

AMB Group

Центр Защиты Ресурсов Информационных Систем

ЦЕЗАРИС

Инфраструктура открытых ключей

Инструкция по эксплуатации

Редакция 1.0

АННОТАЦИЯ

Данный документ содержит описание криптопровайдера "CESARIS Cryptographic Service Provider ©", который входит в состав проекта Центр Защиты Ресурсов Информационных Систем (ЦЕЗАРІС).

Документ предназначен для пользователей и прикладных программистов, разрабатывающих собственные приложения.

СОДЕРЖАНИЕ

1. Описание криптопровайдера CESARIS-CSP	4
1.1. Назначение	4
1.2.Основные характеристики	4
1.3. Реализуемые алгоритмы	5
1.4. Состав программного обеспечения	5
2. Инсталляция криптопровайдера	7
3. Использование утилит	12
3.1. Менеджер РКСS#11	12
3.1.1. Инициализация токена	12
3.1.2. Аутентификация (login)	13
3.1.3. Смена пароля доступа	13
3.1.4. Просмотр свойств объектов	13
3.1.5. Копирование объектов	14
3.1.6. Удаление объектов	14
3.1.7. Дублирование ключей и сертификатов	14
3.1.8. Соглашение по названиям (меткам) объектов	22
Рекомендуемая литература	24

1. Описание криптопровайдера CESARIS-CSP

Разработчик: АМБ-групп. Криптопровайдер: "CESARIS Cryptographic Service Provider ©" Сокращенное название: "CESARIS CSP"

1.1. Назначение

CESARIS-CSP (далее - Криптопровайдер) предназначен для:

• наложения и проверки электронной цифровой подписи (ЭЦП) на электронных документах при обмене ими между пользователями, в соответствии с отечественными стандартами ГОСТ 34.311-95, ГОСТ 34.310-95 и ДСТУ 4145-2002;

• обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования, в соответствии с ГОСТ 28147-89;

• контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;

• управления ключевыми элементами системы в соответствии с регламентом средств защиты.

1.2.Основные характеристики

Длина ключей электронной цифровой подписи:

- 512, 1024 бита при использовании алгоритма ГОСТ 34.310-95;
- 163 431 бит при использовании алгоритма ДСТУ 4145-2002 и полиномиального базиса;
- 173 431 бит при использовании алгоритма ДСТУ 4145-2002 и оптимального нормального базиса.

Длина ключей, используемых при шифровании:

- симметричный ключ 256 бит при использовании алгоритма ГОСТ 28147-89;
- ассиметричное шифрование 1024 4096 бит на базе алгоритма RSA.

Хеширование:

• длина значения хэш-функции по ГОСТ 34.311-95 – 256 бит.

Типы ключевых носителей:

- файл (на любом носителе);
- USB E-Token (производитель Aladdin Knowledge Systems Ltd, <u>http://www.aladdin.com</u>);
- смарт-карты ASECard Crypto с ридером ASEDrive IIIe (производитель Athena, <u>www.athena-scs.com</u>);
- смарт-карты Axalto CyberFlex, Axalto CryptoFlex с ридерами Reflex та E-gate (производитель Axalto Inc, <u>http://www.axalto.com</u>);
- смарт-карты GemPlus (производитель GemPlus, <u>http://www.gemplus.com</u>);
- USB-токены MiniKey, смарт-карты PrivateCard (производитель Algorithmic Research, <u>http://www.arx.com</u>);
- JAVA-смарт-карты (производитель Oberthur Card Systems, www.oberthurcs.com).

1.3. Реализуемые алгоритмы

Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования".

Алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями:

- ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма ";
- ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"

Алгоритм зашифрования/расшифрования данных реализован в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами р, q, а в соответствии с ГОСТ 34.310-95.

При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ 34.311-95 и ГОСТ 28147-89.

1.4. Состав программного обеспечения

Криптопровайдер представляет собой набор библиотек, зарегистрированных в операционной системе (ОС):

- csrs804csp.dll, csrs804ex.dll криптопровайдер ГОСТ 34.310-95 & RSA;
- csrs805csp.dll, csrs805ex.dll криптопровайдер ДСТУ 4145-2002 (полиномиальный базис) & RSA;
- csrs806csp.dll, csrs806ex.dll криптопровайдер ДСТУ 4145-2002 (полиномиальный базис) & ECDH;
- csrs807csp.dll, csrs807ex.dll криптопровайдер ДСТУ 4145-2002 (оптимальный нормальный базис) & RSA;
- csrs808csp.dll, csrs808ex.dll криптопровайдер ДСТУ 4145-2002 (оптимальный нормальный базис) & ECDH;
- cesarisstore.dll модуль хранилища;
- cesaris_dispatch.dll, cesaris_virtual.dll модули поддержки работы с носителями с использованием интерфейса PKCS#11.
- cesaris_file.dll модуль поддержки файловых носителей;
- cesaris_aladdin.dll модуль поддержки носителей Aladdin;
- cesaris_athena.dll модуль поддержки носителей Athena;
- cesaris_axalto.dll модуль поддержки носителей Axalto;
- cesaris_gemplus.dll модуль поддержки носителей GemPlus;
- cesaris_oberthur.dll модуль поддержки носителей Oberthur Card Systems;
- cesaris_ikey.dll модуль поддержки носителей iKey SafeNet;
- cesaris_arl.dll модуль поддержки носителей Algorithmic Research;
- cesaristsp.dll СОМ-объект для работы с TimeStamp;
- cesariscfg.cpl элемент панели управления Windows.

Криптопровайдер подписан цифровой подписью компании Microsoft, а указанные библиотеки регистрируются в операционной системе (OC) Windows пользователя.

В состав инсталляционного пакета Криптопровайдера также входит утилита работы с носителями ключевой информации «Менеджер PKCS#11» описанная в п.3.1.

Операционные системы

CESARIS CSP функционирует в следующих операционных системах:

- Windows 2000;
- Windows XP;
- Windows Server 2003.

2. Инсталляция криптопровайдера

Для установки криптопровайдера пользователь должен иметь **права** администратора на компьютере.

1. Запустить инсталляционный пакет (рис.2-1) и выбрать язык общения при инсталляции.

2. Выбрать тип установки и рабочий каталог.

Тип *"Стандартная"* предусматривает инсталляцию на компьютер пяти криптопровайдеров (ГОСТ 34.310-95 и ДСТУ 4145-2002), модулей РКСЅ#11, поддержку файлового носителя ключей, а также документации.

ид установ	зки		Same 1
Выберите н	аиболее подходящий і	вид установки.	
Выберите в	ид установки.		
• Стандар	лная		
1 ³	Будут установлены в файлового хранилии	зсе компоненты криптопрова ца ключей.	йдера с поддержкой
С <u>В</u> ыборо	чная		
1 ⁴	Выберите компон установить. Расс	ченты криптопровайдера, кот читана на опытных пользоват	орые необходимо гелей.
— Конечная	папка		
C:\\AME	3 Software\CESARIS C	SP	О <u>б</u> зор
IIShield —			
			0

Рис.2-1

3. В случае необходимости дополнительно установить (или исключить) компоненты выберите тип установки *"Выборочная"*. При этом вы сможете добавить поддержку работы с другими доступными носителями ключей. Также в рабочий каталог записываются примеры использования криптопровайдера на языке С.

ид установки Выберите наиболее подходящий вид установки.	Выберите компонентов Выберите компоненты для установки.
Выберите вид установки. Стандартная Будут установлены все компоненты криптопровайдера с поддержкой файлового хранилища ключей. Выберите компоненты криптопровайдера, которые необходимо установить. Рассчитана на опытных пользователей.	Выберите компоненты для установки и снимите Флажок рядом с теми компонентам которые не нужно устанавливать.
Конечная папка	
C.\\AMB Software\CESARIS CSP	Требуется 6,96 MB пространства на диске С Свободно 162585,49 MB пространства на диске С ГеогиПский

Рис.2-2

4. После установки компонентов появится запрос (рис.2-3) создать новый файловый носитель на диске (если его поддержка устанавливалась). Вы можете отказаться, если такой уже создан.

Настройка носителя
Вами установлена поддержка файлового носителя ключей. Для дальнейшей работы с ним необходимо:
🔽 создать файловый носитель
Выберите необходимые действия.

Рис.2-3

5. Запускается утилита настройки криптопровайдера.

Конфигурация ЦЕЗА	РИС	×
Файловый носитель	Работа с ключами Протокол работы Инфор	иация
Каталог хранилища н	лючей	
C:\Documents and S	ettings\TestUsjer\	<u>0</u>
1 - кол	чество слотов	
	🗸 ОК 🗙 Отмена Применить	

Рис.2-4

Настройка файлового носителя (рис.2-4) заключается в выборе каталога, где будут размещаться ключевые файлы token*.dat, и их количества (количества слотов). По умолчанию, установлен рабочий каталог текущего пользователя и один слот.

Имя каталога сохраняется в ключах реестра:

- HKEY_CURRENT_USER\Software\ABM Software\CESARIS CSP\PKCS11\ Providers\StoreDir;
- HKEY_LOCAL_MACHINE\ Software\ ABM Software\CESARIS CSP \PKCS11\Providers\StoreDir.

Количество файлов (слотов) сохраняется в ключе реестра:

- HKEY_LOCAL_MACHINE\ Software\ ABM Software\CESARIS CSP \PKCS11\Providers\ FileSlots.

🚮 Редактор реестра			
Файл Правка Вид Избранное 🤇	правка		
📃 🕀 🧰 ahead	▲ Имя	Тип	Значение
🕀 🧰 Aladdin	🛃 (По ум	D REG_SZ	(значение не присвоено)
🕀 🛄 AMB Group	8 FileSlot	s REG_DWORD	0×00000001 (1)
📄 🧰 AMB Software	Provide	r0 REG_SZ	C:\Program Files\AMB Software\CESARIS CSP\Pr
E CESARIS CSP	StoreD	r REG SZ	C:\Documents and Settings\TestUser\
E-E PKCS11	Virtual	REG_SZ	C:\Program Files\AMB Software\CESARIS CSP\Pi
🗄 💼 Analog Devices 🖉			
🕀 🧰 Andrea Electronics			
🕀 🧰 Ashmanov & Partners			
庄 🧰 ASUS			
🕀 🧰 Audible			
😥 🧰 BCL Technologies			
😟 💼 🛅 Borland			
🕀 🧰 Bumble-Bee Software			
😟 🧰 C07ft5Y			
庄 🧰 Classes			
庄 🧰 Clients			
😥 🛅 Codec tweak Tool			
🕀 🦳 Crystal Decisions			
Мой компьютер\HKEY_LOCAL_MACHIN	E\SOFTWARE\A	MB Software\CESAR	RIS CSP\PKCS11\Providers //

В случае установки на сервер необходимо выбрать каталог, доступный для чтения-записи серверному процессу.

Кроме настройки файлового носителя утилита позволяет:

• установить временную задержку запроса пароля ключа (рис.2-5).



Рис.2-5

• включить/отключить протоколирование (рис.2-6). Этот режим рекомендуется только на стадии отладки программного обеспечения.



Рис.2-6

просмотреть список установленных криптопровайдеров (рис.2-7)

Конфигурация ЦЕЗА	РИС			×
Файловый носитель	Работа с ключами	Протокол работы	Информация	
На Вашем компьютер	е установлены след	ующие CESARIS-CSI	P	3
CESARIS DSTU 4145-2 CESARIS DSTU 4145-2 CESARIS DSTU 4145-2 CESARIS DSTU 4145-2 CESARIS GOST 34.310	2002(ONB) and ECDH 2002(ONB) and RSA (2002(PB) and ECDH (2002(PB) and RSA Cry 1-95 and RSA Cryptog	I Cryptographic Provide Cryptographic Provider Cryptographic Provider yptographic Provider raphic Provider	er	
[🗸 ОК 🔰	Отмена Прим	енить	

Рис.2-7

6. Если вы выбрали опцию создания файлового носителя (рис.2-3), после настройки криптопровайдера запустится соответствующая утилита (рис.2-8)



Рис.2-8

При создании файлового носителя необходимо выбрать метку носителя, а также установить собственный пароль для работы с ключами.

По умолчанию выбирается имя текущего пользователя. Можно изменить значение метки на любое другое, но не более 32 символов.

Если хотите установить свой пароль сразу после создания файлового носителя, необходимо выбрать опцию "заменить пароль немедленно".

После нажатия кнопки "Создать" проверяется наличие в каталоге раннее созданного файла. При этом выдается предупреждение, что файл уже существует, и запрос подтвердить (или отказаться от процедуры) создания нового файла (рис.2-9).



Рис.2-9

В случае подтверждения будет создан файл с начальным паролем "12345678" и появится запрос ввода нового пароля (ПИНа) (рис.2-10).

Введите но	овый PIN
Пароль	******
Повторно	******
	OK Cancel

Рис.2-10

<u>Ограничения:</u> Длина пароля от 6 до 255 символов.

Пароль не должен содержать двух одинаковых символов подряд или три одинаковых символа во всей строке. Также не допускается использование последовательностей клавиш раскладки клавиатуры для составления пароля (типа - qwerty).

В случае ошибки во время смены пароля файл останется с начальным паролем "12345678".

7. Провайдер готов к работе.

3. Использование утилит

В комплект инсталляционного пакета криптопровайдера входят утилиты для создания файлового носителя (токена) и работы с объектами на подключенных устройствах, поддерживающих API-интерфейс PKCS#11.

Работа с утилитой создания файлового носителя описана в разделе 2.

3.1. Менеджер РКСЅ#11

Менеджер используется для инициализации носителей (токенов), смены паролей и просмотра/удаления объектов. Описание интерфейса PKCS#11 дано в [2]. Общий вид окна утилиты показан на рисунке 3-1.

Менеджер объектов РКС5#11	6	
Cryptoki Cryptoki Cryptoki DefaultName Mechanisms Session [15] - RW - User Logged Tac7495d-a888-487f-987e-22eb Tac7495d-a888-487f-987e-22eb Tac7495d-a888-487f-987e-22eb	Слот Токен Сесси 76740/56-sign-805-cert [1002] 76740/56-sign-805-fname [1003]	Хеш Я Объекты
 ✓ 7ac7495d-a888-487f-987e-22eb ✓ 7ac7495d-a888-487f-987e-22eb ✓ 7ac7495d-a888-487f-987e-22eb ✓ 9eb8183b-b299-4de6-ae09-e80- ✓ 9eb8183b-b299-4de6-ae09-e80- 	76740/56-sign-805-pri [1] 76740/56-sign-805-pub [1001] 4dbaf0844-keyx-805-cert [1005] 4dbaf0844-keyx-805-fname [1006]	Режим просмотра слото с токенами
 Geb8183b-b299-4de6-ae09-e80- Geb8183b-b299-4de6-ae09-e80- Geb8183b-b299-4de6-ae09-e80- 	4dbaf0844-keyx-805-pri [2] 4dbaf0844-keyx-805-pub [1004]	только активные

Рис.3-1

Каждый узел дерева имеет собственное меню, которое соответствует перечню функций интерфейса PKCS#11 для данного класса.

В качестве примера на рисунке 3-2 показано меню сессии.

Cryptoki		Хеш
Mechanisms Session [15] - F	Close Session (Закрьть текущую сесиию)	
	Login (Вход с паролем) Logout (Выход)	-
	Init User PIN (Устансвка начального пароля) Set PIN (Смена пароля)	
	Objects •	🔽 только активные
	Get Session Info	

Рис.3-2

3.1.1. Инициализация токена

Инициализация токена производится:

- во время создания нового файла ключей (для неактивного слота меню "Создать токен");
- при необходимости очистить данные и пароли в существующем токене.

Процедура выполняется в 2 этапа:

<u>1 этап</u>	инициализа администра	ция токена тора (Security (с уст Officer, SO	ановкой	пароля
<u>2 этап</u>	установка пользовател	начального ля (User).	пароля	доступа	для

Для инициализации токена необходимо выполнить пункт меню активного токена "*Init Token*" или пункт меню неактивного слота "*Create Token*". При этом вводится метка токена (до 32 символов) и пароль администратора (SO PIN).

Для установки начального пароля пользователя необходимо двойным щелчком (или через меню токена "Open RW-session") открыть RW-сессию (Read-Write, для чтения и записи) и выполнить пункт меню сессии "Init User PIN". При этом вводится пароль администратора и новый пароль пользователя.

3.1.2. Аутентификация (login)

При открытии дерева объектов пользователь получает доступ на просмотр и удаление общедоступных (public) объектов. При этом сессия содержит надпись "Not logged" и иконку красного цвета.

Для получения доступа к приватным объектам необходимо выполнить пункт меню сессии "Login", выбрать тип пользователя и ввести пароль. После успешной проверки пароля сессия будет содержать надпись "USER logged" ("SO logged") и иконку зеленого цвета.

В случае аутентификации в качестве SO доступ к приватным объектам будет заблокирован. Данный тип пользователя необходим только для проведения начальной установки пароля пользователя.

3.1.3. Смена пароля доступа

Для смены пароля необходимо провести аутентификацию ("Login") и выполнить пункт меню сессии "Set PIN".

3.1.4. Просмотр свойств объектов

Просмотр свойств объекта производится с помощью двойного щелчка мышкой или через меню объекта (рис. 3-3).

Окно свойств (атрибутов, ATTRIBUTES) объекта показывает заголовок, размер объекта и общие атрибуты для всех объектов PKCS#11:

- CKA_CLASS класс объекта;
- CKA_LABEL метка объекта
- СКА_ТОКЕN признак того, что объект сохранен на токене (не сессионный);
- CKA_PRIVATE доступ к объекту только после аутентификации;
- СКА_MODIFIABLE разрешение модификации объекта.

	Заголовок	1005	Размер	1494	
Класс	CKO_CERT	IFICATE			
Метка	9eb8183b-b299-4de6-ae09-e804dbaf0844-keyx-805-cert				
🔽 СК.	A_TOKEN		ATE 🔽 CK	A_MODIFIABLE	
CK.	A_TOKEN		ATE 🔽 CK	A_MODIFIA	

Рис.3-3

Для объектов типа СЕРТИФИКАТ (СКО_CERTIFICATE¹) в меню есть дополнительный пункт "*View X.509 certificate*" (рис.3-4) для просмотра содержания сертификата средствами ОС Windows.

■ View (Просмотр) View X.509 certificate (просмотр сертификата) SecondaryAuth (сменить пароль ключа)			
Copy object (копировать объект)			
🗙 Destroy objects (удалить объекты)			

рис.3-4

3.1.5. Копирование объектов

Копирование выполняется только для объектов типа СКО_DATA с помощью пункта меню "Copy object" (рис.3-4).

После этого объект можно вставить на любой токен, выполнив пункт меню сессии "Objects/Insert object".

3.1.6. Удаление объектов

Удаление одного или нескольких объектов выполняется с помощью пункта меню "Destroy objects" (рис.3-4) или кнопкой Del.

Возможно удаление сразу нескольких выделенных в дереве объектов.

3.1.7. Дублирование ключей и сертификатов

Дублирование ключей предназначено для обеспечения возможности возобновления работы с ключами в случае утери оригиналов вследствие выхода из строя носителя или оборудования, за исключением случаев компрометации ключей. Дублирование ключей предусмотрено службой дублирования ключей ЦСК и является обязательной процедурой для ключей Центра сертификации в соответствии с Общим описанием ЦСК и Инструкциями по обращению с ключевыми данными.

¹ типы объектов согласно PKCS#11

Копии ключей создаются в защищенном виде по стандарту PKCS#12 на контролируемых носителях. Экспорт и импорт сертификатов а также, при необходимости, персональных ключей и других связанных объектов (открытый ключ, дружественное имя) на резервные носители выполняется средствами утилиты «Менеджер PKCS#11».

1) Экспорт сертификатов и ключей из хранилища операционной системы Windows.

Выполняется стандартными средствами ВЕБ-броузера, который поддерживает работу с сертификатами формата X.509, например Internet Explorer версий 5 и старше по пути: Tools-> Internet options-> Contetnt-> Certificates, кнопкой «Экспорт» на выбранном сертификате:

Сертификаты					
Назначение:	<bce< th=""><th>></th><th></th><th></th><th>~</th></bce<>	>			~
Личные Другие пользователи Промежуточные центры сертификации Доверенны 🆘					
Кому выдан		Кем выдан	Срок де	Понятное имя	~
🔛 Бєлов Сергій Ва	але але	ЦСК 'Інтер-Метл' Ц CA Inter-Metl CESARI	27.01.2011 03.02.2010	DSTU(PB)_sign AMB-RSA-new	
Бєлов Сергій Ва Бєлов Сергій Ва Іванов Іван Іва	але але	CA Inter-Metl CESARI CA Inter-Metl CESARI	19.02.2010 28.05.2010 02.12.2009	RSA-new_cert RSA-sign-tst Setun 1	
🔤 Іванов Іван Іва	но	test-carsa	05.10.2010	stf1	
Сидоров Іван Пит		CA RSA	02.12.2009	Setup 2	
Сорос Семен Се	эме	test-ca rsa	05.10.2010	str4-AdmCert	
<u>Импорт</u>	порт	. Удалить		Дополнитель	но
<bce></bce>				Просмо	тр
				Закр	ыть

Рис.3.5

Далее следует выполнить действия, предложенные «Мастером экспорта сертификатов».

Экспорт сертификата происходит в любой заданный файл без пароля, для экспорта сертификата вместе с персональным ключом

Мастер экспорта сертификатов	×
Экспортирование закрытого ключа	
Можно произвести экспорт закрытого ключа вместе с сертификатом.	
Закрытые ключи защищены паролем. Если вы хотите произвести экспорт закрытого ключа вместе с сертификатом, необходимо указать пароль в последующих диалоговых окнах.	
Экспортировать закрытый ключ вместе с сертификатом?	
Да, экспортировать закрытый ключ	
ОН <u>е</u> т, не экспортировать закрытый ключ	
)
<hr/> <u>Назад</u> алее > Отмена	

Рис.3.6

лицо - владелец сертификата обязательно задает пароль (не менее 6 символов) и результирующий файл (.pfx) будет зашифрован на этом пароле (рис. 3.7-1 ? 3.7-3):

Формат экспортируемого файла Сертификаты могут быть экспортированы в различных форматах. Выберите формат файла сертификата: Файлы в DER-кодировке X.509 (.CER) Файлы в Base64-кодировке X.509 (.CER) Файлы в Base64-кодировке X.509 (.CER) Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
Выберите формат файла сертификата: Файлы в DER-кодировке X.509 (.CER) Файлы в Base64-кодировке X.509 (.CER) Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
 Файлы в DER-кодировке X.509 (.CER) Файлы в Base64-кодировке X.509 (.CER) Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
 Файлы в Base64-кодировке X.509 (.CER) Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
 Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b) Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
 Включить по возможности все сертификаты в путь сертификата Файл обмена личной информацией - PKCS #12 (.PFX) Включить по возможности все сертификаты в путь сертификата
• Файл обмена личной информацией - PKCS #12 (.PFX) • Включить по возможности все сертификаты в путь сертификата
Включить по возможности все сертификаты в путь сертификата —
Включить усиленную защиту (требуется IE 5.0, NT 4.0 SP4 или выше)
🔲 Удалить закрытый ключ после успешного экспорта
< <u>Н</u> азад Далее > Отмена

Рис.3.7-1

Мастер экспорта сертификатов
Пароль Для обеспечения безопасности следует защитить закрытый ключ паролем.
Введите и пароль и подтверждение.
<u>пароль:</u> ******
Годтверждение:

< <u>Н</u> азад Далее > Отмена
Рис.3.7-2

Мастер экспорта сертификатов	
Имя файла экспорта Укажите имя экспортируемого файла	
Имя фа <u>й</u> ла:	06300
	< <u>Н</u> азад Далее > Отмена
	Duo 272

Рис.3.7-3

В дальнейшем для использования экспортированного сертификата и личного ключа необходимые данные устанавливаются на компьютер из полученного файла формата PKCS#12 с расширением .PFX с помощью того же «Мастера экспорта сертификатов».

2) Экспорт сертификатов и ключей с одной смарт-карточки на другую

Для экспорта сертификата из защищенного носителя, которым является смарткарта или файловый токен, на другой носитель (смарт-карту, файловый токен), необходимо в окне менеджера PKCS#11 (далее - менеджер), который входит в состав инсталляции криптопровайдера, выделить необходимый для экспорта элемент сертификат и нажать на нем правой клавишей мыши и далее в контекстном меню выбрать пункт "Export to SIM":

ил онд		
Cryptoki Imartyn <	024] 560] 7024] 7024] 7024] 31488] 62560] 3168] 3828096] 3168] 93632] 4704] 93632] 4704] 304-pub [14090240] 3056] 2880] 3056] 2880]	Хеш
Mechanisms		
Session [2] - RW - User Logged		

Рис.3.8

Примечание: для выполнения экспорта оба носителя должны быть включены и выполнен вход по доступу к ним с использованием соответствующего персонального пароля (см. далее).

После чего будет предложено выбрать смарт-карту, на которую будет скопирована ключевая информация (карта-приемник должна быть установлена в другом ридере смарт-карточек):



Рис.3.9

После нажатия «Ок» выполняется экспорт ключевой информации и в результате вместе с сертификатом будут экспортированы все связанные с ним объекты (public key, private key, friendly name).

В том случае, если для смарт-карты, которая является первичным источником (носителем) ключевой информации, не был выполнен вход с паролем, экспорт персонального ключа будет невозможен, о чем пользователь будет предупрежден:



Если при этом выбрать «Да», то будут экспортированы все объекты, связанные с выбранным сертификатом, кроме персонального ключа, при выборе «Нет» - экспорт не будет выполняться.

Если пользователь выполнил вход с паролем на носитель, который является «источником», а для носителя-«приемника» выполнен вход без пароля, то для продолжения экспорта будет выведено приглашение ввести пароль доступа к смарт-карте приемника:



Необходимо выбрать «обычный пользователь». Для входа с правами «администратор» необходимо знать административный пароль смарт-карточки.

Токен: А	uthentIC Sm	art Card	
Введите Р	ขท		
1			
	OK	Cancel	
	Рис	.3.12	

После ввода правильного пароля выделенный сертификат и все его объекты будут экспортированы на новый носитель.

Менеджер объектов РКСЅ#11		
Файл Вид		
💫 (05) Rainbow Technologies iKeyVirtualReader 0	~	
a martyn		Хеш
- 🖑 Mechanisms		
O2fd0985-1f4f-4a21-95aa-4a962e3a2a6b [5505024]		
🔶 💁 02fd0985-1f4f-4a21-95aa-4a962e3a2a6b [5570560]		
🔤 0575b34c-63e4-462f-b748-3122c8cd1e6c-keyx-805-cert [13565952]		
🔶 0575b34c-63e4-462f-b748-3122c8cd1e6c-keyx-805-pri [13697024]		
↔ 0575b34c-63e4-462f-b748-3122c8cd1e6c-keyx-805-pub [13631488]		
🔤 14fab24d-5659-4bc0-9591-331bc7cc3bbc-sign-805-cert [13762560]		
14fab24d-5659-4bc0-9591-331bc7cc3bbc-sign-805-fname [13828096]		
🗛 14fab24d-5659-4bc0-9591-331bc7cc3bbc-sign-805-pub [13893632]		
🔤 1572e8fe-eebe-d70a-e253-37f12b27d4c2-sign-804-cert [14024704]		
🛶 1572e8fe-eebe-d70a-e253-37f12b27d4c2-sign-804-pri [14155776]		
😽 1572e8fe-eebe-d70a-e253-37f12b27d4c2-sign-804-pub [14090240]		
🔤 cad59da0-8b31-40a0-91ae-ed792da0a5/6 (4653056)		
😽 cad59da0-8b31-40a0-91ae-ed792da0a5/6 (5242880)		
🔶 f33cf23d-f8cf-4589-b67c-591a398eee3d [4980736]		
🔤 f33cf23d-f8cf-4589-b67c-591a398eee3d [5046272]		
😽 f33cf23d-f8cf-4589-b67c-591a398eee3d [5111808]		
💫 [25] OMNIKEY CardMan 3x21 0		
AuthentIC Smart Card		
- 🖑 Mechanisms		
Session [2] - RW - User Logged		
🔤 0575b34c-63e4-462f-b748-3122c8cd1e6c-keyx-805-cert [12]		
🛶 0575b34c-63e4-462f-b748-3122c8cd1e6c-keyx-805-pri [14]		
🔤 Сидоров Иван Иванович from AM-Alex CA RSA [1]	~	🔽 только активные
		1.

Рис.3.13

Если при выполнении экспорта менеджер обнаружит, что объект с таким идентификатором-меткой уже существует на приемнике, будет выведено предупреждение:



Рис.3.14

Если выбор «Да» - импорт такого объекта, дубликат которого уже существует на носителе, будет пропущен и будет выполнен импорт оставшихся объектов. Если будет далее снова найден дубликат, будет выведено такое же окно. Для того, чтобы избежать появления этого диалогового окна, необходимо выбрать «Да для всех», в этом случае все найденные дубликаты будут игнорироваться без появления диалогового окна. Выбор кнопки «Нет» останавливает импорт.

Аналогично вышеуказанному описанию дублирования ключевой иінформации со смарт-карточки на другую, выполняется дублирование из файлового токена на смарт-карточку и наоборот (пример на рис. 3.15):



Рис.3.15

Последующее использование полученного дубликата носителя ключевой информации регламентируется соответствующими Инструкциями и Регламентом ЦСК «Цезарис».

3.1.8. Соглашение по названиям (меткам) объектов

Криптопровайдер работает с виртуальными контейнерами ключей. Контейнер может содержать два типа ключевых пар: AT_SIGNATURE – для подписи, AT_KEYEXCHANGE – для обмена симметричными ключами шифрования.

Кроме того, в контейнер помещаются сертификаты соответствующих ключевых пар и объекты с дружественными именами сертификатов (friendly name)².

Для работы криптопровайдера метка объекта должна содержать:

- имя контейнера ключей как правило, в формате GUID;
- назначение контейнера ключей: "sign" – подпись;

"keyx" - распределение ключей.

AMB Group©

² если они указаны для соответствующих сертификатов

тип провайдера: •

"804" – ГОСТ 34.310-95 и RSA; "805" – ДСТУ 4145-2002 (полиномиальный базис) и RSA; "806" – ДСТУ 4145-2002 (полиномиальный базис) и ECDH; "807" – ДСТУ 4145-2002 (оптимальный нормальный базис) и RSA; "808" – ДСТУ 4145-2002 (оптимальный нормальный базис) и ЕСDH. тип объекта: "pri" – объекта СКО PRIVATEKEY, приватный ключ;

•

"pub" – объект СКО_PUBLICKEY, открытый ключ;

"cert" – объект СКО_СЕRТІГІСАТЕ, сертификат;

"fname" – объект СКО DATA, дружественное имя сертификата).

Рекомендуемая литература

- 1. А.Щербаков, А.Домашев "Прикладная криптография. Использование и синтез криптографических интерфейсов". Москва: Русская редакция, 2003.
- 2. RSA Laboratories. PKCS#11: Cryptographic Token Interface Standard.
- 3. ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хеширования".
- 4. ГОСТ 34.310-95 "Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма ";
- 5. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"
- 6. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".
- 7. RSA Laboratories. PKCS#1: RSA Cryptography Standard.