ESMART®

# *Использование ESMART Token в инфраструктуре PKI*

# Содержание

# 1. Возможности использования

*Аппаратно-программный комплекс ESMART Token предназначен для разработки средств обеспечения информационной безопасности с использованием сертификатов X.509 на смарт-картах. При работе с картами используется криптопровайдер, являющийся надстройкой над Microsoft Base SmartCard Cryptoprovider. Криптопровайдер (т.е. поставщик служб шифрования) представляет собой библиотеку isbccsp.dll, которая используется для работы с интерфейсом программирования приложений CryptoAPI от Microsoft. Работу по открытому стандарту PKCS#11 обеспечивает библиотека sbc_pkcs11_main.dll.*

*Библиотеки в Windows устанавливаются автоматически в системный каталог при установке при помощи программы-инсталлятора.*

*Для установки программного обеспечения и управления ПК при помощи консолей на ОС Windows Vista и выше требуются права администратора.*

*Возможности использования:*

- *Авторизация в Windows AD;*
- *Установка VPN соединений;*
- *Авторизация в Web по клиентскому SSL-сертификату;*
- *ЭЦП документов (в том числе шифрование PDF);*
- *Шифрование и ЭЦП электронной почты;*
- *Безопасное хранение паролей и конфиденциальных данных.*

*Если нет возможности автоматически скачивать драйвера посредством Windows Update, например, отсутствует выход в интернет или он ограничен, перед использованием ESMART Token необходимо установить драйвера из папки drivers для выбранной операционной системы. Для USB-ключа драйвера устанавливаются из папки drivers/ ESMART Token USB 64K.*

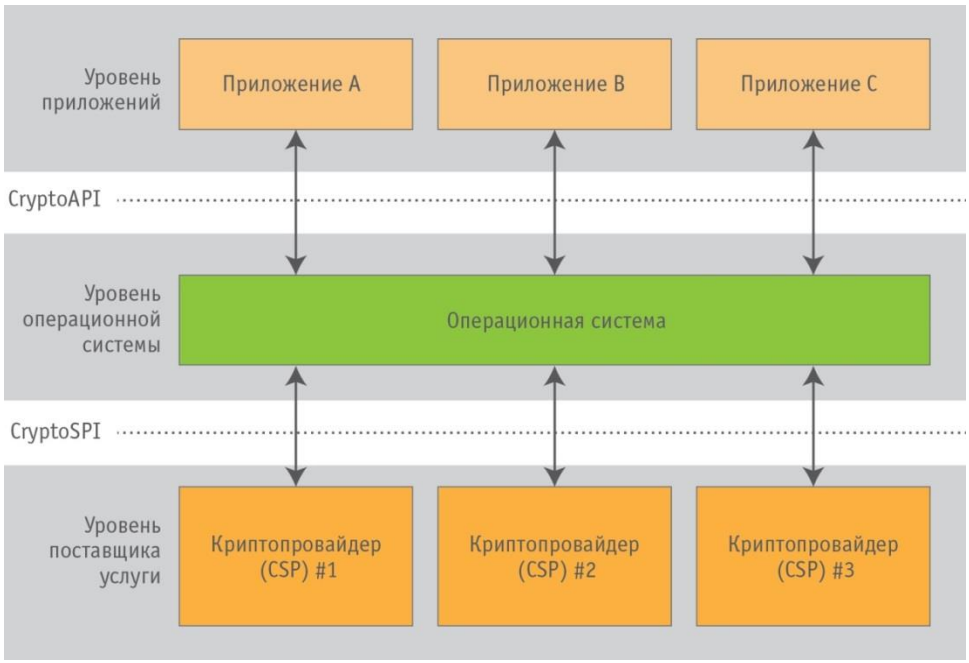
# 2. Криптографическая система Microsoft

## 2.1 CryptoAPI

*Криптографическая система Microsoft Windows состоит из нескольких уровней:*

- *приложений*
- *операционной системы*
- *криптопровайдеров*

*Приложения взаимодействуют с операционной системой через интерфейс программирования приложений CryptoAPI. Интерфейс CryptoAPI позволяет разработчикам программного обеспечения использовать в своих приложениях возможность аутентификации, кодирования и шифрования файлов. Операционная система взаимодействует с криптопровайдером через интерфейс CryptoSPI (cryptographic service provider interface).*




*Криптопровайдер (CSP – Cryptographic Service Provider) представляет собой независимый программный модуль, который выполняет криптографические алгоритмы для аутентификации, кодирования и шифрования. Криптопровайдер экспортирует набор обязательных функций, которые формируют системный программный интерфейс CryptoSPI. Каждая функция, экспортируемая криптопровайдером, соответствует определенной функции CryptoAPI.*

*Приложения не работают напрямую с криптопровайдером. Они вызывают функции CryptoAPI из библиотек Advapi32.dll и Crypt32.dll.*
*Операционная система фильтрует вызовы этих функций и вызывает соответствующие функции CryptoSPI, которые непосредственно взаимодействуют с криптопровайдером.*

*Криптопровайдер может состоять из одной или нескольких библиотек криптографических функций со стандартизованным интерфейсом. Как правило, файлы dll-библиотек помещаются в папку C:\Windows\System32\ для 32 битных систем, а для 64-битных систем в папки C:\Windows\System32\ и C:\Windows\sysWOW64.*

*В состав программных компонентов входит криптопровайдер ESMART CSP (библиотека C:\Windows\System32\isbccsp.dll). Библиотека устанавливается автоматически при установке пакета ESMART.*

*Прим.: библиотека C:\Windows\System32\isbc_pkcs11_main.dll реализует PKCS#11 для работы с картами, а не функции криптопровайдера. См. раздел 2.3.*

### 1.1 *CNG API*


*В операционных системах Windows Vista и Windows Server 2008 и старше используется обновленная и расширенная версия CryptoAPI – Cryptography Next Generation («криптография следующего поколения»).*

*CNG полностью поддерживает все функции API предыдущего поколения. Кроме того, CNG позволяет использовать в приложениях сторонние и собственные алгоритмы, например, алгоритмы шифрования на эллиптических кривых (EEC).*

***Структура CNG***

*В упрощенной структуре основное внимание уделено множеству криптографических примитивов bCrypt, служащих, например, для генерации случайных чисел, вычисления хэш, подписи и шифрования. Множество nCrypt выполняет функцию хранения ассиметричных ключей, а также обеспечивает поддержку аппаратных средств шифрования, например, смарт-карт.*

*CNG ориентирован на взаимодействие с интерфейсами провайдеров алгоритмов, а не привязан к определенному алгоритму.*

### *2.2 PKCS#11*

*Дополнительно к криптопровайдерам или в качестве альтернативы стандартным средствам Microsoft для работы со смарт-картами в Windows может использоваться модуль защиты, соответствующий открытому криптографическому стандарту PKCS#11. PKCS#11 является основным средством для работы со смарт-картами в ОС Linux. В Mac OS X имеется собственная службы для работы со смарт-картами, но многие приложения поддерживают именно работу по стандарту PKCS#11.*

*Стандарт PKCS#11 от RSA Laboratories описывает набор функций, алгоритмов и параметров для работы с криптографическими устройствами. Текст стандарта Documentation\Руководства администратора\pkcs-11v2-20.pdf.*

*В состав программных компонентов входят библиотеки для работы с картами по стандарту PKCS#11 isbc_pkcs_main.dll и isbc_esmart_token_mod.dll для Windows, libisbc_pkcs11_main.so и libisbc_esmart_token_mod.so для linux или libisbc_esmart_token_mod.dylib и libisbc_pkcs11_main.dylib для Mac OS X.*

*В частности, PKCS#11 может использоваться следующими приложениями:*

- *браузер Mozilla Firefox;*
- *почтовый клиент Mozilla Thunderbird;*
- *приложение для работы с PDF Adobe Acrobat.*

*На примере данных программ показано, как настроить работу приложений с картой по стандарту PKCS#11.*

*Подготовительные этапы описаны в руководстве администратора. ESMART Token – Настройка пользовательских приложений в Windows.*

# *3. Смарт-карты в Windows*

*Смарт-карты ESMART Token являются надежным и защищенным от подделки средством хранения данных, в том числе ключей и сертификатов. Ключи могут быть сгенерированы на самой смарт-карте или импортированы.*

*Смарт-карты и токены ESMART Token могут использоваться для хранения*

- *сертификатов и ключей стандарта X.509;*

- *симметричных ключей AES, DES, 3DES.*

*В ОС Windows смарт-карты рассматриваются как важный компонент PKI (см. раздел 4PKI – инфраструктура открытых ключей). Сертификаты на смарт-картах могут применяться для:*

- *авторизации по сертификату в домене;*
- *авторизации по SSL-сертификату на web-сайт;*
- *доступа по VPN в корпоративную сеть;*
- *ЭЦП и шифрования файлов;*
- *ЭЦП и шифрования электронной почты;*
- *шифрования EFS.*

*Смарт-карты ESMART Token можно использовать в качестве надежного и удобного средства хранения важных конфиденциальных данных, например паролей (см. раздел* Ошибка! Источник ссылки не найден.*). Смарт-карты оптимальны для хранения электронных сертификатов для подписи документов и электронной почты, а также для шифрования и дешифрования файлов.*

***Преимущества использования смарт-карт:***

- *надежное средство хранения закрытых ключей сертификатов и другой персональной информации, которое невозможно подделать;*
- *ПИН-код смарт-карты защищен от подбора методом прямого перебора, после заданного числа неверных попыток карта блокируется;*
- *ПИН-код карты может быть не только цифровым четырехзначным, как у большинства банковских карт, а содержать также буквы в разных регистрах и служебные символы;*
- *аутентификация, ЭЦП и обмен ключами происходит на смарт-карте, наиболее важная информация для обеспечения безопасности не передается в ПК;*
- *наиболее защищенное средство для обмена небольшими объемами информации, например логинами и паролями, между личным ПК,*
  *рабочим ПК и ноутбуком.*

# *4. PKI – инфраструктура открытых ключей*

*Инфраструктура открытых ключей (PKI – Public Key Infrastructure) является комплексной системой, в основе которой лежит использование криптографической системы с открытым ключом. В PKI предусмотрены средства для создания, управления, распространения, использования и отзыва цифровых сертификатов, которые удостоверяют, что соответствующий открытый ключ принадлежит определенному владельцу.*

*Основой PKI является* ***CA (Certification Authority)*** *— Центр Сертификации или Удостоверяющий центр*[1]*.*

*В зависимости от требуемых функциональных возможностей, бюджета, наличия квалифицированных специалистов и ряда других факторов организация может остановить свой выбор на собственном УЦ, внешнем УЦ или их комбинации.*

***Преимущества собственного ЦС****:*

- *возможность интеграции с Active Directory;*
- *полное управление выписываемыми сертификатами;*
- *дополнительная функциональность и пользователи могут быть добавлены по мере необходимости без значительных дополнительных расходов.*

***Недостатки собственного ЦС****:*

- *установка и настройка собственного центра сертификации может занимать длительное время и сопровождается дополнительными затратами;*

[1] *Далее в руководстве используется термин Центр сертификации в соответствии с текущей локализацией Microsoft Windows Server*

- *решение всех проблем, связанных с организацией и управлением PKI полностью ложится на организацию;*

*Выдачу и поддержку сертификатов при необходимости можно передать авторитетной сторонней организации.*

***Преимущества внешнего ЦС**:*

- *более высокий уровень доверия к сертификатам, выпущенным авторитетным центром;*
- *короткие сроки и более низкие затраты на начальном этапе;*
- *техническая поддержка и рекомендации специалистов.*

***Недостатки внешнего ЦС**:*

- *как правило, расходы на сертификат выше, чем при использовании собственного центра сертификации;*
- *меньше возможностей конфигурации и управления сертификатами;*
- *ограниченная интеграция с внутренней структурой предприятия.*

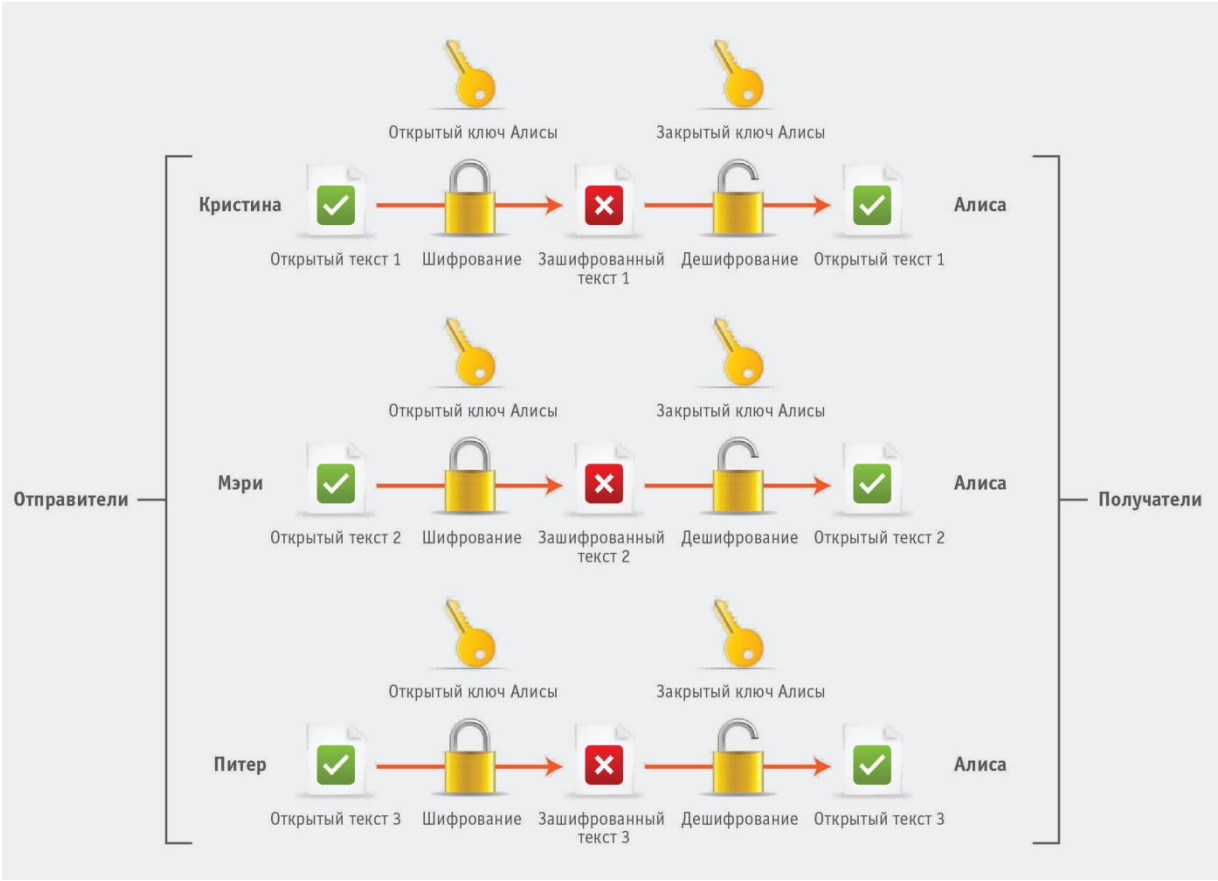
***Репозиторий сертификатов** обычно размещается на сервере каталогов, организованных в соответствии с международным стандартом X.500 и его подмножеством. Большинство серверов каталогов и прикладное программное обеспечение пользователей поддерживают упрощенный протокол доступа к каталогам LDAP (Lightweight Directory Access Protocol). Такой унифицированный подход позволяет обеспечивать функциональную совместимость приложений PKI и дает возможность доверяющим сторонам получать информацию о статусе сертификатов для верификации цифровых подписей.*

## *4.1 Шифрование открытым ключом*

*При шифровании открытым ключом для шифрования и дешифрования информации используются разные ключи. Закрытый ключ (private key) известен только владельцу сертификата и должен храниться в условиях максимальной секретности, а открытый ключ (public key) можно и необходимо передавать другим.*

*Два ключа отличаются по своим функциям и дополняют друг друга. Открытый ключ пользователя можно опубликовать в сертификате и сделать его доступным, например, через Active Directory, оттуда другие сотрудники смогут получить этот ключ и использовать его для шифрования. Для дешифрования может быть использован только соответствующий закрытый ключ пары.*

## 4.2 Схема шифрования и дешифрования открытыми ключами




## 4.3 Электронная цифровая подпись

*Стандартным способом применения ассиметричного шифрования является цифровая подпись. Цифровая подпись – это способ гарантировать целостность и происхождение данных. Цифровые подписи обычно используются при распространении данных в виде обычного текста в незашифрованной форме, когда требуется убедиться, что данные действительно исходят от указанного лица и не были изменены.*

*Автор шифрует данные своим закрытым ключом и прикладывает к письму подпись с зашифрованными данными. Для проверки получатель открытым ключом расшифровывает подпись и сравнивает расшифрованное сообщение с полученным сообщением.*

*Даже если файл или сообщение будут перехвачены, создать новую цифровую подпись, которая была бы действительной, злоумышленник не сможет.*

*Тем не менее, шифровать цифровой подписью весь объем данных непрактично по следующим причинам:*

- *Зашифрованный текст в подписи будет того же размера, что и соответствующий текст без шифрования, поэтому размер файла удвоится, что приводит к использованию больших объемов памяти;*
- *Шифрование открытым ключом больших объемов информации оказывает высокую нагрузку на процессор, что может отрицательно сказываться на производительности ПК;*
- *Шифрование информации в полном объеме при перехвате приведет к получению злоумышленником большого объема шифрованного текста, что облегчает несанкционированную расшифровку информации.*

*Поэтому для цифровой подписи используется не полный текст сообщения, а его свертка (хэш-сумма) (160 или 128 бит). Это позволяет сократить объем данных для шифрования, снизить нагрузку и усложнить процесс криптоанализа.*

### *4.4 Стандарты PKCS*

*Криптографические стандарты открытого ключа (Public Key Cryptography Standards) являются спецификациями для работы с открытым ключом.*

- ***Стандарт Cryptographic Message Syntax (PKCS #7)***
  *Формат PKCS#7 поддерживает хранение сертификатов и всех сертификатов в пути сертификации. Также используется в качестве запроса на обновление сертификата в УЦ.*
- ***Запрос Certificate Signing Request (PKCS #10)***
  *Формат PKCS#10 (.p10) используется для подачи заявки на сертификат. Запрос уже содержит в себе основные данные будущего сертификата.*
- ***Интерфейс Cryptoki (cryptographic token interface PKCS #11)***
  *Стандарт определяет программный интерфейс доступа к смарт-картам, не зависящий от выбранной платформы.*
- ***Файл обмена личной информацией (PKCS #12)***
  *Формат PKCS #12 (.p12 или .pfx) поддерживает безопасное хранение сертификатов, закрытых ключей. Файл содержит сертификат и соответствующий закрытый ключ.*

### *4.5 Электронные сертификаты*

*Сертификат открытого ключа, обычно называемый просто сертификатом, представляет собой документ с цифровой подписью, связывающий значение открытого ключа с удостоверением пользователя, устройства или службы, которым принадлежит соответствующий закрытый ключ.*

*В сертификате указана информация о субъекте, которому принадлежит открытый ключ, периоде действия сертификата, а также для каких целей предназначен выданный сертификат.*

*Для работы с сертификатами открытых ключей используется иерархическая PKI с одним или несколькими УЦ.*

*Цифровой сертификат, выданный и заверенный центром сертификации, обеспечивает достаточно высокий уровень безопасности, поскольку он может быть отозван (объявлен недействительным) в любой момент, выдавшим его центром.*

# 5. Сертификат X.509 версии 3


*При описании работы с ESMART Token использованы сертификаты X.509 версия 3 для PKI на основе Windows Server 2003. В сертификатах версии 3 поддерживаются следующие поля:*

***Subject (**Субъект**).** Поле хранит имя ПК, пользователя, сетевого устройства и сервиса, для которого УЦ выписал сертификат. Название субъекта обычно представлено в формате X.500 или Lightweight Directory Access Protocol (LDAP).*

***Serial Number (**Серийный номер**).** Уникальный идентификатор для каждого сертификата, выпушенного определенным CA.*

***Issuer (**Издатель**).** Понятное имя CA, который выписал сертификат. Имя издателя обычно представлено в формате X.500 или Lightweight Directory Access Protocol (LDAP).*

***Valid From (**Действителен с…**).** Дата и время, когда сертификат становится действительным.*

***Valid To (**Действителен до…**).** Дата и время, когда сертификат становится недействительным.*

***Внимание**! Сертификат считается действительным только в указанном диапазоне дат.*

***Public Key (**Открытый ключ**).** Открытый ключ или ключевая пара, соответствующая данному сертификату.*

*Дополнительные поля:*

***Subject alternative name (**Альтернативное имя субъекта**).** Имя субъекта может быть представлено в различных форматах. Например, если на сертификате в качестве обязательного имени указано название аккаунта пользователя в формате LDAP, в качестве дополнительных имен можно использовать электронную почту или имя участника-пользователя (user principal name - UPN),*

***CRL distribution points (CDP) (**Пункты распределения списков отозванных сертификатов**).** Когда пользователь, сервис или ПК предоставляет сертификат необходимо определить, не был ли он*

*отозван до того, как истечет срок его действия. В данном поле указан один или несколько URL, по которым сервис или приложение может получить список отозванных сертификатов (CRL).*

***Authority Information Access (AIA) (****Доступ к информации о родительском сертификате****).*** *Приложению или сервису необходимо определить подлинность и родительского сертификата УЦ, т.к. он также мог истечь или быть отозван. В данном поле предоставлен один или несколько URL, по которым можно получить родительский сертификат соответствующего УЦ.*

***Enhanced Key Usage (EKU) (****Расширенное использование ключа****).*** *В данном поле указан идентификатор объекта (object identifier - OID) каждого приложения или сервиса, для которых может быть использован сертификат. OID представляет собой уникальную последовательность номеров из единого всемирного реестра.*

***Certificate policies (****Политики сертификата****).*** *Описывают, какие меры предпринимает организация для проверки перед выдачей сертификата. Данные указаны в виде уникального идентификатора OID и URL с подробным описанием.*

## *5.1 Шаблоны сертификатов*

*В корпоративном Enterprise CA для Windows Server 2003 используются шаблоны сертификатов, которые хранятся в Active Directory. Шаблоны сертификатов используются для быстрого создания сертификатов с определенным набором атрибутов, например, возможностей использования сертификата, формата субъекта, длиной открытых ключей и сроком службы сертификата.*

*Информация о шаблонах сертификатов хранится в Active Directory в контейнере:*

```
CN=Certificate Templates,CN=Public Key
Services,CN=Services,CN=Configuration, DC= ForestRootNameDN
```

*где* `ForestRootNameDN` *это LDAP-имя леса корневого домена.*

## *5.2 Типы шаблонов сертификатов*

*Только что установленному УЦ первоначально доступны только несколько типов шаблонов, остальные необходимо подключить при необходимости.*

*Шаблоны можно подразделить на 2 основных типа: те, которые выдаются компьютерам, и те, которые выдаются пользователям. Кроме того, шаблоны могут делиться по следующему принципу:*

***Single function (****С одной функцией****).*** *Шаблон сертификата может содержать крайне ограниченный набор параметров и использоваться только для одной единственной функции. Например, можно создать сертификат только для EFS-шифрования и дешифрования файлов (Basic EFS).*

***Multiple functions (****Многофункциональные****).*** *Шаблон сертификата может использоваться для выполнения набора функций, например, для шифрования и дешифрования файлов, авторизации на сервер, защищенной работы с электронной почтой и др. с использованием одного и того же сертификата.*

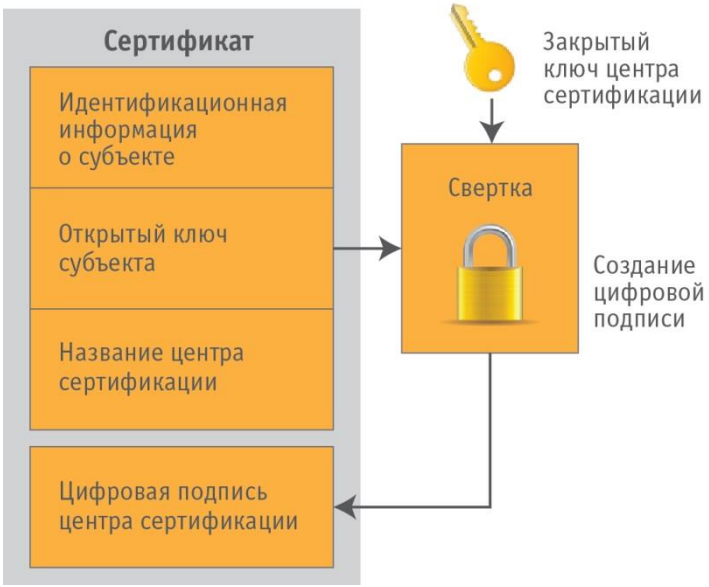
*В руководствах ESMART Token рассматриваются пользовательские сертификаты, созданные на основе шаблона* ***Smartcard User*** *(Пользователь со смарт-картой):*

| *Название шаблона* | *Описание* | *Основное назначение* | *Тип субъекта* | *Опубликован в Active Directory* |
|---|---|---|---|---|
| *Smartcard User* | *Позволяет владельцу сертификата авторизоваться и защищать электронную почту при помощи смарт-карты* | *Подпись и шифрование* | *Пользователь* | *Да* |

*Некоторые параметры шаблона сертификата можно изменять из консоли управления сертификатами **certmgr.msc**. Выберите сертификат и в контекстном меню откройте **Свойства › Общие**. Например, можно изменить способы использования сертификата.*

### 5.3 Цифровая подпись сертификата в УЦ

*УЦ использует свой закрытый ключ для цифровой подписи каждого сертификата, который он выпускает. Для создания цифровой подписи CA составляет свертку или дайджест сообщения (message digest) с сертификата и кодирует свертку своим закрытым ключом, прилагая ЭЦП как часть сертификата. Для проверки подлинности сертификата используется именно эта свертка. Если сертификат поврежден или он был подделан, свертка в цифровой подписи не совпадет со сверткой поддельного сертификата.*




*В сертификатах X.509 версии 3 в поле **Subject Public-Key Value (Значение открытого ключа субъекта)** указано, в каких целях можно использовать открытые и закрытые ключи. Как правило, открытые ключи применяются для следующих базовых криптографических операций:*

| *Операция* | *Назначение* |
|---|---|
| *Подпись* | *ЭЦП, аутентификация, подлинность* |
| *Шифрование* | *Шифрование и расшифровка данных* |
| *Подпись и шифрование* | *Шифрование и расшифровка данных, ЭЦП, аутентификация* |
| *Подпись и логин по смарт-карте* | *Логин по смарт-карте, ЭЦП* |

## 6. Возможности использования

*К клиентскому ПК должен быть подключен считыватель смарт-карт, установлены драйвера и криптопровайдер для используемых карт. В качестве программ для управления картами на ПК может быть установлена пользовательская утилита ESMART PKI Client. Программа распространяется бесплатно, но подходит для работы только с картами и USB-ключами ESMART Token.*

### 6.1 Хранение конфиденциальных данных на смарт-картах

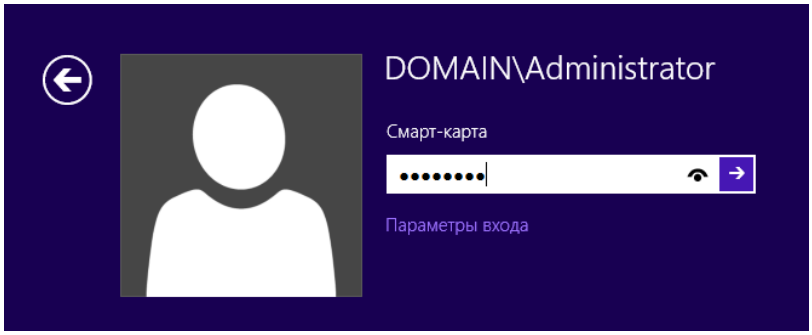
*Смарт-карты могут использоваться в качестве надежно защищенного хранилища текстовой информации. Память смарт-карты позволяет хранить только небольшой объем текста, например, логины и пароли.*

*Данные можно хранить в открытом виде, либо в защищенном виде, когда доступ к информации можно получить только после ввода верного ПИН-кода. Подробно процедура записи текстовых данных на карту описана в руководстве* ***Безопасное хранение паролей и конфиденциальных данных на смарт-карте****.*

## *6.2 Авторизация по смарт-картам*

*Авторизация по смарт-картам в домене при помощи смарт-карт является наиболее безопасным способом аутентификации пользователя благодаря тому, что необходимо предъявить саму смарт-карту с действующим сертификатом.*

*Чтобы войти в домен по смарт-карте не нужно вводить логин. Когда смарт-карта определена считывателем, Windows выдаст окно, в котором поле Логин уже будет заполнено. Пользователь вводит также не пароль к логину в домене, а ПИН-код смарт-карты (на рис. интерфейс Windows 8).*




*Для использования смарт-карт в домене требуется:*

- *развернутая в домене инфраструктура PKI, т.е. по крайней мере, один УЦ для выдачи сертификатов;*
- *настроенная Active Directory;*
- *наличие сертификата Enrollment Agent, позволяющего запрашивать сертификаты от имени других пользователей;*
- *наличие шаблонов сертификатов Smartcard User или Smartcard Logon;*
- *оснащение рабочих мест пользователей считывателями и установка драйверов.*

*Для получения максимально защищенной конфигурации в политике безопасности можно прописать обязательное предъявление смарт-карты для входа в домен, а также принудительную блокировку, выход из системы или завершение работы*
*при изъятии пользователем смарт-карты из считывателя.*

*Подробно развертывание центра сертификации и использование доменных групповых политик описано в Руководстве по развертыванию центра сертификации Windows Server 2008. Использование локальных политик представлено в руководстве ESMART Token - Авторизация в домене.*

## *6.3 VPN-авторизация по смарт-картам*

*Виртуальные частные сети VPN обладают рядом преимуществ, позволяя осуществлять надежную и безопасную передачу данных по открытым каналам связи. VPN позволяет предоставить удаленным сотрудникам надежный защищенный доступ к корпоративной сети без угрозы компрометации конфиденциальных данных.*

*Внедрение смарт-карт для установления VPN-соединения позволяет использовать преимущества двухфакторной аутентификации – требование смарт-карты и введение ПИН-кода. Кроме того,*

*использование смарт-карты и короткого ПИН-кода более удобно для пользователей, чем запоминание длинных и сложных паролей.*

*Для использования смарт-карт требуется:*

- *наличие хотя бы одного УЦ;*
- *наличие, как минимум, шаблонов Enrollment Agent, Smartcard Logon или Smartcard User;*
- *настройка VPN-сервера для работы с сертификатами;*
- *настройка ПК клиента и подключение считывателя.*

*VPN-соединение может быть установлено как для небольшого регионального офиса, так и для одного сотрудника, находящегося в командировке. В зависимости от требований, можно выбрать настольный считыватель или миниатюрный считыватель, который легко умещается в кармане.*

*Развертывание центра сертификации для использования смарт-карт описано в отдельном руководстве. Более подробно рекомендации по настройке виртуальных частных сетей описаны в руководстве ESMART Token -Защищенное VPN-соединение по сертификату X.509.*

### *6.4 ЭЦП и шифрование документов и почты*

*Шифрование и электронно-цифровая подпись становятся неотъемлемой частью ежедневных задач любой компании, которая заботится о безопасности и конфиденциальности своих данных.*

*Шифрование документов используется для передачи файлов или электронной почты таким образом, чтобы прочитать информацию мог только строго определенный адресат. В отличие от шифрования электронно-цифровая подпись решает другие задачи:*

- ***удостоверение источника файла/сообщения**. Имея открытый ключ субъекта можно однозначно определить, что информация действительно была создана именно пользователем, имеющим доступ к закрытому ключу, связанному с сертификатом, которым был подписан документ или сообщение.*
- ***защиту от случайного или преднамеренного изменения**. Даже если сообщение/файл были перехвачены и изменены, злоумышленник не сможет создать новую цифровую подпись, которая была бы действительна.*
- ***невозможность отказа от подписи**. Поскольку создать действительную цифровую подпись можно, только имея закрытый ключ, невозможно отрицать факт подписания.*

*Использование сертификатов X.509, выданных корпоративным УЦ на основе Windows Server описано в руководстве для пользователей **ESMART Token - ЭЦП и шифрование в Windows**. Необходимые подготовительные этапы приведены в руководстве для администраторов **ESMART Token – Настройка пользовательских программ в Windows**.*

### *6.5 Шифрование Windows EFS*

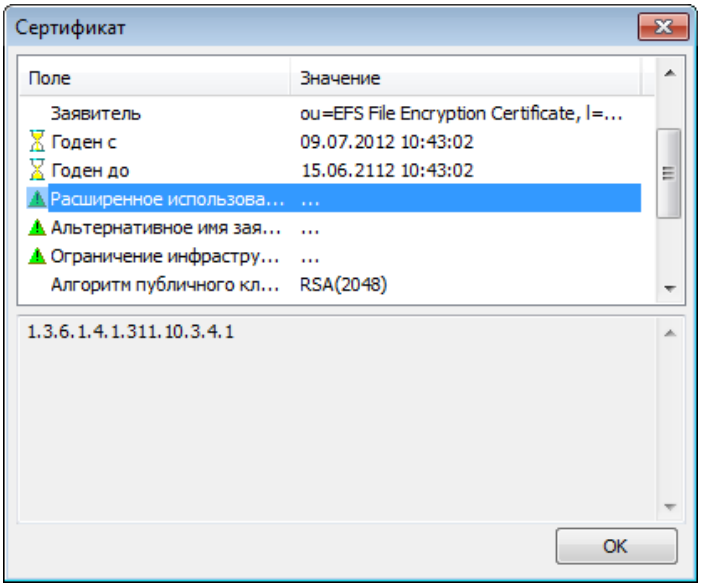
*В операционной системе Windows предусмотрен встроенный способ шифрования конфиденциальных данных при помощи сертификатов X.509. Шифрование EFS может использоваться **только** в файловой системе NTFS. Шифрование средствами EFS позволяет только ограничить доступ к важным данным нежелательных лиц, но не гарантирует целостности и достоверности источника файла.*

*Кроме того, файлы, зашифрованные при помощи EFS, не предназначены для передаче одному или нескольким лицам. Несмотря на то, что EFS позволяет добавить пользователей, которые имеют доступ к файлу, это применимо, в основном, к участникам Active Directory.*

*Возможности EFS ограничены в «домашних версиях» семейств ОС Windows XP, Windows Vista, Windows 7 и Windows 8.*

*Использование смарт-карт для хранения сертификатов EFS шифрования полностью поддерживается Windows. Возможно формирование самоподписанных сертификатов. Такие сертификаты могут быть*

*использованы только для шифрования файловой системы, они выдаются сроком на 100 лет и имеют только один идентификатор (OID 1.3.6.1.4.1.311.10.3.4.1) в разделе* ***Расширенное использование****.*




*Шифрование EFS с использованием сертификатов описано в руководстве ESMART Token - EFS шифрование.*