Инструкция по использованию

ПАК криптографической защиты информации «Рутокен CSP»



ЖТЯИ.00071-01 90 01

© ООО "Крипто-Про", 2000-2009. Все права защищены.

Авторские права на средство криптографической защиты информации Рутокен CSP и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Документ входит в комплект поставки программного обеспечения СКЗИ Рутокен CSP, на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "КРИПТО-ПРО" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

АННОТАЦИЯ

Настоящий документ содержит описание программно-аппаратного комплекса криптографической защиты информации «Рутокен CSP» (СКЗИ «Рутокен CSP»), предназначенного для защиты открытой информации в информационных системах общего пользования (вычисление и проверка электронной цифровой подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах.

Документ предназначен для пользователей как ознакомительный материал перед установкой и эксплуатацией СКЗИ «Рутокен CSP».

Информация о разработчике ПК «КриптоПро Рутокен CSP»:

ООО «Крипто-Про» 127 018, Москва, Улица Образцова, 38 Телефон: (495) 933 1168 Факс: (495) 933 1168 <u>http://www.CryptoPro.ru</u> E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Инст	алляция СКЗИ «Рутокен CSP»	5
1.1.	Установка дистрибутива СКЗИ Рутокен CSP	5
1.2. V	Изменение, исправление или удаление программы	8
2. Инте	рфейс СКЗИ «Рутокен CSP»	. 10
2.1. J	Доступ к панели управления СКЗИ «Рутокен CSP»	. 10
2.2. (Общая настройка СКЗИ	. 10
2.3. H	Настройка оборудования	. 10
2.4. F	Работа с контейнерами и сертификатами	. 11
2.4.1	. Копирование и удаление контейнера закрытого ключа	. 11
2.4.2	. Просмотр и установка личного сертификата, хранящегося в контейн закрытого ключа	iepe 14
2.4.3	. Установка личного сертификата, хранящегося в файле	. 19
2.5.	Управление паролями доступа к закрытым ключам	. 24
2.6.	Установка параметров безопасности	. 27
2.7. J	Дополнительные настройки	. 28
2.7.1	. Просмотр версий используемых файлов	. 29
2.7.2	. Установка времени ожидания ввода информации от пользователя	. 29
2.8.	Установка параметров криптографических алгоритмов	. 30
2.9. H	Настройка аутентификации в домене Windows	. 31
3. Инте	рфейс генерации ключей	. 33
3.1. (Создание ключевого контейнера	. 33
3.1.1	. Выбор ключевого носителя	. 33
3.1.2	р. Генерация начальной последовательности ДСЧ	. 33
3.1.3	. Ввод пароля на доступ к закрытому ключу	. 33
3.2. (Открытие ключевого контейнера	. 34
3.2.1	. Отсутствие ключевого носителя	. 34
3.2.2	р. Проверка пароля на доступ к закрытому ключу	. 34
3.3. I	енерация ключей и получение сертификата при помощи УЦ	. 36
4. Счет	чики и ограничения	. 39
5. Пере	ечень сокращений	. 40
6. Пере	ечень рисунков	. 41

1. Инсталляция СКЗИ «Рутокен CSP»

1.1. Установка дистрибутива СКЗИ Рутокен СЅР

Установка дистрибутива СКЗИ Рутокен СЅР должна производиться пользователем, имеющим права администратора.

Для установки программного обеспечения вставьте компакт-диск в дисковод. Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы и удобный для Вас язык установки. Запустите выполнение установки.

🗒 Установка "КриптоПро Рутокен CSP"				
	Вас приветствует программа установки "КриптоПро Рутокен СSP"			
	Программа выполнит установку "КриптоПро Рутокен CSP" на компьютер. Для продолжения нажмите кнопку "Далее".			
	ПРЕДУПРЕЖДЕНИЕ: Данная программа защищена законами об авторских правах и международными соглашениями.			
< Назад Далее > Отмена				

Рисунок 1. Приветственное окно мастера установки.

В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование СКЗИ Рутокен СSP. Если Вы согласны со всеми пунктами соглашения, выделите пункт «Я принимаю условия лицензионного соглашения», и нажмите **Далее** (см. Рисунок 2).

Рисунок 2. Лицензионное соглашение

😸 Установка "КриптоПро Рутокен CSP"				
Лицензионное соглашение				
Пожалуйста, внимательно прочтите следующее лицензионное соглашение.				
ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА				
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ				
1. Термины и определения				
 1.1. Настоящее Лицензионное соглашение является общей офертой между ООО "КРИПТО-ПРО" и Пользователем - физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения права на использование Изделия, в соответствии со ст. 433 ГК РФ имеет силу договора. 1.2. Под Изделием понимается программа/комплекс программ для ЭВМ, включая носители и документацию, авторские права на которые принадлежат ООО «КРИПТО- Г 				
 ⊙ Я принимаю условия лицензионного соглашения ○ Я не принимаю условия лицензионного соглашения 				
< Назад Далее > Отмена				

Для дальнейшей установки Рутокен CSP нажмите **Далее**. Следующим шагом необходимо ввести информацию о пользователе, производящем установку (см. Рисунок 3).

Рисунок 3. Сведения о пользователе.

🗒 Установка "КриптоПро Рутокен CSP"	
Сведения о пользователе	
Укажите сведения о себе.	
Пользователь:	
Иванов И.И.	
Организация:	
Рога и копыта	
< Назад Да	лее > Отмена

После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 4), в котором необходимо выбрать вид установки.

Рисунок 4. Вид установки

😸 Установка "КриптоПро Рутокен CSP"				
Вид установки				
Выбор наиболее подходящего вида установки.				
Выберите вид установки.				
• Обычная Будет установлен стандартный набор компонент.				
 Выборочная Выбор необходимых компонентов программы и папки, в которой они будут установлены. Рассчитана на опытных пользователей. 				
< Назад Далее > Отмена				

СКЗИ Рутокен CSP определяет два вида установки: обычная и выборочная. Если выбран вид установки «Обычная», то устанавливаются основные файлы для работы СКЗИ и компоненты для совместимости с продуктами Microsoft. По желанию можно не устанавливать дополнительные компоненты, в этом случае следует выбрать вид установки «Выборочная» (см. Рисунок 5).

Рисунок 5. Выборочная установка

🛃 Установка "КриптоПро Рутокен CSP"				
Выборочная установка				
Выберите компоненты программы, которые необходимо установить.				
Щелкните значок в списке ниже, чтобы изменить способ	установки компонента. Описание компонента Файлы, необходимые для работы продукта.			
Подсказка < Назад	Далее > Отмена			

Следующее окно мастера служит для подтверждения установки (см. Рисунок 6). При необходимости можно вернуться назад и переопределить параметры установки. Для подтверждения нажмите кнопку **Установить**.

😸 Установка "КриптоПро Рутокен CSP"
Последние приготовения к установке программы
Программа готова к началу установки.
Нажмите кнопку "Установить", чтобы начать установку.
Чтобы просмотреть или изменить параметры установки, нажмите кнопку "Назад". Нажмите кнопку "Отмена" для выхода из программы.
< Назад Установить Отмена

Рисунок 6. Окно подтверждения установки

После выполнения всех описанных шагов мастер устанавливает СКЗИ Рутокен CSP, сопровождая действия комментариями. По окончании установки мастер показывает окно с подтверждением успешной установки, где необходимо нажать кнопку **Готово**.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Рисунок 7. Окончание установки

😸 Сведения о программе установки "КриптоПро Рутоке 🔯				
٩	Для учета изменений в требуется перезагрузка чтобы перезагрузить ко чтобы выполнить перез	настройках КриптоПро Рутокен CSP системы. Нажмите кнопку "Да", мпьютер сейчас, либо кнопку "Нет", агрузку позже вручную.		
	Да	Нет		

1.2. Изменение, исправление или удаление программы

Если мастер установки обнаружит на машине уже установленную версию СКЗИ Рутокен CSP, то сразу после нажатия кнопки Далее в окне приветствия (см. Рисунок 1) появится соответствующая информация с предложением изменить набор установленных компонент, исправить ошибки или удалить Рутокен CSP (см. Рисунок 8).

😸 Установка "КриптоПро Рутокен CSP"				
Обслуживание программы				
Изменение, исправление или удаление программы.				
• Изменить	,			
	Изменение устанавливаемых компонентов программы. Появится			
	диалоговое окно "Выборочная установка", в котором можно изменить способ установки компонентов.			
🔿 Исправит	ь			
F	Исправление ошибок в программе. При выборе данного параметра исправляются отсутствующие или поврежденные файлы, ярлыки и записи реестра.			
⊖Удалить				
8	Удаление "КриптоПро Рутокен CSP".			
	< Назад Далее > Отмена			

Рисунок 8. Изменение, исправление или удаление программы

2. Интерфейс СКЗИ «Рутокен CSP»

2.1. Доступ к панели управления СКЗИ «Рутокен CSP»

Данный раздел является инструкцией по использованию панели управления программно-аппаратного комплекса криптографической защиты информации Рутокен CSP. Панель управления СКЗИ Рутокен CSP доступна из Панели управления Windows (меню Пуск **Э Панель** управления **Э Рутокен CSP**).

КриптоПро CSP для ruToken \mathbf{X} Дополнительно Алгоритмы Безопасность Winlogon Общие Оборудование Сервис КриптоПро CSP Версия ядра СКЗИ: 4.0.0055 КС1 Версия продукта: 3.6.5402 (С) Крипто-Про, 2000-2009, все права защищены Компания Крипто-Про Информация о лицензировании продуктов Крипто-Про теперь доступна через оснастку ММС "КриптоПро РКІ": ΚρиπτοΠρο ΡΚΙ Язык Выберите язык для отображения <Умолчание систег 🗸 окон CSP вашей учетной записи: Выберите язык для отображения окон Русский ¥ CSP пользователей, не задавших язык (умолчание системы): ΟК Отмена Применить

Рисунок 9. Панель управления Рутокен CSP

2.2. Общая настройка СКЗИ

Закладка **Общие** панели управления СКЗИ Рутокен СSP предназначена для просмотра информации о версии установленного ПАК СКЗИ Рутокен CSP и для изменения языка отображения окон, выдаваемых криптопровайдеров.

2.3. Настройка оборудования

Закладка **Оборудование** панели управления СКЗИ Рутокен CSP (см. Рисунок 10) предназначена для изменения набора устройств хранения и считывания ключевой информации и датчиков случайных чисел (ДСЧ).

Рисунок 10. Закладка «Оборудование» панели управления Рутокен CSP

КриптоПро CSP для ruToken					
Дополнительно	Дополнительно Алгоритмы Безопа		сть	Winlogon	
Общие	Оборудов	Оборудование		Сервис	
Считыватели закрытых ключей Позволяет добавить или удалить считыватели закрытых ключей.					
Датчики случайных чисел Позволяет добавить или удалить датчики случайных чисел. Настроить ДСЧ					
Типы ключевых н Позвол носите	Типы ключевых носителей Позволяет добавить или удалить типы ключевых носителей. Настроить типы носителей				
ОК Отмена Применить					

При установке СКЗИ Рутокен СЅР все необходимые считыватели, ключевые носители и датчики случайных чисел устанавливаются автоматически. Данная закладка предназначена для работы с совместимыми устройствами.

2.4. Работа с контейнерами и сертификатами

Закладка **Сервис** панели управления СКЗИ Рутокен СSP предназначена для выполнения следующих операций:

- Копирование и удаление закрытого ключа, находящегося в существующем контейнере;
- Просмотр и установка сертификатов, находящихся в существующем контейнере закрытого ключа на носителе;
- Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе;
- Изменение и удаление запомненных паролей (PIN-кодов) доступа к носителям закрытых ключей.

2.4.1. Копирование и удаление контейнера закрытого ключа

Контейнер закрытого ключа Рутокен CSP со смарткарты Магистра скопировать нельзя. Мастер копирования оставлен только для совместимых ключевых носителей. Для того, чтобы удалить контейнер, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Удалить контейнер**.

Рисунок 11. Закладка «Сервис» панели управления Рутокен CSP

цополнительно	Алгоритмы	Безопасн	ость	Winlogor
Общие	Оборудов	ание		Сервис
Контейнер закрыт Эти мастера позво закрытого ключа Скопировать ко	гого ключа оляют скопироват с носителя. нтейнер)	ь или удалит Удалить і	гь конте контейн	ейнер
Сертификаты в ки	нтейнере закрыт	000 KRK043		
в контейнере закрытого ключа, и установить их в хранилище сертификатов. Просмотреть сертификаты в контейнере Личный сертификат Этот мастер позволяет связать сертификат из файла с контейнером закрытого ключа, установив этот сертификат в				
Личный сертифик. Этот мастер позво контейнером закр	ат эляет связать сер ытого ключа, уст	тификат из ф ановив этот	райла с сертифі	икат в
Личный сертифик. Этот мастер позво контейнером закр хранилище.	ат оляет связать сер ытого ключа, уст	тификат из ф ановив этот	райла с сертифи	икат в
Личный сертифик Этот мастер позво контейнером закр хранилище.	ат оляет связать сер ытого ключа, уст Установить	тификат из ф ановив этот • личный сер	райла с сертифи гификат	икат в
Личный сертифик. Этот мастер позво контейнером закр хранилище. Пароли закрытых Эти мастера позво ключей или удали Изменить па	ат оляет связать сер ытого ключа, уст Установить ключей оляют измененить пь запомненные р роль Уд	тификат из ф ановив этот личный сер пароли (ПИн анее пароли цалить запом	райла с сертификат 1-коды) ненные	икат в г закрытых пароли

Система отобразит окно «Удаление контейнера закрытого ключа» (см. Рисунок 12).

Рисунок 12. Удаление контейнера закрытого ключа

Удаление контейнера закрытого ключа 🛛 🔀				
Контейнер закрытого ключа Введите или укажите контейнер закрыт удалить	ого ключа, который необходимо			
Имя ключевого контейнера: Введенное имя задает ключевой контейнер: Пользователя	Обзор По сертификату			
Компьютера Выберите CSP для поиска ключевых контейнер	ров:			
GOST R 34, 10-2001 Rutoken CSP				
	< Назад Готово Отмена			

В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Рисунок 13. Выбор ключевого контейнера для копирования

КриптоПро CSP для ruToken			
5. C	0:09:56		
выеер ключевого контеинера			
-В списке показывать:			
 Дружественные имена Уникальные имена 			
Список ключевых контейнеров пользователя:			
счит имя контейнера			
ФКН Директ 60046575-8870-4648-8800-01294130020	9		
ФКН Директ 98b59d58-83e7-45b8-863a-1836a5e46b	27		
ФКН Директ f548f9a6-3359-418c-8c0f-b2cb95682e9	0		
ОК От	мена		

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, контейнер которого необходимо удалить (см. Рисунок 14).

Рисунок 14. Выбор сертификата для удаления контейнера

Вы	юор сертифика	та			? 🗙
Выберите сертификат из хранилища "Личные" текущего пользователя.					
	Кому выдан	Кем выдан	Назначения	Понятное	Срок де
1	🕮 Клава Мышк	Test Cente	Проверка	Отсутствует	24.11.20
	🚟 Василий Пупкин	Test Cente	Проверка	Отсутствует	24.11.20
	(111	I		
	_				
		ок	Отмена	Просмотр серти	фиката



Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

Опция **Введенное имя задает ключевой контейнер** (см. Рисунок 12) может быть установлена в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически.

Опция **Выберите СSP для поиска ключевых контейнеров** (см. Рисунок 12) позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку Готово.

Система отобразит окно подтверждения удаления ключевого контейнера (см. Рисунок 15). Нажмите кнопку **Да.** СКЗИ «Магистра CSP» произведет удаление ключевого контейнера.

Рисунок 15. Окно подтверждения удаления ключевого контейнера

КриптоПро CSP для ruToken			
1	Сейчас будет произведено удаление всех закрытых ключей и сертификатов контейнера '727792b8-06af-4797-94ad-ffc4e9295e9a'. Контейнер перестанет существовать, восстановить ключи с этого контейнера будет невозможно. Продолжить?		
	Да Нет		

2.4.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа

Для того, чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Просмотреть сертификаты в контейнере**.

Система отобразит окно «Сертификаты в контейнере закрытого ключа» (см. Рисунок 16).

Рисунок 16. Сертификаты в контейнере закрытого ключа

Сертификаты в контейнере закрытого ключа			
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере			
Имя ключевого контейнера: Обзор Введенное имя задает ключевой контейнер: По сертификату По сертификату По сертификату Выберите CSP для поиска ключевых контейнеров: СОСТ. В. 24. 10-2001. Вытоков CSP.			
GOST R 34. 10-2001 Rutoken CSP			
< Назад Далее > Отмена			

В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, контейнер которого необходимо удалить (см. Рисунок 14).



Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

Опция **Введенное имя задает ключевой контейнер** может быть установлена в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически.

Опция **Выберите CSP для поиска ключевых контейнеров** позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Сертификат для просмотра» (см. Рисунок 17).



Если в контейнере закрытого ключа сертификат отсутствует, то будет отображено окно с соответствующей информацией.

В этом случае просмотр сертификата будет недоступен.

Сертификаты в контейнере закрытого ключа 🛛 🔀			
Сертификат для Просмотрите и	просмотра выберите сертификат		
Сертификат:	Василий Пупкин		
Субъект:	С=RU, CN=Василий Пупкин		
Поставщик:	E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPT(
Действителен с:	24 ноября 2009 г. 19:26:20		
Действителен по:	24 ноября 2010 г. 19:36:20		
Серийный номер:	3060 E617 0002 0000 39CD		
	Установить Свойства Обзор		
	< Назад Готово Отмена		

Рисунок 17. Окно «Сертификат для просмотра»

Для просмотра основных свойств сертификата нажмите кнопку **Свойства**. Система отобразит окно «Сертификат», со свойствами выбранного сертификата (см. Рисунок 18).

Рисунок 18. Окно просмотра свойств сертификата

Сертификат 🛛 🕄 🔀				
Общие Состав Путь сертификации				
Сведения о сертификате				
Этот сертификат предназначается для:				
 Подтверждает удаленному компьютеру идентификацию вашего компьютера 				
Кому выдан: Василий Пупкин				
Кем выдан: Test Center CRYPTO-PRO				
Действителен с 24.11.2009 по 24.11.2010				
Есть закрытый ключ, соответствующий этому сертификату.				
Установить сертификат Заявление поставщика				
ОК				

Если требуется установить сертификат, находящийся в контейнере, в хранилище сертификатов, то следует в окне просмотра свойств сертификата нажать на кнопку **Установить сертификат**. Будет запущен **Мастера импорта сертификатов** (см. Рисунок 19).

Рисунок 19. Мастер импорта сертификатов



Нажмите кнопку **Далее**. Система отобразит окно «Хранилище сертификатов», в котором необходимо указать, в какое хранилище требуется поместить сертификат (см. Рисунок 20).

Рисунок 20. Выбор хранилища

Мастер импорта сертификатов 🛛 🔀
Хранилище сертификатов
Хранилища сертификатов - это области системы в которых производится хранение сертификатов.
Выбор хранилища может быть произведен Windows автоматически, или же можно указать размещение сертификата вручную.
 Автоматически выбрать хранилище на основе типа сертификата
О Поместить все сертификаты в следующее хранилище
Хранилище сертификатов;
Обзор
·
< Назад Далее > Отмена

Установите переключатель **Автоматически выбрать хранилище на основе типа сертификата**, если Вы хотите, чтобы сертификат из контейнера закрытого ключа был установлен в хранилище «Личные» текущего пользователя. Так же есть возможность указать размещение сертификата вручную, для этого следует выбрать опцию **Поместить все сертификаты в следующее хранилище** и в появившемся окне выбрать нужное хранилище.

При необходимости установки сертификата в хранилище «Личные» локального компьютера следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Установить личный сертификат**.

После выполненных действий нажмите кнопку **Далее**. Система отобразит окно «Завершение работы мастера импорта сертификатов» (см. Рисунок 21).

<text><image><image>

Рисунок 21. Завершение мастера импорта сертификатов

Проверьте правильность выбранных параметров и нажмите кнопку **Готово.** Будет отображено окно, информирующее пользователя об успешной установке сертификата.

2.4.3. Установка личного сертификата, хранящегося в файле

Для того, чтобы связать личный сертификат, хранящийся в файле с контейнером закрытого ключа, установив сертификат в хранилище «Личные» следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Установить личный сертификат**.

Будет запущен Мастер установки личного сертификата (см. Рисунок 22). Ознакомьтесь с текстом и нажмите кнопку **Далее.**

Рисунок 22. Мастер установки личного сертификата



Система отобразит окно «Расположение файла сертификата» (см. Рисунок 23). В поле **Имя файла сертификата** укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее.**

Рисунок 23. Окно «Расположение файлов сертификата»

Мастер установки личного сертификата 🛛 🔀				
Расположение файла сертификата Введите или укажите расположение файла устанавливаемого сертификата				
Имя файла сертификата: Documents and Settings\Пользователь\Мои документы\123.cer Обзор				
Формат файла может одним из следующих: Файл сертификата - X.509 (.CERCRT) Сообщение стандарта PKCS #7 (.P7B,.P7M,.DER) Хранилище сериализованных сертификатов (.SST) Замечание: Некоторые форматы файлов могут содержать в одном файле более одного сертификата.				
< Назад Далее > Отмена				

Система перейдет к окну «Сертификат для установки» (см. Рисунок 24). В нем выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

Рисунок 24. Окно	«Сертификат	для	установки»
------------------	-------------	-----	------------

Мастер установки личного сертификата			
Сертификат для установки Просмотрите и выберите сертификат для установки			
Сертификат:	Василий Пупкин		
Субъект:	C=RU, CN=Василий Пупкин		
Поставщик:	E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPTO-		
Действителен с:	24 ноября 2009 г. 19:26:20		
Действителен по:	24 ноября 2010 г. 19:36:20		
Серийный номер:	3060 E617 0002 0000 39CD		
	Свойства		
	Обзор		
	< Назад Далее > Отмена		

Нажмите кнопку **Далее**. Система отобразит окно «Контейнер закрытого ключа» (см. Рисунок 25).

Рисунок 25. Окно «Контейнер закрытого ключа»

Мастер установки личного сертификата 🛛 🔀				
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа, который соответствует выбранному сертификату				
Имя ключевого контейнера:				
Обзор				
Введенное имя задает ключевой контейнер: Пользователя Компьютера				
Выберите CSP для поиска ключевых контейнеров:				
GOST R 34.10-2001 Rutoken CSP				
< Назад Далее > Отмена				

В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Опция «Введенное имя задает ключевой контейнер» может быть установлена в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер.

Опция «Выберите CSP для поиска ключевых контейнеров» позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Хранилище сертификатов» (см. Рисунок 26).

С помощью кнопки **Обзор** выберите хранилище «Личные». Сертификат будет установлен в хранилище «Личные» текущего пользователя или в хранилище «Личные» локального компьютера, в зависимости от значения переключателя опции «Введенное имя задает ключевой контейнер», заданной на предыдущем шаге. Изменить значение данной опции нельзя; оно определяется расположением контейнера закрытого ключа.

Мастер устан	ювки личного сертификата	\sim
Хранилище Укажите ранее се	е сертификатов эхранилище сертификатов для установки в него выбра ртификата.	отонна
	Выбор хранилища сертификата 🛛 🔹 🔀	
	Выберите хранилище сертификатов.	
Указанный ра компьютера ог	Личные Доверенные корневые центры сертиф	вателя или
Имя хранилищ Личные	Доверительные отношения в предпри Промежуточные центры сертификаци Доверенные издатели Сертификаты, к которым нет доверии	Обзор
	Показать физические хранилища	а сертификатов: аля а
Установить	ОК Отмена	
	< Назад Дале	е > Отмена

Рисунок 26. Окно «Хранилище сертификатов»

После выбора хранилища система отобразит окно «Завершение работы мастера установки личного сертификата» (см. Рисунок 27).

Рисунок 27. Завершение работы мастера установки личного сертификата

Мастер установки лично	го сертификата	$\overline{\mathbf{X}}$
	Завершение рабо установки личної Работа мастера установки завершена. Были указаны спедующие г	оты мастера го сертификата личного сертификата успешно параметры:
	Взять сертификат из файла имя сертификата субъект поставщик действителен с действителен по серийный номер Проставить ссылку на заклытый ключ Убедитесь, что выбраны пр нажмите кнопку "Готово" д	С:\Documents and Setting Василий Пупкин C=RU, CN=Василий Пуп E=info@cryptopro.ru, C=F 24 ноября 2009 г. 19:26: 24 ноября 2010 г. 19:36: 3060 E617 0002 0000 39 Шистоования равильные параметры и иля выполнения установки.
	< Назад	Готово Отмена

Проверьте правильность указанных данных и нажмите кнопку **Готово.** СКЗИ «Магистра CSP» произведет установку сертификата.

2.5. Управление паролями доступа к закрытым ключам

Для того чтобы изменить пароль на доступ к закрытому ключу, следует выбрать вкладку Сервис панели управления Рутокен CSP (см. Рисунок 11) и нажать на кнопку Изменить пароль.

Система отобразит окно «Изменение пароля контейнера закрытого ключа» (см. Рисунок 28).

Рисунок 28. Изменение пароля контейнера закрытого ключа

Изменение пароля контейнера закрытого ключа	
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа, на кото изменить пароль.	ром необходимо
Имя ключевого контейнера: Введенное имя задает ключевой контейнер: Пользователя Компьютера Выберите CSP для поиска ключевых контейнеров: GOST R 34 10-2001 Rutoken CSP 	Обзор По сертификату
GOST R 54, 10-2001 Rutoken CSP	
< Назад	отово Отмена

В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка посредством нажатия кнопки **Обзор.**

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, на доступ к контейнеру закрытого ключа которого необходимо изменить пароль.

Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

Опция **Введенное имя задает ключевой контейнер** может быть установлена в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически.

Опция **Выберите CSP для поиска ключевых контейнеров** позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку **Готово**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его (см. Рисунок 29). Введите пароль и нажмите кнопку **ОК**. Если пароль введен неверно, система попросит повторно ввести пароль.

В СКЗИ Рутокен CSP установлено ограничение числа попыток ввода пароля. Превышение этого числа приведет к блокированию контейнера (см. раздел 4).

КриптоПро CSP	для ruToken		\mathbf{X}
£	0:09:56 Type password and friendly name for container		
Контейнер Имя: 98b59d58-83e	7-45b8-863a-1836	a5e46b27	
Дружественно RU, Клава Мы	е имя: шкина		
			EN
	Пароль:		
 Ограничения — 			
Ост	алось попыток:	2	
Осталось	попыток (CSP):	3	
Счетчин	с ошибок (ФКН):	97	
Счетчик посл	. ошибок (ФКН):	2	
	Счетчик ЕКЕ:	9999960	
	Счетчик Д-Х:	1000000	
Сче	тчик подписей:	9999999	
	ок	Отмена	

Система отобразит окно ввода нового пароля на доступ к закрытому ключу (см. Рисунок 30). Введите дважды новый пароль и нажмите кнопку **ОК**.

КриптоПро CSP для ruToken			
Type password a for container	Type password and friendly name for container		
Контейнер Имя: 98b59d58-83e7-45b8-863a-1836	5a5e46b27		
Дружественное имя:			
RU, Клава Мышкина			
	EN		
Новый пароль:	•••••		
Подтверждение: [•••••		
Счетчик ошибок (ФКН):	97		
Счетчик посл. ошибок (ФКН):	2		
Счетчик ЕКЕ:	9999960		
Счетчик Д-Х:	1000000		
Счетчик подписей:	9999999		
ОК	Отмена		

Рисунок 30. Ввод нового пароля на доступ к закрытому ключу

После ввода пароля СКЗИ «Рутокен CSP» осуществит смену пароля на доступ к закрытому ключу.

СКЗИ «Рутокен CSP» позволяет удалить запомненные пароли доступа к контейнерам закрытых ключей и информацию об использованных съемных носителях.

Для того чтобы удалить запомненный пароль, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать на кнопку **Удалить запомненные пароли.**

Система отобразит окно «Удаление запомненных паролей» (см. Рисунок 31).

Рисунок 31. Окно «Удаление запомненных паролей»

Удаление запомненных	х паролей 🛛 🔀
Удалить все запомненные п	ароли закрытых ключей:
Пользователя	
Компьютера	
Удалить информацию об ис	пользованных съемных носителях:
Пользователя	
Компьютера	
	ОК Отмена

В этом окне установите флаги **Пользователя/Компьютера** для удаления сохраненных паролей и нажмите кнопку **ОК**. Если сохраненных паролей нет, то соответствующая область будет затемнена.

СКЗИ «Рутокен CSP» осуществит удаление сохраненных паролей только из специального хранилища на локальном компьютере, пароль на доступ к закрытому ключу не удаляется.

Кроме того, в этом же окне можно отдельно удалить информацию о физических характеристиках носителей, на которых расположены ключевые контейнеры, использовавшиеся раньше на данном компьютере. Это полезно, если ключевой контейнер на новом носителе имеет то же имя, что один из ранее использовавшихся на данном компьютере контейнеров.

2.6. Установка параметров безопасности

Закладка **Безопасность** (см. Рисунок 32) панели управления СКЗИ Рутокен CSP предназначена для выбора параметров безопасности при работе с СКЗИ «Рутокен CSP».

Рисунок 32. Закладка «Безопасность» панели управления СКЗИ Рутокен CSP

oomne	Оборудов	зание	Сервис
ополнительно	Алгоритмы	Безопасность	Winlogor
Назначенные по у	молчанию CSP дл	я указанных типов	
GOST R 34. 10-200	1 Signature with Di	ffie-Hellman Key Exc	hange:
GOST R 34, 10-20	01 Rutoken CSP		~
	the second second		FI TOT
Режим работы CSP			
ОИспользовать	службу хранения	ключей	
О Хранить ключ	и в памяти прилож	кений	
0.152.010.000			
Настройки кэширо	вания закрытых і	ключей	
Выберите CSP для	я настройки:		_
	1 Rutoken CSP		×
GOST R 34.10-200			
GOST R 34.10-200	ирование	Размер кэша:	8
GOST R 34.10-200	ирование	Размер кэша:	8
GOST R 34.10-200	ирование	Размер кэша:	8
GOST R 34.10-200	ирование	Размер кэша:	8

В данном окне можно назначить криптопровайдер, используемый по умолчанию.

В СКЗИ «Рутокен CSP» хранение ключей (в памяти приложений и в службе хранения ключей) запрещено, все ключи хранятся только на ключевых носителях. Также в СКЗИ «Рутокен CSP» не используется кэширование контейнеров закрытых ключей - ключи не покидают пределов носителя.

2.7. Дополнительные настройки

Закладка **Дополнительно** (см. Рисунок 33) панели управления СКЗИ Рутокен СSP предназначена для выбора параметров безопасности при работе с СКЗИ «Рутокен CSP».

- просмотра версий и путей размещения используемых СКЗИ «Рутокен CSP» файлов;
- установки времени ожидания ввода информации от пользователя.

Рисунок 33. Закладка «Дополнительно» панели управления СКЗИ Рутокен CSP

	Оборудов	зание Сервис
ополнительно	Алгоритмы	Безопасность Winlog
Версии файлов —		
А вий	Версия	Т Путь
accord.dll	3.6.4246.0	x86 C:\Program Files\Cry
advapi32.dll	5.1.2600.5755	x86 C:\WINDOWS\system
bio.dll	3.6.4292.0	x86 C:\Program Files\Cry
charismathics.dll	4.8.0.1	x86 C:\Program Files\Cry
cpadvai.dll	3.6.4515.0	x86 C:\Program Files\Cry
cpcertocm.dll	3.6.4264.0	x86 C:\Program Files\Cry
cpconfig_rcsp.cpl	3.6.4604.0	x86 C:\Program Files\Cry
<	0 2 X001 A	VOE Cultrearen EileelOr
	Скопир	оовать в буфер обмена
Время ожидания в Во время работы К диалоговые окна,	вода риптоПро CSP на требующие ввод	экране могут быть показаны а информации от
пользователя.		
	оить интервал вр будут закрыты, і	ремени, по завершению как будто пользователь
здесь можно настр которого эти окна нажал на кнопку "(Отмена".	

2.7.1. Просмотр версий используемых файлов

Для того чтобы удалить запомненный пароль, следует выбрать вкладку **Дополнительно** панели управления Рутокен CSP (см. Рисунок 33). В области **Версии файлов** в табличной форме представлена информация о версиях и путях размещения использующихся СКЗИ «Рутокен CSP» файлов.

Нажатие на кнопку Скопировать в буфер обмена приведет к сохранению данной информации в буфер обмена.

2.7.2. Установка времени ожидания ввода информации от пользователя

Во время работы СКЗИ «Рутокен CSP» на экране могут появляться диалоговые окна, требующие ввода пользователем определенных данных (например, ввод пароля на доступ к закрытому ключу).

Для того чтобы установить интервал времени, по завершении которого эти окна будут автоматически закрыты (действие, эквивалентное нажатию пользователем кнопки **Отмена**), следует выбрать вкладку **Дополнительно** панели управления Рутокен CSP (см. Рисунок 33)и нажать на кнопку **Установить время ожидания ввода.**

Система отобразит окно «Интервал времени ожидания ввода» (см. Рисунок 34). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умол**чанию для всего компьютера.

Рисунок 34. Окно «Интервал времени ожидания ввода»

Интервал времени ожидания ввода 🛛 🛛 👔			
Введите интервал времени ожидания ввода пользователя в диалоговых окнах КриптоПро CSP в секундах:			
СЗначение пользователя:	1		
• Использовать системное значение по умолчанию			
О Установить бесконечное ожидание			
○ Установить интервал: 600 🛟 секунд			
Значение по умолчанию для всего компьютера:	ĥ		
О Установить бесконечное ожидание			
 Установить интервал: 600 Секунд 			
ОК Отмена			

В этом окне установите необходимые значения переключателей Значение пользователя и Значение по умолчанию для всего компьютера.

Пользователь, не являющийся администратором на локальном компьютере, может осуществить только установку переключателя **Значение пользователя** (переключатель **Значение по умолчанию для всего компьютера** будет затемнен) в одно из следующих положений:

- Использовать системное значение по умолчанию устанавливает значение, определенное переключателем Значение по умолчанию для всего компьютера;
- Установить бесконечное ожидание устанавливает бесконечное ожидание ввода данных от пользователя;
- Установить интервал определяет интервал времени, во время которого пользователь должен ввести данные.

Изменить значение переключателя **Значение по умолчанию для всего компьютера** может только пользователь, являющийся администратором локального компьютера. По умолчанию установлено ожидание ввода в течение 600 секунд.



Значение интервала времени ожидания ввода от пользователя имеет больший приоритет по отношению к значению, заданному для всего компьютера. Например, если значение переключателя **Значение по умолчанию для всего компьютера** установлено в положение «Установить интервал - 600 секунд», а переключатель **Значение пользователя** в положение «Установить бесконечное ожидание», то действительным будет значение «Установить бесконечное ожидание».

2.8. Установка параметров криптографических алгоритмов

Закладка Алгоритмы (см. Рисунок 35) панели управления СКЗИ Рутокен СSP предназначена для установки различных параметров реализованных криптографических алгоритмов.

Рисунок 35. Закладка «Алгоритмы» панели управления СКЗИ Рутокен CSP

риптоПро CSP для	a ruToken			×	
Общие	Оборудов	Оборудование Сервис			
Дополнительно	Алгоритмы Безопасность Winlogon				
Параметры алгори	тмов				
Purferenza zun CSI					
BEIDEPUTE TUR CS	 для настроики п 	араметров:	/au Eurla		
GUST R 34, 10-20	DI Signature with D	ittle-Heilman K	ley Excha	ange : 🗡	
Параметры	алгоритма хэширо	вания:			
FOCT P 34	11-94, параметры	по умолчани	110	¥	
Параметры	алгоритма шифро	вания:			
ГОСТ 28147-89, параметры по умолчанию					
Параметры	алгоритма подпис	и:			
FOCT P 34	10-2001, параметр	ры по умолча	анию (~	
Параметры	алгоритма Диффи	1-Хеллмана:			
ГОСТ Р 34.10-2001, параметры обмена по умолча 💌					
	ОК		ена	Применить	
	OK		ена	применить	

На закладке **Алгоритмы** можно выбрать тип криптопровайдера, для которого будет осуществляться настройка. В СКЗИ «Рутокен CSP» доступен единственный тип криптопровайдера - GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange.

Настройка параметров реализована для следующих криптографических алгоритмов:

- алгоритм хеширования ГОСТ Р 34.11-94 (параметры по умолчанию);
- алгоритм шифрования ГОСТ 28147-89 (параметры по умолчанию, параметры Оскар 1.0, параметры Оскар 1.1, параметры РИК1, параметры шифрования 1, параметры шифрования 2, параметры шифрования 3);
- алгоритм выработки и проверки электронной цифровой подписи ГОСТ Р 34.10-2001 (параметры по умолчанию, параметры Оскар 2.х, параметры подписи 1);
- алгоритм Диффи-Хеллмана ГОСТ Р 34.10-2001 (параметры обмена по умолчанию, параметры обмена 1).

2.9. Настройка аутентификации в домене Windows

Закладка **Winlogon** (см. Рисунок 36) панели управления СКЗИ Рутокен СSP предназначена для настройки аутентификации в домене с использованием алгоритмов ГОСТ.

Рисунок 36. Закладка «Winlogon» панели управления СКЗИ Рутокен СSP

	Оборудова	ание		Сервис
lополнительно	Алгоритмы	Безопас	ность	Winlogon
Ключевой считыв	атель по умолчани	ю		
Выберите CSP дл	я настройки:			
GOST R 34, 10-20	01 Rutoken CSP			~
Выберите считыв	атель:		61.00	
Не установлен				~
Параметры				
🗌 Отключить Кр	иптоПро Winlogon			
Использовать	алгоритмы Крипто	Про CSP на	a KDC	
EAP-TLS: Vicno)	ньзовать протокол	OCSP		
EAP-TLS: He no	оверять аннулиро	вание серт	ификата	сервера
				14
	контроллеров дом	ена		
Идентификаторы				
Идентификаторы Контроллер домен	1a;		C	
Идентификаторы Контроллер домен	ia:	~	Экспор	гировать
Идентификаторы Контроллер домен Идентификатор к	на: онтроллера домен-	-	Экспор	гировать
Идентификаторы Контроллер домен Идентификатор к	на: онтроллера домен	3:	Экспор	пировать ілоны

Подробно настройка КриптоПро Winlogon рассматривается в сопроводительной документации, поставляемой вместе с продуктом КриптоПро Winlogon.

При необходимости можно полностью отключить использование алгоритмов ГОСТ при аутентификации в домене. Для этого предназначена опция **Отключить КриптоПро Winlogon**.

3. Интерфейс генерации ключей

3.1. Создание ключевого контейнера

3.1.1. Выбор ключевого носителя

Окно выбора ключевого носителя отображается в том случае, когда пользователь имеет несколько устройств, служащих ключевыми считывателями. В СКЗИ Рутокен CSP изначально установлен только один ключевой считыватель, который выбирается автоматически, и окно выбора ключевого носителя не отображается.

3.1.2. Генерация начальной последовательности ДСЧ

После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, система отобразит окно «Биологический датчик случайных чисел» (см. Рисунок 37).

Рисунок 37. Биологический датчик случайных чисел

КриптоПро CSP для ruToken
0:09:57
Биологический датчик случайных чисел
Нажимайте клавиши или перемещайте указатель
мыши над этим окном до тех пор, пока ключ не будет создан
Нет
Отмена

Биологический датчик случайных чисел предназначен для генерации начальной последовательности датчика случайных чисел.

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.1.3. Ввод пароля на доступ к закрытому ключу

После завершения работы биологического датчика случайных чисел система отобразит окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 38).

КриптоПро CSP для ruToken			
Type password a for container	0:08:54 and friendly name		
Контейнер Имя: e10991c1-d125-4b28-96df-28b8a	ae27a253		
Дружественное имя: Иванов И.И.			
	RU		
Новый пароль:	•••••		
Подтверждение:	••••••		
Счетчик ошибок (ФКН):	100		
Счетчик посл. ошибок (ФКН):	3		
Счетчик ЕКЕ:	1000000		
Счетчик Д-Х:	1000000		
Счетчик подписей:	1000000		
ОК	Отмена		

Рисунок 38. Ввод пароля на доступ к закрытому ключу

В этом окне существует возможность ввода текстового пароля на доступ к закрытому ключу создаваемого контейнера (один и тот же пароль необходимо ввести в поля **Новый па-роль** и **Подтверждение**).

После ввода пароля нажмите кнопку ОК.

3.2. Открытие ключевого контейнера

3.2.1. Отсутствие ключевого носителя

В случае отсутствия ключевого носителя при открытии ключевого контейнера система отобразит окно, сообщающее об отсутствии носителя. После того, как носитель будет подключен, система перейдет к окну ввода пароля на доступ к закрытому ключу открываемого контейнера (см. Рисунок 39).

Если требуемый носитель установить не удается, нажмите кнопку **Отмена**. В этом случае процесс открытия контейнера прекратится.

В случае, когда необходимый ключевой носитель подключен, окно, сообщающее об отсутствии ключевого носителя, отображаться не будет.

3.2.2. Проверка пароля на доступ к закрытому ключу

После того, как необходимый носитель установлен, система потребует подтверждение пароля на доступ к закрытому ключу открываемого контейнера (см. Рисунок 39).

КриптоПро CSP для ruToken		
Type password a for container	0:09:53 and friendly name	
Контейнер Имя: e10991c1-d125-4b28-96df-28b8a Дружественное имя:	ae27a253	
Иванов И.И.		
Пароль:	RU	
Ограничения		
Осталось попыток:	3	
Осталось попыток (CSP):	3	
Счетчик ошибок (ФКН):	100	
Счетчик посл. ошибок (ФКН):	3	
Счетчик ЕКЕ:	9999992	
Счетчик Д-Х:	1000000	
Счетчик подписей:	1000000	
ОК	Отмена	

Рисунок 39. Проверка пароля на доступ к закрытому ключу

Если пароль введен неверно, система попросит повторно ввести пароль (см. Рисунок 40). В СКЗИ Рутокен СSP установлено ограничение числа попыток ввода пароля. Превышение этого числа приведет к блокированию контейнера (см. раздел 4).

КриптоПро CSP для ruToken		
0:09:58 Неправильный пароль. Осталось попыток: 2.		
-Контейнер Имя:		
e10991c1-d125-4b28-96df-28b8	ae27a253	
Дружественное имя:		
Иванов И.И.		
	RU	
Пароль:		
Ограничения Осталось попыток:	2	
Осталось попыток (CSP):	2	
Счетчик ошибок (ФКН):	100	
Счетчик посл. ошибок (ФКН):	3	
Счетчик ЕКЕ:	9999992	
Счетчик Д-Х:	1000000	
Счетчик подписей:	1000000	
ОК	Отмена	

Рисунок 40. Повторный ввод пароля на доступ к закрытому ключу

3.3. Генерация ключей и получение сертификата при помощи УЦ

Для формирования личных ключей и получения сертификатов можно воспользоваться тестовым Центром Сертификации <u>http://www.CryptoPro.ru/CertSrv</u> (см. Рисунок 41) либо <u>http://www.CryptoPro.ru/CertSrv vista</u> для OC Windows Vista и Windows 2008.

Рисунок 41. Генерация ключа при помощи УЦ

Microsoft Службы серти	рикации Active Directory Test Center CRYPTO-PRO
Расширенный запр	ос сертификата
Идентифицирующие св	едения:
Имя: Иван	ов И.И.
Электронная почта: ivanov	/@mail.ru
Организация:	
Подразделение:	
Город:	
Область, штат:	
Страна, регион: RU	
Нужный тип сертифика	та:
	Сертификат проверки подлинности клиента 💌
Параметры ключа:	
CSP: [Использование ключей: (Размер ключа: [([[] Дополнительные парам	GOST R 34.10-2001 Rutoken CSP ● Exchange ● Подпись ● Оба 512 Минимальный:512 (стандартные размеры ключей: 512.) ● Автоматическое имя контейнера ключа ● Заданное пользователем имя контейнера ключ Пометить ключ как экспортируемый Включить усиленную защиту закрытого ключа ■ Использовать локальное хранилище компьютера для сертификата Сохраняет сертификат в локальном хранилище вместо пользовательского хранилища сертификатов. Не устанавливает корневой сертификат ЦС. Необходимо быть администратором, чтобы создать локальное хранилище. метры:
Формат запроса: (
Алгоритм хеширования:	GOST R 34.11-94 💌 1спользуется только для подписания запроса.
I	Сохранить запрос
Атрибуты:	
Понятное имя:	
	Runny N

В диалоге создания ключа и формирования запроса на сертификат задайте имя владельца сертификата и введите адрес электронной почты.



Если введенный адрес электронной почты не совпадает с зарегистрированным адресом в Outlook Express (Outlook), использовать криптографические функции в электронной почте будет нельзя.

Выберите нужный тип сертификата в зависимости от его назначения.

В поле **Параметры ключа** выберите тип криптопровайдера Magistra CSP. Задайте остальные параметры ключа и дополнительные параметры, исходя из своих требований к создаваемому ключу.

Нажмите на кнопку Выдать.

4. Счетчики и ограничения

В СКЗИ Рутокен CSP поддерживается набор счетчиков на выполнение криптографических операций, количество попыток ввода пароля и количество ошибок. Обнуление любого из данных счетчиков приведет к блокировке контейнера.

Описание счетчиков приведено в таблице:

Таблица 1. Счетчики, используемые в СКЗИ Рутокен CSP

Счетчик	Максимальное значение	Описание
Счетчик попыток ввода пароля	3	Минимальное значение среди всех счетчиков.
Счетчик попыток ввода пароля (CSP)	3	Число попыток ввода пароля через диалог СКЗИ Руто- кен СSP. При правильном вводе пароля значение счет- чика восстанавливается.
Счетчик ошибок (ФКН)	100 - 256*	Число ошибок аутентификации в протоколе взаимо- действия с ФКН.
Счетчик последо- вательных ошибок (ФКН)	3 - 5*	Число ошибок аутентификации идущих подряд в про- токоле взаимодействия с ФКН.
Счетчик ЕКЕ	10 000 000*	Количество внутренних криптографических операций ФНК.
Счетчик Диффи- Хеллмана	10 000 000*	Количество операций Диффи-Хеллмана.
Счетчик подписей	10 000 000*	Количество подписей, которое может быть создано с использованием закрытого ключа из данного контей- нера.

* Значение определяется ключевым носителем.

5. Перечень сокращений

- CSP Криптопровайдер (Cryptographic Service Provider)
- EKE Протокол электронного обмена ключами (Electronic Key Exchange)
- ОС Операционная система
- ПАК Программно-аппаратный комплекс
- СКЗИ Средство криптографической защиты информации
- ФКН Функциональный ключевой носитель

6. Перечень рисунков

Рисунок 1. Приветственное окно мастера установки	5
Рисунок 2. Лицензионное соглашение	6
Рисунок 3. Сведения о пользователе	6
Рисунок 4. Вид установки	7
Рисунок 5. Выборочная установка	7
Рисунок 6. Окно подтверждения установки	8
Рисунок 7. Окончание установки	8
Рисунок 8. Изменение, исправление или удаление программы	9
Рисунок 9. Панель управления Рутокен CSP 10	0
Рисунок 10. Закладка «Оборудование» панели управления Рутокен CSP 1	1
Рисунок 11. Закладка «Сервис» панели управления Рутокен CSP 12	2
Рисунок 12. Удаление контейнера закрытого ключа 13	3
Рисунок 13. Выбор ключевого контейнера для копирования 13	3
Рисунок 14. Выбор сертификата для удаления контейнера 14	4
Рисунок 15. Окно подтверждения удаления ключевого контейнера 14	4
Рисунок 16. Сертификаты в контейнере закрытого ключа 1	5
Рисунок 17. Окно «Сертификат для просмотра» 10	6
Рисунок 18. Окно просмотра свойств сертификата 1	7
Рисунок 19. Мастер импорта сертификатов 18	8
Рисунок 20. Выбор хранилища 18	8
Рисунок 21. Завершение мастера импорта сертификатов 19	9
Рисунок 22. Мастер установки личного сертификата 20	0
Рисунок 23. Окно «Расположение файлов сертификата» 20	0
Рисунок 24. Окно «Сертификат для установки» 2	1
Рисунок 25. Окно «Контейнер закрытого ключа» 22	2
Рисунок 26. Окно «Хранилище сертификатов» 22	3
Рисунок 27. Завершение работы мастера установки личного сертификата 22	3
Рисунок 28. Изменение пароля контейнера закрытого ключа 24	4
Рисунок 29. Ввод пароля на доступ к закрытому ключу 2	5
Рисунок 30. Ввод нового пароля на доступ к закрытому ключу 20	6
Рисунок 31. Окно «Удаление запомненных паролей» 2	7
Рисунок 32. Закладка «Безопасность» панели управления СКЗИ Рутокен СSP 28	8
Рисунок 33. Закладка «Дополнительно» панели управления СКЗИ Рутокен CSP 29	9
Рисунок 34. Окно «Интервал времени ожидания ввода» 30	0
Рисунок 35. Закладка «Алгоритмы» панели управления СКЗИ Рутокен СSP 32	1
Рисунок 36. Закладка «Winlogon» панели управления СКЗИ Рутокен CSP 32	2
Рисунок 37. Биологический датчик случайных чисел 32	3
Рисунок 38. Ввод пароля на доступ к закрытому ключу 34	4
Рисунок 39. Проверка пароля на доступ к закрытому ключу 3	5
Рисунок 40. Повторный ввод пароля на доступ к закрытому ключу 30	6
Рисунок 41. Генерация ключа при помощи УЦ 3	7