АО «СИГНАЛ-КОМ»

УТВЕРЖДЁН

ШКНР.033-07 90 05-ЛУ

БИБЛИОТЕКА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«Signal-COM CSP»

Версия 3.2

Модуль настроек и сервисных функций

Руководство пользователя

ШКНР.033-07 90 05

Листов 20

2020

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Данный документ содержит руководство по использованию программы Администратор, предназначенной для настройки параметров "Signal-COM CSP", а также для выполнения операций с ключевыми контейнерами: копирование, удаление, изменение пароля, импорт и экспорт сертификатов.

2. ЛИЦЕНЗИЯ

Если Вы не ввели ключ продукта (лицензии) при установке "Signal-COM CSP", данное программное обеспечение будет функционировать в течение 30 дней с момента установки.

Чтобы ввести ключ продукта необходимо выполнить следующие действия:

- Выберите пункт меню "Операция-Лицензия".
- В окне "Введите лицензионные данные" задайте имя владельца, наименование организации (необязательно) и ключ продукта. Нажмите "OK".

Примечание. Если ранее уже был задан ключ продукта на неограниченную по времени лицензию, пункт меню "Лицензия" будет недоступен.

3. ПРОСМОТР СЕРТИФИКАТА

Данная операция позволяет просмотреть свойства сертификата в ключевом контейнере.

Сертификат может быть помещен в ключевой контейнер с помощью операции Импорт сертификата из файла или операции Импорт сертификата из локального хранилища.

Сертификат может быть экспортирован из ключевого контейнера в локальное хранилище сертификатов, в отдельный файл или перенесен на ключевом носителе на другой компьютер.

Для просмотра сертификата в ключевом контейнере необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Сертификат-Просмотр" (или "Просмотр-Сертификат") или нажмите соответствующую кнопку на инструментальной панели.
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- Если сертификат в ключевом контейнере отсутствует, на экран будет выдано окно с соответствующим сообщением и операция будет прервана.
- Если сертификат в ключевом контейнере присутствует, на экран будет выдано стандартное окно "Сертификат" со свойствами сертификата.

Примечание. Не используйте в окне "Сертификат" кнопку "Установить сертификат": для установки сертификата необходимо использовать операцию Экспорт сертификата в локальное хранилище.

4. ИМПОРТ СЕРТИФИКАТА ИЗ ФАЙЛА

Импорт сертификата в ключевой контейнер необходим для дальнейшего переноса этого сертификата на ключевом носителе на любой другой компьютер и экспорт в его локальное хранилище сертификатов.

Для импорта сертификата из файла в ключевой контейнер необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Сертификат-Импорт-Из файла".
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- Если сертификат в ключевом контейнере уже существует, на экран будет выдано окно с предупреждением (для просмотра свойств сертификата в ключевом контейнере используйте операцию Просмотр сертификата). Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".
- В стандартном окне для открытия файла выберите сертификат и нажмите кнопку "Открыть".
- Если выбранный сертификат не соответствует ни одному из ключей данного контейнера, на экран будет выдано окно с сообщением об ошибке и операция будет прервана.
- В случае успешного импорта сертификата и его отсутствия в локальном хранилище, Вам будет предложено экспортировать сертификат в локальное хранилище сертификатов. Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".

5. ИМПОРТ СЕРТИФИКАТА ИЗ ЛОКАЛЬНОГО ХРАНИЛИЩА

Импорт сертификата в ключевой контейнер необходим для дальнейшего переноса этого сертификата на ключевом носителе на любой другой компьютер и экспорта его в локальное хранилище этого компьютера.

Для импорта сертификата из локального хранилища необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Сертификат-Импорт-Из хранилища".
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- Если сертификат в ключевом контейнере уже существует, на экран будет выдано окно с предупреждением (для просмотра свойств сертификата в ключевом контейнере используйте операцию Просмотр сертификата). Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".
- Если подходящий сертификат в локальном хранилище не найден, на экран будет выдано окно с сообщением об ошибке и операция будет прервана.

6. ЭКСПОРТ СЕРТИФИКАТА В ЛОКАЛЬНОЕ ХРАНИЛИЩЕ

Данная операция помещает сертификат из ключевого контейнера в локальное хранилище сертификатов и устанавливает связь между сертификатом и ключевым контейнером. Эта связь необходима для формирования электронных подписей и расшифрования сообщений с использованием данного сертификата и ключевого контейнера.

Для экспорта сертификата из ключевого контейнера в локальное хранилище сертификатов необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Сертификат-Экспорт-В хранилище" или нажмите соответствующую кнопку на инструментальной панели.
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- Если сертификат в ключевом контейнере отсутствует, на экран будет выдано окно с соответствующим сообщением и операция будет прервана. Если сертификат в ключевом контейнере присутствует, операция будет продолжена.
- Если сертификат для данного ключевого контейнера в локальном хранилище уже существует, на экран будет выдано окно с предупреждением. Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".

7. ЭКСПОРТ СЕРТИФИКАТА В ФАЙЛ

Для экспорта сертификата из ключевого контейнера в файл необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Сертификат-Экспорт-В файл".
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- Если сертификат в ключевом контейнере отсутствует, на экран будет выдано окно с соответствующим сообщением и операция будет прервана. Если сертификат в ключевом контейнере присутствует, операция будет продолжена.
- В стандартном окне для записи файла задайте имя файла сертификата и нажмите кнопку "Сохранить".
- Если файл с заданным именем уже существует, на экран будет выдано окно с предупреждением. Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".

8. КОПИРОВАНИЕ КЛЮЧЕВОГО КОНТЕЙНЕРА

Данная операция позволяет скопировать ключевой контейнер с одного ключевого носителя на другой или на один и тот же, но с другим именем.

Для копирования ключевого контейнера необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Копировать".
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- В окне ввода имени нового ключевого контейнера задайте новое имя или оставьте старое имя без изменений. Нажмите "OK".
- В окне со списком ключевых носителей и контейнеров выберите ключевой носитель для создания нового ключевого контейнера. Нажмите "OK".
- Если ключевой контейнер с заданным именем на выбранном ключевом носителе уже существует, на экран будет выдано окно с предупреждением. Для того чтобы выбрать другой ключевой носитель нажмите "Нет", для того чтобы переписать существующий ключевой контейнер нажмите "Да".

9. УДАЛЕНИЕ КЛЮЧЕВОГО КОНТЕЙНЕРА

Данная операция позволяет удалить ключевой контейнер на ключевом носителе.

Для удаления ключевого контейнера необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Удалить" или нажмите клавишу "Delete".
- На экран будет выдано окно с предупреждением. Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".

10. ДОБАВЛЕНИЕ ТИПОВ КЛЮЧЕВЫХ НОСИТЕЛЕЙ

Некоторые типы зарегистрированных ключевых носителей могут быть исключены из списка доступных типов для ускорения работы "Signal-COM CSP". Данная операция позволяет сделать эти ключевые носители доступными для "Signal-COM CSP".

Для добавления типа ключевого носителя необходимо выполнить следующие действия:

- Выберите пункт меню "Операция-Добавить" или нажмите клавишу "Insert".
- В окне со списком типов ключевых носителей выберите тип, который необходимо добавить. Нажмите "OK".

12. УДАЛЕНИЕ ТИПОВ КЛЮЧЕВЫХ НОСИТЕЛЕЙ

Неиспользуемые типы зарегистрированных ключевых носителей замедляют работу "Signal-COM CSP". Данная операция позволяет сделать эти ключевые носители недоступными для "Signal-COM CSP".

Для удаления типа ключевого носителя из списка доступных типов необходимо выполнить следующие действия:

- В списке ключевых носителей отметьте тип ключевого носителя, который необходимо удалить.
- Выберите пункт меню "Операция-Удалить" или нажмите клавишу "Delete".
- На экран будет выдано окно с предупреждением. Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".

13. ПАРОЛЬ КЛЮЧЕВОГО КОНТЕЙНЕРА

"Signal-COM CSP" позволяет защитить доступ к ключевому контейнеру индивидуальным паролем.

Для того чтобы установить защиту ключевого контейнера на пароле, необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Пароль".
- В окне выбора операции для пароля ключевого контейнера задайте операцию "Установить". Нажмите "OK".
- В окне ввода нового пароля ключевого контейнера дважды введите новый пароль. Нажмите "OK".

Примечание. Для ключевых носителей, имеющих встроенную систему аутентификации, защита ключевых контейнеров на пароле не предусмотрена.

Для того чтобы изменить пароль ключевого контейнера, необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Пароль".
- Если доступ к ключевому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- В окне выбора операции для пароля ключевого контейнера задайте операцию "Изменить". Нажмите "OK".
- В окне ввода нового пароля ключевого контейнера дважды введите новый пароль. Нажмите "OK".

Для того чтобы отменить защиту ключевого контейнера на пароле, необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Пароль".

- Если доступ к ключевому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- В окне выбора операции для пароля ключевого контейнера задайте операцию "Отменить". Нажмите "OK".

14. ЭКСПОРТ КЛЮЧЕВОГО КОНТЕЙНЕРА В ФОРМАТЕ СКЗИ "КРИПТО-КОМ"

Данная процедура предназначена для экспорта ключевого контейнера в виде файловой структуры ключевого носителя СКЗИ "Крипто-КОМ".

Для экспорта ключевого контейнера необходимо выполнить следующие действия:

- В списке ключевых носителей и контейнеров отметьте необходимый контейнер.
- Выберите пункт меню "Операция-Экспорт".
- Если выбранный ключевой контейнер защищен на пароле, и доступ к этому контейнеру ранее не осуществлялся, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- В стандартном окне выберите существующий каталог, в который будет экспортирован ключевой контейнер. Нажмите "OK".
- Если в выбранном каталоге уже находятся файлы СКЗИ "Крипто-КОМ", Вам будет предложено удалить их. Будьте осторожны, чтобы не потерять необходимую ключевую информацию! Чтобы прервать операцию нажмите "Нет", для продолжения операции нажмите "Да".
- Вам будет предложено зашифровать парный секретный ключ на пароле. Если Вы выбрали шифрование, в окне ввода нового пароля дважды введите новый пароль и нажмите "OK".

15. ИМПОРТ КЛЮЧЕВОГО КОНТЕЙНЕРА В ФОРМАТЕ СКЗИ "КРИПТО-КОМ"

Данная процедура предназначена для создания ключевого контейнера на основе файловой структуры ключевого носителя СКЗИ "Крипто-КОМ".

Для создания ключевого контейнера необходимо выполнить следующие действия:

- Выберите пункт меню "Операция-Импорт".
- В окне диалога задайте имя нового ключевого контейнера, которое не должно совпадать с именами существующих контейнеров.
- Задайте путь к каталогу ключевого носителя СКЗИ "Крипто-КОМ", который может быть выбран в стандартном диалоге, появляющемся после нажатия расположенной справа кнопки.
- Задайте путь к файлу парного секретного ключа, который может быть выбран в стандартном диалоге, появляющемся после нажатия расположенной справа кнопки. Если ключевому носителю СКЗИ "Крипто-КОМ" соответствует только один парный секретный ключ, и этот ключ находится в каталоге по умолчанию (подкаталог KEYS), задавать путь к этому ключу не обязательно. Нажмите "OK".
- Если парный секретный ключ защищен на пароле, на экран будет выдано окно для ввода пароля. Введите пароль и нажмите "OK".
- В окне со списком ключевых носителей и контейнеров выберите ключевой носитель для создания нового ключевого контейнера. Нажмите "OK".
- Если указанному ключевому носителю СКЗИ "Крипто-КОМ" соответствуют более одного парного секретного ключа, повторите данную операцию для всех остальных ключей.

16. ПОДПИСЬ ФОРМ

В "Signal-COM CSP" реализована опциональная возможность генерации электронной подписи HTML-форм при использовании браузера MS Interner Explorer для совместимости с системой «Inter-PRO» (см. руководство пользователя программы «Inter-PRO Client»).

По умолчанию данная функция отключена, для ее подключения и настройки других параметров подписи необходимо выполнить следующие действия:

- Выберите пункт меню "Операция-Подпись форм".
- В окне диалога установите одно из значений переключателя "Подпись форм":

  «Обязательная» - подписываются все HTML-формы;

  «Выборочная» - подписываются только формы, имеющие определенный формат (см. руководство администратора программы «Inter-PRO Server»).

  Если установлено значение «Нет», формы не подписываются.

- Установите флажок "Запрашивать подтверждение на подпись формы", если Вы хотите контролировать подписываемые данные (рекомендуется). Если данный флажок установлен, перед подписью формы будет выдаваться окно с запросом, в котором будут отображаться подписываемые данные формы. Если Вы не подтверждаете запрос на подпись формы, то параметры формы на сервер не передаются.
- Установите флажок "Использовать скролируемое окно", если подписываемые данные необходимо выдавать в скролируемом окне (рекомендуется, если формы содержат большой объем данных, который не может быть отображен на экране полностью).
- Установите флажок "Не кэшировать информацию ключевого носителя", если необходимо чтобы при каждой подписи осуществлялось обращение к ключевому носителю (рекомендуется).
- Нажмите "OK".

17. ИНИЦИАЛИЗАЦИЯ ДАТЧИКА СЛУЧАЙНЫХ ЧИСЕЛ

"Signal-COM CSP" использует встроенный датчик случайных чисел (ДСЧ), который должен быть инициализирован перед использованием. Инициализация ДСЧ осуществляется двумя способами: с использованием существующего ключевого контейнера или с помощью специальной процедуры, которая требует нажатий клавиатуры или перемещений курсора мыши.

Если у Вас есть ключевой контейнер, Вы можете использовать его для инициализации ДСЧ. Чтобы упростить процедуру инициализации, Вы можете предварительно задать этот контейнер в настройке программы Администратор. Для этого выполните следующие действия:

- Выберите пункт меню "Операция-Инициализация ДСЧ".
- В окне со списком доступных ключевых устройств и контейнеров выберите соответствующий ключевой контейнер.

ЛИТЕРАТУРА

1. СКЗИ «Крипто-КОМ 3.4». Формуляр. ШКНР.00046-01 30 02, ЗАО «Сигнал-КОМ», 2017.