ESMART®

ESMART Token – CSP

Содержание

1. Общая информация

Криптопровайдер ESMART Token CSP позволяет осуществлять криптографические операции со смарт-картами ESMART Token[1] в операционной системе MS Windows.

2. Требования к операционной системе

- *Windows XP 32 и 64 бита[2];*
- *Windows Server 2003 32 и 64 бита;*
- *Windows Server 2008 32 и 64 бита;*
- *Windows Server 2012 32 и 64 бита;*
- *Windows Vista 32 и 64 бита;*
- *Windows 7 32 и 64 бита;*
- *Windows 8 32 и 64 бита.*

3. Автоматическая установка

*Криптопровайдер для ESMART Token устанавливается автоматически при установке ESMART PKI Client. Подробно установка при помощи программы-инсталлятора описана в руководстве **ESMART PKI Client – Руководство администратора**. Программа помещает динамические библиотеки dll в соответствующие системные папки для 32-битных и 64-битных систем. Вносятся изменения в реестр.*

*При установке программы в папке **X:\Program Files\ESMART** создаются директории с файлами изменения реестра для установленных библиотек. См. раздел **Удаление компонентов**.*

4. Ручная установка

Для 32-битных систем:

*Скопируйте **isbccsp.dll** из папки **SystemFolder** в системную папку Windows (X:\Windows\System32)*

Для 64-битных систем:

*Скопируйте **isbccsp.dll** из папки **SystemFolder** в системную папку Windows (X:\Windows\System32), а **isbccsp.dll** из папки **System64Folder** в системную папку **syswow64.***

*Запустите файлы реестра **csp x86.reg** для 32-битной версии Windows или **csp x64.reg** для 64-битной версии Windows.*

Если библиотеки были помещены не в системные папки, скорректируйте файлы изменения реестра.

Для Windows Vista и выше импорт файлов реестра должен запускаться под Администратором.

Перезагрузите ПК.

5. Хранилище сертификатов

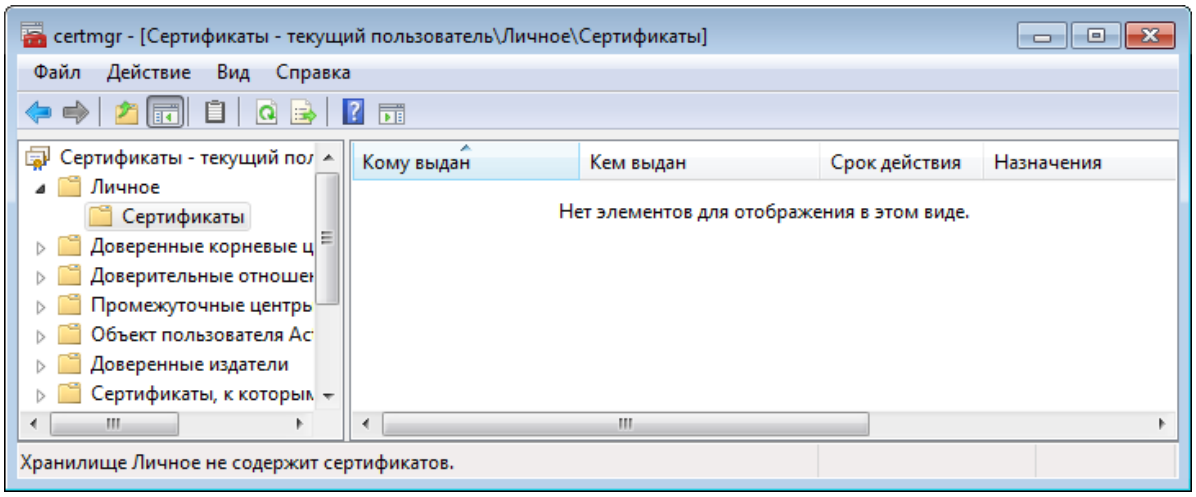
Windows помещает сертификаты в специальное хранилище, в котором сертификаты разбиты на группы по типу и назначению.

---

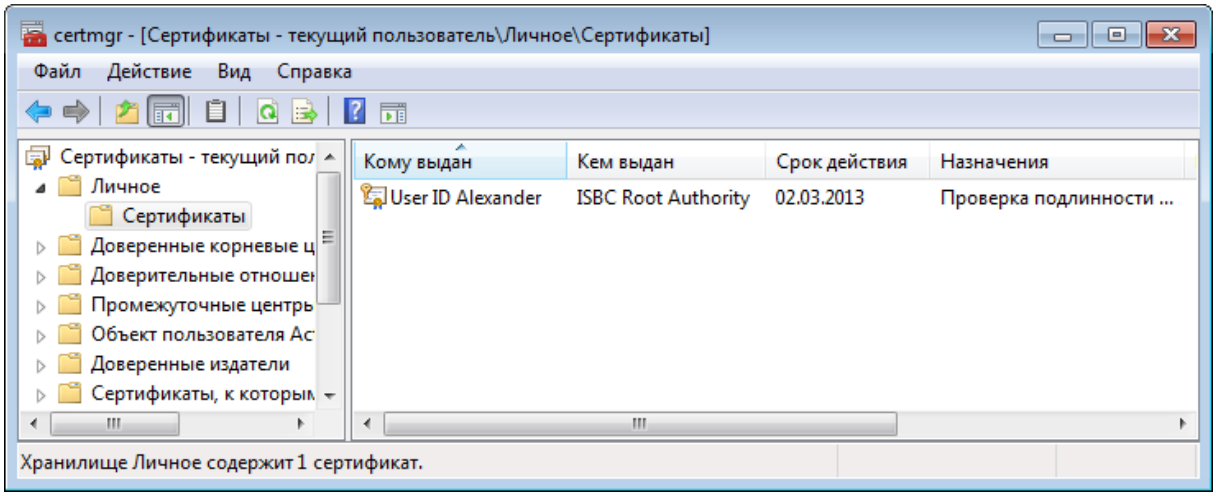
1 ПИН-код пользователя и ПИН-код администратора ESMART Token по умолчанию 12345678

2 Требуется установка пакета Base CSP
http://www.microsoft.com/en-us/download/details.aspx?id=4670

*Вызвать хранилище можно командой **certmgr.msc** или добавить «Сертификаты» текущего пользователя в качестве оснастки в Microsoft Management Console (mmc).*



Если библиотеки установлены правильно, когда карта вставлена в считыватель, сертификат (или сертификаты) находящиеся на ней, будут импортированы в хранилище Windows. Чтобы увидеть новые сертификаты, обновите окно через панель меню или F5.



Необходимо обратить внимание, что в хранилище импортируется только сертификат с открытым ключом, а закрытый ключ остается на карте. При извлечении карты закрытый ключ будет не доступен операционной системе, следовательно, невозможно будет использовать сертификат для электронной подписи или шифрования.

6. Использование сертификата с приложениями

Сертификаты, импортированные в хранилище Microsoft, становятся доступны для использования в следующих приложениях:

- *MS Windows для безопасного входа в систему с двухфакторной авторизацией;*
- *Microsoft Office для электронной подписи документов;*
- *Adobe Acrobat для цифровой подписи и шифрования документов PDF;*
- *Интернет-браузерами для передачи данных по протоколам SSL и TLS, авторизации на сайте:*
    - *Internet Explorer;*

- *Opera;*
- *Google Chrome.*

7. Удаление компонентов

При использовании автоматической установки воспользуйтесь панелью управления Windows, раздел ***Удаление программ****.*

Если использовалась ручная установка, удалите файлы библиотек .dll, а также запустите файлы изменения реестра ***remove csp x64.reg*** *или* ***remove csp x86.reg****, входящие в комплект.*