ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-05 92 01–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 5.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВАМБ.00060-05 92 01

2016

Аннотация

Данный документ содержит описание процесса эксплуатации средства криптографической защиты информации (СКЗИ) «Валидата CSP».

Документ предназначен для пользователей как руководство по эксплуатации криптографического провайдера «Валидата CSP».

Содержание

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ 4
1.1 Назначение . . . 4
1.2 Условия применения . . . 4

2 СЧИТЫВАТЕЛИ КЛЮЧЕЙ 5
2.1 Настройка считывателей ключей . . . 5
2.2 Графический интерфейс пользователя при работе с ключами . . . 7
2.2.1 Интерактивный выбор ключа . . . 7
2.2.2 Пароли для защиты ключа . . . 9
2.2.3 Особенности работы с различными ключевыми носителями . . . 10

3 ДАТЧИКИ СЛУЧАЙНЫХ ЧИСЕЛ 12
3.1 Настройка ДСЧ . . . 12
3.2 Инициализация ДСЧ . . . 14
3.2.1 Автоматическая инициализация . . . 14
3.2.2 Принудительная инициализация . . . 15

4 СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ КОНФИГУРАЦИИ 16
4.1 Операции с ключами . . . 16
4.1.1 Копирование ключа . . . 16
4.1.2 Удаление ключей . . . 17
4.1.3 Смена пароля ключа . . . 18
4.1.4 Преобразование ключа . . . 18
4.1.5 Обновление масок ключа . . . 18
4.2 Операции с сертификатами . . . 19
4.2.1 Установка сертификата в системное хранилище . . . 19
4.2.2 Запись сертификата на смарт-карту . . . 22
4.3 Настройки совместимости . . . 24
4.3.1 Настройка сертификата шифрования по умолчанию для «Валидата CSP» СКАД «Сигнатура» . . . 24
4.4 Дополнительные операции . . . 26
4.4.1 Уничтожение содержимого файла . . . 27
4.4.2 Проверка подписи модулей . . . 27
4.4.3 Форматирование и смена ПИН-кода ключевого носителя . . . 28

5 ПРОГРАММА ПРЕОБРАЗОВАНИЯ КЛЮЧЕЙ 31

ПЕРЕЧЕНЬ РИСУНКОВ 32

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

1.1 Назначение

Криптографический провайдер «Валидата CSP» предназначен для:

– вычисления и проверки электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– выполнения зашифрования и расшифрования данных в соответствии с ГОСТ 28147-89;

– вычисления имитозащиты данных в соответствии с ГОСТ 28147-89 (при этом поддерживаются имитозащита длиной 4 байта и имитозащита длиной 8 байт);

– вычисления ключа парной связи Диффи-Хелмана с использованием пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– вычисления хэш-функции данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;

– выработки случайного числа заданной длины;

– создания (генерации) закрытых ключей в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;

– вычисления открытых ключей в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.

1.2 Условия применения

Криптографический провайдер «Валидата CSP» работает под управлением следующих ОС:

– Microsoft Windows Vista с пакетом обновлений 1 и выше;

– Microsoft Windows Server 2008 с пакетом обновлений 1 и выше;

– Microsoft Windows 7;

– Microsoft Windows Server 2008 R2;

– Microsoft Windows 8/8.1;

– Microsoft Windows Server 2012/2012 R2.

При этом поддерживаются как 32-битные ОС Microsoft Windows (x86), так и 64-битные ОС Microsoft Windows (x64).

2 СЧИТЫВАТЕЛИ КЛЮЧЕЙ

Для выполнения большинства криптографических операций требуются ключи. Секретная (закрытая) часть ключа обычно хранится на отчуждаемых носителях (дискетах, USB flash, «таблетках» - Touch Memory и т.д.). Для чтения и записи ключей на ключевые носители предназначены программные модули - считыватели ключей. В состав ПО «Валидата CSP» могут входить несколько считывателей ключей, их использование регулируется **конфигурационной программой** «Валидата CSP».

2.1 Настройка считывателей ключей

Для запуска **конфигурационной программы** «Валидата CSP» необходимо вызвать пункт меню «Пуск»→«Программы»→«Валидата CSP»→«Конфигурационная программа СКЗИ». Для настройки считывателей ключей надо перейти на закладку «Считыватели ключа» (Рисунок 1).

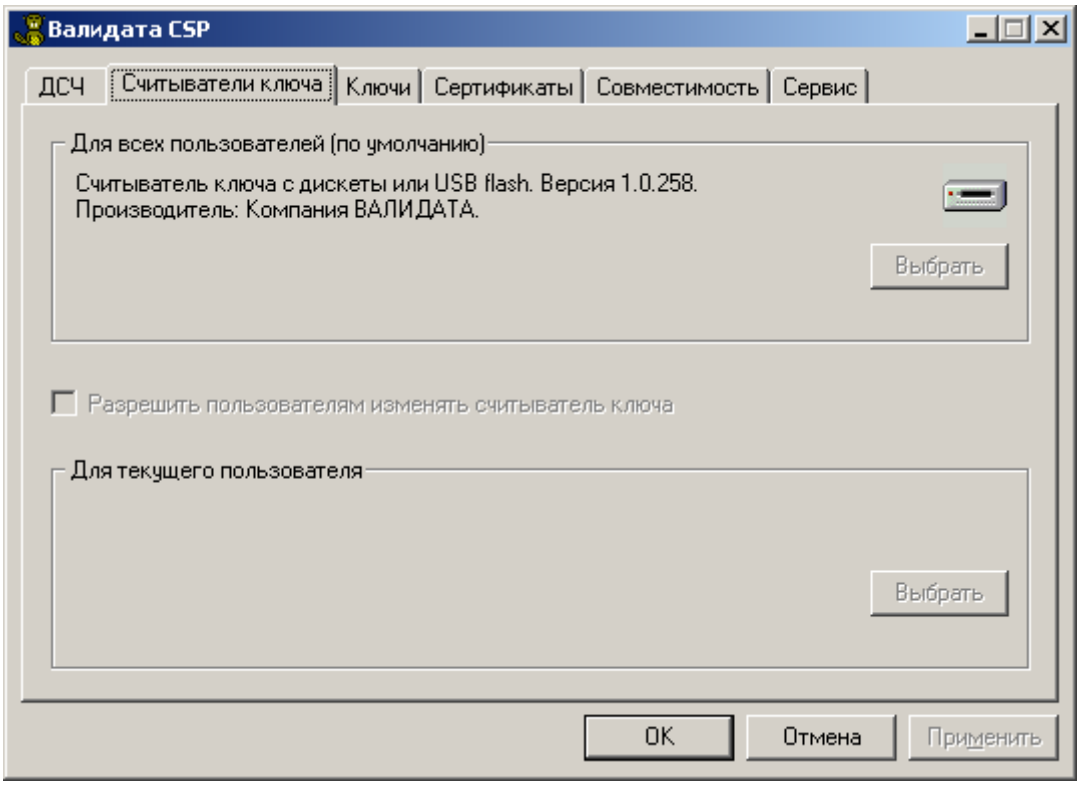

Рисунок 1 – Закладка «Считыватели ключа»

Считыватель ключа по умолчанию может быть задан администратором (см. «Программный комплекс «Валидата CSP» Руководство Администратора» ВАМБ.00060-04 34 01). Если администратор задал считыватель ключа с дискеты или USB flash (см. Рисунок 1), то все пользователи при попытке чтения ключа будут обращаться к дискете или флэш-памяти. Пользователь не может изменить эту установку, но если администратор разрешил пользователям изменять считыватель ключа, то пользователь получает возможность задать считыватель ключа только для себя, нажав кнопку «Выбрать» в нижней части закладки (Рисунок 2).

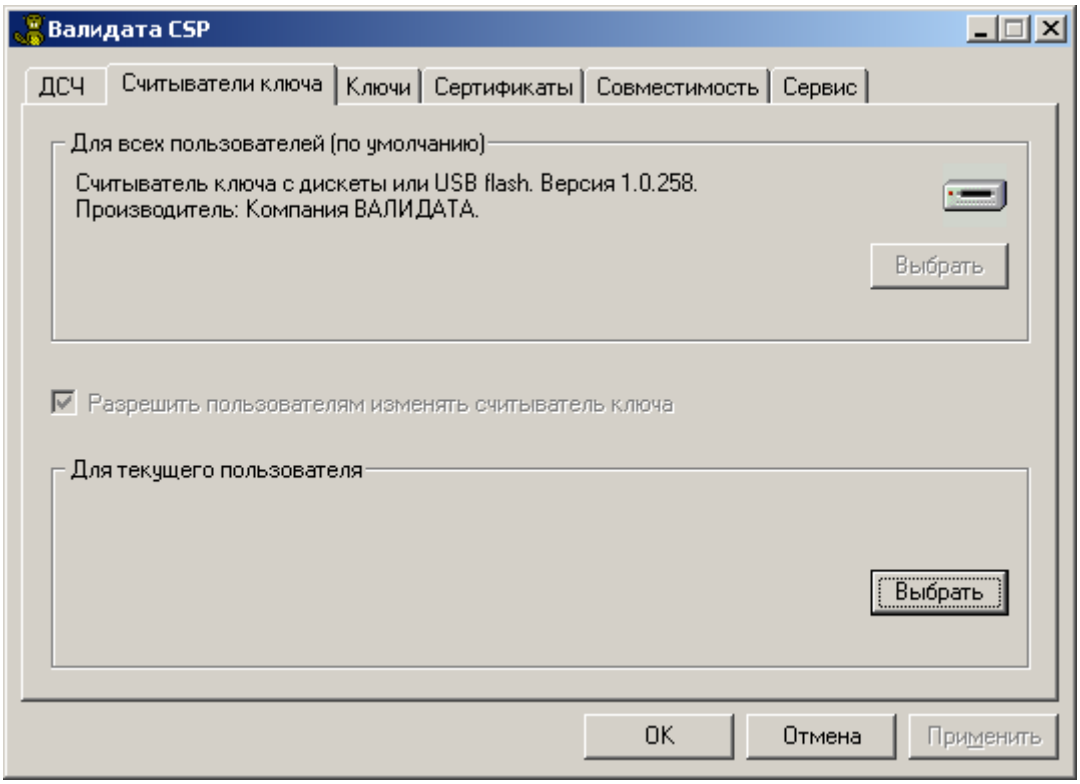

Рисунок 2 – Пользователь может изменить настройку считывателя ключа

На экране появится диалоговое окно выбора считывателей ключа (Рисунок 3).

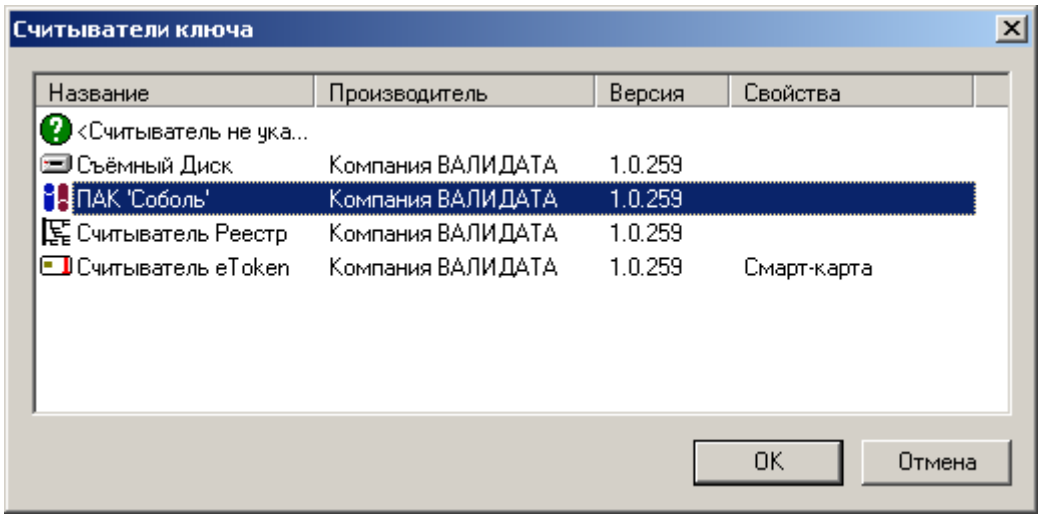

Рисунок 3 – Диалог выбора считывателя ключа

Выберите другой считыватель ключа и нажмите кнопку «OK». Появится диалоговое окно (Рисунок 4).

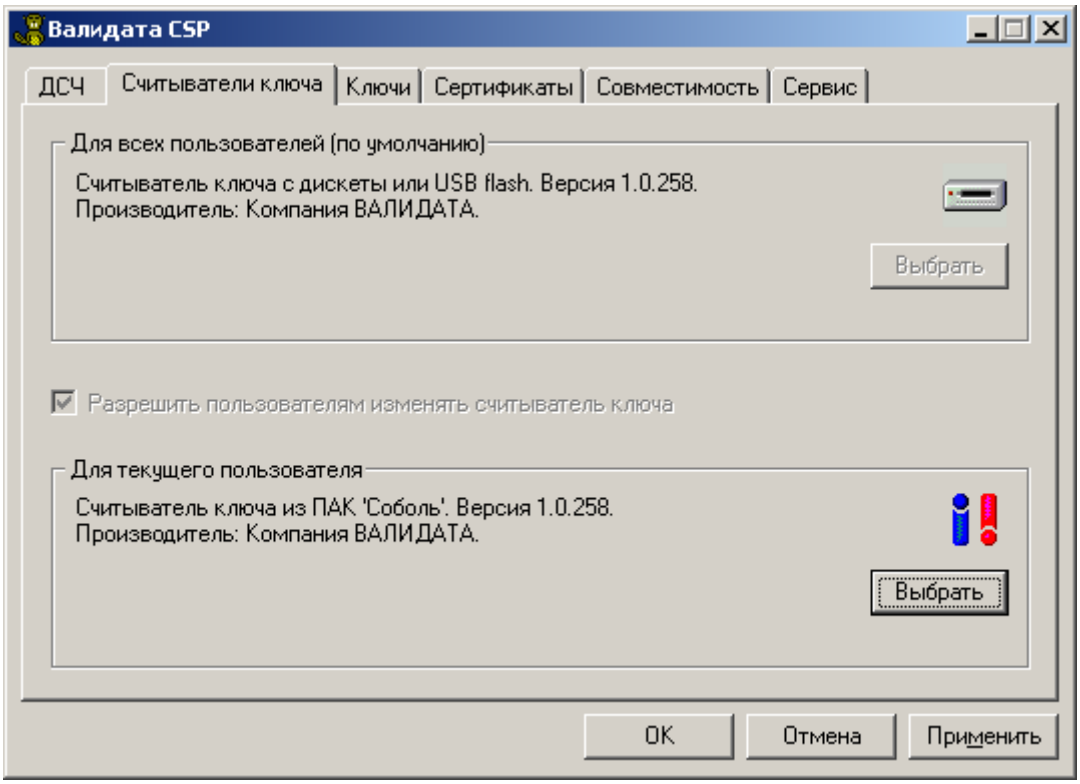

Рисунок 4 – Изменение считывателя ключа для текущего пользователя

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить».

2.2 Графический интерфейс пользователя при работе с ключами

2.2.1 Интерактивный выбор ключа

В общем случае алгоритм выбора считывателя ключа таков: если пользователю разрешено изменять считыватель ключа, и он сделал это, используется считыватель ключа, указанный пользователем. Если нет - используется считыватель ключа, заданный администратором. Если и администратор не назначил считыватель ключа по умолчанию, на экран выдаётся диалоговое окно, предлагающее выбрать считыватель ключа (Рисунок 5).

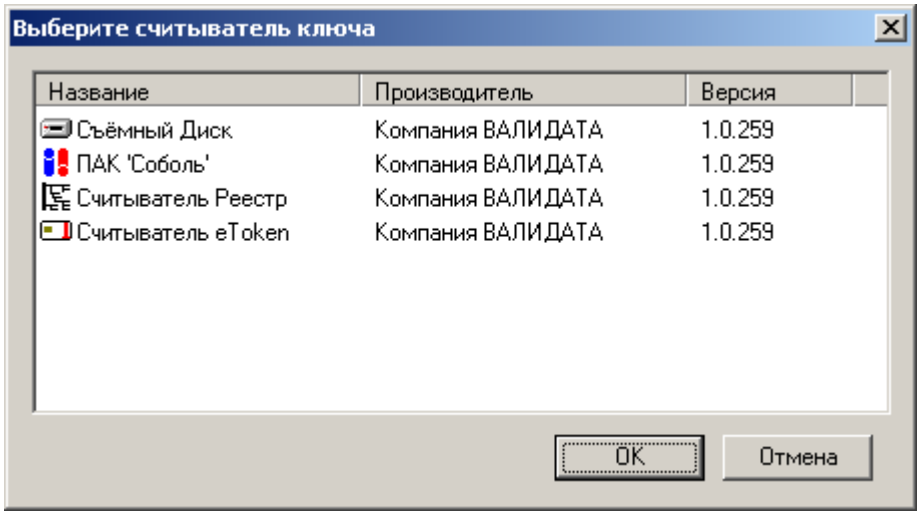

Рисунок 5 – Диалог выбора считывателя ключа

Выберите считыватель ключа для текущей операции с ключом. Сделанный таким образом выбор считывателя ключа не становится постоянным - при следующем обращении к ключу, этот диалог будет вызван снова. В некоторых случаях такой диалог будет возникать даже при назначенном считывателе ключа по умолчанию - например, в ситуации, когда надо скопировать ключ с одного типа устройства на другое. В процессе обращения к ключам некоторыми считывателями ключа могут возникать дополнительные диалоги, требующие дополнительного указания источника ключевой информации. Например, при использовании считывателя ключа с дискеты или USB flash, на экране может появиться диалог (Рисунок 6), предлагающий выбрать диск, на котором находится ключ.

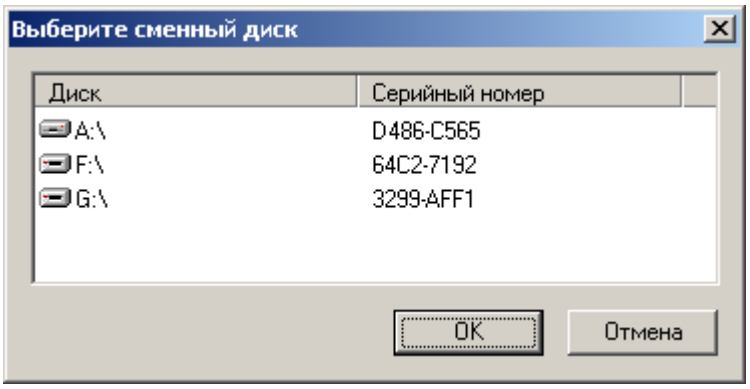

Рисунок 6 – Диалог выбора диска

Если считыватель ключа не обнаруживает ни одного диска, он выдаст сообщение (Рисунок 7).

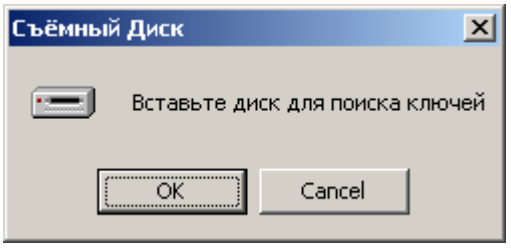

Рисунок 7 – Сообщение об отсутствии ключевого носителя

После выбора ключевого носителя часто бывает необходимо выбрать один из нескольких, находящихся на нём ключей. Для этого служит диалог выбора ключа (Рисунок 8).

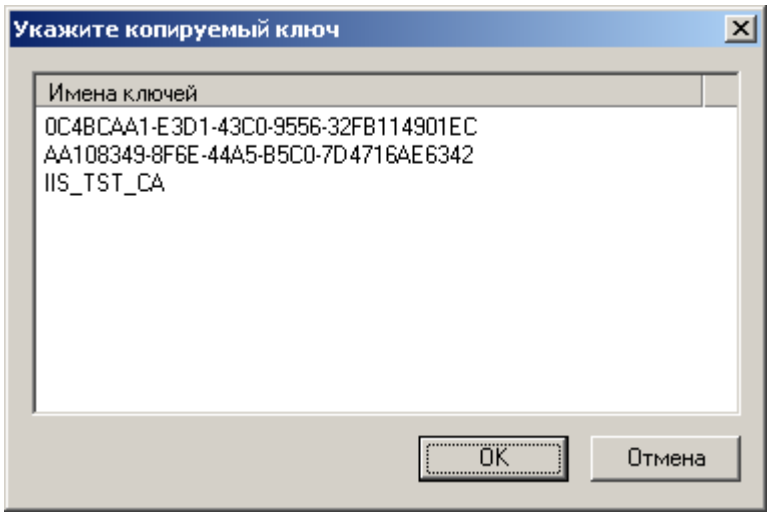

Рисунок 8 – Диалог выбора ключа

Выберите ключ для операции, название которой указано в заголовке окна и нажмите кнопку «OK».

2.2.2 Пароли для защиты ключа

При записи (генерации и т.д.) ключа пользователю предлагается ввести пароль для защиты ключа (Рисунок 9).

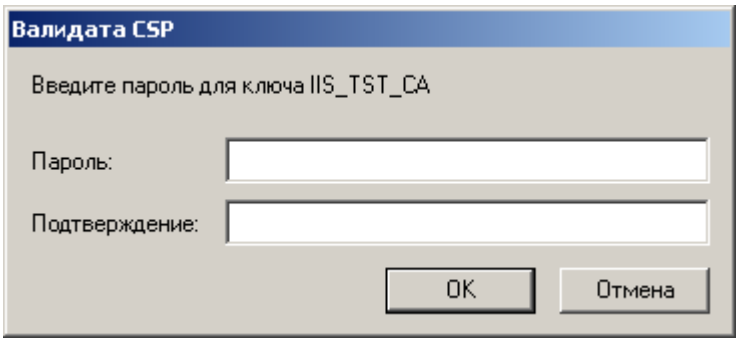

Рисунок 9 – Диалог задания пароля ключа

Введите пароль два раза и нажмите кнопку «OK». Если введённые значения отличаются друг от друга, система предложит повторить попытку (Рисунок 10).

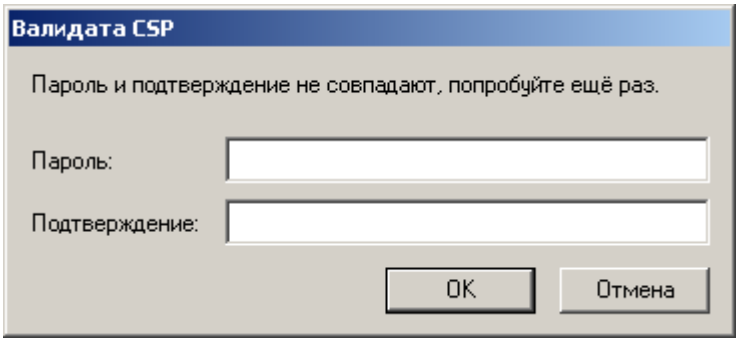

Рисунок 10 – Диалог повторного задания пароля ключа

Если пользователь не хочет защищать ключ паролем, он должен нажать кнопку «OK», не вводя пароля. Нажатие кнопки «Отмена» отменяет не пароль, а всю операцию с ключом.

При чтении ключа, защищённого паролем, пользователю предлагается ввести пароль (Рисунок 11).

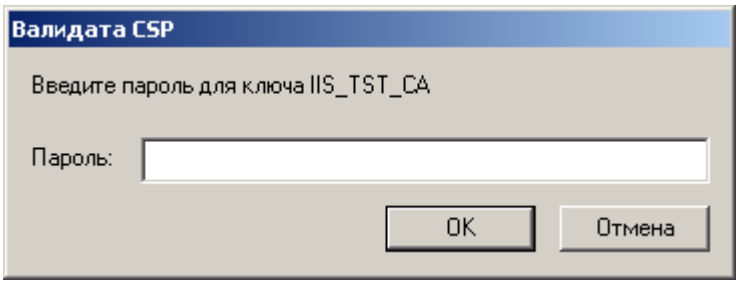

Рисунок 11 – Диалог проверки пароля ключа

При неправильном вводе пароля пользователю предлагается повторить ввод с указанием количества оставшихся попыток (Рисунок 12).

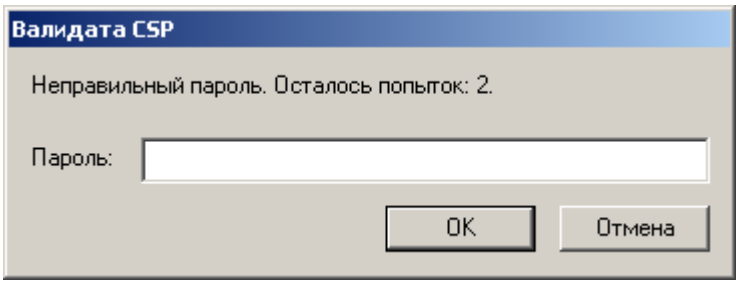

Рисунок 12 – Диалог повторной проверки пароля ключа

Если количество неуспешных попыток ввода пароля ключа ЭП становится равным максимально возможному (3 попытки), загрузка ключа ЭП не производится и соответствующий код ошибки возвращается прикладному программному обеспечению (ППО).

Если ключ ЭП не защищен паролем, то при его чтении диалоговое окно проверки пароля ключа не выдается.

2.2.3 Особенности работы с различными ключевыми носителями

Считыватели Рутокен

В случае возникновения ошибки 0xE0BE50DE «Ошибка ф-ии RtlLoginToken» при использовании считывателя Рутокен, необходимо отключить кэширование PIN-кодов на закладке Настройки Панели управления Рутокен, запустив ее из Панели управления ОС Windows (Рисунок 13).

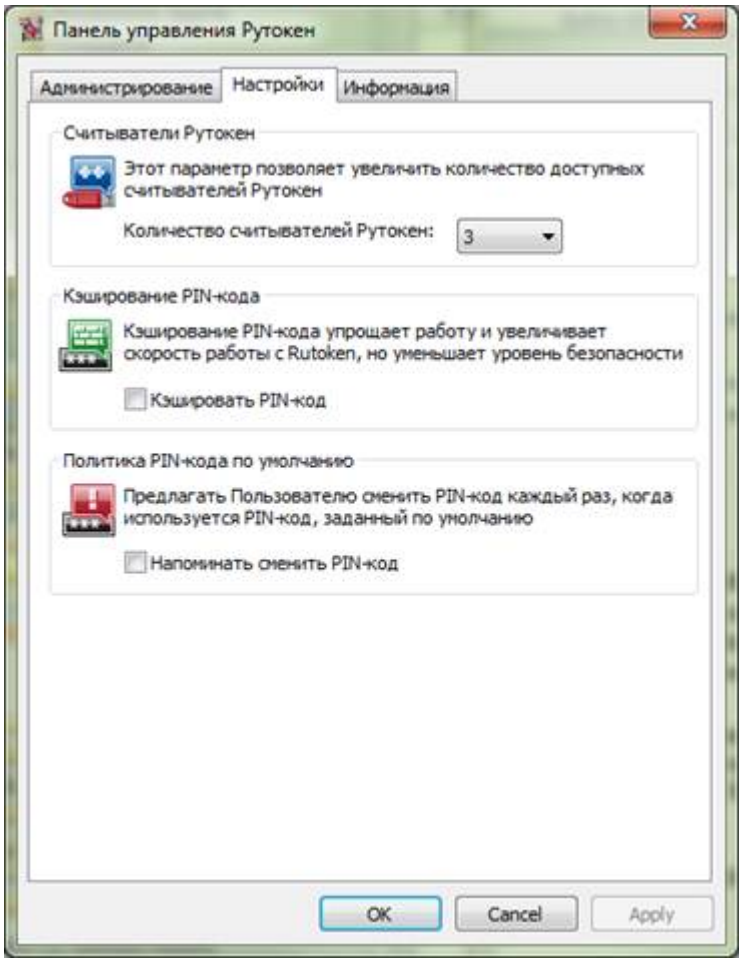

Рисунок 13 – Панель управления Рутокен

3 ДАТЧИКИ СЛУЧАЙНЫХ ЧИСЕЛ

Для работы «Валидата CSP» требуется датчик случайных чисел (ДСЧ). ПО «Валидата CSP» может работать с различными типами ДСЧ, их использование регулируется конфигурационной программой «Валидата CSP».

3.1 Настройка ДСЧ

Для запуска конфигурационной программы «Валидата CSP» необходимо вызвать пункт меню «Пуск»→«Программы»→«Валидата CSP»→«Конфигурационная программа СКЗИ». Настройка ДСЧ производится на закладке «ДСЧ» (Рисунок 14).

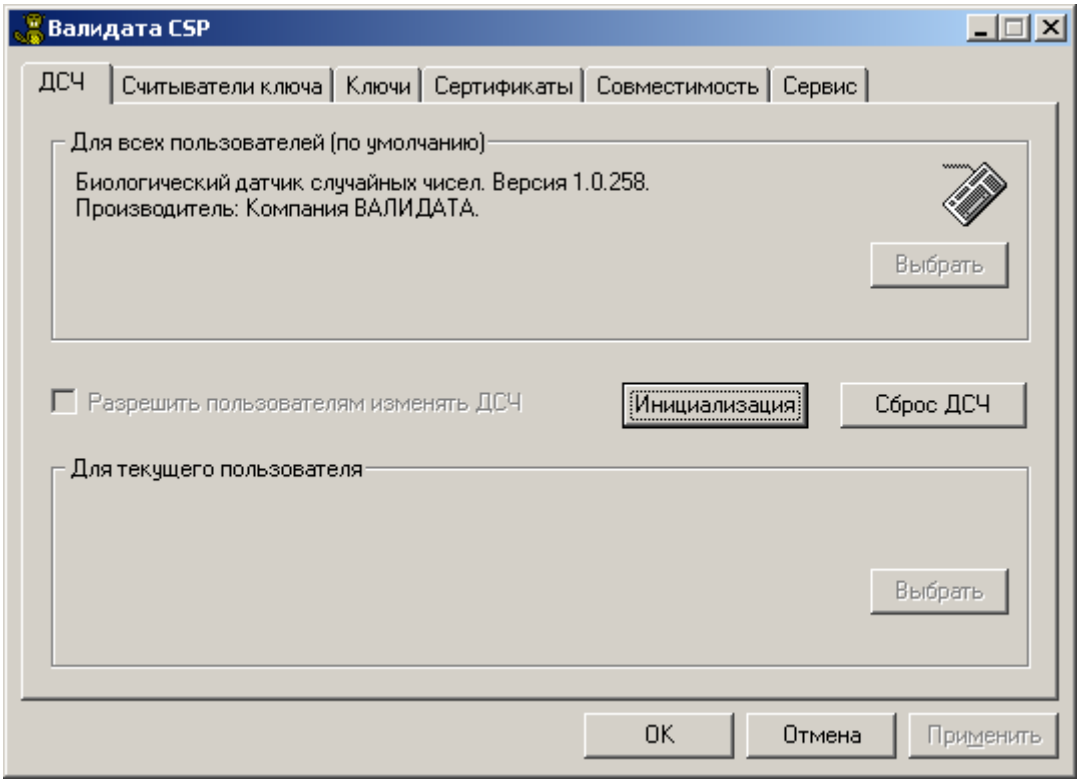

Рисунок 14 – Закладка ДСЧ

Тип ДСЧ по умолчанию может быть задан администратором (см. «Программный комплекс «Валидата CSP» Руководство Администратора» ВАМБ.00060-04 34 01).

Если администратор задал биологический ДСЧ (см. Рисунок 14), то для всех пользователей будет вызываться этот датчик. Пользователь не может изменить эту установку, но если администратор разрешил пользователям задавать тип ДСЧ, то пользователь получает возможность изменить тип ДСЧ только для себя, нажав кнопку «Выбрать» в нижней части закладки (Рисунок 15).

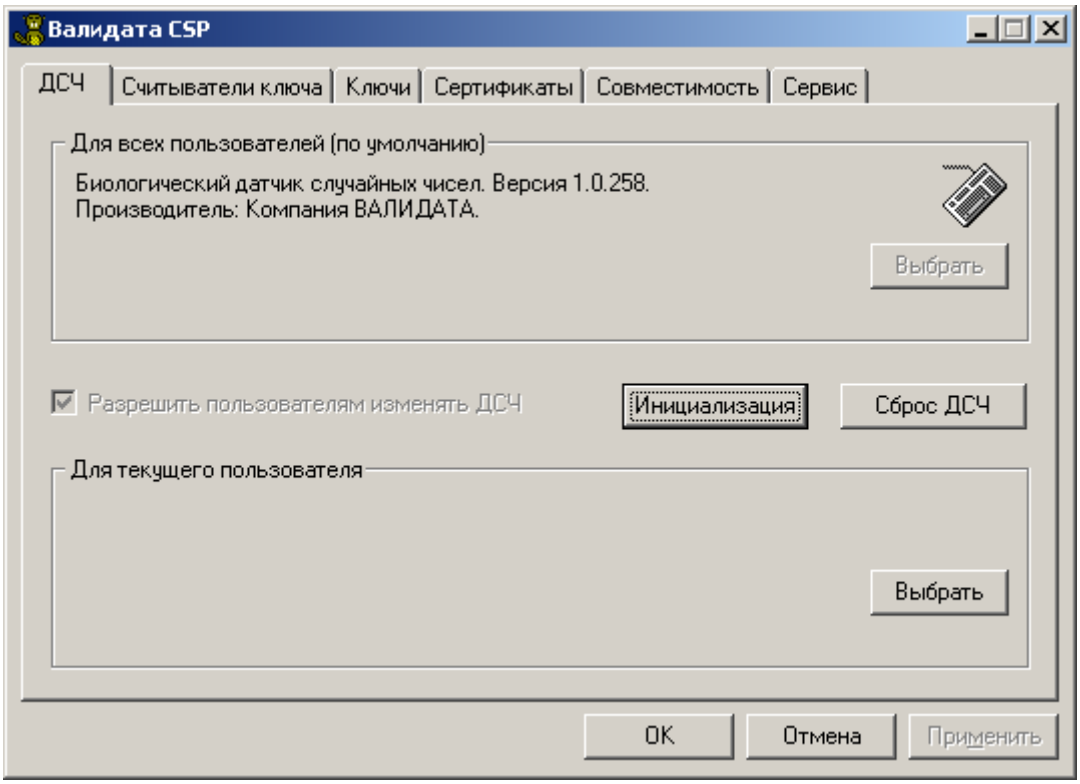

Рисунок 15 – Пользователь может изменить настройку ДСЧ

На экране появится диалоговое окно выбора типа ДСЧ (Рисунок 16).

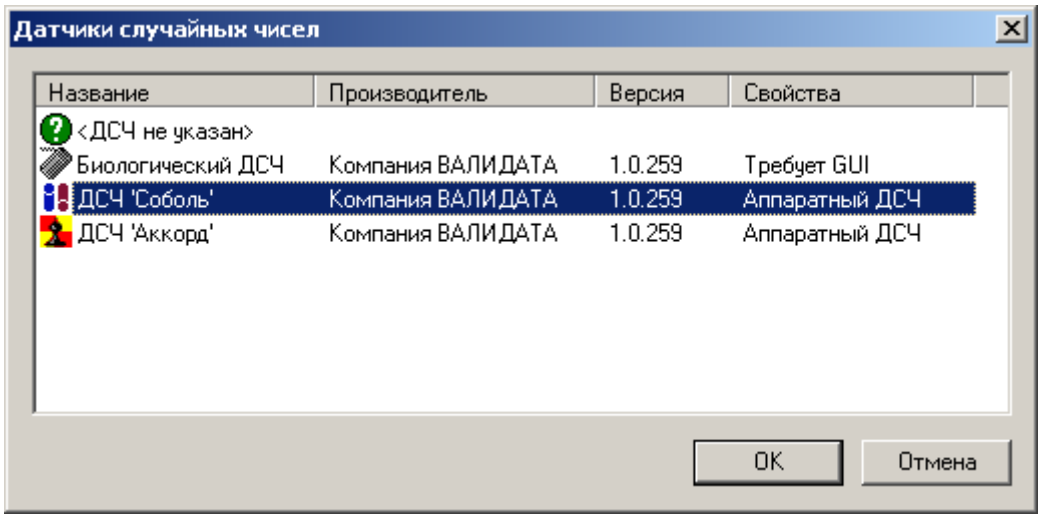

Рисунок 16 – Диалог выбора ДСЧ

Выберите тип ДСЧ и нажмите кнопку «OK». На экране появится исходное окно с информацией о выбранном ДСЧ (Рисунок 17).

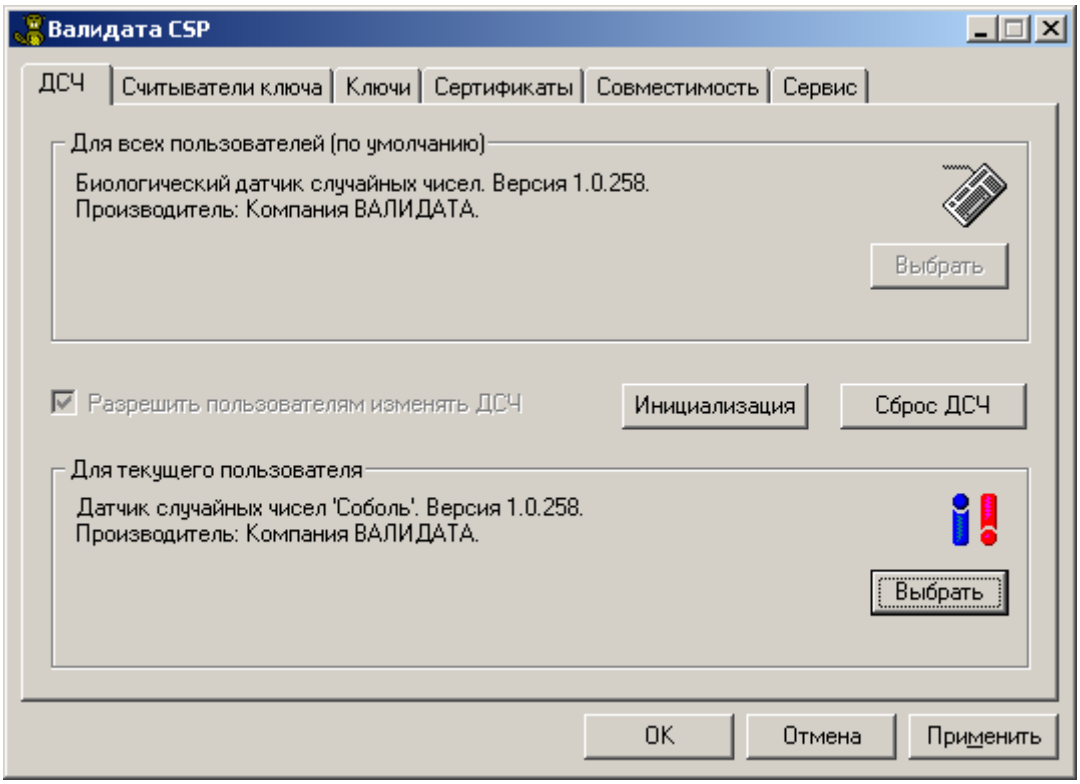

Рисунок 17 – ДСЧ для текущего пользователя изменён

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить».

3.2 Инициализация ДСЧ

ДСЧ требует инициализации после каждой загрузки ОС «Windows».

3.2.1 Автоматическая инициализация

Инициализация ДСЧ происходит автоматически при выполнении первой криптографической операции после загрузки ОС «Windows».

Примечание - Для инициализации ДСЧ СКЗИ «Валидата CSP» закрытый ключ не требуется.

Для некоторых датчиков, например, биологического ДСЧ, набор первичных случайных данных требует вмешательства пользователя (произвольных нажатий кнопки клавиатуры или движений «мышкой») (Рисунок 18).

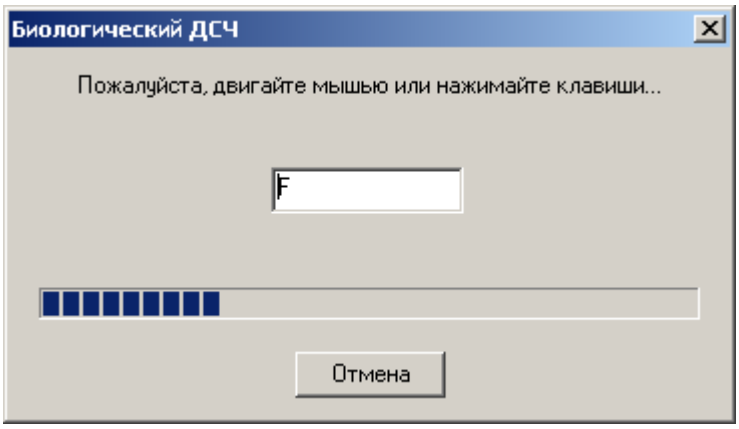

Рисунок 18 – Получение случайных чисел с помощью пользователя

3.2.2 Принудительная инициализация

В некоторых случаях, например, при работе с серверными приложениями, удобно выполнить инициализацию ДСЧ принудительно. Для этого надо нажать кнопку «Инициализация» на закладке ДСЧ программы конфигурации «Валидата CSP». Программа выполнит инициализацию ДСЧ так же, как было описано в пункте 3.2.1 и выдаст сообщение (Рисунок 19).

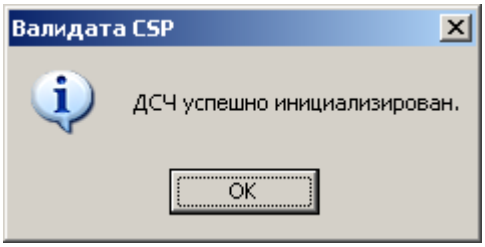

Рисунок 19 – Сообщение об удачной инициализации ДСЧ

При повторной попытке принудительной инициализации программа выдаст сообщение (Рисунок 20).

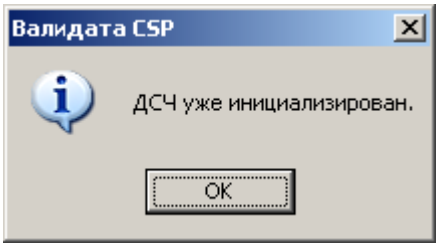

Рисунок 20 – Сообщение об инициализованном ДСЧ

Чтобы вернуть ДСЧ в начальное (неинициализированное) состояние пользователь может нажать кнопку «Сброс ДСЧ» на закладке ДСЧ.

4 СЕРВИСНЫЕ ФУНКЦИИ ПРОГРАММЫ КОНФИГУРАЦИИ

4.1 Операции с ключами

На закладке «Ключи» расположены кнопки, позволяющие копировать, удалять, менять пароли, преобразовывать ключи и обновлять маски ключей (Рисунок 21).

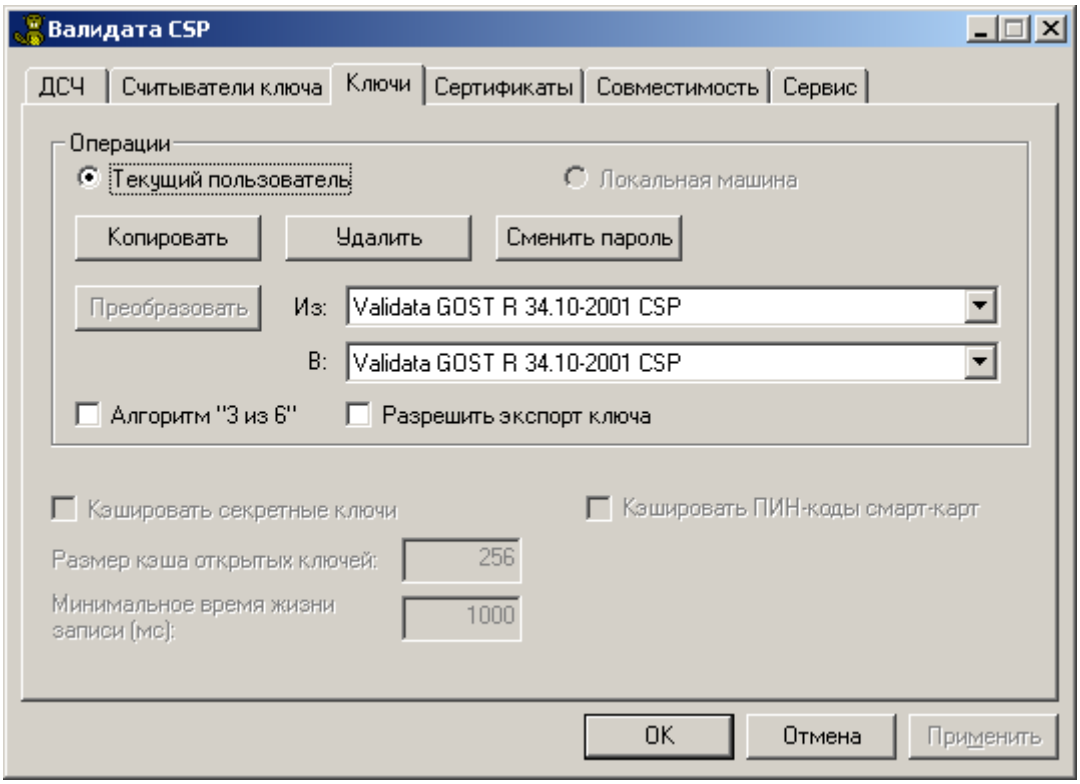

Рисунок 21 – Закладка «Ключи»

4.1.1 Копирование ключа

Для копирования ключа с одного носителя на другой нажмите кнопку «Копировать». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. пункт 3.2.1). Затем, даже если в конфигурации задан считыватель ключа по умолчанию, на экране появится диалог выбора считывателя ключа. Это делается для того, чтобы пользователь мог копировать ключи с разных ключевых носителей. После того, как пользователь выберет ключ для копирования, на экране появится сообщение (Рисунок 22).

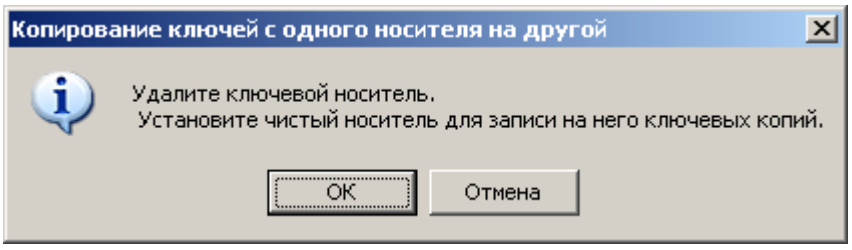

Рисунок 22 – Сообщение о замене ключевого носителя

Если для установки ключевого носителя, на который пользователь хочет скопировать ключ, необходимо удалить текущий ключевой носитель, это надо сделать после появления такого сообщения. В противном случае (например, при копировании с дискеты на USB-flash), данное сообщение можно оставить без внимания. После нажатия на кнопку «OK» необходимо выбрать считыватель ключа, на который будет производиться копирование ключа, и дождаться завершения операции. На экране появится сообщение об успешном завершении или сообщение об ошибке, например (Рисунок 23).

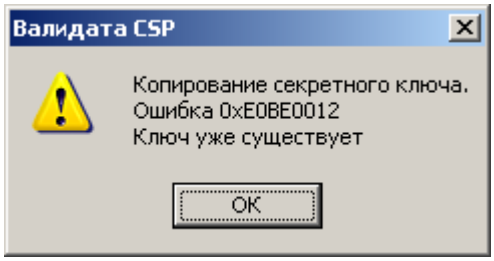

Рисунок 23 – Сообщение об ошибке при копировании ключа

Следует отметить, что доли секрета ключей, сформированных по алгоритму «3 из 6» или «2 из 3», копируются по отдельности.

4.1.2 Удаление ключей

Для удаления ключей нажмите кнопку «Удалить». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем на экране появится диалог выбора ключей (Рисунок 24). В отличие от остальных операций, при удалении пользователь может выбрать сразу несколько ключей, пользуясь клавишами Shift и Control.

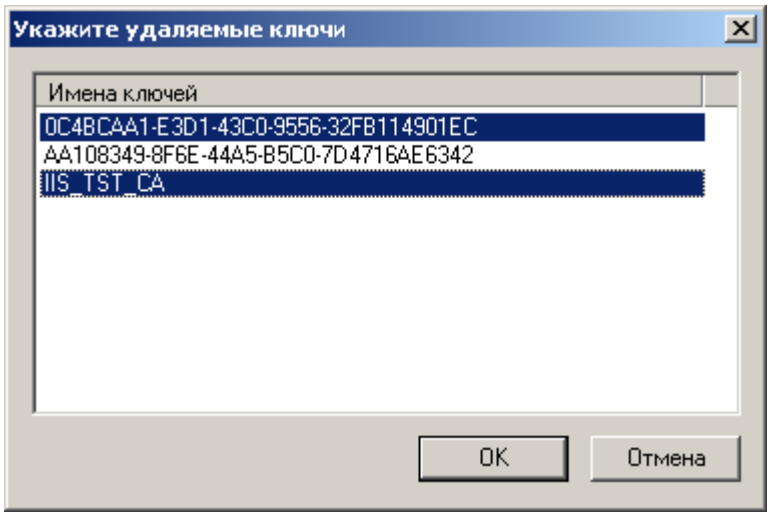

Рисунок 24 – Диалог выбора ключей для удаления

По окончании операции на экране появится сообщение об успешном завершении или сообщение об ошибке. При удалении ключа происходит трёхкратное затирание той части физической памяти носителя, где находился ключ, поэтому операция удаления может продолжаться дольше, чем просто запись ключа.

4.1.3 Смена пароля ключа

Для смены пароля ключа нажмите кнопку «Сменить пароль». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем на экране появится диалог выбора ключа. Если пользователь выбрал ключ, на который уже был установлен пароль, пользователь должен ввести его, а затем задать новый пароль с подтверждением (см. п. 2.2.2).

4.1.4 Преобразование ключа

Функцию преобразования закрытого ключа следует использовать при необходимости копирования закрытого ключа из одного криптографического провайдера в другой.

Выполнение преобразования возможно только для закрытых ключей, разрешенных для экспорта в зашифрованном виде. Выполнение преобразования закрытых ключей, совместимых со Средством КЗИ СКАД «Сигнатура» версия 3.6, невозможно.

Для преобразования ключа необходимо выбрать из соответствующих списков криптографические провайдеры - источник и приемник. Далее следует нажать кнопку «Преобразовать» (кнопка «Преобразовать» становится доступной при выборе допустимого набора параметров - Рисунок 25).

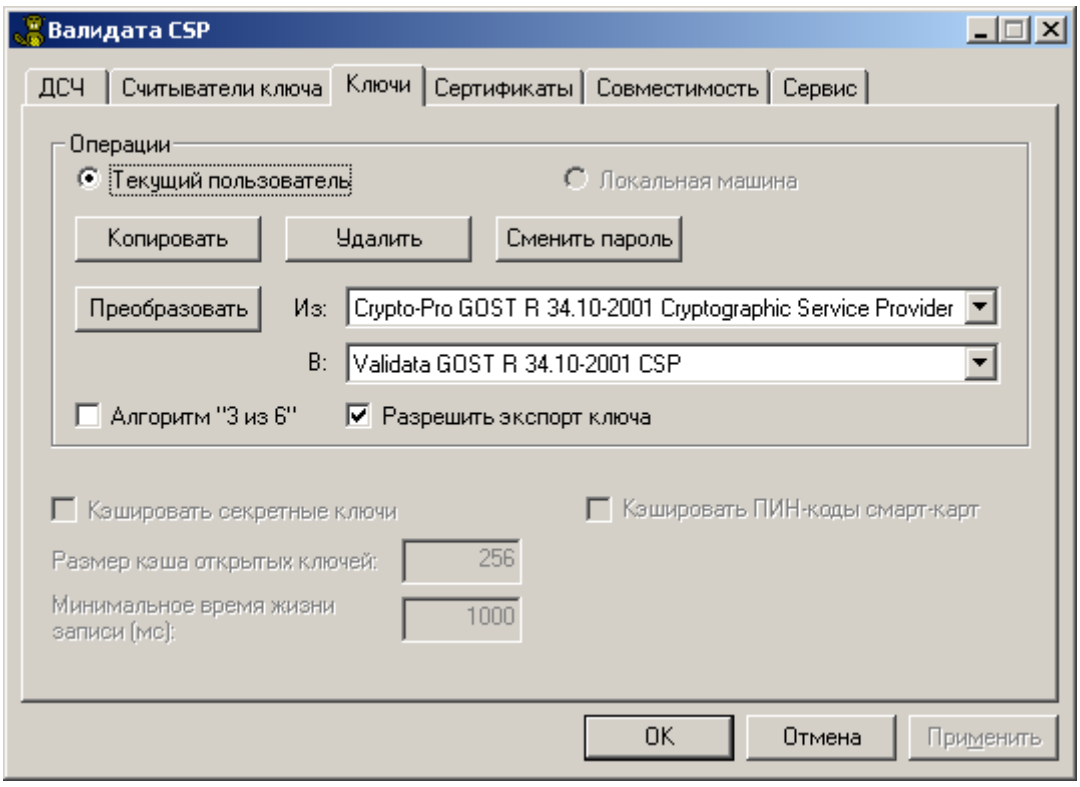

Рисунок 25 – Параметры преобразования установлены

На экран будет выдан список имен доступных для преобразования ключей. Выберите ключ из списка и нажмите кнопку «OK». При необходимости введите пароль для ключа и укажите ключевой носитель для записи преобразованного ключа.

4.1.5 Обновление масок ключа

Функцию обновления масок (перегенерации) закрытого ключа следует использовать исключительно для перегенерации закрытых ключей квалифицированных сертификатов, сформиро-

ванных по алгоритму «3 из 6» или «2 из 3». Данную процедуру необходимо применять для возможности использования таких закрытых ключей в течение увеличенного интервала времени.

Для обновления масок закрытого ключа нажмите кнопку «Обновить маски». Если инициализация ДСЧ ещё не была выполнена, на экране появятся диалоги инициализации ДСЧ (см. п. 3.2.1). Затем на экране появится диалог выбора ключа, сформированного по алгоритму «3 из 6» или «2 из 3». Следует загрузить требуемое количество ключей-долей секрета (3 - для ключей, сформированных по алгоритму «3 из 6»; 2 - для ключей, сформированных по алгоритму «2 из 3»), после чего произвести запись обновленных ключей-долей секрета (6 - для ключей, сформированных по алгоритму «3 из 6»; 3 - для ключей, сформированных по алгоритму «2 из 3») на чистые ключевые носители.

4.2 Операции с сертификатами

Перейдя на закладку «Сертификаты», пользователь может выполнять операции по установке сертификатов в различные хранилища (Рисунок 26).

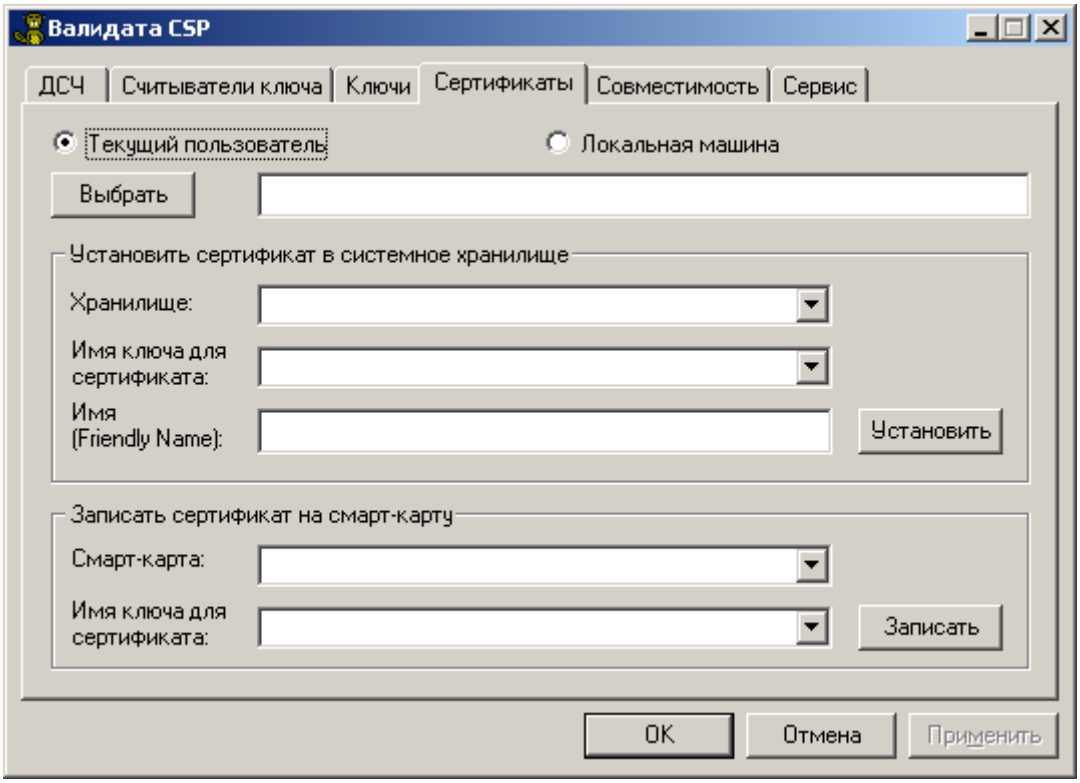

Рисунок 26 – Закладка «Сертификаты»

4.2.1 Установка сертификата в системное хранилище

Конфигурационная программа «Валидата CSP» позволяет помещать сертификат в системное хранилище ОС Windows. Сначала пользователь должен выбрать сертификат, для этого надо нажать кнопку «Выбрать» и в стандартном диалоговом окне выбрать файл сертификата. После этого на экране появится диалог, отображающий выбранный сертификат (Рисунок 27).

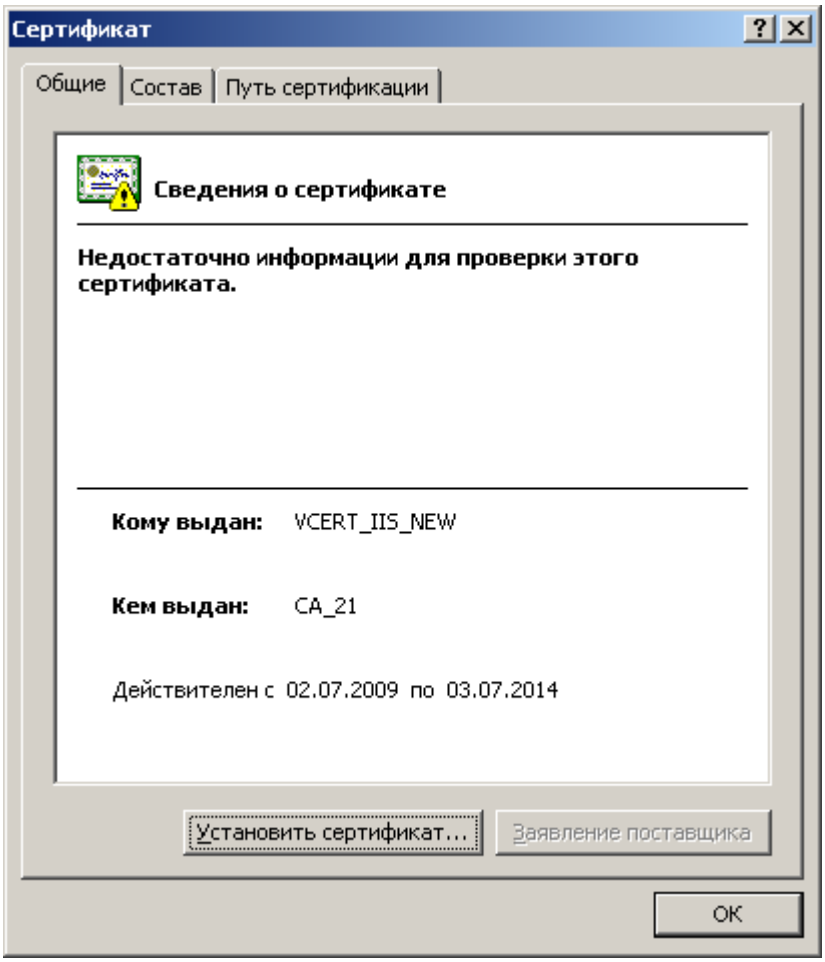

Рисунок 27 – Отображение выбранного сертификата

Конфигурационная программа анализирует выбранный сертификат и предлагает системное хранилище, в которое его следует установить. Далее программа пытается извлечь из сертификата имя (идентификатор) соответствующего закрытого ключа. Программа записывает его (если обнаружит) в поле «Имя ключа для сертификата», а извлечённое из сертификата имя владельца - в поле «Имя (Friendly Name)» (Рисунок 28).

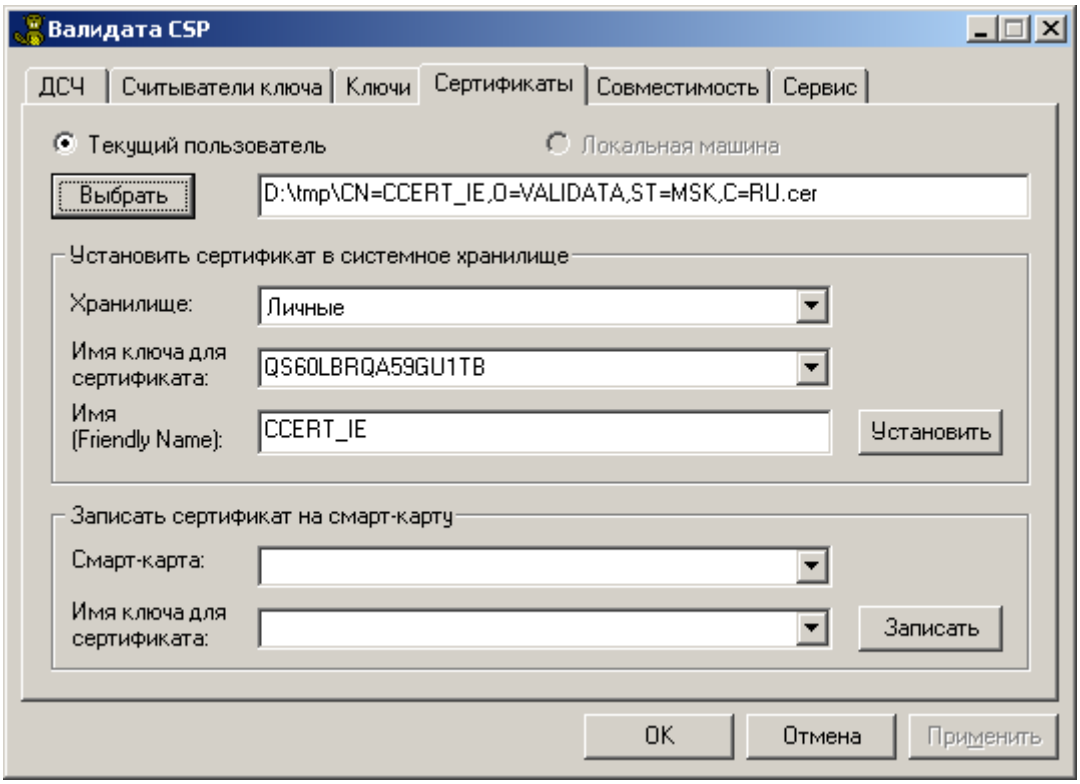

Рисунок 28 – Сертификат выбран

Пользователь может изменить хранилище, в которое следует поместить выбранный сертификат (Рисунок 29).

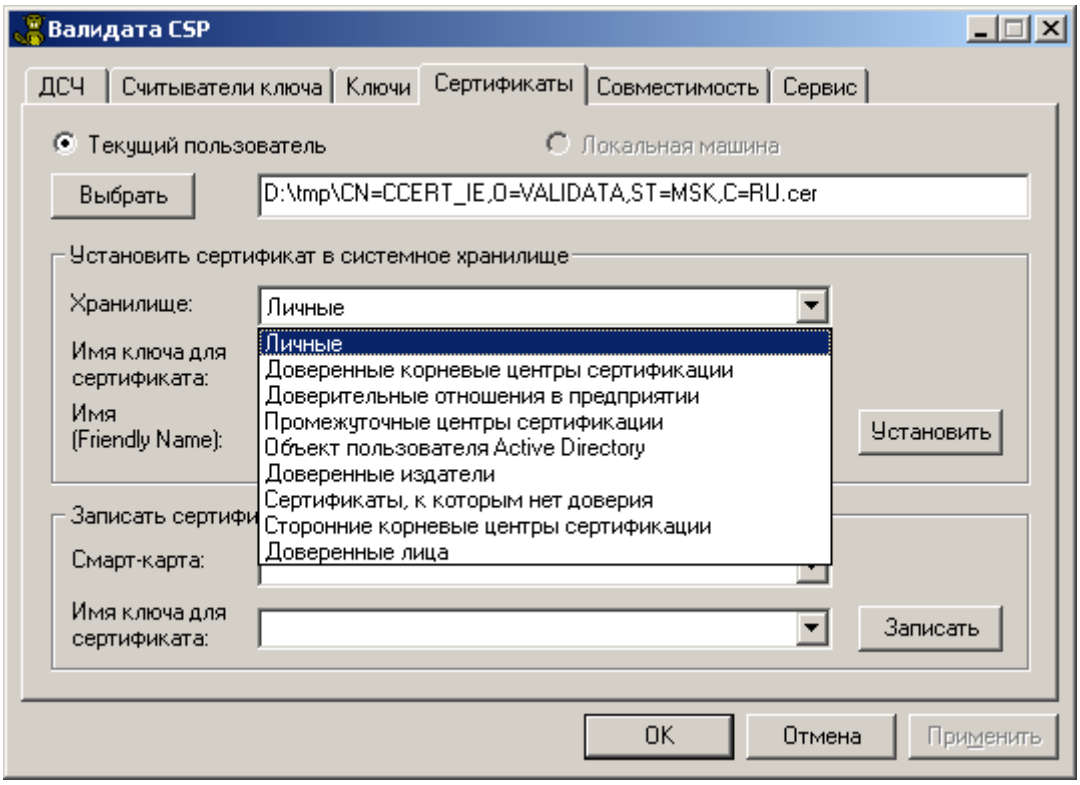

Рисунок 29 – Выбор хранилища для сертификата

Пользователь также может изменить имя (идентификатор) закрытого ключа, который будет привязан к сертификату через свойства (Property) системного хранилища. Для этого следует либо ввести имя вручную, либо выбрать из открывающегося списка. Если привязка закрытого ключа не требуется, пользователь может очистить это поле. Содержимое поля «Имя (Friendly Name)», которое помещается в соответствующее свойство системного хранилища, также может быть отредактировано вручную. Обычный пользователь может помещать сертификаты в системное хранилище только в раздел «Текущий пользователь». Если у пользователя есть соответствующие права, он может помещать сертификаты в раздел «Локальный компьютер». Для этого необходимо перевести переключатель в верхней части закладки в положение «Локальная машина».

После того, как все параметры заданы, пользователь должен нажать кнопку «Установить». Программа определяет, в какое хранилище должен быть установлен сертификат и помещает его туда. В случае успеха выдаётся сообщение (Рисунок 30).

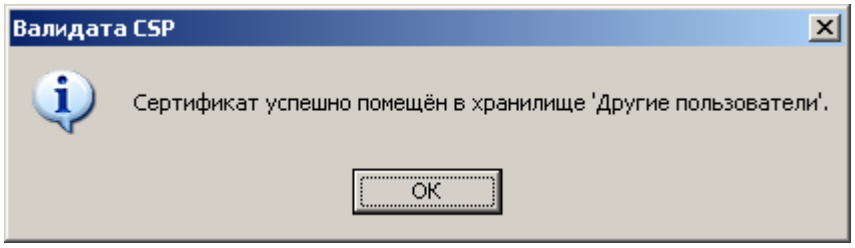

Рисунок 30 – Сообщение об успешном размещении сертификата

4.2.2 Запись сертификата на смарт-карту

Конфигурационная программа «Валидата CSP» позволяет записывать сертификат на смарт-карту, на которой находится соответствующий сертификату ключ ЭП. Сначала пользователь должен выбрать сертификат, для этого надо нажать кнопку «Выбрать» и в стандартном диалоговом окне выбрать файл сертификата. После этого на экране появится диалог, отображающий выбранный сертификат. Затем необходимо выбрать смарт-карту из открывающегося списка подключённых к компьютеру смарт-карт (Рисунок 31).

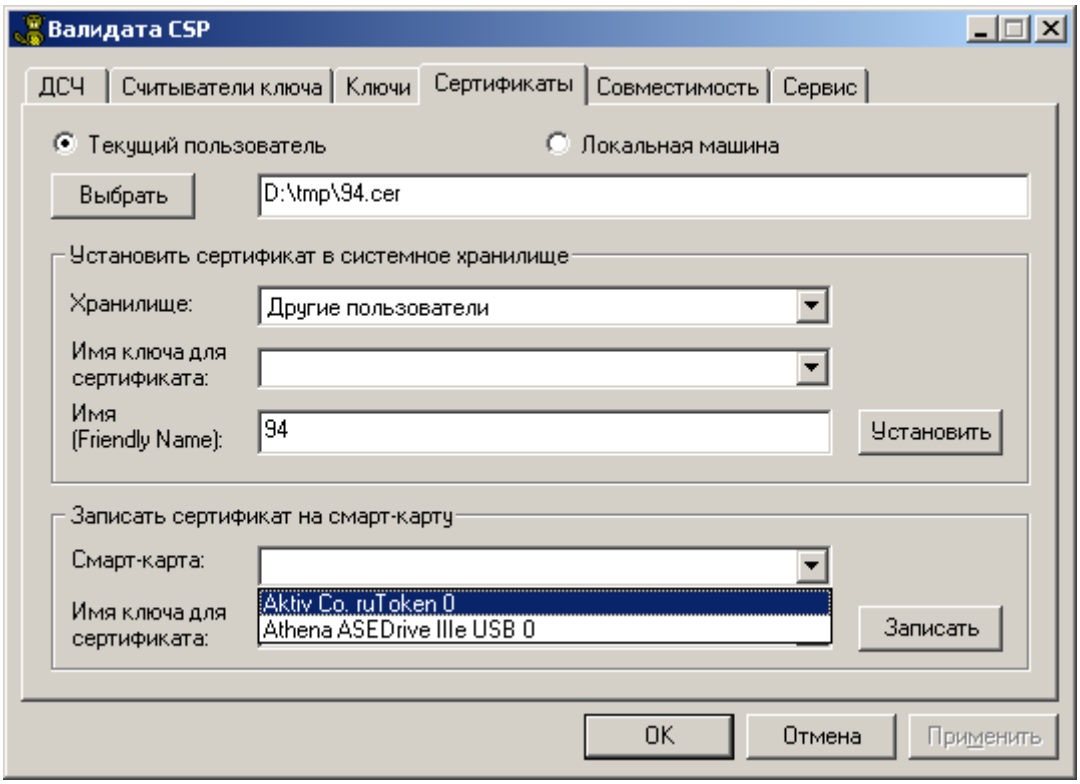

Рисунок 31 – Выбор смарт-карты

Если для выбранного типа смарт-карты не установлен считыватель ключа ЭП, будет выдана ошибка (Рисунок 32).

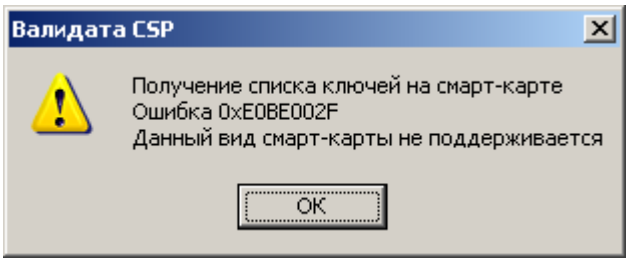

Рисунок 32 – Сообщение о неподдерживаемом типе смарт-карты

Затем следует выбрать из списка закрытых ключей, обнаруженных на смарт-карте, тот ключ, который соответствует записываемому сертификату, и нажать кнопку «Записать». В случае успеха выдаётся сообщение (Рисунок 33).

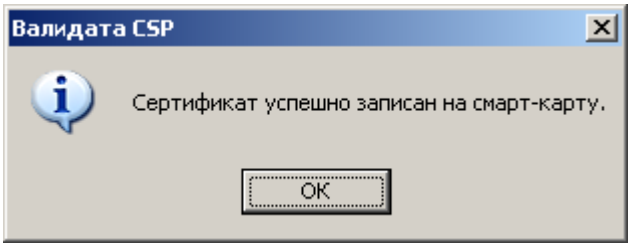

Рисунок 33 – Сообщение об успешной записи сертификата

При использовании смарт-карт с записанными на них сертификатами рекомендуется отключить их автоматическое распространение (т.е. помещение этих сертификатов в системные хранилища ОС Windows). Для этого следует настроить параметры службы «Распространение сертификата» (CertPropSvc) ОС Windows посредством редактирования групповой политики локального компьютера, установив значение параметра «Включить распространение сертификатов со смарт-карты» (находящегося в папке «Конфигурация компьютера»->«Административные шаблоны»->«Компоненты Windows»->«Смарт-карта») в «Отключить».

4.3 Настройки совместимости

Параметры совместимости с другими СКЗИ настраиваются на закладке «Совместимость» (Рисунок 34).

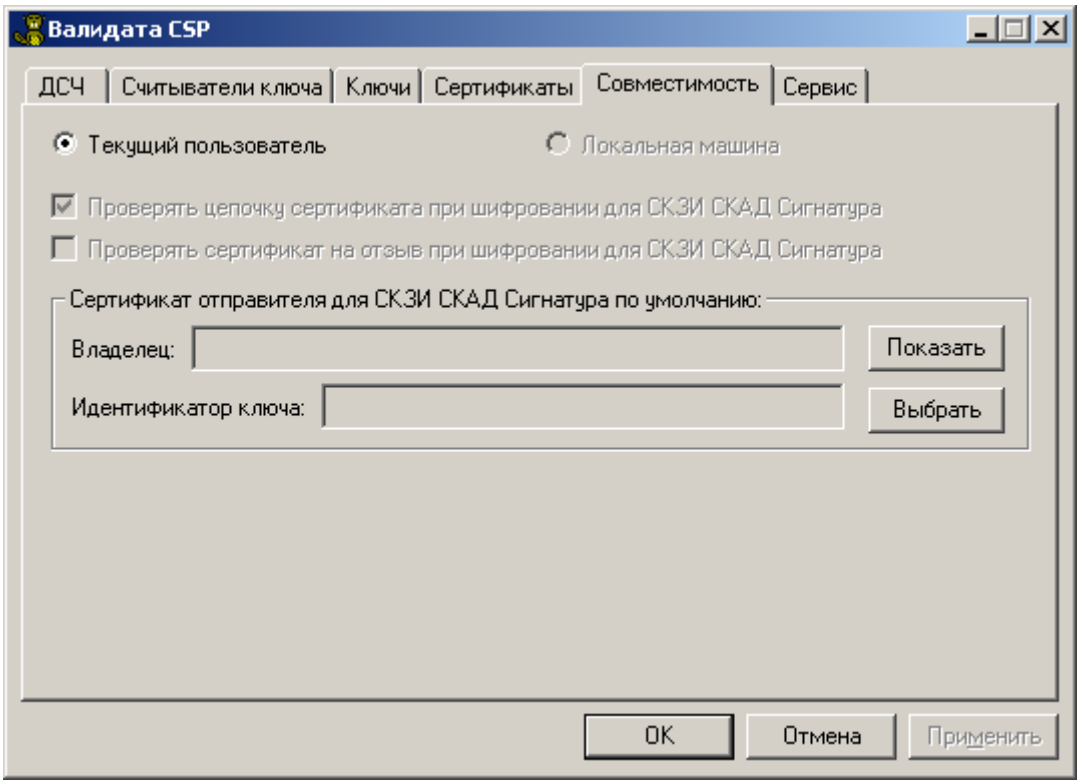

Рисунок 34 – Закладка «Совместимость»

4.3.1 Настройка сертификата шифрования по умолчанию для «Валидата CSP» СКАД «Сигнатура»

При шифровании для СКАД «Сигнатура» криптопровайдеру необходим ключ (сертификат) шифрования отправителя шифрованного сообщения. Некоторые программы, например Microsoft Office Outlook, не передают этот ключ (сертификат) провайдеру. В этом случае пользователь должен задать его в конфигурации. Для этого необходимо нажать кнопку «Выбрать» напротив поля «Идентификатор ключа». На экране откроется диалог со списком сертификатов с ключами шифрования для СКАД «Сигнатура», лежащих в системном хранилище «Личные» текущего пользователя (Рисунок 35).

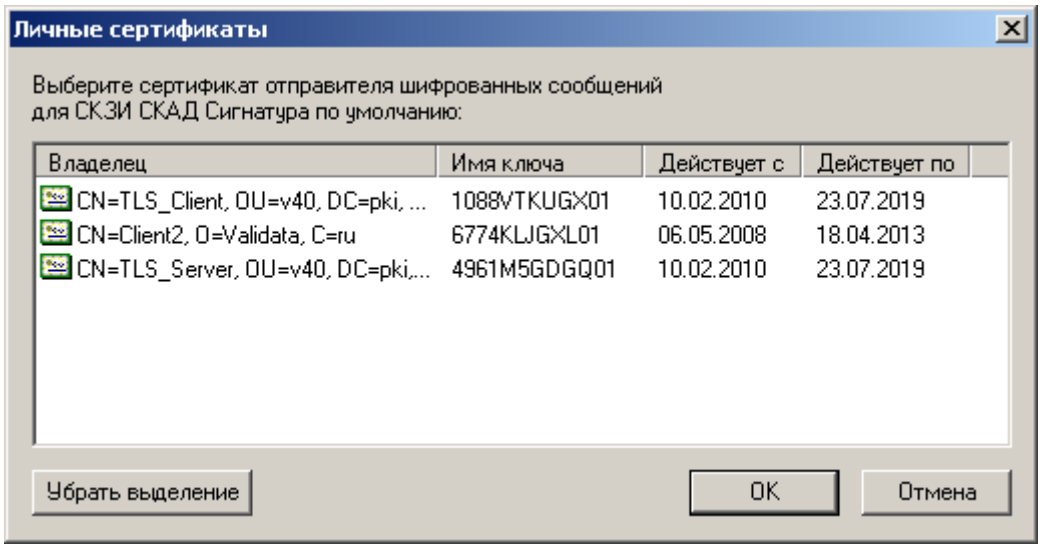

Рисунок 35 – Список личных сертификатов для шифрования

Если отображаемой в списке информации недостаточно, пользователь может дважды кликнуть правой кнопкой «мышки» на любом сертификате. Это приведёт к появлению на экране стандартного диалога просмотра сертификата (Рисунок 36).

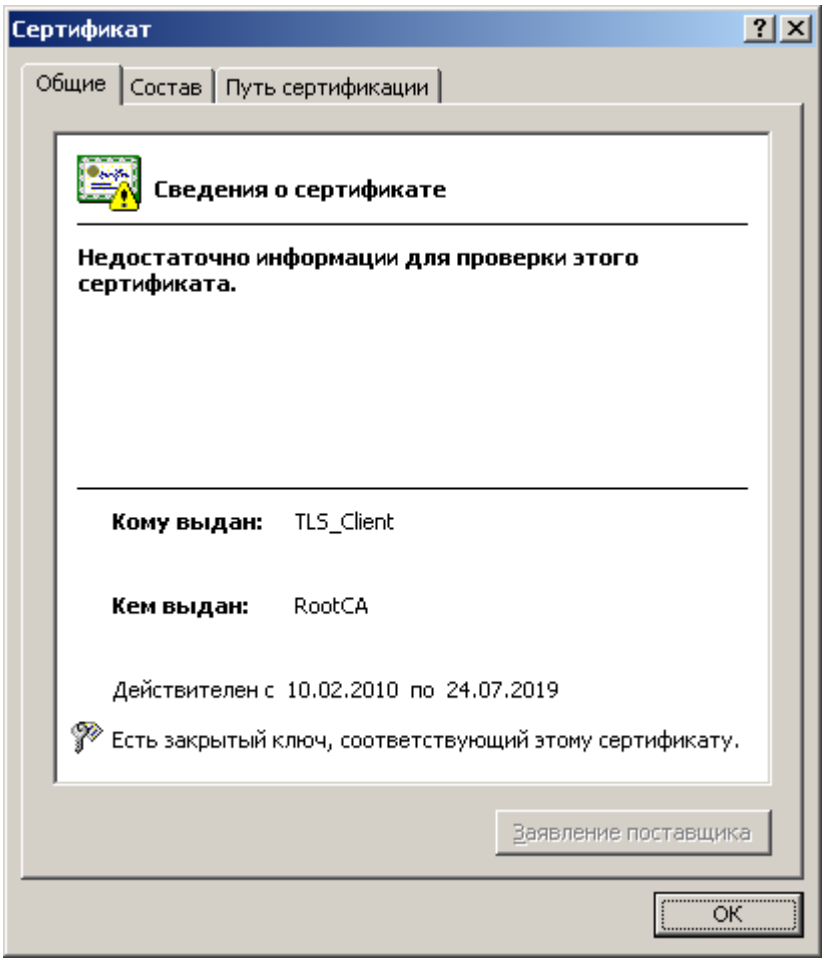

Рисунок 36 – Детальный просмотр сертификата из списка

Пользователь должен выбрать в списке сертификат, который по умолчанию будет исполь-

зоваться для шифрования для СКАД «Сигнатура» и нажать кнопку «ОК». Информация о выбранном сертификате отобразится на закладке «Совместимость» (Рисунок 37).

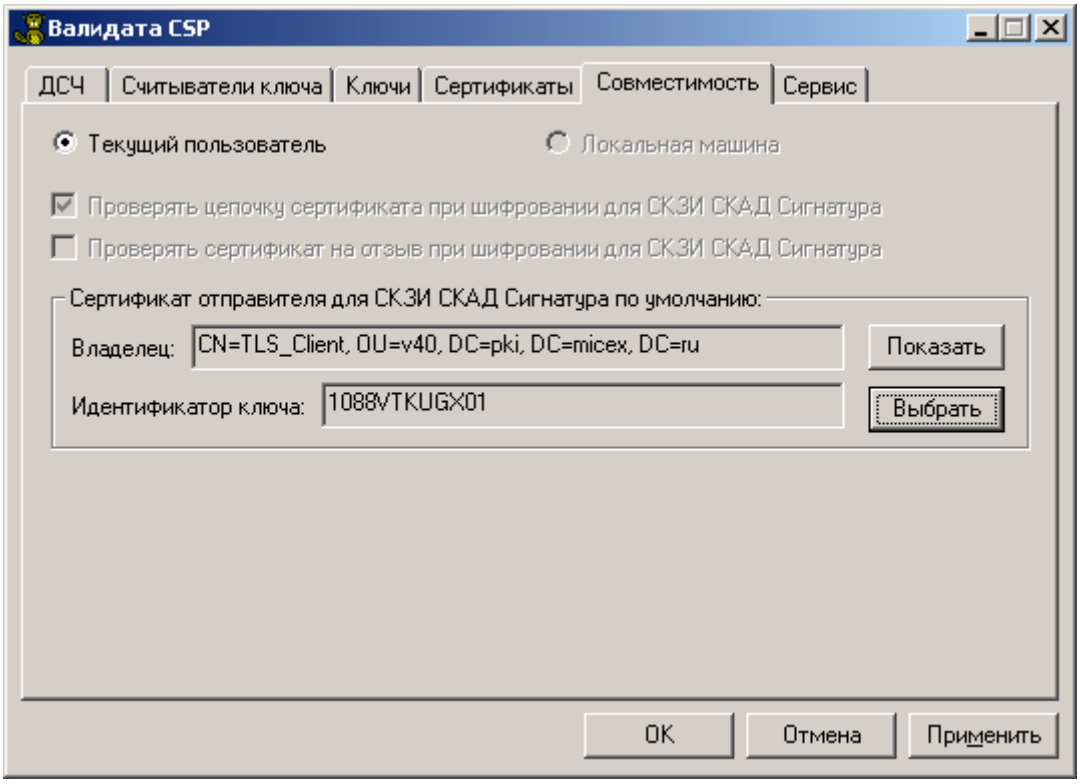

Рисунок 37 – Сертификат для шифрования выбран

Для того чтобы сделанные изменения вступили в силу, нажмите кнопку «Применить». Чтобы просмотреть информацию о выбранном сертификате, надо нажать кнопку «Показать». Чтобы изменить выбранный сертификат, необходимо ещё раз нажать кнопку «Выбрать» и выбрать другой сертификат. Непосредственное изменение параметров «Владелец» и «Идентификатор ключа» вручную невозможно. Чтобы очистить эти поля (отменить выбор сертификата по умолчанию) необходимо нажать кнопку «Выбрать» и в открывшемся диалоге нажать кнопку «Убрать выделение».

4.4 Дополнительные операции

Сервисные функции, не имеющие отношения к ключам и сертификатам, реализованы на закладке «Сервис» Конфигурационной программы «Валидата CSP» (Рисунок 38).

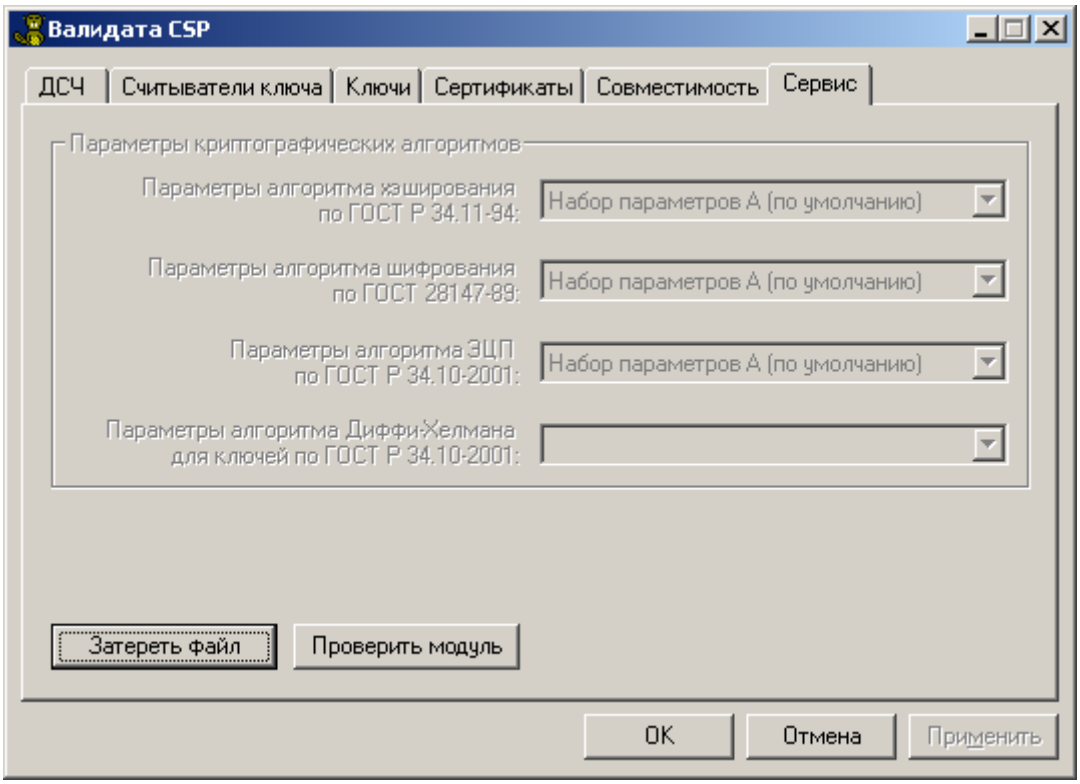

Рисунок 38 – Закладка «Сервис»

4.4.1 Уничтожение содержимого файла

Для надёжного уничтожения содержимого файла пользователь должен нажать кнопку «Затереть файл» и указать затираемый файл в стандартном диалоге выбора файла. Программа попросит подтверждение (Рисунок 39).

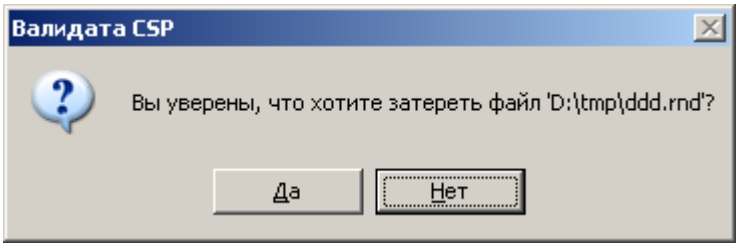

Рисунок 39 – Подтверждение затирания файла

Если пользователь нажмёт кнопку «Да», содержимое файла будет трижды перезаписано, после чего файл будет удалён из файловой системы.

4.4.2 Проверка подписи модулей

Во избежание умышленной или случайной подмены все исполняемые модули, входящие в ПО «Валидата CSP», подписаны. Нижеследующие модули, ответственные за выполнение криптографических операций и работу с ключами ЭП, подписаны по ГОСТ Р 34.10-2012 с использованием ключа ЭП разработчика ПО:

– модули криптографических библиотек;

– модуль библиотеки работы с подключаемыми модулями;

– подключаемые модули ДСЧ и считывателей;

– модуль конфигурационной программы;

– модуль программы преобразования ключей.

Остальные модули подписаны с использованием сертификата разработчика, полученного в компании VeriSign, с помощью утилиты Sign Tool (signtool.exe) из состава Microsoft Windows WDK. Проверка ЭП модулей, ответственных за выполнение криптографических операций и работу с ключами ЭП и закрытыми ключами шифрования, выполняется автоматически перед их загрузкой, т.е. исполняемый модуль не будет загружен при возникновении ошибки при проверке его ЭП.

При необходимости пользователь может проверить подпись любого модуля ПО, нажав кнопку «Проверить модуль» и выбрав модуль в стандартном диалоге выбора файла. В случае успеха на экран будет выдано сообщение (Рисунок 40). Следует иметь в виду, что при проверке vdcspe.dll выдаётся ошибка проверки подписи, т.к. данный модуль подписан компанией Microsoft и средствами конфигурационной программы не может быть проверен.

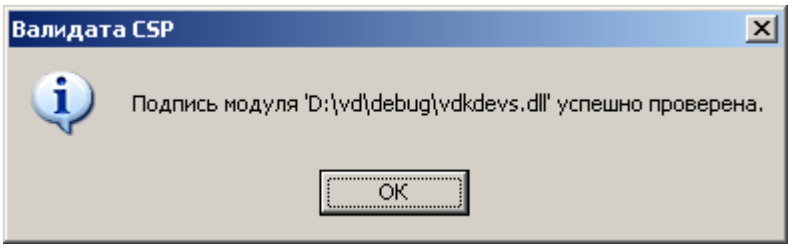

Рисунок 40 – Сообщение об успешной проверке подписи модуля

В противном случае будет выдано сообщение об ошибке, например (Рисунок 41).

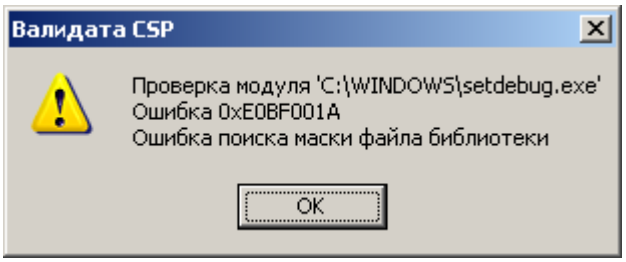

Рисунок 41 – Сообщение об отсутствии подписи в модуле

4.4.3 Форматирование и смена ПИН-кода ключевого носителя

В настоящее время функция форматирования поддерживается для считывателей vdToken (ФКН), vdToken, Соболь и SecretNet.

Для подготовки ключевого носителя к работе можно использовать функцию форматирования ключевого носителя. Для этого пользователь должен нажать кнопку «Форматировать» и указать требуемый считыватель в диалоговом окне выбора считывателей ключа (Рисунок 5).

Далее следует выбрать ключевой носитель для форматирования (Рисунок 42).

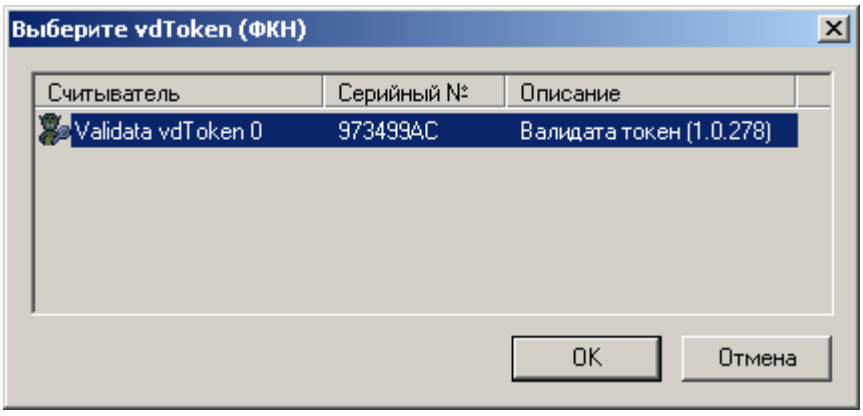

Рисунок 42 – Выбор ключевого носителя

В диалоговом окне ввода параметров форматирования ключевого носителя (Рисунок 43) следует указать требуемые параметры форматирования и нажать кнопку «OK»:

– параметр «Максимальный размер сертификата» указывает максимальный размер сертификата в DER-кодировке, который можно будет записать на ключевой носитель;

– при включении опции «Работать без ПИН-кода» использование носителя в качестве функционального ключевого носителя (ФКН) будет невозможным;

– при включении опции «Усиленная защита ключа» ключевой носитель невозможно будет использовать с предыдущими версиями СКЗИ «Валидата CSP».

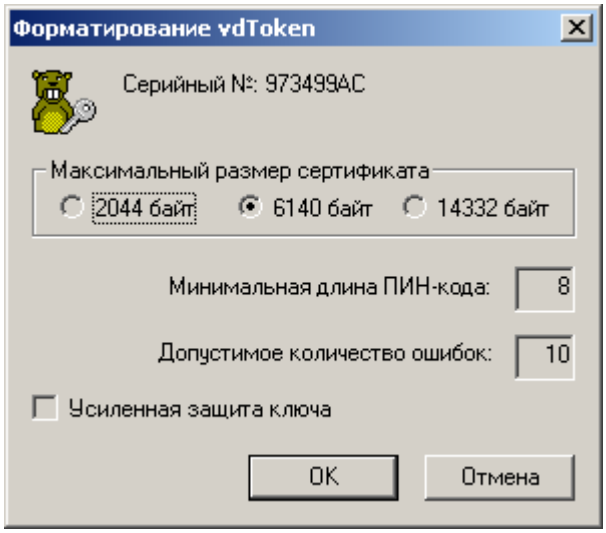

Рисунок 43 – Параметры форматирования

Перед началом процедуры форматирования будет выдано предупреждение о необратимом удалении данных на форматируемом носителе.

В настоящее время функция смены ПИН-кода поддерживается для считывателей vdToken (ФКН) и vdToken.

Для смены ПИН-кода ключевого носителя пользователь должен нажать кнопку «Сменить ПИН-код» и указать требуемый считыватель в диалоговом окне выбора считывателей ключа (Рисунок 5).

Далее следует выбрать ключевой носитель для смены ПИН-кода (Рисунок 42).

В диалоговом окне смены ПИН-кода ключевого носителя (Рисунок 44) следует ввести старый ПИН-код (если он был установлен ранее), ввести два раза новый ПИН-код и нажать кнопку «ОК».

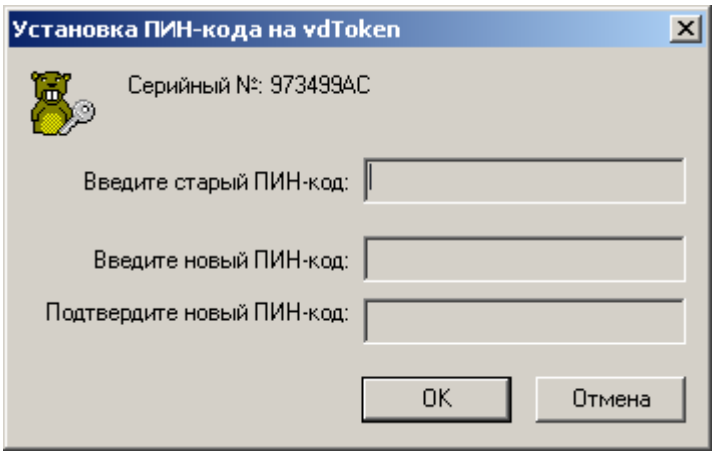

Рисунок 44 – Смена ПИН-кода

5 ПРОГРАММА ПРЕОБРАЗОВАНИЯ КЛЮЧЕЙ

В состав СКЗИ «Валидата CSP» входит программа преобразования ключей, с помощью которой можно выполнить преобразование ключа из формата СКАД «Сигнатура» в формат криптографического провайдера «Валидата CSP».

Программа преобразования ключей выполнена в виде утилиты командной строки WO2CSP.EXE, которая находится в каталоге установки криптографического провайдера (по умолчанию C:\Program Files\Validata\VDCSP).

С помощью программы WO2CSP.EXE можно выполнить преобразование ключей, которые находятся на ключевом носителе типа «дискета» или на ключевом носителе типа «флэш-память». Если ключ расположен на ключевом носителе другого типа (например, Touch Memory «Аккорда»), то перед выполнением преобразования необходимо скопировать ключ при помощи «Валидата CSP» СКАД «Сигнатура» на ключевую «дискету» или на ключевой носитель «USB-flash».

Для выполнения преобразования необходимо установить ключевую «дискету» в дисковод или ключевой носитель «USB-flash» в USB порт. После этого запустить из главного меню ОС Windows консоль «командной строки», перейти в каталог установки криптографического провайдера с помощью команды CD «C:\Program Files \Validata \VDCSP» и запустить программу преобразования следующим образом:

wo2csp.exe 1 a:

- для «дискеты» или

wo2csp.exe 1 f:

- для носителя «USB-flash», который подключена как диск «f:» (возможны варианты «d:», «e:», ...).

Программа преобразования считает ключ в формате СКАД «Сигнатура» с носителя типа «дискета» или с носителя типа «флэш-память» и выдаст диалоговое окно для выбора ключевого носителя, который поддерживается криптографическим провайдером «Валидата CSP». Установите носитель и укажите его в диалоговом окне для записи на него копии ключа СКАД «Сигнатура» в формате «Валидата CSP».

Если в командной строке запуска программы преобразования ключей задать номер 3 (например, wo2csp.exe 3 a:), то будет выполнено преобразование ключа СКАД «Сигнатура», сформированного по алгоритму «3 из 6». В этом случае для чтения ключа нужно будет последовательно установить в дисковод три ключевые «дискеты», а после этого для записи копии ключа потребуется последовательно установить шесть чистых ключевых носителей.

Дополнительно программа преобразования может выполнять преобразование ключей из следующих ключевых форматов:

– формат ключа («VCERT PKI») только для выполнения ЭП (в командной строке нужно указать номер 2);

– формат ключа («VCERT PKI») для выполнения ЭП и шифрования (в командной строке нужно указать номер 4);

– формат ключа по схеме «3 из 6» («VCERT PKI») на один ключевой носитель в формате «Валидата CSP» (в командной строке нужно указать номер 5);

– формат ключа по схеме «3 из 6» («VCERT PKI») на 6 ключевых носителей («3 из 6») в формате «Валидата CSP» (в командной строке нужно указать номер 6).

ПЕРЕЧЕНЬ РИСУНКОВ

1 Закладка «Считыватели ключа» . . . 5
2 Пользователь может изменить настройку считывателя ключа . . . 6
3 Диалог выбора считывателя ключа . . . 6
4 Изменение считывателя ключа для текущего пользователя . . . 7
5 Диалог выбора считывателя ключа . . . 7
6 Диалог выбора диска . . . 8
7 Сообщение об отсутствии ключевого носителя . . . 8
8 Диалог выбора ключа . . . 9
9 Диалог задания пароля ключа . . . 9
10 Диалог повторного задания пароля ключа . . . 9
11 Диалог проверки пароля ключа . . . 10
12 Диалог повторной проверки пароля ключа . . . 10
13 Панель управления Рутокен . . . 11
14 Закладка ДСЧ . . . 12
15 Пользователь может изменить настройку ДСЧ . . . 13
16 Диалог выбора ДСЧ . . . 13
17 ДСЧ для текущего пользователя изменён . . . 14
18 Получение случайных чисел с помощью пользователя . . . 15
19 Сообщение об удачной инициализации ДСЧ . . . 15
20 Сообщение об инициализованном ДСЧ . . . 15
21 Закладка «Ключи» . . . 16
22 Сообщение о замене ключевого носителя . . . 16
23 Сообщение об ошибке при копировании ключа . . . 17
24 Диалог выбора ключей для удаления . . . 17
25 Параметры преобразования установлены . . . 18
26 Закладка «Сертификаты» . . . 19
27 Отображение выбранного сертификата . . . 20
28 Сертификат выбран . . . 21
29 Выбор хранилища для сертификата . . . 21
30 Сообщение об успешном размещении сертификата . . . 22
31 Выбор смарт-карты . . . 23
32 Сообщение о неподдерживаемом типе смарт-карты . . . 23
33 Сообщение об успешной записи сертификата . . . 23
34 Закладка «Совместимость» . . . 24
35 Список личных сертификатов для шифрования . . . 25
36 Детальный просмотр сертификата из списка . . . 25
37 Сертификат для шифрования выбран . . . 26
38 Закладка «Сервис» . . . 27
39 Подтверждение затирания файла . . . 27
40 Сообщение об успешной проверке подписи модуля . . . 28
41 Сообщение об отсутствии подписи в модуле . . . 28
42 Выбор ключевого носителя . . . 29
43 Параметры форматирования . . . 29
44 Смена ПИН-кода . . . 30

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					