

ТОВ «САЙФЕР ПРО» Адреса: 04107, Київ, вул. Нагірна, 25-27 Тел.: +38 044 484 46 12, 484 46 17 E-mail: info@cipher.com.ua

Системи захисту інформації www.cipher.com.ua

Мережний криптографічний модуль Шифр-HSM

Інструкція користувача для налаштування Сайфер Шифр-HSM в IIT Користувач

Заголовок: Мережний криптографічний модуль Шифр-HSM

3MICT

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ	. 3
ПІДГОТОВКА РОБОЧОГО МІСЦЯ	.4
Встановлення IIT Користувач	.4
Встановлення та налаштування клієнтської бібліотеки	.4
Налаштування IIT Користувач	.4
Розміщення клієнтських бібліотек	.4
Вказівка СМР-серверу ЦСК	.4
Налаштування бібліотеки для OC Windows	.5
ЗЧИТУВАННЯ КЛЮЧА	.9

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

- CMP Certificate management protocol
- HSM Hardware security module
- PIN Personal Identification Number
- PKCS#10 Certification Request Syntax Specification
- IIT Інститут інформаційних технологій
- МКМ Мережний криптографічний модуль
- ОС Операційна система

ПІДГОТОВКА РОБОЧОГО МІСЦЯ

Встановлення IIT Користувач

Завантажити з офіційного сайту <u>IIT</u> дистрибутив – Користувач центру сертифікації ключів. Інсталяційний пакет (OC Microsoft Windows), або одразу завантажити файл <u>за посиланням</u>.

Встановлення та налаштування клієнтської бібліотеки

Отримати від розробника Сайфер Шифр-HSM набір бібліотек чи дистрибутив setup_CiHSM_Client.exe з набором бібліотек.

Пакет містить набір файлів, наприклад, для архітектури х86-64.

Назва	Опис			
cihsm.dll	РКСЅ#11 бібліотека для роботи з Мережним криптографічним модулем "Шифр-HSM"			
libcrypto-1_1.dll	Бібліотека залежностей			
libssl-1_1.dll	Бібліотека залежностей			
pkcs11_tester.exe	Тестова утиліта, яка дозволяє здійснити перевірку доступність і працездатність МКМ			

Налаштування IIT Користувач

Розміщення клієнтських бібліотек

Перейти за шляхом:

C:\Program Files (x86)\Cipher\CiHSM_Client\PKCS11\Win

та скопіювати повний вміст папки у папку, де розміщуються бібліотеки для роботи з IIT Користувач: C:\Program Files (x86)\Institute of Informational Technologies\Certificate Authority-1.3\End User Варто зауважити, що бібліотеки мають бути тієї розрядності, як і IIT Користувач, на даний момент це x86.

Вказівка СМР-серверу ЦСК

Для того, щоб вказати адресу, треба запустити IIT Користувач, перейти за шляхом «Встановити параметри» - «СМР-сервер» - вказати позначку «Використовувати СМР-сервер».

В даному випадку використовується Тестовий ЦСК Сайфер, то адреса буде наступна

http://ca39.cipher.com.ua/cmp

Натискаємо «Ок» для збереження змін.

Файлове сховище	📮 СМР-сервер ЦСК	
Ргоху-сервер	Використовувати СМР-сервер ——————————————————————————————————	
ТSP-сервер	DNS-ім'я чи IP-адреса сервера: http://	com.ua/cmp
OCSP-сервер	ТСР-порт: 80	3 сертифіката
LDAP-сервер		
СМР-сервер		
X Особистий ключ		
сертифікати та СВС		
Реєстрація подій		
	ОК	Відміна Застосувати

Рис. 1. Налаштування параметрів СМР-серверу ЦСК

Налаштування бібліотеки для OC Windows

Параметри роботи

Для роботи бібліотек, які було скопійовано раніше, вказується адреса і порт МКМ у захищеній мережі МКМ через створення змінної середовища ОС.

В ОС Windows переходимо у "Властивості системи", розділ «Змінні середовища», Рис. 2-4.



Рис. 2. Пуск "Зміна системних змінних середовища"





Рис. 4. Змінні середовища

Далі, створюємо нову змінну, Рис. 5.

Iser variables for C				
Variable	Value			
CipherInstallerConfigsPath	C:\Users\?			
MOZ_PLUGIN_PATH	C:\Program Files (x86)\Foxit Software\Foxit PDF Reader\plugins\			
OneDrive	C:\Users\?			
ath C:\Users\C.::L,Li\AppData\Local\Microsoft\WindowsApps;				
TEMP	C:\Users\2			
TMP	C:\Users\?			
	New Luit Delete			
ystem variables	Derece			
ystem variables Variable	Value			
ystem variables Variable PKCS11_PROXY_SOCKET	Value /			
ystem variables Variable PKCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR	Value tcp://emeranee.23454 XE AMD64			
ystem variables Variable PKCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IENTIFIER PROCESSOR_IENTIFIER	Value tcp://emeranee.23454 E AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel			
ystem variables Variable PKCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_PEVISION	Value tcp://www.cuit Delete tcp://www.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit Delete tcp://www.cuit.cuit.cuit.cuit.cuit.cuit.cuit.cuit			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath	Value tcp://www.com/com/com/com/com/com/com/com/com/com/			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_LEVISION PSModulePath TEMP	Value tcp://www.commence.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C\Windows\TEMP			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath TEMP TMP	Value tcp://theseseses.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C:\Windows\TEMP C:\Windows\TEMP			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath TEMP TMP	Value tcp://www.commence.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C\Windows\TEMP C:\Windows\TEMP			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath TEMP TMP	Value tcp://dwww.eeeeeee.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C:\Windows\TEMP C:\Windows\TEMP New Edit Delete			
ystem variables Variable PRCCS11_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath TEMP TMP	Value tcp://dwww.eeeeeee.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C:\Windows\TEMP C:\Windows\TEMP C:\Windows\TEMP			
ystem variables Variable PRCC511_PROXY_SOCKET PROCESSOR_ARCHITECTUR PROCESSOR_IDENTIFIER PROCESSOR_LEVEL PROCESSOR_REVISION PSModulePath TEMP TMP	Value tcp://www.weightscheelee.23454 RE AMD64 Intel64 Family 6 Model 140 Stepping 1, GenuineIntel 6 8c01 %ProgramFiles%\WindowsPowerShell\Modules;C:\Windows\sys C:\Windows\TEMP C:\Windows\TEMP C:\Windows\TEMP			

Рис. 5. Створення змінноі

Вказуємо наступні значення для змінноі. Наприклад, для серверу 0.0.0.0 з портом 23454, створюється змінна середовища РКСS11_PROXY_SOCKET, зі значенням змінноі – «tcp://0.0.0.23454», Рис. 6.

Edit System Variable		×
Variable name:	PKCS11_PROXY_SOCKET	
Variable value:	tcp://01.101.202.100:23454	
Browse Directory	Browse File OI	Cancel

Рис. 6. Створення нової змінної

Перегляд новоствореноі змінноі середовища та збереження змін, Рис. 7.

Variable	Value	
PKCS11_PROXY_SOCKET	tcp://2 2 22:23454	
PROCESSOR_ARCHITECTURE	AMD64	
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 140 Stepping 1, GenuineIntel	÷
PROCESSOR_LEVEL	6	
PROCESSOR_REVISION	8c01	
DSM adula Dath	% Drogram Eilor% \\ Mindows Dower Shall \ Medules: (C) \ Mindows \ sys	
PSIVIOUUIEPatri	%Programmies % (WindowsPowerSheir (Modules, C. (Windows (sys.	••
TEMP	C:\Windows\TEMP	
TEMP TMP	C:\Windows\TEMP C:\Windows\TEMP	•
TMP	C:\Windows\TEMP C:\Windows\TEMP New Edit Delete	•
тылынан ТЕМР ТМР	C:\Windows\TEMP C:\Windows\TEMP New Edit Delete	•

Рис. 7. Оновлений список змінних середовища

Заголовок: Мережний криптографічний модуль Шифр-HSM

Натискаємо «Ок» для збереження змін, Рис. 8.

System Properties	S				×
Computer Name	Hardware	Advanced	System Protection	Remote	
You must be lo	gged on as a	an Administra	ator to make most of	these chang	ges.
Visual effects, memory	processor s	scheduling, n	nemory usage, and v	irtual	
				Settings	
User Profiles Desktop settin	igs related to	o your sign-ir	1		
				Settings	
Startup and Red	covery				
System startu	p, system fa	ilure, and del	bugging information		
				Settings	
			Environme	nt Variables	i
		ОК	Cancel	Арр	oly

Рис. 8. Збереження змін

ЗЧИТУВАННЯ КЛЮЧА

Запускаємо IIT Користувач та обираємо в розділі «Особистий ключ» - «Зчитати», Рис. 9.

😼 IIT Ka	рристувач ЦСК-1		_		×
•	ит Центр сертифікації ключів Користувач ЦСК				ΙΙΤ
≣	Користувач ЦСК				
	Підписати файли Підпис файлів на особистому ключеві	Перевірити файли Перевірка підпису на підписаних файлах			
	Зашифрувати файли Зашифрування файлів на одного чи декількох користувачів	Розшифрувати файли Розшифрування зашифрованих файлів			
	Переглянути сертифікати Перегляд сертифікатів у файловому сховищі	Переглянути СВС Перегляд СВС у файловому сховищі			
	Встановити параметри Встановлення параметрів роботи користувача	Згенерувати ключі Генерація ключів із запитами або формування нових сертифікатів	I.		
	Допомога	Особистий ключ		-	
	 Про програму Перейти до web-сайту ЦСК 	Эчитати 			

Рис. 9. Зчитування ключа

З'являється вікно з переліком носіїв, серед них треба обрати «криптомодуль Сайфер Шифр-HSM», натиснувши на нього стає доступним пункт Cipher-HSM, Рис. 10.

Стає доступним поле для введення Паролю, але тут є особливість для правильного введення, Рис. 11. Маска є наступною:

##SlotID##PIN

SlotID – задається у 10-ковій чи в 16-ковій системі числення. Якщо значення вказується в 16-ковій системи числення вказується на початку"0х".

Приклад заповнення:

- о 10-кова система числення 1060006000
- о 16-кова система числення -0x3F2E6870
- PIN пін-код до слоту.

Тобто, в даному випадку значення матиме наступний вигляд:

##1060006000##12345678

АБО

##0x3F2E6870##12345678

Не допускайте пробілів та інших спецсимволів.





Рис. 11. Вказівка PIN-коду

Після введення значень, натискаємо «Зчитати» для збереження змін. Далі може з'явитися вікно із запитом на завантаження сертифікату СМР-сервера з СМР-сервера ЦСК, Рис. 12. У випадку, якщо натиснемо «No» подальший процес буде припинено, якщо погодимося, буде запропоновано підтягнути сертифікати за адресою, яку вказували в налаштуванні, Рис. 13.

Товідомлення оператору	\times
Завантажити сертифікат СМР-сервера з СМР-сервера ЦСК?	
Yes No	
Рис. 12. Запит користувачеві	
Завантажені сертифікати 🛛 🕹	
Завантажені з СМР-сервера ЦСК сертифікати: Кольоровий Семен Семенович Новый ЦСК ТОВ "Сайфер БІС" OCSP-HSM-DSTU OCSP-HSM-DSTU TSA-HSM-DSTU TSP-сервер ТОВ «Сайфер PRO» Кольоровий Семен Семенович Імпортувати їх у файлове сховище сертифікатів?	
Yes No	

Рис. 13. Повідомлення про отримання сертифікатів

Як результат відображається головне вікно застосування, де зазначається, що особистий ключ успішно зчитано та можна здійснювати підписання документів, Рис. 14.





Натиснувши на пункт «Переглянути власний сертифікат», можна переглянути терміни дії сертифікатів, ким виданий та іншу детальну інформацію, Рис. 15.

Власний сертифікат		×
📄 Сертиф	ікат	
Lick:	Новый ЦСК ТОВ "Сайфер БІС"	
Користувач:	Кольоровий Семен Семенович	
Дійсний:	з 17.01.2024 до 16.01.2025	
Реєстраційний номер:	12BC54CB58FEAC524367D11DE463B1DCD6036358	
Використання ключів:	ЕЦП, Неспростовність у державних алгоритмах і протоколах	
Детальна інфо Наступний сер	рмація тифікат	
	ОК	

Рис. 15. Перегляд власного сертифікату