constraints	•	
Include Symmetric algorithm	•	~
ОК Скасувати Заи	стосув	вати

9. В розділі розширених налаштувань переконайтеся, що вказано автентифікацію сервера і клієнта:

Certificate Properties	×
General Subject Extensions Private Key	
	`
☑ Make these key usages critical	
Extended Key Usage (application policies)	
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.	l
Available options: Selected options:	
Підписування л	
Захищена електронна п	
Установлення позначки Підписування списку до Add >	
Установлення позначки	
Кінцева система IP-безп < Remove	
Припинення тунелюван	
Файлова система із шиф	
□ Make the Extended Key Usage critical	
Basic constraints *	,
ОК Скасувати Застосуват	ти

10. У вкладці Private Key (Приватний ключ) переконайтесь, що обрано RSA ключ:

ertificate Properties	>
General Subject Extensions Private Key	
Cryptographic Service Provider	^
A CSP is a program that generates a public and private key pair used in many certificate-related processes.	
Select cryptographic service provider (CSP):	
☑ RSA Microsoft Software Key Storage Provider	^
DH,Microsoft Software Key Storage Provider	
DSA,Microsoft Software Key Storage Provider	
ECDH, Microsoft Software Key Storage Provider	
ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider	
ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider	~
Show all CSPs	
Key options	
Select Hash Algorithm	•
Colort Cignature Format	
Servici signature rotmat	
ОК Скасувати За	стосуват

- 11. В розділі параметрів ключа встановіть довжину ключа (рекомендовано 2048). За потреби, встановіть прапорець **Make private key exportable** додати можливість експортувати ключ.
- 12. В розділі Хеш-алгоритму оберіть алгоритм (рекомендовано sha256):

Certificate Properties	×
General Subject Extensions Private Key	
Cryptographic Service Provider	*
Kauastias	
key options	<u> </u>
Set the key length and export options for the private key. Key size: 2048	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
Select Hash Algorithm	^
Select Hash Algorithm to be used for this request	
Hash Algorithm: sha256	
Select Signature Format	*
ОК Скасувати Засто	сувати

- 13. Застосуйте обрані властивості і натисніть ОК.
- 14. У наступному вікні натисніть Далі.
- 15. Вкажіть ім'я і розташування файлу ключа, переконайтеся, що обрано Base64:

	-		×
🔄 Certificate Enrollment			
Where do you want to save the offline request?			
If you want to save a copy of your certificate request or want to process the request late your hard disk or removable media. Enter the location and name of your certificate requ Finish.	er, save t uest, and	he request I then click	to
File Name: C:Desktop \testFredo Sert Request		Browse	
File format:			
Готов	80	Скасува	ти

#### 16. Натисніть Готово.

Отриманий файл необхідно відправити вашому КНЕДП для створення сертифіката.

Подбайте, щоб довірений видавець передав вам сертифікат у форматі pfx.

# Імпорт сертифіката в сховище

Для коректної роботи сертифікат необхідно імпортувати в сховище сертифікатів <u>як на сервері, так і на всіх</u> <u>станціях</u>.

1. Імпортуйте отриманий сертифікат в утиліті ММС. Запустіть mmc.exe в командному рядку Windows:

💷 Виконати	$\times$
Введіть ім'я програми, папки, документа або ресурсу Інтернету, і Windows відкриє їх.	
<u>В</u> ідкрити: mmc.exe	~
ОК Скасувати О <u>г</u> ляд	

2. В меню Файл виберіть Додати/видалити оснастку:

	Фай,	л Дія	Вигляд	Уподобання	Вікно	Довід
¢		Створит	ги		Ctrl	+N
<b>~</b>		Відкрит	и		Ctrl	+0
		Зберегт	и		Ctrl	+S
		Зберегт	и як			
		Додати	/видалити	оснастку	Ctrl+	M N
		Параме	три			h
		1 C:\Win	idows\\ce	ertmgr.msc		
		2 C:\Win	dows\\de	evmgmt.msc		
		3 C:\Win	idows\\co	mpmgmt.msc		
		4 C:\Win	idows\\se	ervices.msc		
		Вийти				

3. Додайте оснастку Сертифікати:

CURCTUR	Постацальник	^		📔 Коренева папка консолі	Змінити розширення.
	Постачальник			Certificates - Current User	энний роздирения.
Authorization Manager	Microsoft Corp				Видалити
Certificates	Microsoft Corp				
Event Viewer	Microsoft Corp				
IP Security Monitor	Microsoft Corp				Вгору
IP Security Policy Ma	Microsoft Corp				Ruup
Local Users and Gro	Microsoft Corp		Додати >		DHNS
Performance Monitor	Microsoft Corp		Hohenn	J	
Print Management	Microsoft Corp				
Security Configuratio	Microsoft Corp				
Security Templates	Microsoft Corp				
Services	Microsoft Corp				
Shared Folders	Microsoft Corp				
Task Scheduler	Microsoft Corp				Додатково
TDM Management	Microsoft Corp	•			

Якщо при інсталяції вимагається вказати користувача – оберіть поточного користувача.

4. Для коректної роботи SSL-шифрування в М.Е.Doc сертифікат необхідно додати в сховище довірених кореневих сертифікатів.

Консоль1 - [Коренева папка консолі\Certificates - Current User\Довід         Файл       Дія       Вигляд       Уподобання       Вікно       Довідка         Файл       Дія       Вікно       Довідка       Вікно       Довідка         Файл       Дія       Вікно       Довідка       Вікно       Довідка         Файл       Дія       Вікно       Довідка       Вікно       Довідка         Файл       Дія       Вигляд       Уподобання       Вікно       Довідка         Файл       Дія       Вигляд       Уподобання       Вікно       Довідка         Файл       Дія       Вигляд       Уподобання       Вікно       Довідка         Файл       Віко       Вікно       Довідка       Вікно       Вікно         Віко       Віко       Віко       Віко       Віко       Віко         Віко       Віко       Віко       Віко       Віко       Віко <td< th=""><th>зені кореневі центри сертифікації] — — Х — В Х Д<b>ї</b></th></td<>	зені кореневі центри сертифікації] — — Х — В Х Д <b>ї</b>
Certificates - Current User     Certificates	Довірені кореневі центри сертифік… 🔺
Соонст     Соорені усладжаї нацтиц салт     Сетіfi Find Certificates     Довірені     Сетіfi Find Certificates     Довірені     Соб'єк ко Вигляд     Відкрити нове вікно звідси     Відкрити нове вікно звідси     Соронні Оформлення списку завдань      Соронні Оформлення списку завдань     Соронні Оформлення списку завдань     Соронні Оформлення списку завдань     Соронні Оформлення списку завдань     Соронні Оформлення списку завдань     Соронні Оформлення списку завдань     Соронні Соронні Оформлення списку завдань     Соронні Оф	nd Certificates
Add a certificate to a store	,

5. Вкажіть шлях до файлу сертифіката (в форматі \*.cer, \*.crt, \*.pfx):

873 .		
3° N	Лаистер імпорту сертифікатів	
Фа	йл для імпорту	
	Укажіть файл, який потрібно імпортувати.	
	Ім'я файлу:	
	Iм'я файлу: C:1 Fredo TestCert.crt	Огляд
	Iм'я файлу: C: Fredo TestCert.crt Примітка. Кілька сертифікатів може зберігатися в одному	Огляд файлі в таких формата:
	Iм'я файлу: C: Fredo TestCert.crt Примітка. Кілька сертифікатів може зберігатися в одному Файл обміну особистими відомостями – РКСЅ #12 (.PFX,.	Огляд файлі в таких форматал P12)
	<ul> <li>Iм'я файлу:</li> <li>C: Fredo TestCert.crt</li> <li>Примітка. Кілька сертифікатів може зберігатися в одному о Файл обміну особистими відомостями – РКСЅ #12 (.PFX,. Стандарт Cryptographic Message Syntax – сертифікати РК</li> </ul>	Огляд файлі в таких форматал P12) CS #7 (.P7B)

6. Для сертифікатів в форматі pfx необхідно ввести пароль. Також на цьому етапі можна позначити сертифікат придатним для експорту:

🔶 😺 Майстер імпорту сертифікатів	×
Захист за допомогою закритого ключа Задля підтримки безпеки закриті ключі захищено паролями.	
Введіть пароль для закритого ключа.	
Пароль: •••• Відобразити пароль	
Параметри імпорту: Увімкнути сильний захист закритого ключа. Якщо ввімкнути цей параметр, щоразу під час використання програмою закритого ключа буде з'являтися запит.	
Позначити цей ключ як придатний до експорту. Це дозволить створювати резервні копії ключів або передавати їх пізніше.	]
<ul> <li>Захист закритого ключа за допомогою віртуалізованої системи безпеки (не придатне для експорту)</li> <li>Включити всі розширені властивості.</li> </ul>	5
Далі Скасу	/вати

7. Оберіть розташування сертифіката – Довірені кореневі центри сертифікації:

Mai	ten iunontu contudiuatin	
Inidan	пер мпорту сертифкать	
Сховии	е сертифікатів	
Cx	вища сертифікатів – це системні області, в яких зберіга	аються сертифікати.
Mo	кна визначити розташування сертифіката вручну або д dows автоматично вибрати сховише сертифікатів.	озволити системі
	Э Вибирати сховище сертифіката на основі типу сертиф	іката автоматично
	Розташовувати всі сертифікати в такому сховищі	
	Сховище сертифікатів:	
	Довірені кореневі центри сертифікації	Ornan

Сертифікат буде додано в сховище:

🔶 🙋 🔣 🐇 📷 😹								- 8
Коренева папка консолі		Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem^	Дії	
Certificates - Current User	Acute Services	01012028	America giornale unic.	Section (AAA)			Certificates	
> 🛄 Особисті	Esternal CA-Root	1005,2020	America giorgia calc.	Serligs (Add/huit)			Deserved all	
<ul> <li>Довірені кореневі центри серт</li> </ul>	Calue Prant Root	13-06-2625	Aground page and	DepCart Baltimore R.			Додаткові дії	
Certificates	1	1106,007	Aprenting to again a state	Cartum			D/WONI	
Довірені підприємства	united National CA	21.12.2029	America picacia colo.	Carbon Trusted Nat.			Rosstvoni sil	
Проміжні центри сертифікації	blic Primary Cartification .	10.08.2108	Aprentedpicação colo.	Wetlige Class 3 Pub.			додаткові дн	
<ul> <li>Об'єкт користувача Active Direi</li> <li>Порідоці ризорці</li> </ul>	1858 Cartification Author.	1947-2018	Approximation and	Section Remarks Co.				
<ul> <li>Довірені видавці</li> <li>Наворівскі сортифікати</li> </ul>	1 (c) 1997 Microsoft Corp.	21.12.1999	Personal Income	Manual Tenestern.				
Сторонні кореневі нентри серг		31.12.2023	<all></all>	Fredo Test Sert				
Повірені коритива центря сер		3112,3625	utility.	076010			1	
Постачальники послуг автенти	sourced 4D Root CA	10111-0001	Agrantegia agia cala.	DigiCart				
інші користувачі	Studial Root CA	10112001	Americania cal.	Digilari				
Local NonRemovable Certificate	<b>Jodnal Root 52</b>	1521,208	American provide state.	DigiCart Global Ros.				
Запити заяв на реєстрацію сер	Agh Assurance EV Root CA	10.11.2001	Americação cas.	DigiCart				
Э Довірені кореневі папки смарт	Fusted Root G4	15.01.2038	Appendix provide solid.	DipCart Trusted Ro.				
	18207 FulderRoot	08/01/2023	America and an	DO NOT TRUST Ful.				
	CR.80	1008-2021	America di scisti.	DS7 Root CA.RJ				
	ust Cartification Authority	6712,2096	America picaula colo.	Entrustown				
	e Cartification Authority (	1407.0029	Agrossive give a state.	Entrust (2048)				
		16/01/2029	Aprentu (picauja calc.)	Globallige Root CA .				
	a.	15.12.3821	Agrounted in success.	Google Foat Service.				
	a.	1601,2038	America picauja cos.	Globallige ECC Ass.				
	+ Cash Series has ME	1825,2045	Conversion of the local division of the loca	Outputting: Code 5.				
3	4					2		

# Експорт сертифіката в форматі pfx

Якщо КНЕДП передав сертифікат в форматі \*.cer, \*.crt, то його також потрібно імпортувати в сховище, як в попередньому розділі. Для підключення SSL-сертифіката в М.Е.Doc такий сертифікат необхідно експортувати в форматі \*.pfx.

1. Експортуйте імпортований сертифікат в форматі pfx.

- (-)	10.00.000	7 converse	month frequences	R Terrestanti. R
	31.12.2023	<all></all>	Medoc1	TestSert
	11.12,2023	100	Open	
esured 4D Root CA Indeal Root CA	10.11.2091	Annos	Усі завдання	Open
John Root G2	15.01.2036	(Annual A	Вирізати	Export
high Assurance EV Root CA	10112001	<b>Rental A</b>	Копіювати	-
humad Root G4	1521-2036	Remon	Видалити	shad No
78/07 FableRoot	08/11/2023	<b>Remon</b>		107.Ful.
CA.83	30.09.2021	<b>Annah</b>	Властивості	10 8
pot Cartification Authorit,	0712,0090	<b>Anna</b> H	Ловілка	
# Cartification Authority (,	24/07 2029			1{
	18.01.2029	TH	page on, Soluti	ign Riset Ck., R

2. Оберіть Експортувати закритий ключ:

	$\times$
🗧 😺 Майстер експорту сертифікатів	
Експортувати закритий ключ	
Можна експортувати закритий ключ разом із сертифікатом.	
Закриті ключі захищено паролем. Щоб експортувати закритий ключ разом із сертифікатом, необхідно ввести пароль у наступних діалогових вікнах.	
Експортувати закритий ключ разом із сертифікатом?	
<ul> <li>Так, експортувати закритий ключ</li> </ul>	
<ul> <li>Ні, не експортувати закритий ключ</li> </ul>	

Зауваження. Якщо ця опція недоступна, зверніться до вашого КНЕДП для отримання сертифіката в форматі pfx (див. розділ <u>Імпорт сертифіката в сховище</u>).

3. Для експорту в форматі pfx оберіть Файл обміну особистими відомостями – PKCS #12:

Форм	ат файлу експорту ертифікати можна експортувати у файли різних форматів.
в	иберіть формат, який слід використовувати:
	) Файл у DER-кодуванні X.509 (.CER)
	Файл у Вазе64-кодуванні Х.509 (.CER)
	<ul> <li>Стандарт Cryptographic Message Syntax – сертифікати РКСЅ #7 (.Р7В)</li> </ul>
	За можливості додати всі сертифікати до шляху сертифікації
	<ul> <li>Файл обміну особистими відомостями – РКСЅ #12 (.PFX)</li> </ul>
	За можливості додати всі сертифікати до шляху сертифікації
	Видалити закритий ключ після успішного експортування
	Експортувати всі розширені властивості
	🖂 Увімкнути конфіденційність сертифіката
	Сховище серіалізованих сертифікатів Microsoft (.SST)

4. Введіть пароль з підтвердженням, оберіть тип шифрування

Безпека Зад	ля підтримки безпек	ки потрібно зах	истити закри	тий ключ принц	ипалом
	мена груп або корис	тувачів (реком	ендовано)		
				Додати	
				Видалити	
2 <b>1</b>	ароль:				
, i	Підтвердження:				

5. Вкажіть ім'я і шлях збереження файлу сертифіката:

			_		
\overline а Збереження файлу					×
$\leftarrow$ $\rightarrow$ $\checkmark$ $\bigstar$ 🗖 · Цей ПК	<ul> <li>Робочий стіл</li> </ul>	~	õ	🔎 Пошук:	Робочий стіл
Упорядкувати 🔻 Створит	и папку				≣≡ ▼ (?)
💻 Цей ПК	^ Ім'я	^			Дата змінення
🧊 3D-об'єкти	temp				05.08.2021 17:18
Downloads					
🛃 Відеозаписи					
🚔 Документи					
📧 Зображення					
🎝 Музика					
📃 Робочий стіл					
🏪 Локальний диск (С:)					
🛖 Install (S:)	~ <				>
Iм'я файлу: testKey.pfx					~
		10 mar 11 (* = fr.)			
тип фаилу: Фаил оомп	чу особистими відо	мостями (п.ртх)			· · · ·
<ul> <li>Приховати папки</li> </ul>				Зберегти	Скасувати

6. У вказаний каталог буде експортовано сертифікат у форматі pfx:

Ім'я	Дата змінення	Тип	Розмір
Chempsels to appears oproducty t.	26.04.2022 10:14	Zosponst Microso	2 586 455
Chill BetChannel di	26/24/2022 17:47	Propagational parts	
🎯 testKey.pfx	26.04.2022 12:02	Обмін приватни	3 КБ
a lest, medice, 2022 04-25-084445.cm	26/24/2522 11:45	Captophan Secret.	
C testiliay	26/04/2022 11/07	dials.	
W TextTylearenet.Inf	25-04-2022 15-42	mails 717	4.15
Client_server_login_to_SSLeet.pcaping	25.04.2022 12:49	Winshark capture .	6.408.455
clert, anar, login, with, Silvert prograp	25.04.2022 12.44	Wreshark capture -	8.272.45

# Підключення сертифіката

- 1. Запустіть з правами адміністратора утиліту **ConnectionSetup.exe**, яка знаходиться в кореневій папці встановленої програми FREDO.
- (наприклад, c:\Program Files\FREDO\FREDO \ConnectionSetup.exe)
- 2. Втановіть опцію Використовувати SSL.
- 3. В полі Сертифікат вкажіть шлях до сертифіката у форматі pfx.
- 4. В полі Пароль введіть пароль сертифіката.
- 5. Натисніть Зберегти".

При використанні функції **Створити сертифікат** шлях до сертифіката і пароль автоматично заповнюються вказаними в функції даними.

🍪 Налаштування з'єдна	ння	_	
			Довідка
Основні Налаштування Гі	rebird		
Сервер			
Служба сервера:	FREDOService16		
Адреса:			
Порт:	10016 🜩		
📃 Змінити налаштуван	ня Клієнта		
📃 Виконувати запуск т	ермінального клієнта без кої	піювання файлів	програми
🗹 Використовувати SS	L		
Сертифікат:	C:N.	VT HEDOCIC PI	l.pfx 🛄
Пароль:	***	Створити	сертифікат
Налаштування рівня прото За допомогою повзунка в програми	колювання системних подій: жажіть рівень деталізації дл	я запису до log	-файлів
- Помил -	китапопередже <del>нн</del> я		
Робоча станція			
Адреса:	10.200.87.62		
Порт:	10016		
		Зберегти	Відмінити