Інструкція користувача

«Управління ключами сховища РКСЅ#12»

Зміст

1.	Загальні відомості	1
	1.1. Призначення	1
	1.2. Системні вимоги	1
	1.3. Склад Інструменту	2
	1.4. Ліцензійні вимоги	2
	1.5. Реквізити розробника	2
2.	Опис операцій	3
	2.1. Порядок запуску	3
	2.2. Створення сховища PKCS#12	3
	2.3. Завантаження сховища PKCS#12	4
	2.4. Генерація ключа та запиту PKCS#10	6
	2.5. Створити сертифікат	9
	2.6. Інсталяція сертифікату	. 12
	2.7. Імпорт/експорт ключів	. 14
	1 1	

1. Загальні відомості

1.1. Призначення

Інструмент «Управління ключами сховища РКСЅ#12» (надалі – Інструмент) призначений для:

- створення файлового сховища PKCS#12 ключів та сертифікатів;
- імпорту/експорту ключів та сертифікатів до/із сховища;
- генерації асиметричної ключовою пари із записом цієї пари до сховища, та створення запиту на сертифікат у форматі PKCS#10;
- генерації сертифікату для ключової пари, що є у сховищі, з підписанням на вибраному ключі у сховищі;
- генерації сертифікату із зовнішнього запиту PKCS#10 (файлу) з підписанням на вибраному ключі у сховищі;
- імпорт сертифікату для ключової пари чи заміна існуючого сертифікату.

1.2. Системні вимоги

Інструмент створено на мові Java як десктоп-інструмент (desktop) робочого столу, що може виконуватися у будь-якому операційному середовищі під управлінням віртуальної машини Java 1.6 та вище.

1.3. Склад Інструменту

Інструмент постачається у складі бібліотек (в папці lib) та командного файлу:

lib\ Pkcs12Tools.bat

Склад бібліотек: ambapi.jar – бібліотека додаткових інструментів; ambprovider.jar – криптографічний сервіс провайдер Java JCA/JCE (Java ^{тм} Cryptography Architecture/ Java ^{тм} Cryptography Environment); PKCS#12.jar – інструмент «Управління ключами сховища PKCS#12».

1.4. Ліцензійні вимоги

Ліцензування є обов'язковим для використання бізнес-користувачами, тобто працівниками державних та комерційних організацій та установ.

Правильність функціонування Інструменту та його супроводження забезпечується тільки для ліцензованого Інструменту.

1.5. Реквізити розробника

ТОВ «Базис» 0304, Україна, м. Київ, вул. Платонівська 18 Тел.: +38 044 244-02-25 tech@itsway.kiev.ua

2. Опис операцій

2.1. Порядок запуску

Програма тестування виконується запуском командного файлу:

Pkcs12Tools.bat

Файл для Java JRE v1.7: "C:\Program Files\Java\jre7\bin\java.exe" -Xmx1024m -cp "./lib/PKCS#12.jar;./lib/ambprovider.jar;./lib/ambapi.jar" com.amb.api.pkcs12.PKCS12App

Файл для Java JRE v1.6: "C:\Program Files\Java\jre6\bin\java.exe" -Xmx1024m -cp "./lib/PKCS#12.jar;./lib/ambprovider.jar;./lib/ambapi.jar" com.amb.api.pkcs12.PKCS12App

2.2. Створення сховища РКСЅ#12

В основному вікні Інструменту вибрати кнопку «Створити...»

e	🏄 Управление ключами хранилища PKCS#12								
	Файл Генерация ключа Помощь								
е и !	Создать или загрузить РКСЅ#12 хранилище: Создать Загрузить	6							

Ввести пароль доступу до сховища (та повторити його), і вибравши команду «Зберегти як…» записати сховище до файлу:

	🍰 Управление ключами хранилища PKCS#12					
Файл Генерация ключа Помощь						
ic IF	Создать или загрузить РКСS#12 хранилище:					
11	Создать Загрузить					
	Пароль					
	Повторите					
	Сохранить как Отменить					

2.3. Завантаження сховища РКСЅ#12

Якщо сховище вже існує, то в основному вікні Інструменту вибрати кнопку «Завантажити…», та після вибору файлу ввести пароль доступу:

lp.	📓 Управление ключами хранилища PKCS#12 📃 🗖 🔀
2	Файл Генерация ключа Помощь
ал Г С	Создать или загрузить РКСЅ#12 хранилище:
С Л F	Имя файла C:\Key\store.p12
ē	Пароль Отменить
	Псевдоним Общее имя Цепочка Алгоритм ключа

При наявності у сховищі ключів та сертифікатів вони будуть відображені у таблиці:

📓 Управление ключами хранилища PKCS#12								
Файл Генерация ключа Помощь								
Создать или загрузить РКСЅ#12 хранилище: Создать Загрузить								
Псевдоним Общее имя Шелочка Алгоритм ключа								
	LICK AD "VCC" DEA	Цепочка						
4f504fa6-58eb-26a4-630c-4e90550	UCK // VCC" Poot	1 сертификата	РСА, ПОДПИСЬ ТОЛЬКО					
Удалить Экспортировать в *.pfx Импорт из *.pfx	треть сертификат Просмотре а с цепочкой	ть цепочку сертификатов						
				0				

У стовпці «Ланцюг» (сертифікатів) показано скільки сертифікатів з ланцюга міститься у сховищі. Якщо запис пустий, то ця ключова пара не має сертифікату – це пара, на яку сформовано запит PKCS#10 на отримання сертифікату.

Якщо сертифікат присутній, то його можна переглянути, вибравши конкретний запис та потім натиснувши кнопку «Подивитися сертифікат»:

📓 Управление ключами хранилища PKCS#12							
Файл Генерация ключа Помощь							
Создать или загрузить РКСЅ#12 хранилище:							
Создать Загрузить Псевдоним ↓453е8:05-0еа8-53f0-е193-64a58b4 ↓4f504fa6-58eb-26a4-630c-4e99550 ↓4f504fa6-58eb-26a4-630c-4e99550	Общее имя ЦСК ДП "УСС" RSA ЦСК ДП "УСС" Root	Цепочка 1 сертификата	Алгоритм ключа RSA, Подпись только RSA, Подпись только		∠≈		
Импорт из *.pfx							
				0			

2.4. Генерація ключа та запиту РКСЅ#10

Генерація ключа виконується у відкритому сховищі (див. п.2.3.).

Для генерації ключа та одночасно запиту (чи само підписаного сертифікату) вибрати меню «Генерація ключа/ Запит сертифікату РКСЅ#10...»:

🕌 Управление ключами хранилища PKCS#12						
Файл	Генерация ключа	Помощь				
Coor	Запрос сертифин	ката PKCS#10				
созд	Создат& сертиф	икат	лище:			
C	Инсталлировать	сертификат				
Псевдоним Общее имя						

У новому вікні генерації вибрати алгоритм ключа із доступних у списку алгоритмів:

🅌 Генерация ключевой пары и PKCS#10 запро							
_Г Выбор алгоритма	и длины ключа -						
Алгоритм ключа	DSTU4145PB	Длина ключа					
	DSTU4145PB	``					
_	DSTU4145ONB						
Выберите типовое	RSA	ключа Ключт					
ГДанные о субъект	DSA 냥	рча) ————					
	ECDSA Fp						
	ECDSA F2m						
Орган	GOST34310						
	ECGost34310						
0	бласть						

де

DSTU4145PB – стандарт ДСТУ 4145-202, поліноміальний базис;

DSTU4145ONB – стандарт ДСТУ 4145-202, оптимальний нормальний базис;

RSA – стандарт RFC 3447:2003, FIPS 186-3:2009, PKCS #1 v2.1;

DSA – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-3:2002;

ЕСDSA Fp – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-2:2002;

ECDSA F2m – стандарт FIPS 186-3:2009, ДСТУ ISO/IEC 14888-2:2002;

GOST34310 – стандарт ГОСТ 34.310-95;

ЕСGost34310 -стандарт ГОСТ 34.310-2004.

Для стандарту **ECDSA** підтримуються еліптичні криві, визначені такими стандартами:

- **SEC2** Standards for Efficient Cryptography (SEC), SEC 2: Recommended Elliptic Curve Domain Parameters September 20, 2000, Version 1.0, Certicom Corp.
- NIST FIPS 186-3: Digital Signature Standard (DSS); Annex D.1 NIST Recommended Elliptic Curves June, 2009
- **X9.62** X9.62-2005: Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

Brainpool - ECC Brainpool:

- 1) ECC Brainpool Standard Curves and Curve Generation, Version 1.0, 2005. <u>http://www.ecc-brainpool.org/ecc-standard.htm</u>; and
- 2) **BSI** TR-03111: Technical Guideline TR-03111. Elliptic Curve Cryptography, Version 1.11" – BSI (Bundesamt fur Sicherheit in der Informationstechnik), 2009 – <u>https://www.bsi.bund.de/cae/servlet/contentblob/471398/publicationFile/3</u> 0909/BSI-TR-03111_pdf.pdf;
- 3) ECC Brainpool Standard Curves and Curve Generation RFC draftlochter-pkix-brainpool-ecc-03, March 6, 2009.

Вибрати довжину ключа чи еліптичну криву (за назвою чи ідентифікатором). Для ДСТУ ключів додатково вибрати ДКЕ (довготривалий ключовий елемент):

4	🕌 Генерация ключевой пары и PKCS#10 запроса							
	_Г Выбор алгоритма и длины ключа —							
	Алгоритм ключа DSTU4145PB 💟 Длина ключа 163 🛩 ДКЕ							
			. I X		Nº2			
ľ	ыверите типовое использ	ования ключа	Ключ цифровои	подпи	N63			
	Данные о субъекте (владе	льце ключа) ——			Nº4	≣		
	CN/DNS				N95	5	Numb	
	Организация				N95 N97		елен	
					N98	~		
	Область						Гор	

Вибрати типове використання ключа:

4	🕌 Генерация ключевой пары и PKCS#10 запроса							
	_Г Выбор алгоритма и длины ключа ————————————————————————————————————							
	Алгоритм ключа DSTU4145PB 💙 Длина ключа 163 💙 ДКЕ №1 💙							
E	Выберите типовое использования ключа Ключ цифровой подписи 🔹 🌅 Расшир							
	-Данные о субъекте (владе	льце ключа) ——	Ключ цифровой подписи	^]			
	CN/DNS		Ключ шифрования					
			Ключ подписи и шифрования 💦 🔪					
	Организация		Согласование/Шифрование ключей К					
			Ключ подчиненного ЦСК					
	Область		Ключ корневого ЦСК					
			Ключ службы фиксирования времени					
	Должность		Ключ службы OCSP	~				

Якщо необхідно, вибрати «Розширений запит», та встановити розширення запиту:

📓 Генерация ключевой г	пары и РКСS#10 запроса 📃 🗖 🔀							
_г Выбор алгоритма и длины ключа —								
Алгоритм ключа DSTU414	Алгоритм ключа DSTU4145PB 💙 Длина ключа 163 💙 ДКЕ Nº1 💌							
Выберите типовое использ	Выберите типовое использования ключа Ключ цифровой подписи 💌 🔽 Расширенный запрос							
Назначение ключа Здесь устанавлены флаги К	(eyUsage для выбранной модели типового использования ключа							
Цифровая подпись	✓ Не-отказуемость Шифрование ключей Шифрование данных							
Согласование ключей	Подпись сертификатов Подпись CRL Только зашифрование Только расшифрование							
Расширенное использован	ние ключа —							
🔲 Защита электронной поч	нты 🔲 Подписывание кода 👘 SSL Аутентификация клиента 📄 SSL Аутентификация сервера							
🔲 IPSec пользователь	IPSec конечная система IPSec тунель Формирование меток времени							
Подписывание OCSP	OCSP Cert No Check MS Smart Card Logon MS Domain Controller							
МS Шифрование файлов	ой системы 🔲 MS Восстановление зашифрованной файловой системы							
_Г Данные о субъекте (владе	льце ключа) —							
😑 CN/DNS	Serial Number							
Организация	Подразделение							
Область	Город							
Должность	e-mail							
Дополнительные данные								
🗌 Создать как корневой 🛛 🔵 🗢 Срок жизни в годах								
Генерация Сохрани	ть как Посмотреть РКС5#10 Отказаться							

Заповнити реквізити підписувача (власника ключа).

На завершення, встановити прапорець «Створити як кореневи», якщо треба додатково створити само підписаний сертифікат (за записати його в сховище), а також визначити термін дії сертифікату в роках.

Після цього вибрати кнопку «Генерація».

Кнопкою «Зберегти як..» треба виконати збереження запиту РКСЅ#10 у файл.

2.5. Створити сертифікат

Меню «Створити сертифікат» призначається для створення/ генерації сертифікату із запиту РКСЅ#10:

🖆 Управление ключами хранилища PKCS#12								
Г	Файл	Генерация ключа	Помощь					
4	0	Запрос сертифин	ката PKCS#10					
	созд	Создать сертиф	икат	лище.				
		Инсталлиробать	о сертификат					
1				06	Henerius			
2		псевдоним		Оощее имя	цепочка			
		453e8c05-0ea8-53)f0-e193-64a58b4 Ц	СК ДП "УСС" RSA				
d.	🔲 📕 4f504fa6-58eb-26a4-630c-4e99550 ЦСК ДП "УСС" Root 1 сертификат							
r								
d.								

Сертифікат при цьому підписується ключем, який вибирається в сховищі. Отже, створити сертифікат можна лише після створення в сховищі ключової пари та її сертифікату, який може бути само підписаним (див. п.2.4.), або імпортований із файлу ззовні (див. п. «Імпортувати сертифікат»)

Вікно «Створити сертифікат»:

🕌 Создать сертификат				
Выберите ключ/сертификат, кото	орым надо подписать запро	00		
Псевдоним	Общее имя	Алгоритм ключа		
4f504fa6-58eb-26a4-630c-4e995	ЦСК ДП "УСС" Root	1 сертификата	RSA, Подпись только	
Dufernantin				
выверите ключ/запрос, для кото	рого надо создать сертифи	кат, или внешнии	РКС5#10 фаил:	
45209c05-0009-5260-0102-6405		ценочка		
Серийный номер сертификата		0 🗢	Срок жизни в годах	
Точка распространения базового CRL				
Точка распространения частичного/дель	Ta CRL			
Генерация Сохранить как	Показать сертификат			

1) Вибрати сертифікат/ ключ, яким слід підписати новий (створюваний) сертифікат

🍰 Создать сертификат			
Выберите ключ/сертифик	ат, которым надо подписать	запрос	
Псевдоним	Общее имя	Цепочка	Алгоритм ключа
🔽 4f504fa6-58eb-26a4-630c-4e995 ЦСК ДП "УСС" Root		1 сертификата	RSA, Подпись только

- 2) Вибрати запит
 - а. Якщо сертифікат створюється із запиту для ключової пари, що є у сховищі, то слід вибрати цю пару:

здоним	Общее имя	Цепочка	Алгоритм ключа
c05-0ea8-53f0-e193-6	54а5 ЦСК ДП "УСС" RSA		RSA, Подпись только

b. Якщо сертифікат створюється із зовнішнього запиту (файлу), то слід вибрати прапорець зовнішнього файлу та відповідний файл:

I	Выберите ключ	и/запрос, для которого надо создать сертификат, или внешний PKCS#10 файл: 🗹
	Файл PKCS#10	Выбрать

вибрати файл:

🍰 Открыть		×
Смотреть в	B 🛅 PKCS#12 🥑 📴 🕶	
Недавние документы	 isvn build dist nbproject 	
Рабочий стол	in src in test a a a a	
() Мои документы	a2 apem build Sec cert	
Мой компьютер	c cert.pem chain manifest.mf uss_rsa	
Сетевое окружение	Имя файла Открыть Тип файлов Все файлы Отменить	

3) Задати серійний номер для сертифікату, що створюється, та його термін життя/ дії у роках:

Серийный номер сертификата		0 🗢 Срок жизни в годах				
Точка распространения базового CRL						
Точка распространения частичного/дельта CRL						
Генерация Сохранить как Показать сертификат						

Додатково слід ввести точки розповсюдження списків відкликання (основного, та часткового), як URL, наприклад:

http:://example.com.ua/crllisl.crl – основний CRL http:://example.com.ua/crllisl+.crl – частковий CRL

На завершення, натиснути кнопку «Генерація».

Генерований сертифікат слід зберегти як файл (кнопка «Зберегти як…», та додатково можна переглянути (кнопка «Показати сертифікат»).

2.6. Інсталяція сертифікату

Інсталяція сертифікату виконується за командою меню «Інсталювати сертифікат...»:



Вибрати файл сертифікату:

🕌 Открыть								X
Смотреть в	🛅 Key				~		• 📰 -	
Недавние документы								
Рабочий стол								
() Мои документы								
Мой компьютер								
S	Имя файла						От	крыть
Сетевое окружение	Тип файлов	*.cer,*.p7b),*.crt,*.pem	1		~	Отю	енить

Після вибору файлу сертифіката, програма виконає пошук відповідної ключової пари у сховищі, і у разі відсутності ключової пари завершиться помилкою:



У разі наявності відповідної ключової пари у сховищі буде виконана операція встановлення сертифікату до знайденої ключової пари. Якщо пара вже має сертифікат, то програма надасть попередження та виконає заміну сертифікату лише за підтвердженням.

2.7. Імпорт/експорт ключів

Нижня частина основного вікна містить команди експорту/ імпорту ключів у форматі файлів *.pfx (PKCS#12 стандарт):

Удалить	Просмотреть сертификат Просмотреть цепочку сертификатов	
Экспортировать в *.pfx	🔽 Вместе с цепочкой	
Импорт из *.pfx		
		0