



КАРМА

Руководство пользователя

©Электронные Офисные Системы. 2020 г.

Оглавление

Оглавление	2
Основные понятия.....	4
Компоненты КАРМА.....	5
Модуль поддержки СКЗИ.....	5
Управление настройками	5
Визуальная оболочка КАРМА.....	16
<i>Настройки</i>	17
Вкладка «Обязательные».....	17
Вкладка «Объекты поддержки криптографии».....	21
Вкладка «Штамп времени и OCSP».....	22
Вкладка «Режим удалённой проверки подписей»	23
<i>Профили</i>	23
<i>Мастера операций</i>	24
Мастер создания ЭП.	24
Мастер добавления ЭП к существующей.	26
Мастер заверения ЭП.	27
Мастер проверки ЭП.....	30
Мастер шифрования.....	30
Мастер расшифровывания.	33
Мастер создания подписанного и зашифрованного контейнера	35
Мастер расшифровывания и проверки ЭП подписанного и зашифрованного контейнера.	35
Мастер отсоединения /присоединения подписанного файла данных	35
<i>Списки настроек профиля для операций</i>	35
Создание, добавление, заверение ЭП:.....	35
Шифрование:.....	36
Расшифровывание	36

Вызов функций криптографического сервиса	36
Установка и удаление	36
<i>Установка KARMA</i>	36
<i>Удаление KARMA</i>	36
Работа с криптографическими провайдерами и инфраструктурой открытых ключей	37

Основные понятия

Электронный документ – документ, информация в котором представлена в электронно - цифровой форме.

Средство электронной подписи – средство криптографической защиты информации (СКЗИ) или другое средство, обеспечивающее реализацию следующих функций:

- создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи
- подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе
- создание закрытых и открытых ключей электронных подписей.

Электронная подпись (ЭП) – реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ЭП, а также установить отсутствие искажения информации в электронном документе.

Закрытый ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата открытого ЭП и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

Закрытый ключ электронной подписи действует на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат открытого ключа ЭП, соответствующий данному закрытому ключу не аннулирован (отозван) и действие его не приостановлено.

Открытый ключ электронной подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Список отозванных сертификатов (СОС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписи, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

Владелец сертификата ЭП – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ЭП и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Псевдоним владельца сертификата ЭП – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Сервер штампов времени – удаленный доверенный сервер, который предоставляет доверенную информацию о времени подписания для вложения ее в создаваемую электронную подпись

Сервер OCSP – удаленный доверенный сервер, который предоставляет информацию о состоянии отзыва сертификатов

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

- PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 signed – подписанные данные;
- PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ЭП.

Компоненты КАРМА

Модуль поддержки СКЗИ

Модуль поддержки СКЗИ – исполняемое приложение, обеспечивающее выполнение криптографических операций, заданных вызывающим приложением, средствами криптопровайдера и возврат результатов вызывающему приложению.

Модуль поддержки СКЗИ может быть запущен в двух режимах:

- режим исполняемого приложения
- режим системной службы

В режиме исполняемого приложения модуль поддержки СКЗИ запускается как обычное приложение Windows в пользовательском контексте и полностью реализует все свои функциональные возможности.

В режиме системной службы модуль поддержки СКЗИ регистрируется в списке системных служб Windows и по умолчанию функционирует вне пользовательских контекстов. При этом становятся не доступными функции, использующие графический интерфейс (показ свойств ЭП). Функции, требующие предъявления секретного ключа пользователя (создание ЭП, шифрование/расшифрование данных) по умолчанию недоступны в этом режиме. Запуск службы от учетной записи пользователя позволяет получить доступ к ключам и сертификатам аналогично режиму приложения, за исключением того, что в режиме службы по умолчанию используется хранилище сертификатов компьютера sslm:My.

Управление настройками

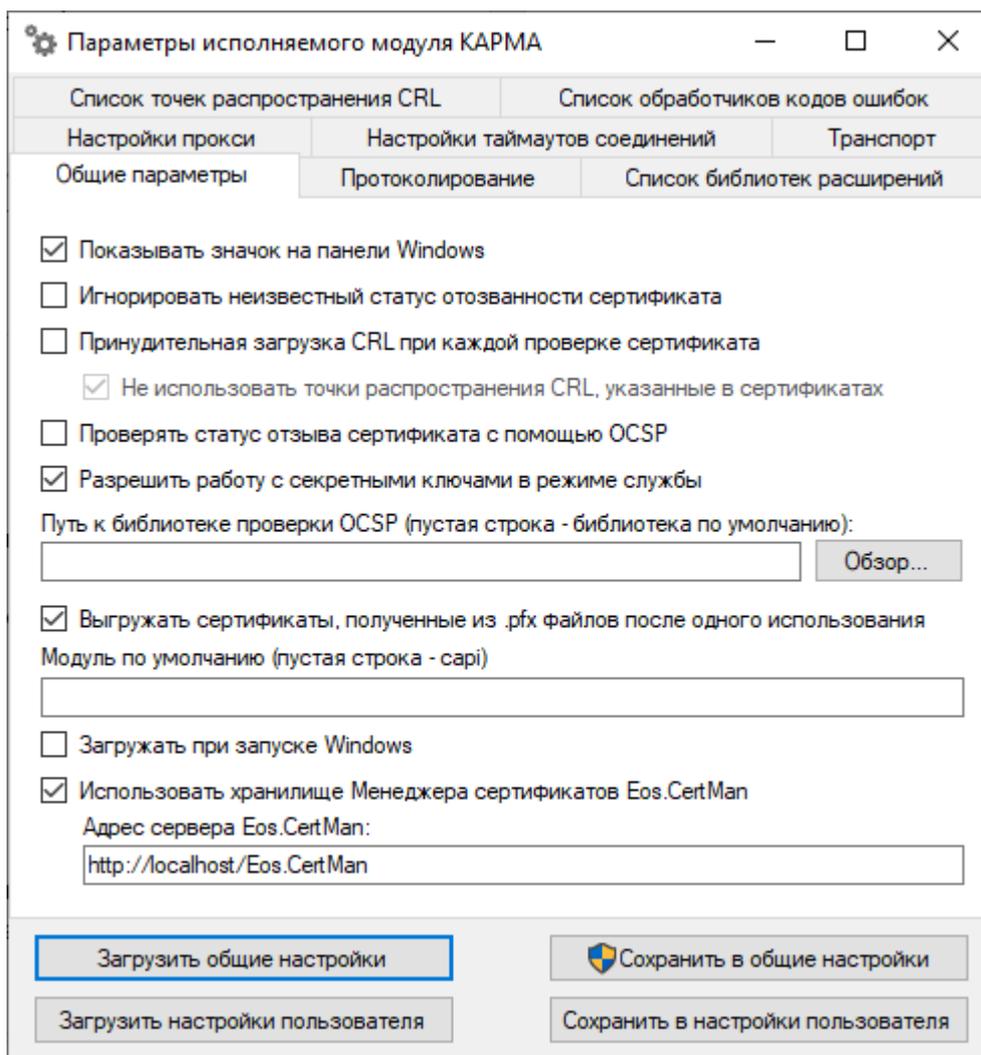
Модуль управления настройками КАРМА - исполняемое приложение с графическим интерфейсом, представляющим собой экранную форму с несколькими страницами-закладками.

Общими для всех страниц настроек являются кнопки сохранения и загрузки общих настроек и настроек пользователя.

Общие настройки – настройки, сохраняемые в общей для всех пользователей папке, используемые в режиме системной службы и при отсутствии настроек текущего пользователя. Для сохранения изменений в общих настройках необходимо иметь права администратора операционной системы.

Настройки пользователя – настройки, сохраняемые для текущего пользователя. При отсутствии этих настроек, используются общие для всех пользователей настройки. Для внесения изменения в настройки текущего пользователя прав администратора не требуется.

На первой закладке собраны настройки режимов работы модуля поддержки СКЗИ:



Показывать значок на панели Windows – параметр, отвечающий за показ иконки на панели Windows во время работы модуля поддержки СКЗИ.

Игнорировать неизвестный статус отозванности сертификата – параметр, вступающий в силу при проверке подписи. Если при проверке подписи единственной ошибкой проверки сертификата является неизвестный статус отозванности, то, если данный параметр включен, ошибки возвращаться не будет и подпись (либо сертификат) будут признаны верными

Принудительная загрузка CRL при каждой проверке сертификата – если данный параметр включен, то при каждой проверке подписи или сертификата система будет пытаться скачать обновление списка отзыва сертификатов (CRL) с точки распространения списка отзывов (CDP),

указанной в сертификате (если указана) и с точек распространения, указанных в настройках системы во вкладке «Список точек распространения CRL». В случае, если скачать список отзыва не удастся, возвращается ошибка.

Принудительная загрузка CRL при каждой проверке сертификата – если данный параметр включен, то загрузка списков отзыва из точек распространения, указанных в сертификате, производиться не будет.

Внимание! Включение данного параметра может быть полезно в закрытых локальных сетях

Разрешить работу с секретными ключами в режиме службы – включение данного параметра разрешит Карме в режиме службы использовать секретные ключи и осуществлять использующие их операции, такие как подписание, шифрование и расшифровывание.

Внимание! Для работы с секретными ключами в режиме службы пароль на контейнер секретного ключа должен быть сохранен средствами криптопровайдера или должен быть пустым. В противном случае возможен возврат с ошибкой или даже зависание *клиентского* процесса.

Проверить статус отзыва сертификата с помощью OCSP – если данный параметр включен, то окончательная проверка CRL производится с помощью механизма OCSP

Внимание! Подробную информацию по логике работы со списками отзыва следует смотреть в документе «Информация по работе со списками отзыва».

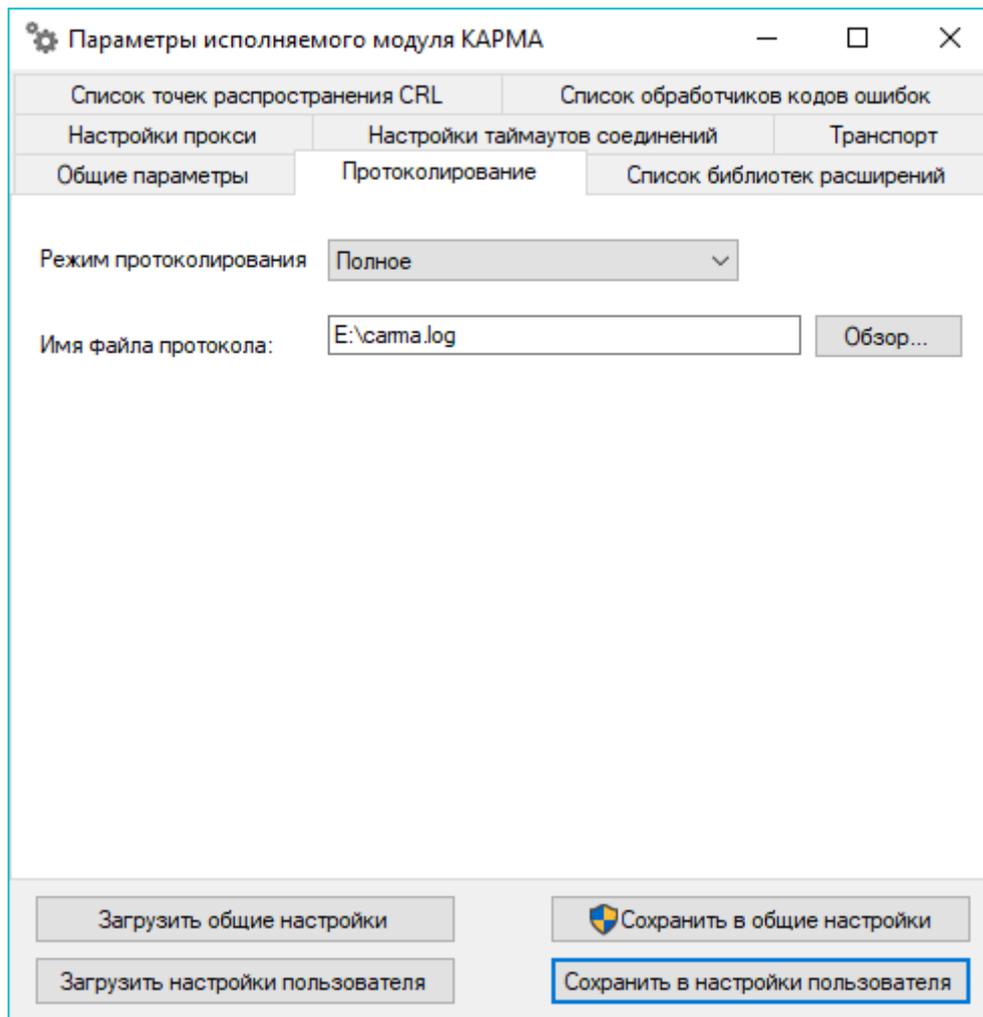
Путь к библиотеке проверки OCSP (пустая строка – библиотека по-умолчанию) – данный параметр позволяет указать системе КАРМА другую библиотеку для проверки OCSP ответов. Если надобности в указании другой библиотеки нет, строку следует оставить пустой.

Выгружать сертификаты, полученные из .rfx файлов после одного использования - если данный параметр отключен, сертификат остается в памяти приложения до его выгрузки.

Модуль по умолчанию (пустая строка - sari) – крипто-модуль, загружаемый сервисом по умолчанию.

Использовать хранилище Менеджера сертификатов Eos.CertMan – параметр, позволяющий подключить хранилище ЭОС PKI – сервиса и осуществлять проверку цепочек сертификатов средствами сервиса.

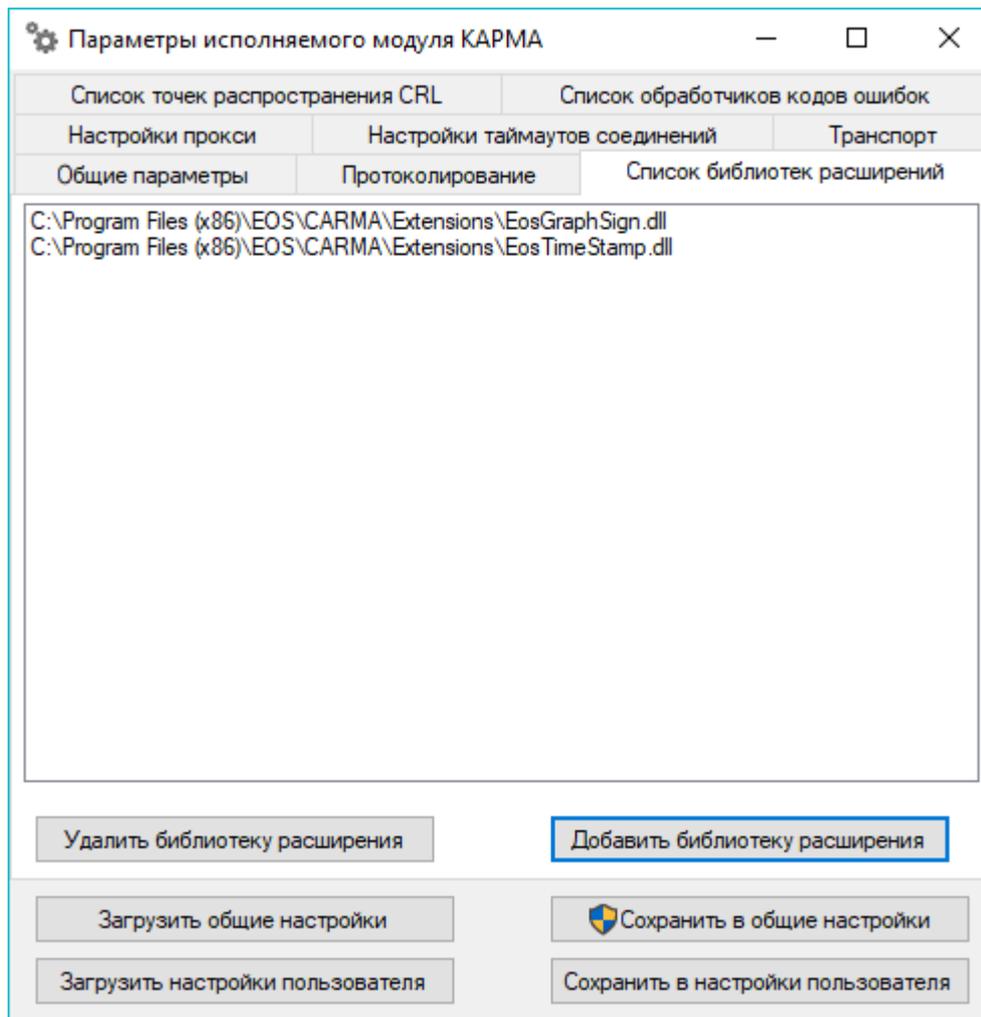
Вторая закладка содержит настройки режимов протоколирования сервиса поддержки СКЗИ:



Режим протоколирования – параметр, определяющий режим протоколирования событий модуля поддержки СКЗИ. Протоколирование может быть отключено (значение параметра - *Отключено*), могут протоколироваться только ошибки (значение параметра – *Только ошибки*) или все события модуля поддержки СКЗИ (значение параметра - *Полное*)

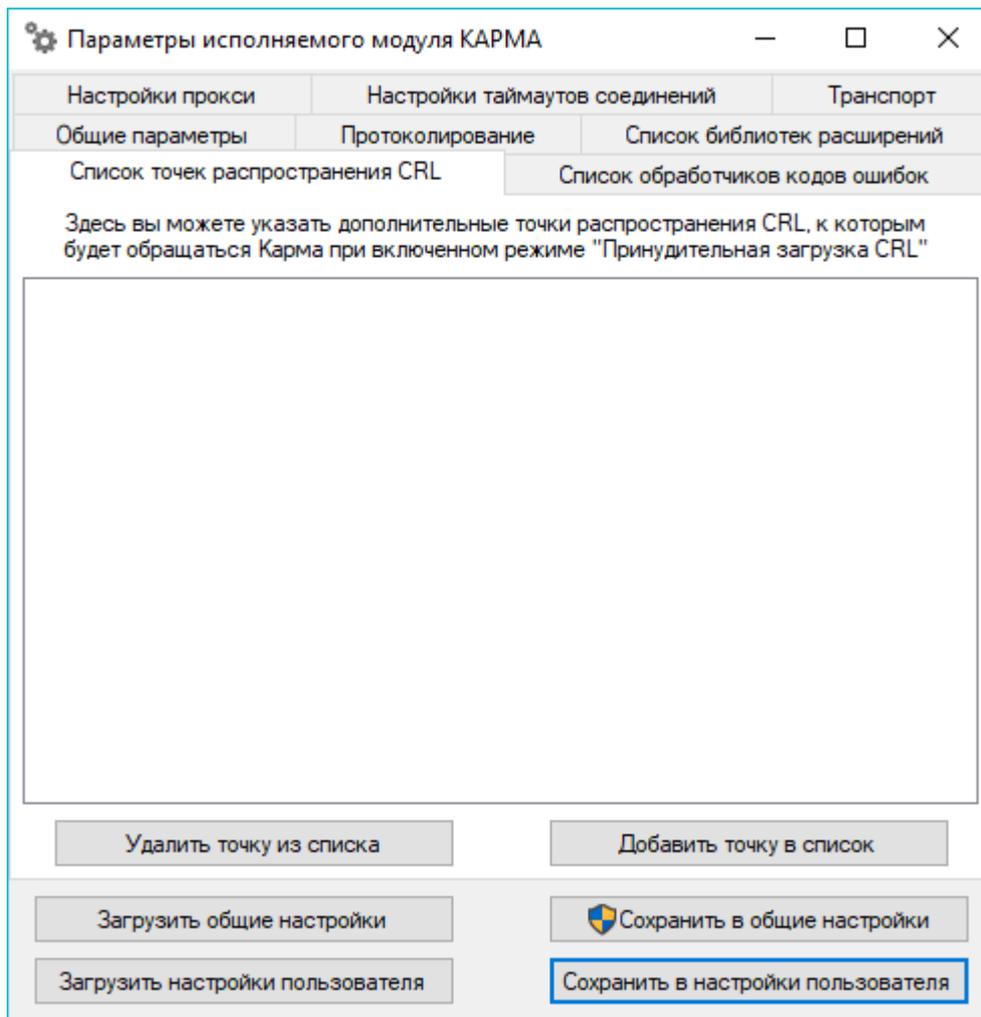
Имя файла протокола – имя файла, в который записывается протокол. При щелчке левой кнопкой мыши на имени файла открывается окно выбора каталога и имени файла протокола.

Третья закладка содержит список расширений, подключенных в данный момент к системе KARMA:



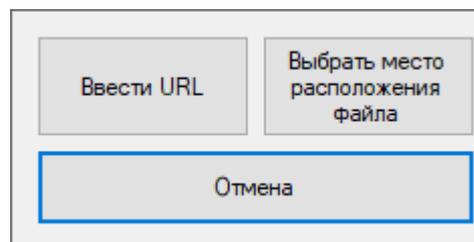
В верхней части окошка показан список расширений с полным путем к файлу библиотеки каждого из них. Кнопки *Добавить библиотеку расширения* и, соответственно, *Удалить библиотеку расширения* добавляют или удаляют выбранное расширение из списка. При нажатии на кнопку *Добавить библиотеку расширения* открывается диалоговое окно выбора каталога и имени файла расширения.

Четвертая закладка содержит список дополнительных точек распространения списков отзыва (CRL):

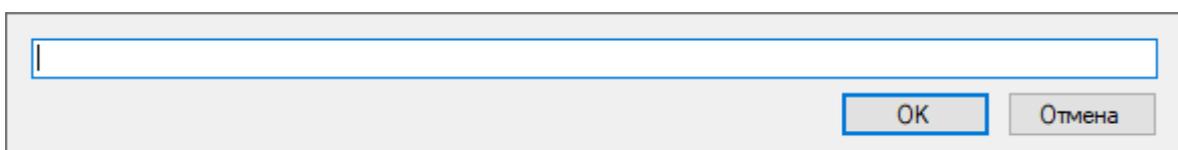


В верхней части окошка показан список дополнительных точек распространения CRL с полным путем к файлу библиотеки каждого из них. Кнопки *Добавить точку в список* и, соответственно, *Удалить точку из списка* добавляют или удаляют выбранную точку распространения из списка.

При нажатии на кнопку *Добавить точку в список* появляется окно выбора вариантов расположения точки:



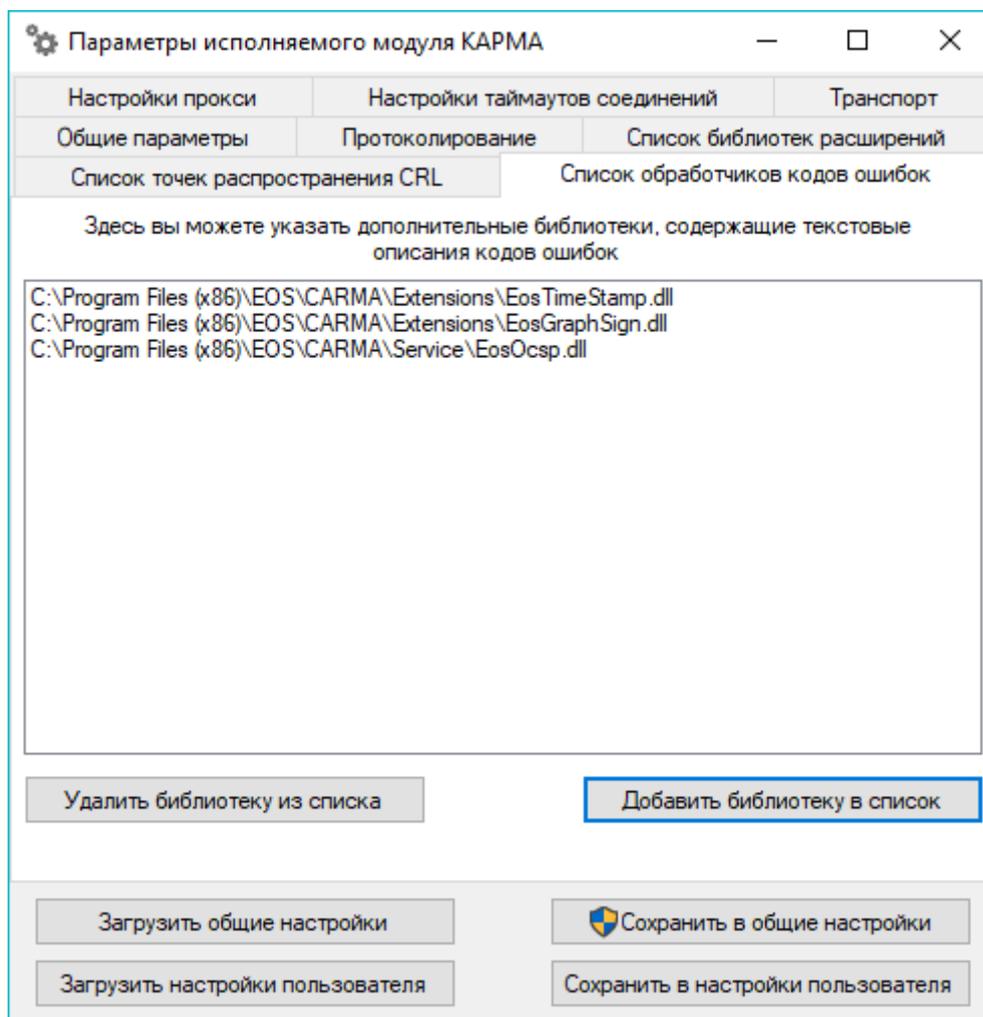
При нажатии на кнопку *Ввести URL* открывается окно для ввода адреса расположения точки распространения CRL (например, `http://` или `ldap://` адреса):



При нажатии на кнопку *Выбрать место расположения файла* открывается диалоговое окно выбора каталога и имени файла CRL, либо, по выбору, окно ввода URL расположения файла CRL:

В данном диалоге можно указать как расположения в папке на данном компьютере либо на удаленном компьютере, так и на FTP.

Пятая закладка содержит список библиотек, содержащих текстовую информацию для демонстрации пользователю по возможным возвращаемым кодам ошибок системы:



В верхней части окошка показан список расширений с полным путем к файлу библиотеки каждого из обработчиков. Кнопки *Добавить библиотеку в список* и, соответственно, *Удалить библиотеку из списка* добавляют или удаляют выбранный обработчик из списка. При нажатии на кнопку *Добавить библиотеку в список* открывается диалоговое окно выбора каталога и имени файла обработчика.

Шестая закладка содержит настройка тайм-аутов соединений:

Параметры исполняемого модуля KAPMA

Общие параметры | Протоколирование | Список библиотек расширений
Список точек распространения CRL | Список обработчиков кодов ошибок
Настройки прокси | **Настройки таймаутов соединений** | Транспорт

Общий таймаут соединений: миллисекунд

Использовать разные таймауты для разных соединений

С сервисом: миллисекунд
С сервером штампов времени: миллисекунд
С точками распространения CRL: миллисекунд
С сервером OCSP: миллисекунд

Загрузить общие настройки | Сохранить в общие настройки
Загрузить настройки пользователя | **Сохранить в настройки пользователя**

Параметр позволяет установить общий таймаут всех соединений или настроить отдельно для разных соединений.

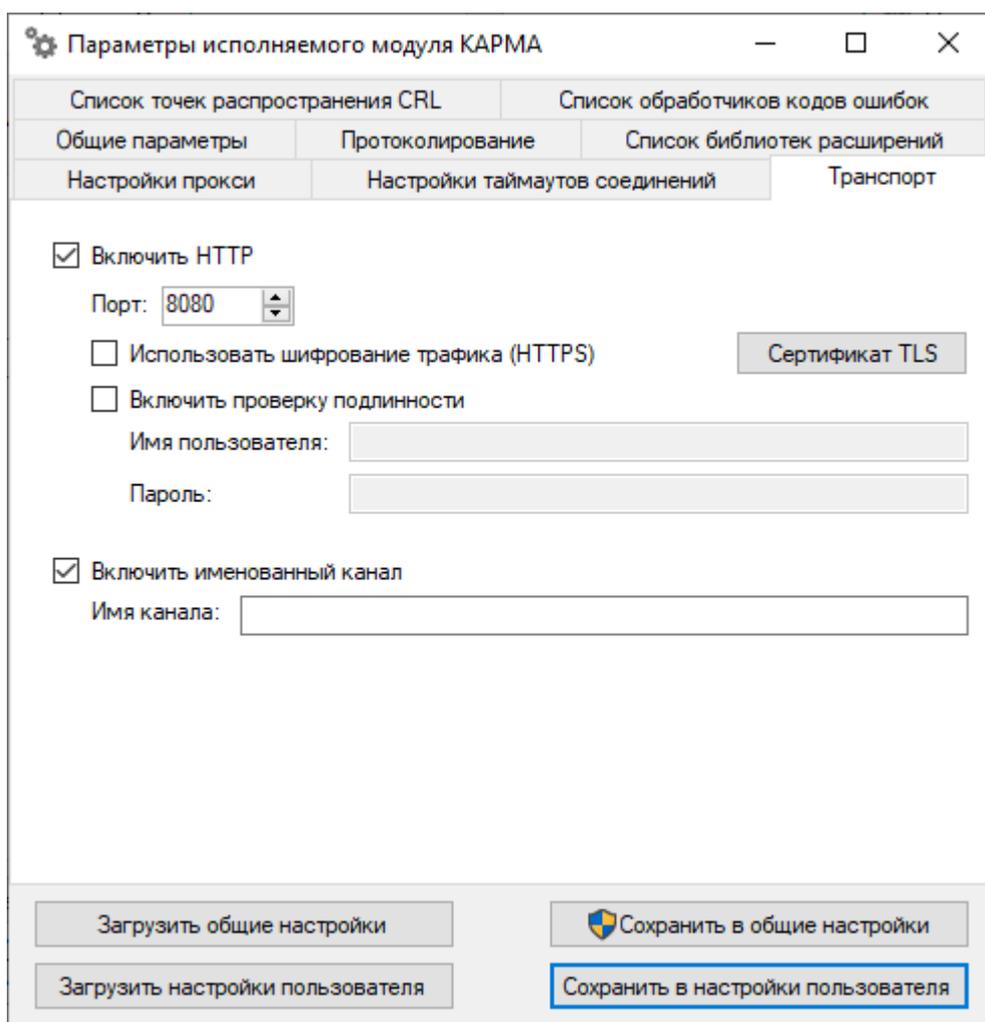
Седьмая закладка содержит настройки прокси:

The image shows a Windows-style dialog box titled "Параметры исполняемого модуля KARMA". It has a tabbed interface with the following tabs: "Общие параметры", "Протоколирование", "Список библиотек расширений", "Список точек распространения CRL", "Список обработчиков кодов ошибок", "Настройки прокси", "Настройки таймаутов соединений", and "Транспорт". The "Настройки прокси" tab is currently selected and active. It contains the following elements:

- An unchecked checkbox labeled "Использовать прокси".
- A dropdown menu labeled "Тип прокси:".
- Two text input fields: "Адрес:" and "Порт:".
- Two text input fields: "Имя пользователя:" and "Пароль:".
- Four buttons at the bottom: "Загрузить общие настройки", "Сохранить в общие настройки", "Загрузить настройки пользователя", and "Сохранить в настройки пользователя". The "Сохранить в настройки пользователя" button is highlighted with a blue border.

В случае необходимости подключения через прокси-сервер, можно указать параметры подключения. Включение параметра *Использовать прокси* – делает активным остальные поля окна.

Восьмая закладка содержит настройки соединения с сервисом KARMA:

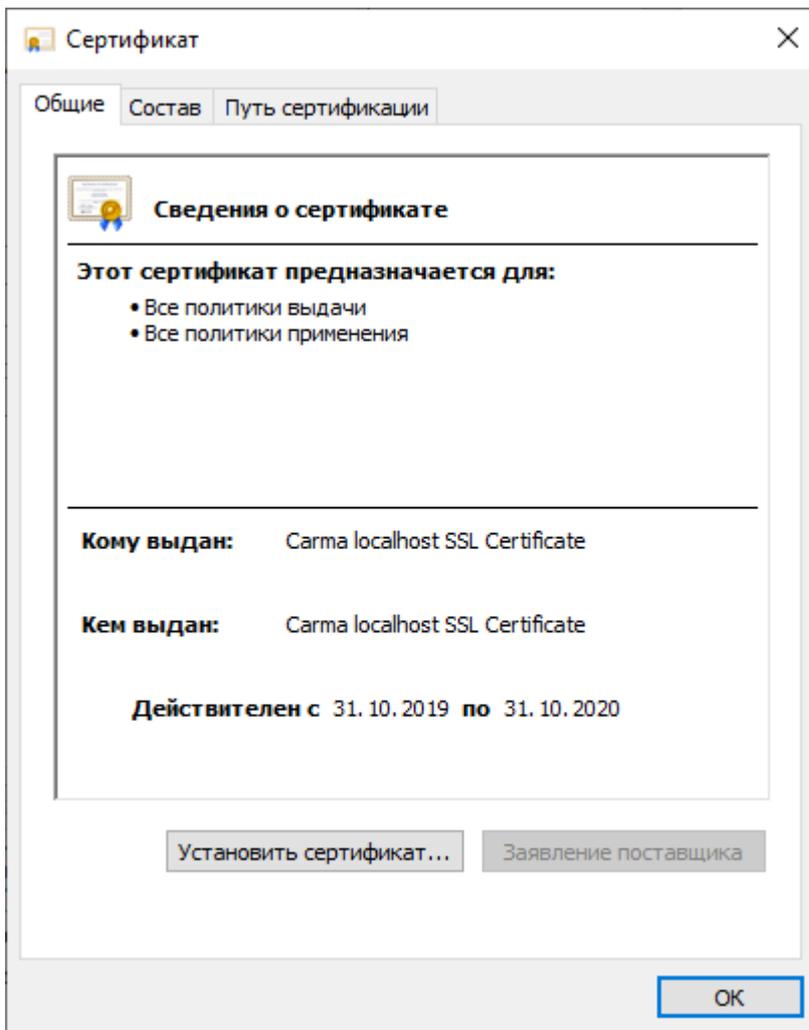


По умолчанию включены оба транспортных протокола: HTTP и Именованные каналы (по умолчанию имя канала: «carma»). Имя канала(пустая строка – имя по-умолчанию), а также порт HTTP – данные параметры позволяют выделить каналы передачи данных для конкретного пользователя на компьютере. Это может быть полезным при работе с терминальными станциями. По умолчанию адрес сервиса в строке инициализации может быть указан следующим образом:

```
SERVER="http://localhost:8080";  
SERVER="pipe://localhost/carma";
```

При необходимости можно настроить доступ к сервису по паре логин\пароль.

Опционально, доступен режим шифрования http трафика между сервисом кармы и клиентами (HTTPS). Сертификат шифрования канала по умолчанию зарегистрирован на хост localhost. Для корректной работы в браузерах в https окружении необходимо установить сертификат TLS в доверенное хранилище компьютера.



Для перевыпуска сертификата либо изменения хоста необходимо воспользоваться утилитой certtool.exe из комплекта поставки КАРМА (<Директория установки>\Service\certtool.exe):

```
certtool.exe -p --bits 4096 --outfile server.pem
```

```
certtool.exe --generate-self-signed --load-privkey server.pem --outfile server.cer --template cert.cfg
```

Содержимое cert.cfg представлено ниже:

```
organization = "Electronic Office Systems (EOS)"
```

```
locality = "Moscow"
```

```
state = Moscow
```

```
country = RU
```

```
# common name
```

```
cn = "Carma internal server SSL Certificate"
```

```
serial = 1
```

```
expiration_days = 3650
```

```
# subjectAltNames
```

```
dns_name = localhost
```

Полученные файлы необходимо копировать в %PROGRAMDATA%\CARMA

Также, все настройки доступны на http странице settings (по умолчанию <http://localhost:8080/settings>):

Настройки

localhost:8080/settings

Общие

Показывать значок на панели Windows	<input checked="" type="checkbox"/>
Игнорировать неизвестный статус отзывности сертификата	<input checked="" type="checkbox"/>
Принудительная загрузка CRL при каждой проверке сертификата	<input type="checkbox"/>
Не использовать точки распространения CRL, указанные в сертификатах	<input type="checkbox"/>
Проверять статус отзыва сертификата с помощью OCSP	<input type="checkbox"/>
Разрешить работу с секретными ключами в режиме службы	<input checked="" type="checkbox"/>
Разрешить удаленную работу с секретными ключами	<input type="checkbox"/>
Путь к библиотеке проверки OCSP (пустая строка - библиотека по умолчанию)	<input type="text"/>
Выгружать сертификаты, полученные из .pfx файлов после одного использования	<input type="checkbox"/>
Модуль по умолчанию (пустая строка - car1)	<input type="text"/>
Язык	Русский ▾

Протоколирование

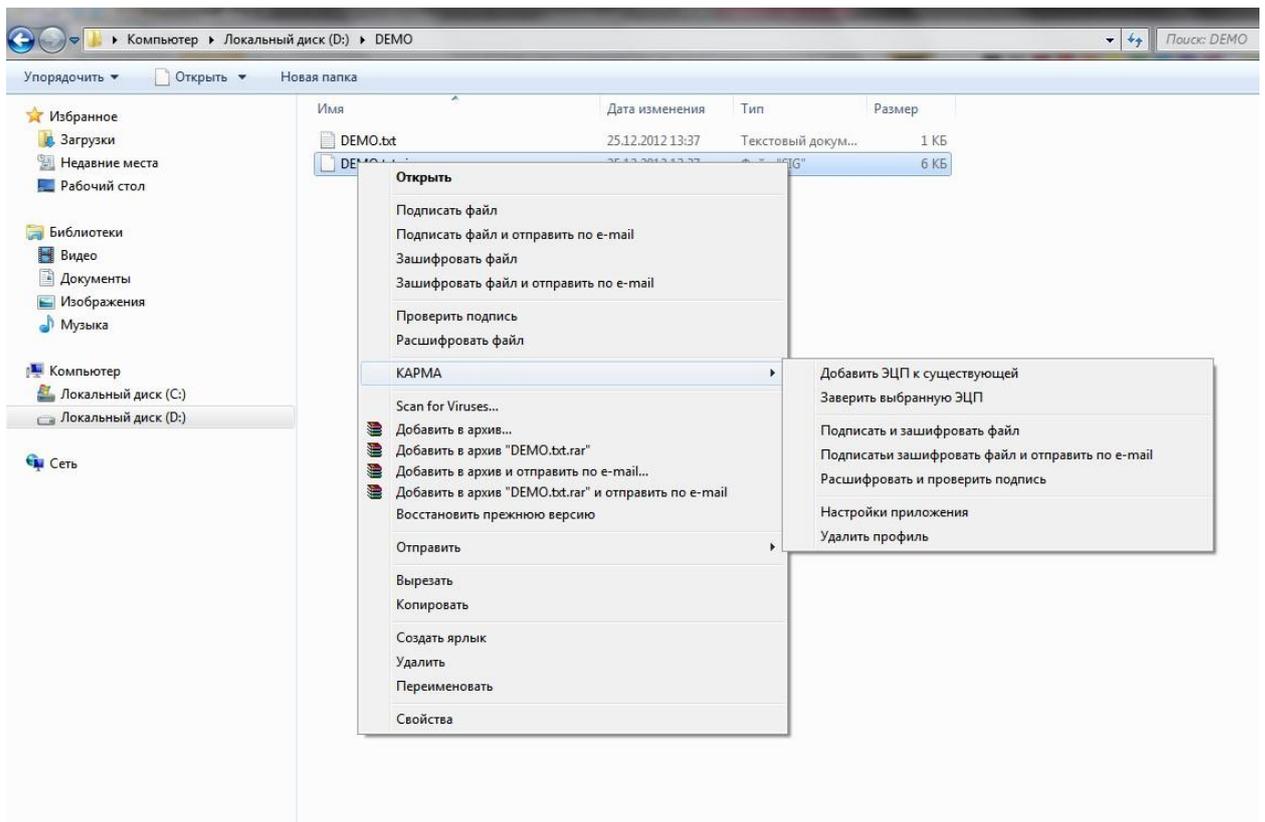
Режим протоколирования	Полное ▾
Имя файла протокола	E:\carma.log

Транспорт

Включить HTTP	<input checked="" type="checkbox"/>
---------------	-------------------------------------

Визуальная оболочка KARMA

Структура меню визуальной оболочки KARMA:



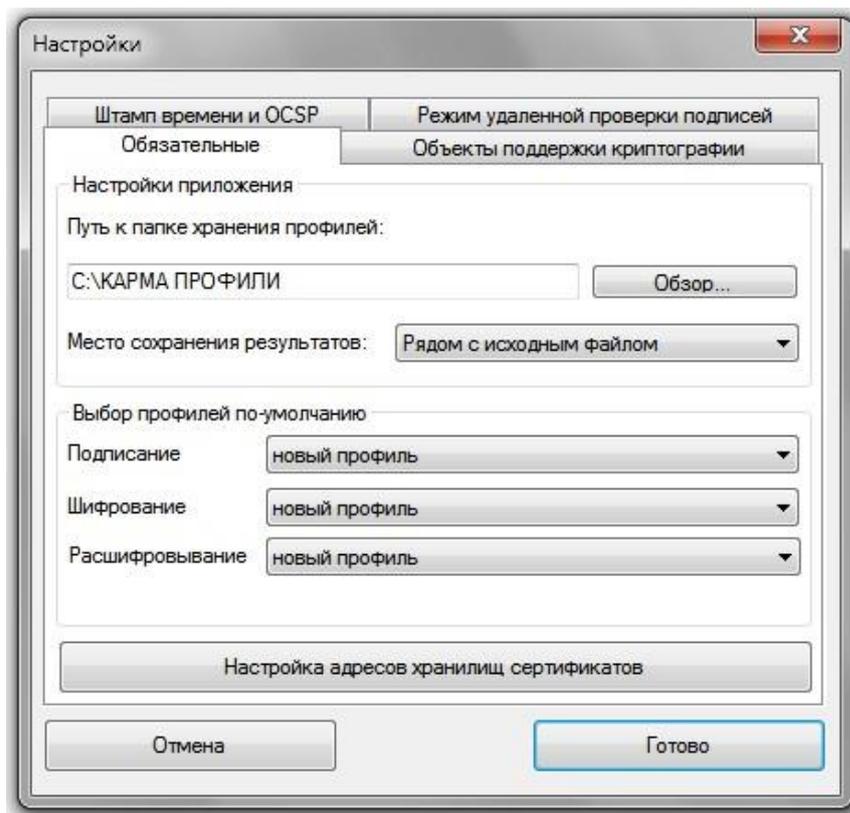
При первом вызове контекстного меню КАРМА доступен только раздел «Настройки».

Помимо пунктов, вызывающих мастера выбранных операций в контекстном меню присутствуют также пункты, позволяющие осуществить выбранную операцию и отправить ее результат по электронной почте.

Настройки

Вкладка «Обязательные»

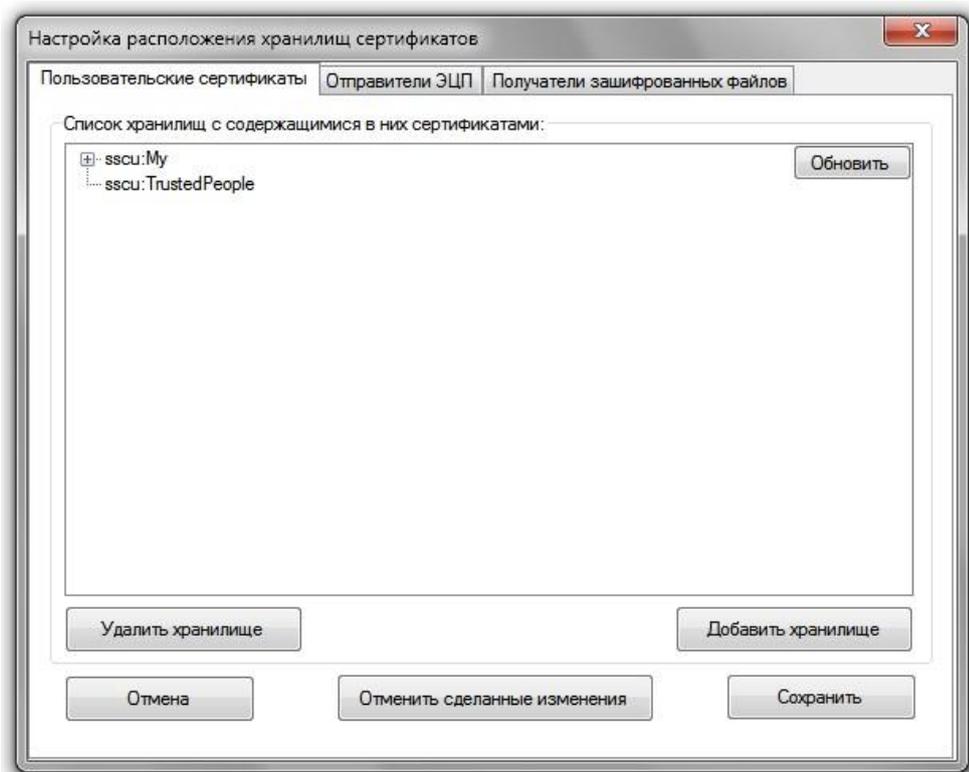
Для того, чтобы стали доступны другие разделы контекстного меню, необходимо заполнить настройки, находящиеся на вкладке «Обязательные» (указать каталог хранения профилей операций, а также выбрать адреса хранилищ сертификатов для различных операций):



Если указать место хранения результатов «*Рядом с исходным файлом*», как это сделано на представленном выше скриншоте, то при выполнении каждой из операций система не будет спрашивать путь к каталогу, в котором необходимо сохранить результат операции (электронную подпись, зашифрованный контейнер, расшифрованный файл и т.п.), а будет сохранять в том же каталоге, что и исходный файл. Если же выбран пункт «*Настраивается для каждого профиля*», то при выполнении каждой операции будет необходимо указать путь к данному каталогу, и он может быть сохранен в этом профиле.

На этой же странице настроек указываются профили по-умолчанию для основных операций – подписания, шифрования и расшифровывания. Если выбран профиль по-умолчанию, именно он будет загружен при запуске соответствующего мастера.

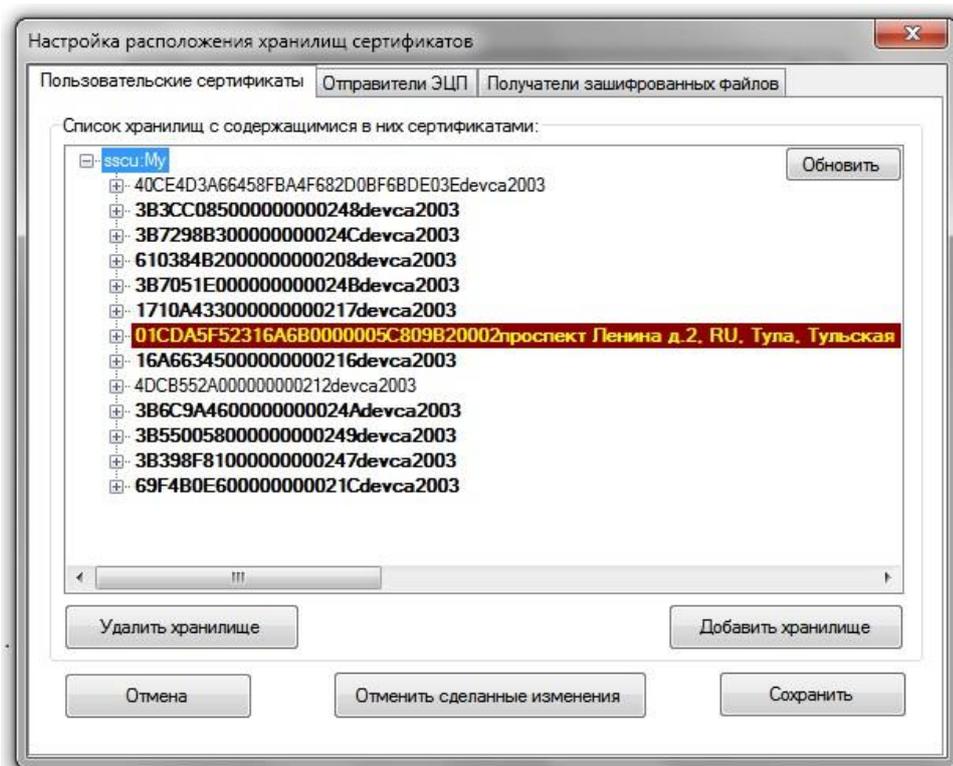
Для настройки адресов хранилищ сертификатов необходимо нажать на кнопку *Настройка адресов хранилищ сертификатов*, после чего появится следующее окно:



Мастер настройки расположения хранилищ сертификатов содержит три этапа: *Пользовательские сертификаты* (сертификаты из данных хранилищ будут извлекаться для операций подписания, шифрования и расшифровывания пользователем), *Отправители ЭП* (сертификаты из данных хранилищ извлекаются при проверке подписи, в случае, если сертификат не содержится в самой подписи) и *Получатели зашифрованного контейнера* (сертификаты из данных хранилищ извлекаются при указании списка получателей зашифрованного файла).

Внимание! Если вы не знаете, для чего вам нужна настройка хранилищ сертификатов, либо не желаете настраивать их сейчас, достаточно просто нажимать кнопку *Далее* и затем кнопку *Готово*. Будут установлены хранилища по умолчанию, а именно – ваше Личное хранилище сертификатов.

В списке хранилищ показаны адреса хранилищ сертификатов, выбранных в данный момент для использования в соответствующей операции, а также сертификаты, содержащиеся в данных хранилищах:

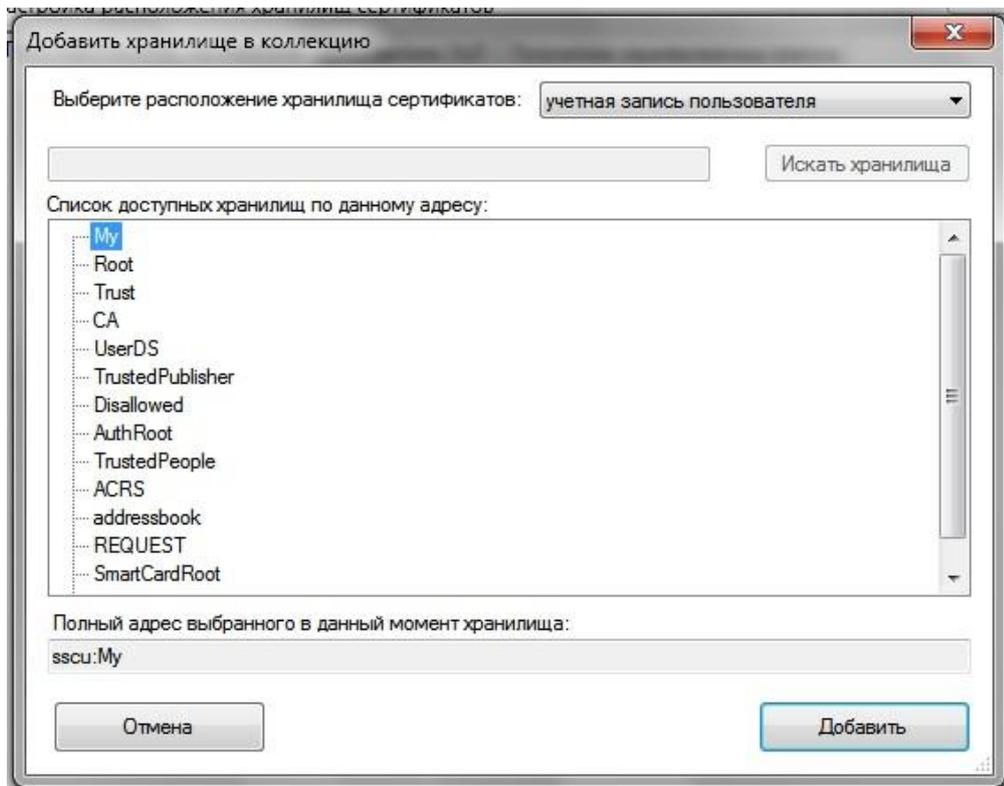


Красным отмечены недействительные на данный момент сертификаты. При наведении указателя мыши на данный сертификат показывается причина признания сертификата неверным.

Жирным шрифтом отмечаются сертификаты, для которых найден связанный с ними закрытый ключ.

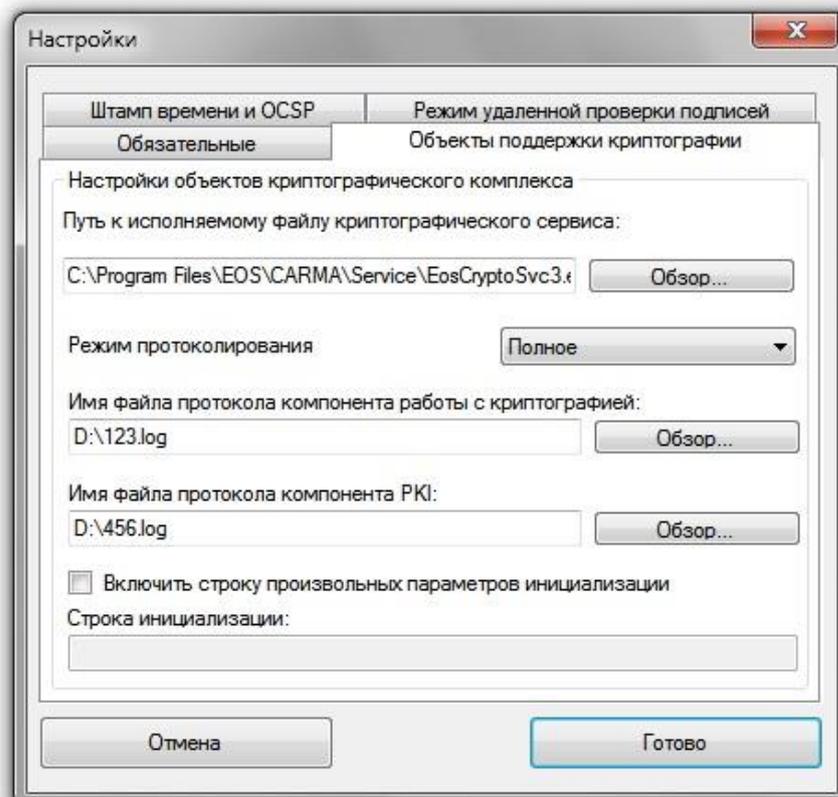
Вы можете обновить содержимое списка нажатием кнопки «Обновить».

Для добавления хранилища сертификатов в коллекцию хранилищ следует нажать кнопку *Добавить хранилище*, в результате чего вы увидите следующее окно:



Система позволяет добавить в коллекцию одно из хранилищ учетной записи *текущего пользователя, компьютера* (в строке адреса необходимо указать полное имя компьютера в виде `\\computer_name`), *системной службы* (в строке адреса необходимо указать полное имя службы в виде `\\computer_name\service_name`), а также *удаленное хранилище* (`http://` или `ldap://`; в строке адреса необходимо указать полный путь к хранилищу сертификатов).

Вкладка «Объекты поддержки криптографии»

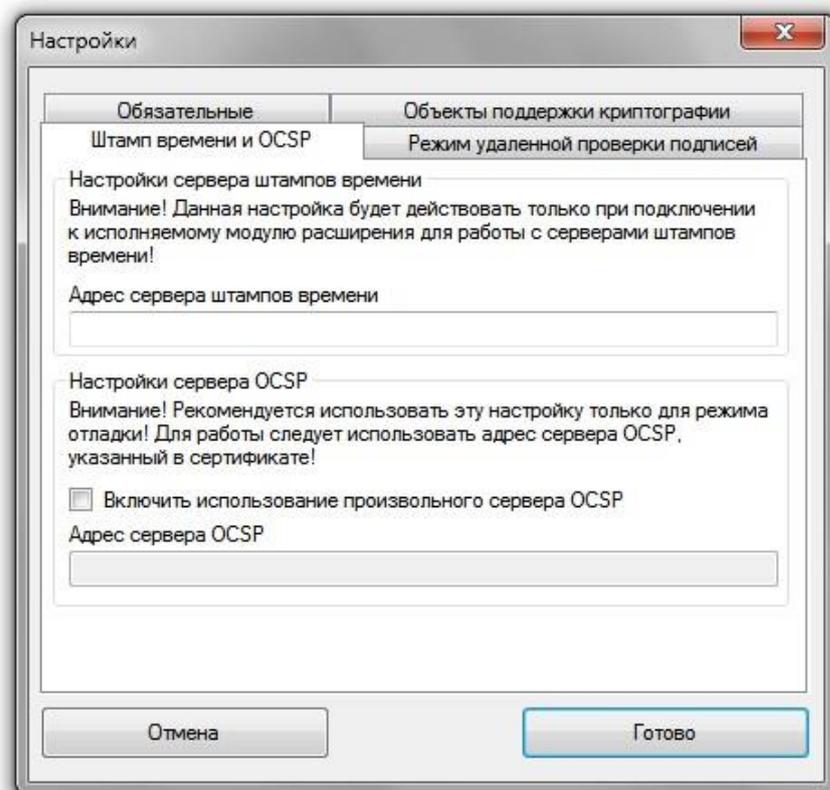


При указании пути к исполняемому файлу криптографического сервиса (**EosCryptoSvc3.exe**) сервис будет автоматически запускаться при обращении к функциям KAPMA.

На этой же вкладке настраивается протоколирование в объектах поддержки криптографии (протоколирование криптографического сервиса настраивается в его собственных настройках).

Параметр «*Включить строку произвольных параметров инициализации*» активирует поле «*Строка инициализации*». В это поле вы можете вручную ввести параметры, передаваемые при инициализации в объекты поддержки криптографии. Это может потребоваться, например, для передачи параметров расширениям, подключенным к криптографическому сервису.

Вкладка «Штамп времени и OCSP»

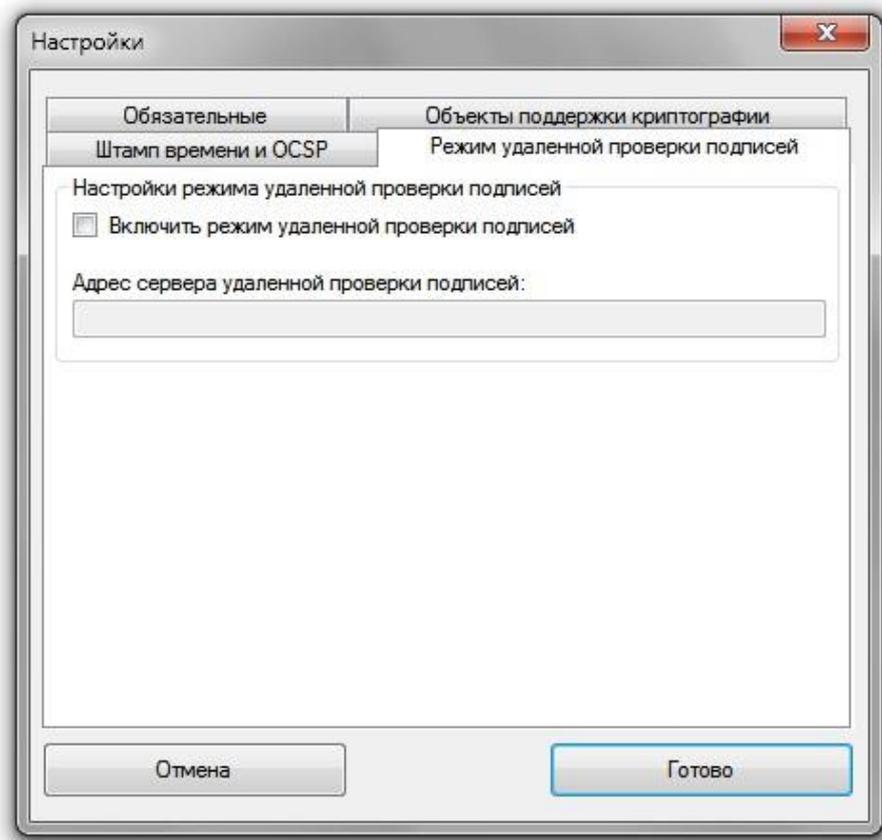


В случае, если указан *Адрес сервера штампов времени*, и подключено соответствующее расширение KAPMA, то при подписании будет происходить обращение по данному адресу для дополнения электронной подписи штампом (меткой) времени подписания, взятом с указанного доверенного сервера (сервера штампов времени).

Кроме того, на этой вкладке возможно включить с помощью параметра «*Включить использование произвольного сервера OCSP*» и ввести в соответствующее поле произвольный адрес сервера OCSP. Если адрес введен, он будет использован вне зависимости от того, какой адрес сервера OCSP указан в проверяемом сертификате.

Внимание! Не рекомендуется использовать данный параметр для целей, отличных от тестирования работы системы.

Вкладка «Режим удалённой проверки подписей»



Режим удалённой проверки подписей позволяет проверять ЭП пользователям, компьютеры которых не оснащены необходимыми криптографическими средствами (отсутствует криптопровайдер). Для того, чтобы проверить подпись удалённо, необходимо включить режим удалённой проверки подписей и указать адрес сервера удалённой проверки подписи (IP-адрес или сетевое имя компьютера). В качестве сервера удалённой проверки может выступать любой доступный в сети компьютер, оснащённый необходимыми криптографическими средствами и системой КАРМА. На сервере удалённой проверки должен быть запущен сервис КАРМА.

Режим настройки КАРМА может быть вызван в любое время выбором соответствующего раздела меню. Кроме того, настройки контекстного меню можно вызывать в любой момент как через непосредственно контекстное меню, так и через ярлык в меню «Пуск»->«Программы»->«КАРМА».

Профили

Профиль представляет собой набор хранимых данных, определяющих режим работы функции криптографического сервиса.

Профиль хранит настройки для каждой операции (для создания ЭП, шифрования, расшифровывания). Непосредственно введение данных настроек осуществляются в разделе, соответствующем настраиваемой операции. По окончании каждой операции, если она не была запущена с уже созданным профилем, вам будет предложено сохранить использованные настройки, чтобы не приходилось их вводить при каждой подобной операции.

В верхней части окна каждого из мастеров всегда располагается список профилей, чтобы в процессе работы можно было быстро выбрать необходимый профиль.

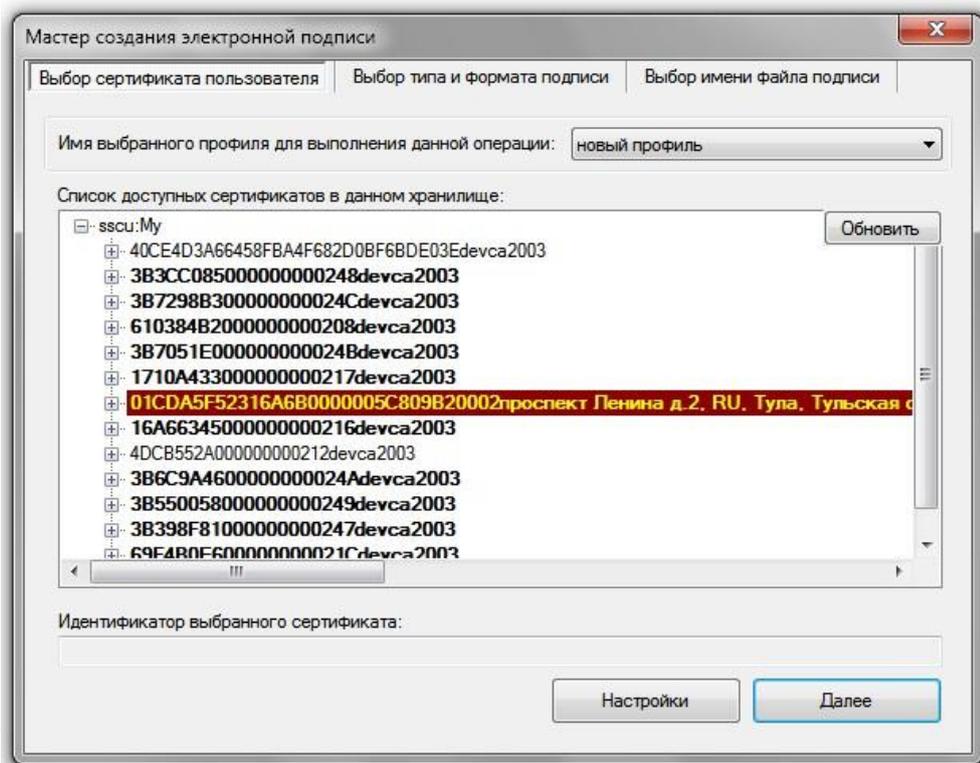
Мастера операций

Мастер представляет собой приложение (оснастку), получающее от пользователя необходимую информацию для запуска функции криптографического сервиса.

Мастер создания ЭП.

Мастер выполняет следующую последовательность действий:

1. Выбор сертификата пользователя из доступных в пользовательском хранилище сертификатов, путь к которому можно изменить в настройках системы. Изменить хранилище можно из настроек системы, которые можно запустить с каждой страницы мастера, нажав кнопку *Настройки*:

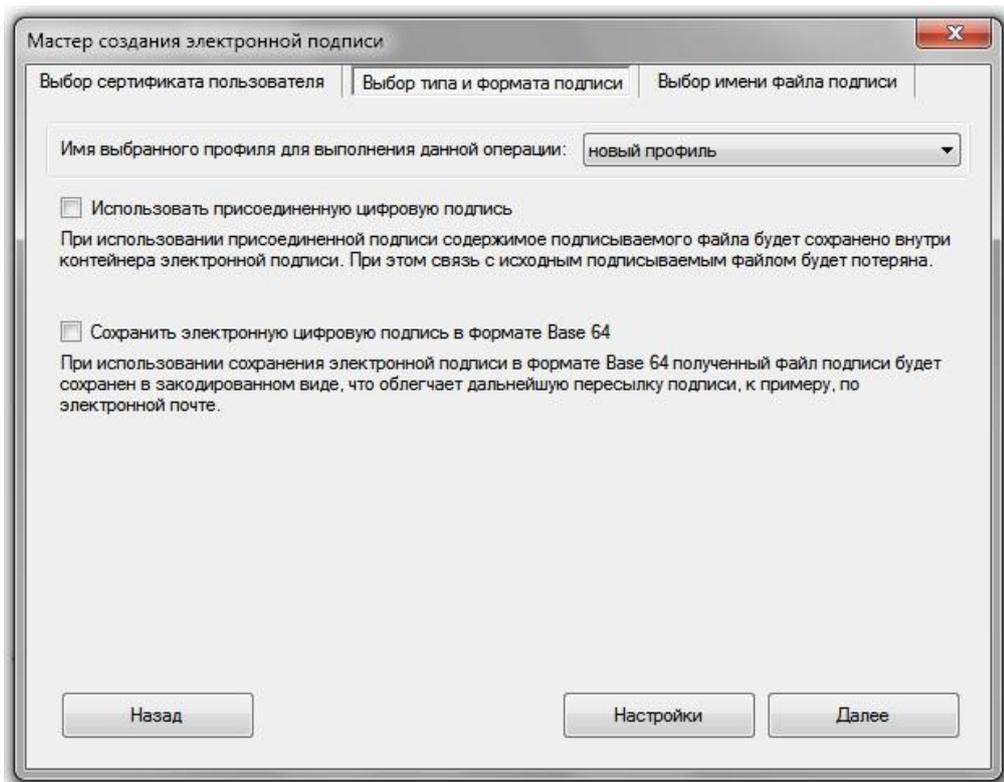


Красным отмечены недействительные на данный момент сертификаты. При наведении указателя мыши на данный сертификат показывается причина признания сертификата неверным.

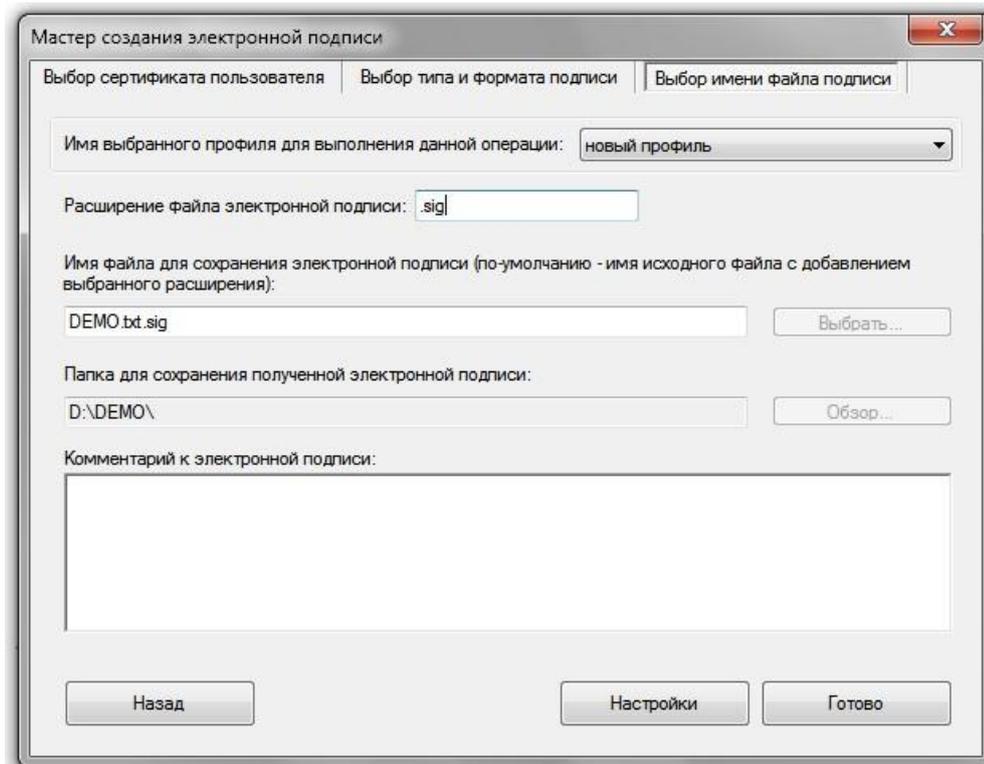
Жирным шрифтом отмечаются сертификаты, для которых найден связанный с ними закрытый ключ.

Вы можете обновить содержимое списка нажатием кнопки «Обновить».

2. Выбор типа подписи (присоединенная или отсоединенная), выбор формата получения (наличие или отсутствие Base64 кодировки):



3. Введение имени файла для сохранения ЭП и комментария к подписи:



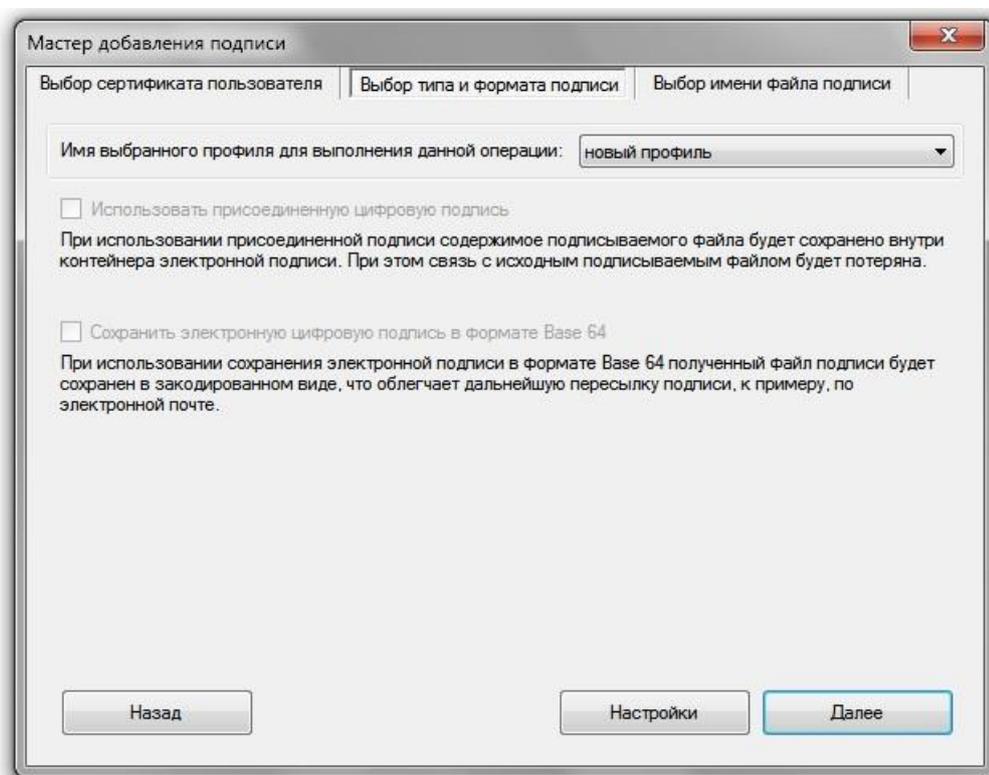
При создании присоединенной (attached) ЭП имя исходного файла сохраняется в поле «идентификатор ресурса» для дальнейшего использования в процессе извлечения исходного файла из подписи.

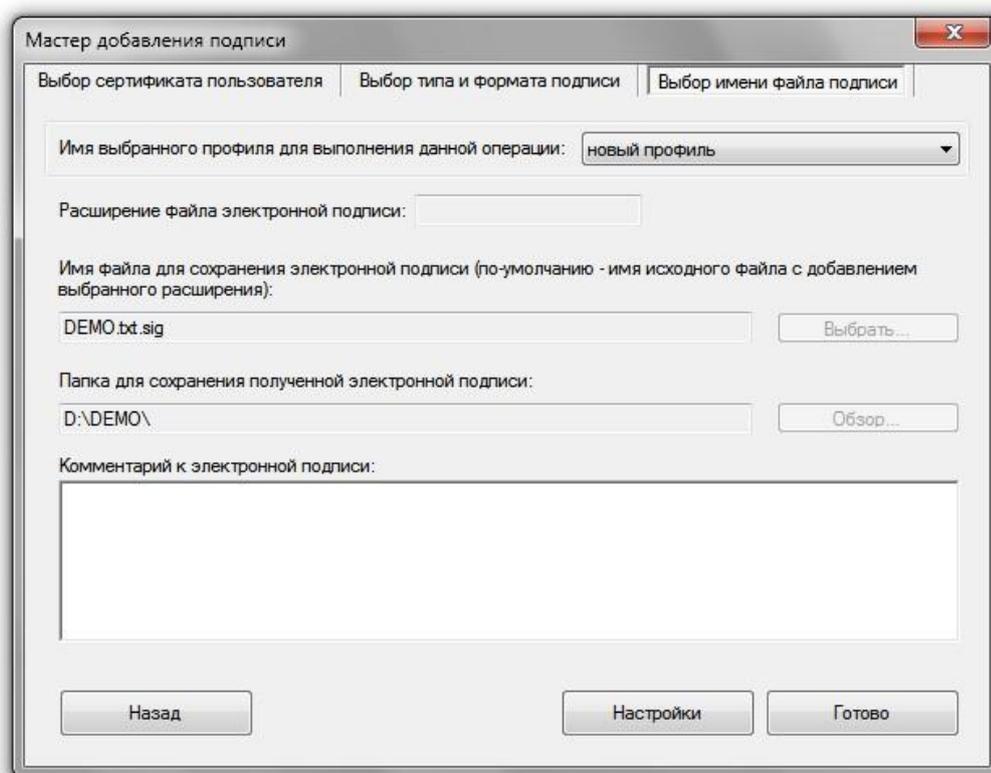
Если в настройках выбран профиль для подписания по умолчанию, то работа мастера начинается с п.3.

Если в настройках указано местоположение файла результатов *Рядом с исходным файлом*, то выбирать каталог для сохранения итогового файла не требуется.

Мастер добавления ЭП к существующей.

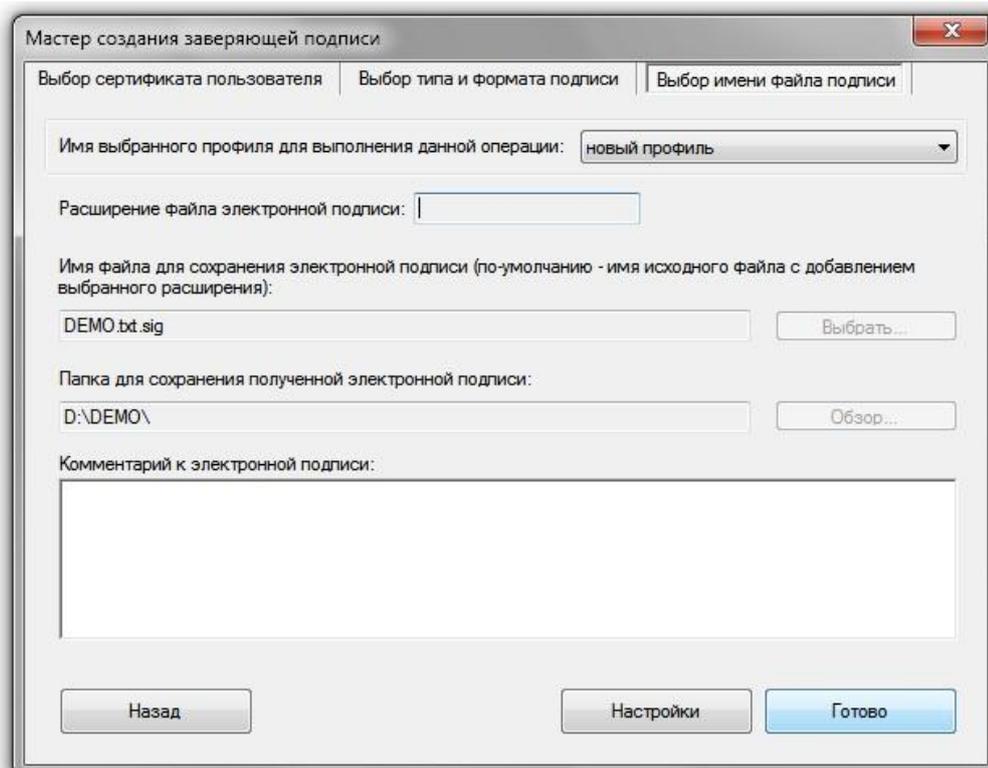
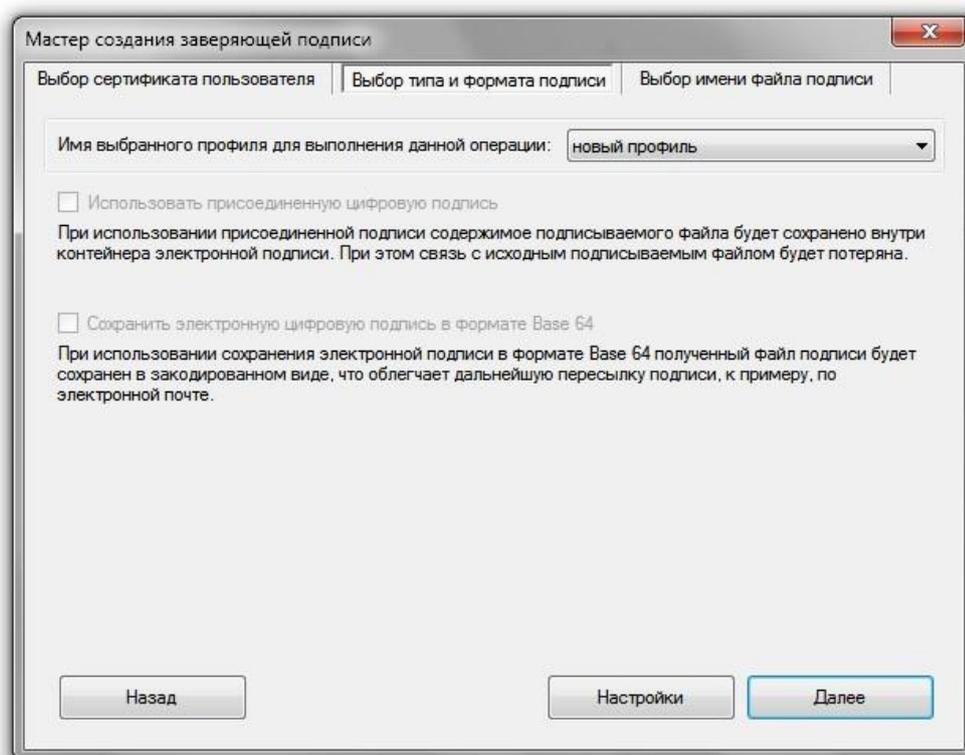
При добавлении подписи к отсоединенной подписи, мастер предварительно предложит выбрать файл, для которого создана исходная подпись. Добавление подписи в недействительную подпись запрещено. В последующих действиях данный мастер полностью повторяет мастер подписания. Профили для данной операции также используются те же, что и для операции подписания. Разница в поведении заключается в том, что в данном мастере нет выбора формата сохранения подписи, а также имени файла и папки для сохранения полученной подписи, так как добавление подписи идет в уже существующий контейнер:



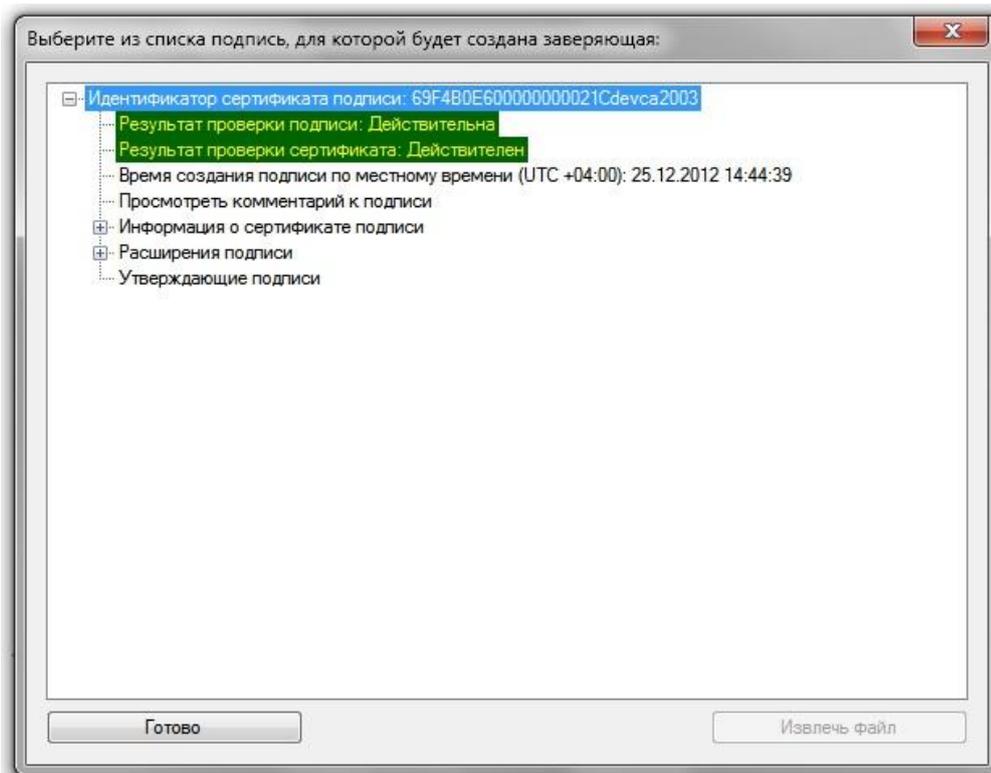
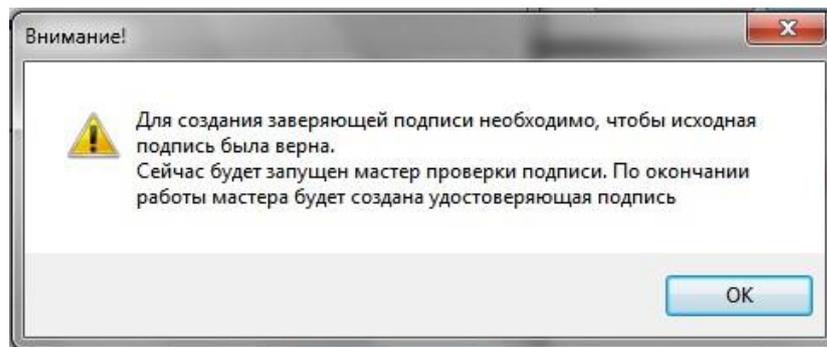


Мастер заверения ЭП.

При заверении отсоединенной подписи, мастер предварительно предложит выбрать файл, для которого создана исходная подпись. Заверение недействительной подписи запрещено. В последующих действиях данный мастер повторяет мастер подписания. Профили для данной операции также используются те же, что и для операции подписания. Разница в поведении заключается в том, что в данном мастере нет выбора формата сохранения подписи, а также имени файла и папки для сохранения полученной подписи, так как добавление подписи идет в уже существующий контейнер:

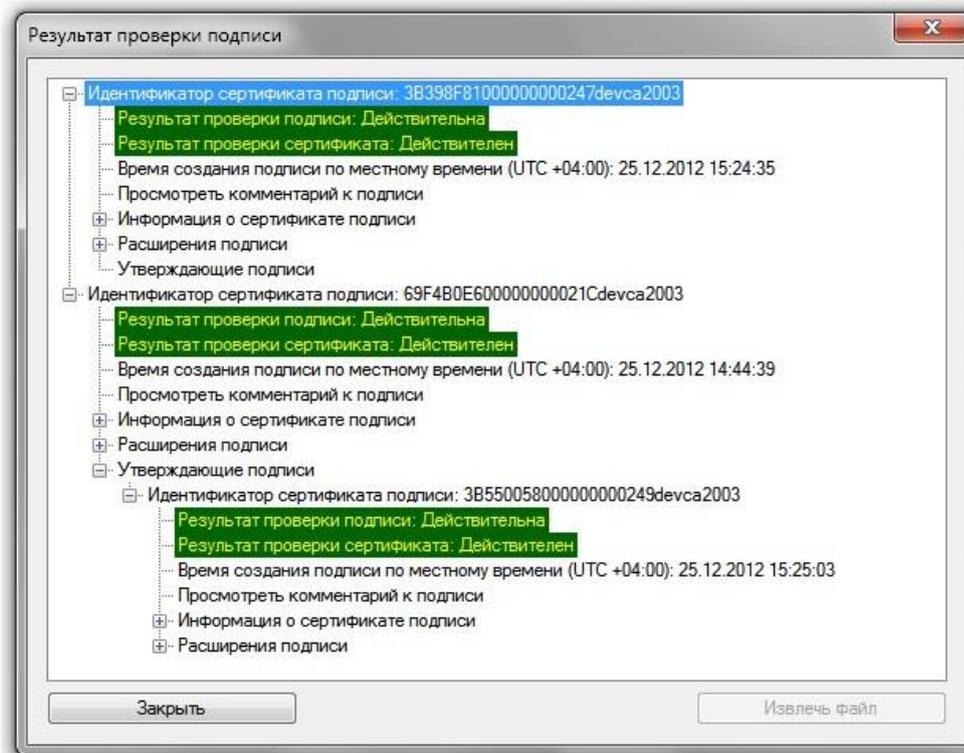


При нажатии кнопки *Готово* система проверит заверяемую подпись и выведет окно для выбора, какую из подписей, содержащихся в файле заверять:



После выбора подписи из списка нажмите *Готово*, и выбранная подпись будет заверена.

Мастер проверки ЭП.



При проверке ЭП выводится окно, в котором показано иерархическое дерево подписей. При этом предоставляется возможность просмотра параметров каждой из подписей списка, сертификата, использованного для создания каждой ЭП и извлечения содержимого присоединенной ЭП в папку, указанную пользователем.

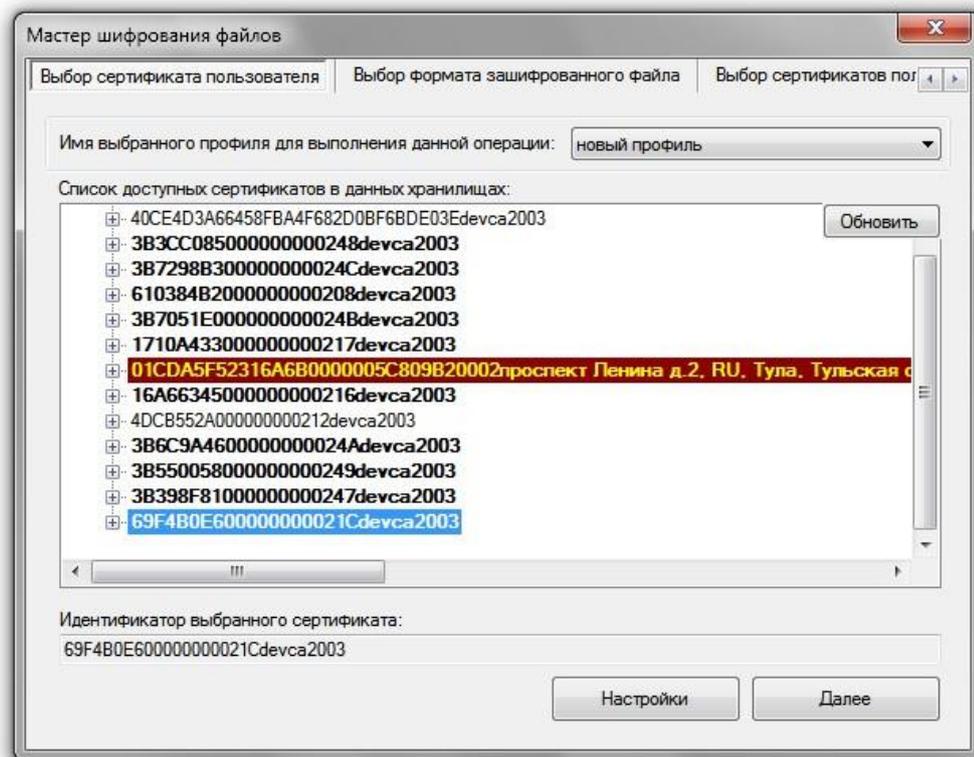
Кроме того, в этом же окне в пункте «*Расширения подписи*» показывается информация, полученная при проверке расширений подписи, например штампа времени или расширения графической подписи.

В случае проверки отсоединенной подписи система сама выведет окно для выбора файла, для которого необходимо проверить данную подпись.

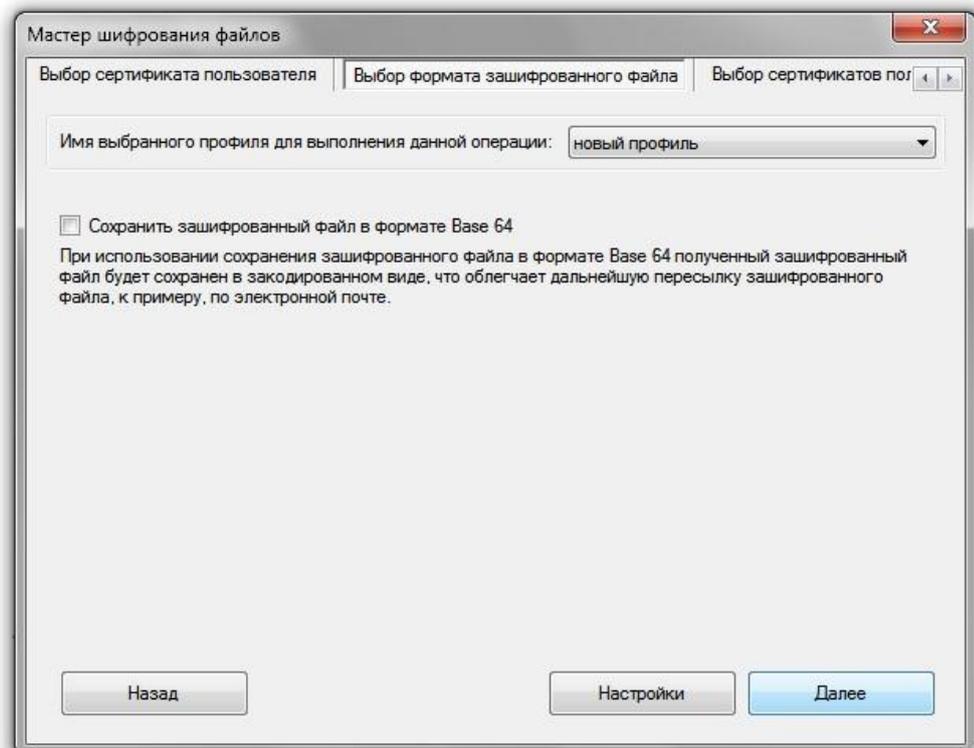
Мастер шифрования.

Мастер выполняет следующую последовательность действий:

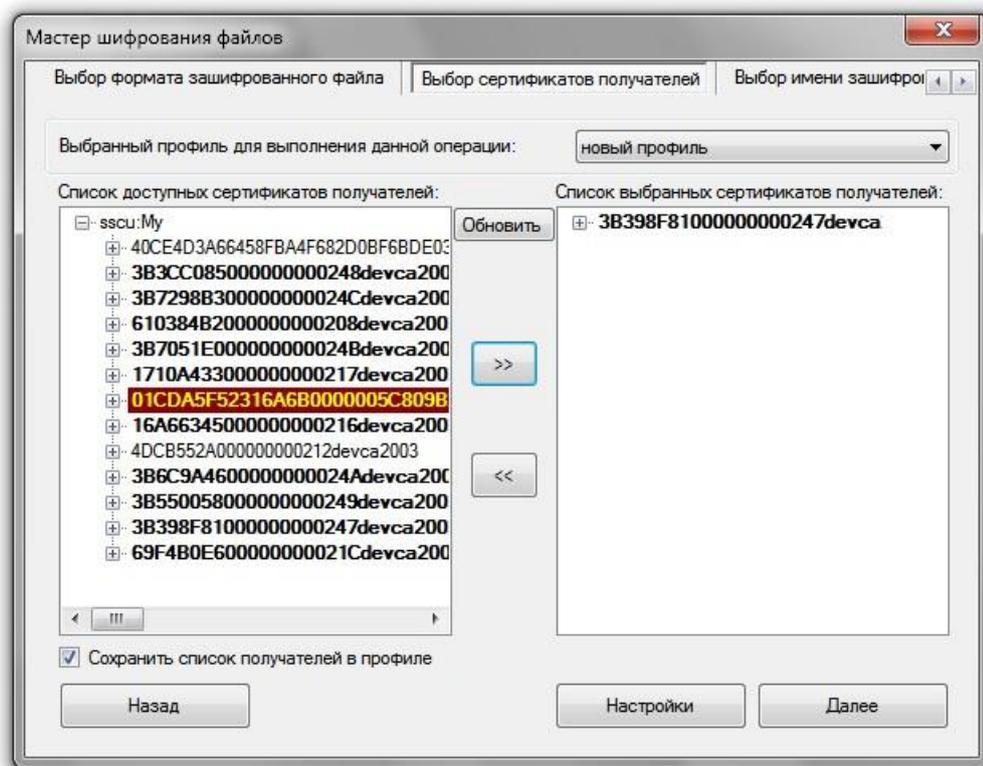
1. Выбор сертификата пользователя из доступных в пользовательском хранилище сертификатов, путь к которому можно изменить в настройках системы. Изменить хранилище можно из настроек системы, которые можно запустить с каждой страницы мастера, нажав кнопку *Настройки*:



2. Выбор формата сохранения полученного зашифрованного файла (наличие или отсутствие кодировки в Base64):



3. Выбор сертификатов получателей зашифрованного файла из списка сертификатов, доступных в хранилище *Получатели зашифрованных файлов*:



Вы можете добавлять сертификаты получателей зашифрованного сообщения в список выбранных получателей как по одному, так и выбрав в списке доступных сертификатов хранилище целиком. В таком случае в список получателей добавляются все сертификаты, содержащиеся в выбранном хранилище.

Красным отмечены недействительные на данный момент сертификаты. При наведении указателя мыши на данный сертификат показывается причина признания сертификата неверным.

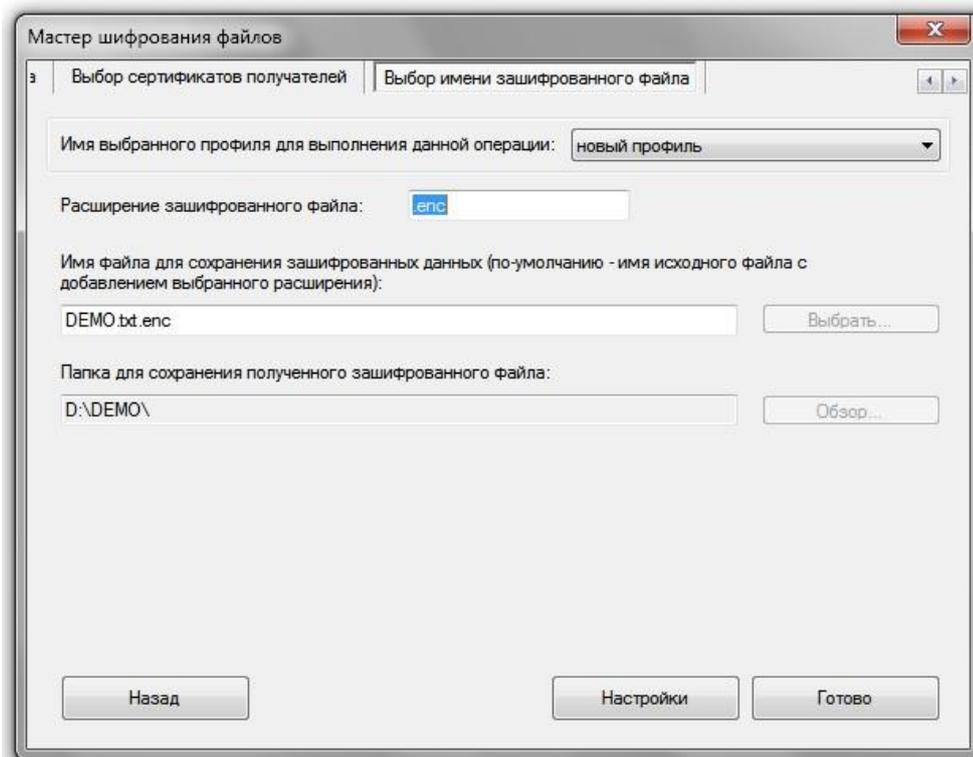
Жирным шрифтом отмечаются сертификаты, для которых найден связанный с ними закрытый ключ.

Вы можете обновить содержимое списка нажатием кнопки «Обновить».

С помощью настройки «Сохранить список получателей» в профиле можно создавать разные профили для шифрования для разных задач. Если у вас множество различных и часто изменяющихся получателей зашифрованных файлов, эту галочку рекомендуется снять. При выборе такого профиля из списка мастер сразу откроется на странице выбора получателей зашифрованного файла.

Если же необходимости в частой смене получателей нет, либо их небольшое фиксированное количество, то гораздо более удобным решением будет создание нескольких профилей с сохраненными в них списками получателей. При таком использовании вам будет достаточно лишь выбрать профиль и имя файла для сохранения результата мастера, а сам мастер будет открыт с последней страницы.

4. Получение имени для сохранения зашифрованного файла



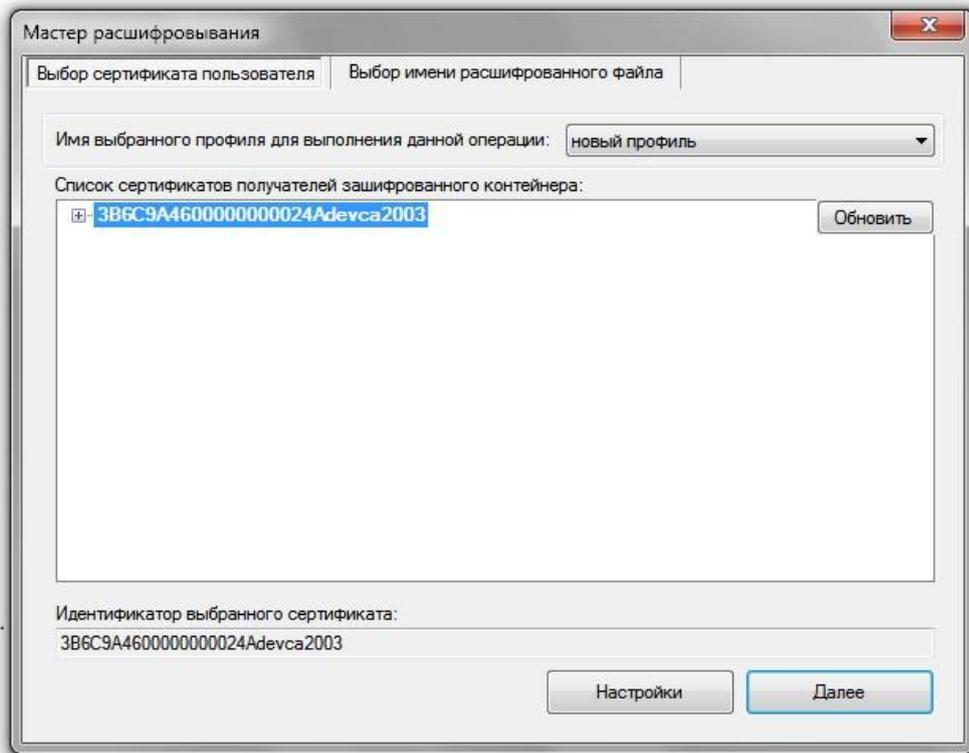
Если в настройках выбран профиль для шифрования по-умолчанию, то работа мастера начинается с п.4 (кроме случаев профилей с пустыми списками получателей; в таких случаях работа мастера начнется с п.3). Если в имени исходного файла отсутствует расширение *.enc, необходимо ввести имя файла.

Если в настройках указано местоположение файла результатов *Рядом с исходным файлом*, то выбирать каталог для сохранения итогового файла не требуется.

Мастер расшифровывания.

Мастер выполняет следующую последовательность действий:

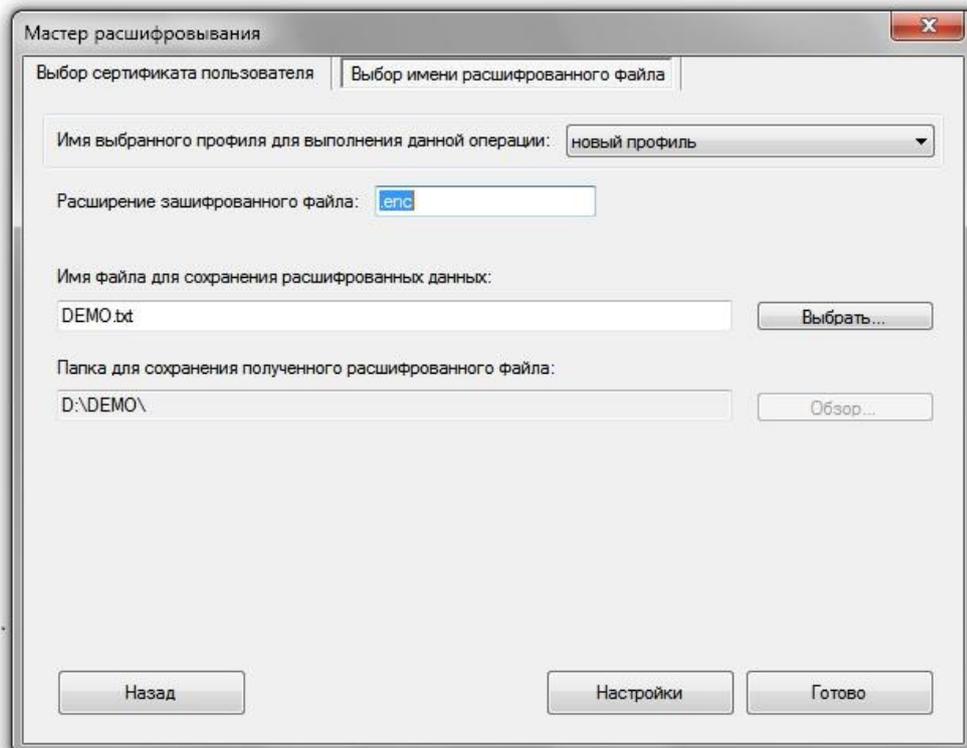
1. Выбор сертификата из списка пользовательских сертификатов, на котором предполагается производить расшифровывание контейнера. Список сертификатов формируется из списка получателей самого контейнера. Если требуемые сертификаты для расшифровывания отсутствуют в вашем пользовательском хранилище сертификатов, их имена будут выделены красным цветом:



Жирным шрифтом отмечаются сертификаты, для которых найден связанный с ними закрытый ключ.

Вы можете обновить содержимое списка нажатием кнопки «Обновить».

2. Получение имени и каталога для сохранения расшифрованного файла. Если в настройках указано местоположение файла результатов *Рядом с исходным файлом*, то выбирать каталог для сохранения итогового файла не требуется:



Если в настройках выбран профиль для расшифровывания по-умолчанию, и выбранный сертификат пользователя есть в списке получателей зашифрованного контейнера, то работа мастера начинается с п.2.

Мастер создания подписанного и зашифрованного контейнера.

Мастер последовательно вызывает мастера подписания и шифрования, результатом работы которых становится подписанный присоединенной подписью и зашифрованный файл – такой файл весьма удобно отправлять по e-mail. В случае, если в настройках пользователей выбраны профили по-умолчанию для операций подписания и шифрования, работа пользователя начнется с п. 4 мастера шифрования, мастер подписания же будет выполнен автоматически.

Мастер расшифровывания и проверки ЭП подписанного и зашифрованного контейнера.

Мастер выполняет следующую последовательность действий:

1. Выбор сертификата из списка пользовательских сертификатов, на котором предполагается производить расшифровывание контейнера. В случае если сертификат не будет явно указан, использовать сертификат по умолчанию.
2. Выбор глубины распаковки контейнера (расшифровать или расшифровать и извлечь исходный файл). В случае расшифровывания предоставляется возможность для указания имени файла контейнера. По умолчанию, данное имя повторяет имя исходного файла с расширением *.sig. В случае извлечения исходного файла предоставляется выбор между введением пользователем имени файла и использованием имени файла, хранящегося в поле «идентификатор ресурса» ЭП. При проверке ЭП выводится окно, в котором показано иерархическое дерево подписей с возможностью просмотра параметров каждой из подписей списка, а также сертификата, использованного для создания каждой конкретной ЭП.

Если во всплывающем меню выбран профиль с заполненными настройками для данной операции, то работа мастера должна начинаться с п.2. Для данной операции в профиле должны быть заполнены настройки как для ЭП, так и для шифрования.

Мастер отсоединения /присоединения подписанного файла данных

Мастер выполняет изменения типа подписи контейнера PKCS#7, отсоединяет или присоединяет файл данных к файлу подписи.

Списки настроек профиля для операций.

Создание, добавление, заверение ЭП:

1. Сертификат пользователя, на котором должна создаваться ЭП.
2. Вид ЭП (присоединенная (attached) или отсоединенная (detached)).
3. Папка для сохранения полученных ЭП.
4. Маска файла (по умолчанию *.sig), согласно которой должно быть сформировано имя полученного файла подписи.
5. Формат сохранения полученной ЭП, т.е. наличие или отсутствие Base64 кодировки.

Шифрование:

1. Сертификат пользователя, на котором должен создаваться зашифрованный контейнер.
2. Список сертификатов получателей зашифрованного сообщения.
3. Папка для сохранения полученных зашифрованных контейнеров.
4. Маска файла (по умолчанию *.enc), согласно которой должно быть сформировано имя полученного зашифрованного файла.
5. Формат сохранения полученного зашифрованного контейнера, т.е. наличие или отсутствие Base64 кодировки.

Расшифровывание

1. Сертификат пользователя, на котором должно быть произведено расшифровывание контейнера.
2. Папка для сохранения полученных расшифрованных файлов.
3. Маска файла (по умолчанию *.enc), согласно которой должно быть сформировано имя полученного файла подписи.

Вызов функций криптографического сервиса

Криптографический сервис запускается после выбора профиля в мастере соответствующей операции с записанными в профиле параметрами (или после формирования нового профиля, если это мастер криптографической операции) и, соответственно, выгружается по окончании выполнения операции.

Установка и удаление

Установка КАРМА

Для установки КАРМА на компьютер запустите исполняемый файл **setup.exe** и следуйте указаниям мастера установки.

Удаление КАРМА

Для удаления КАРМА с компьютера запустите стандартную процедуру деинсталляции из раздела «Установка и удаление программ» панели управления Microsoft Windows и следуйте указаниям программы.

Внимание! В процессе удаления КАРМА может потребоваться перезагрузка компьютера.

Работа с криптографическими провайдерами и инфраструктурой открытых ключей

Криптографический комплекс КАРМА предназначен для работы с криптопровайдерами, реализующими спецификацию Microsoft CryptoAPI на уровне работы с шифрованными/подписанными сообщениями (low level messages functions). КАРМА обрабатывает подписи и зашифрованные сообщения в формате структуры S-MIME согласно спецификации PKCS#7 (CMS).

Пользователь имеет возможность применять сертификаты открытых ключей, размещённые в хранилищах инфраструктуры открытых ключей как на собственном АРМ, так и в сетевых хранилищах, доступных пользователю, включая хранилища каталогов безопасности.

Внимание! Для правильной организации работы с инфраструктурой открытых ключей, рекомендуется прочитать документы *«Информация по работе с сертификатами»* и *«Информация по работе со списками отзыва»*, входящие в состав дистрибутива КАРМА.
