5.1. Создание самоподписанного сертификата

Для работы с BitLocker необходимо выписать сертификаты для шифрования и восстановления устройства.

1 этап: Создание файла с параметрами сертификата для шифрования устройства.

2 этап: Создание файла с параметрами сертификата для восстановления устройства.

3 этап: Создание сертификатов.

Создание файла с параметрами сертификата для шифрования устройства

Для создания файла с параметрами сертификата для шифрования устройства:

1. Откройте **Notepad** или любой другой текстовый редактор.
2. Скопируйте и вставьте следующую информацию в файл.
   ```
   [NewRequest]

   Subject = "CN=BitLocker"

   KeyLength = 2048

   ProviderName = "Aktiv ruToken CSP v1.0"

   KeySpec = "AT_KEYEXCHANGE"

   KeyUsage = "CERT_KEY_ENCIPHERMENT_KEY_USAGE"

   KeyUsageProperty = "NCRYPT_ALLOW_DECRYPT_FLAG"

   RequestType = Cert

   SMIME = FALSE

   [EnhancedKeyUsageExtension]

   OID=1.3.6.1.4.1.311.67.1.1
   ```
3. Сохраните файл с именем **blcert.txt**.

Создание файла с параметрами сертификата для восстановления устройства

Для создания файла с параметрами сертификата для восстановления устройства:

1. Откройте Notepad или любой другой текстовый редактор.
2. Скопируйте и вставьте следующую информацию в файл:

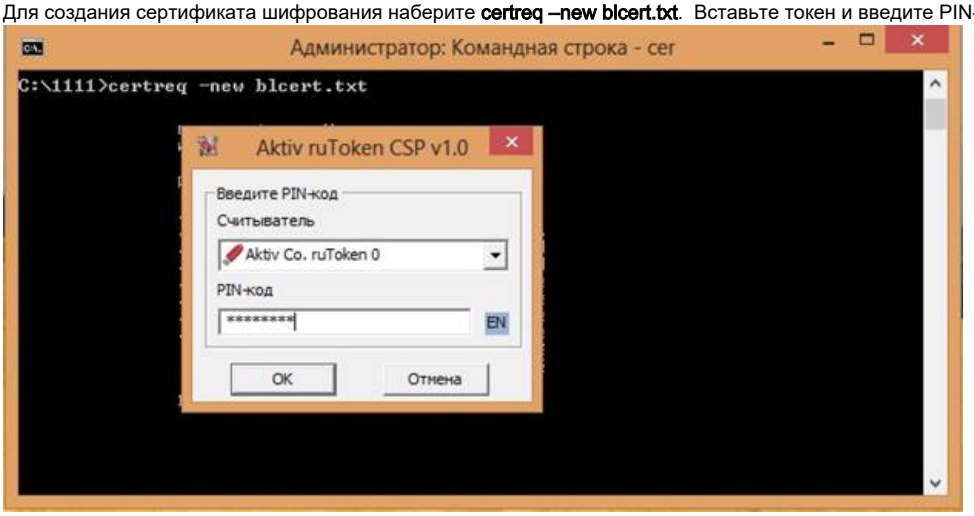
```
[NewRequest]
Subject = "CN=BitLocker DRA"
KeyLength = 2048
ProviderName = "Aktiv ruToken CSP v1.0"
Exportable = TRUE
ExportableEncrypted = FALSE
KeySpec = "AT_KEYEXCHANGE"
 KeyUsage = "CERT_KEY_ENCIPHERMENT_KEY_USAGE"
KeyUsageProperty = "NCRYPT_ALLOW_DECRYPT_FLAG"
RequestType = Cert
SMIME = FALSE
[EnhancedKeyUsageExtension]
OID=1.3.6.1.4.1.311.67.1.2
```

3. Сохраните файл с именем **bldracert.txt**.

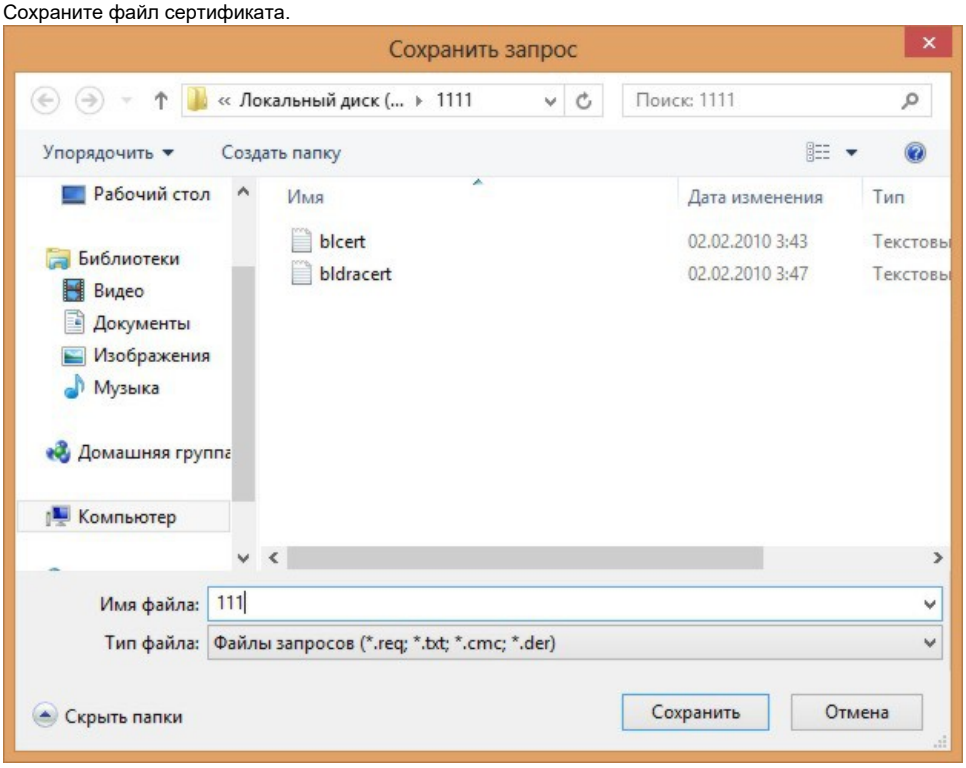
3. Создание сертификатов

Для создания сертификатов:

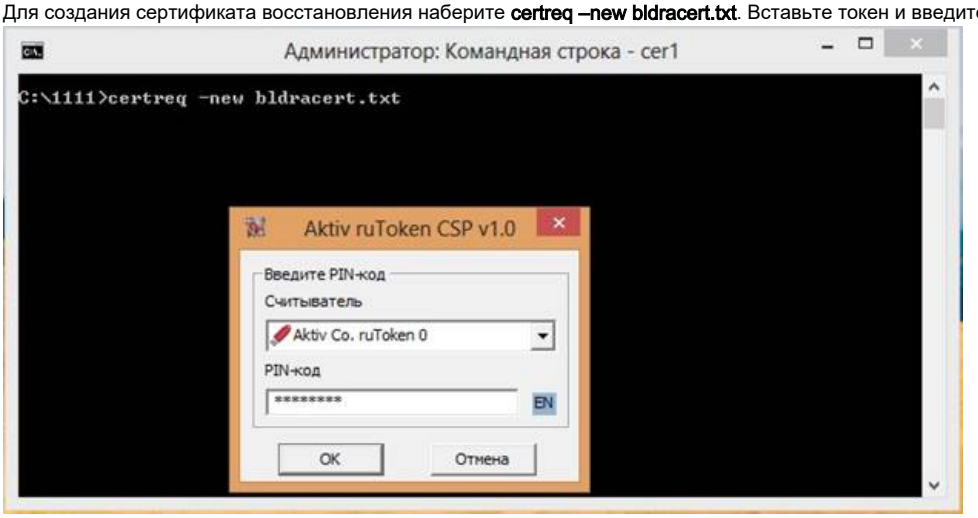
1. Откройте командную строку.
2. Для создания сертификата шифрования наберите **certreq –new blcert.txt**. Вставьте токен и введите PIN-код.



3. Сохраните файл сертификата.

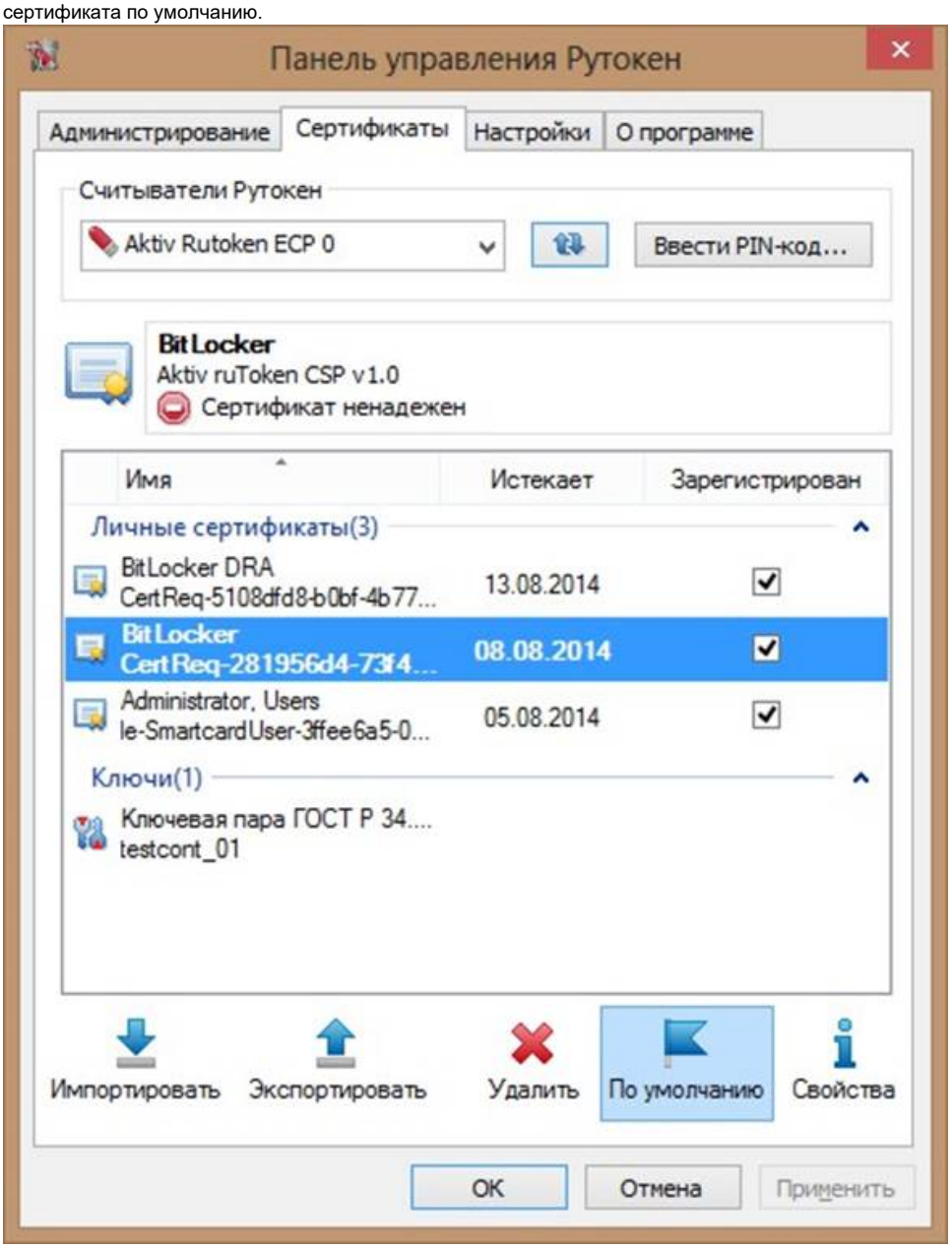


4. Для создания сертификата восстановления наберите **certreq –new bldracert.txt**. Вставьте токен и введите PIN-код.



5. Сохраните полученный файл сертификата.

6. Для того чтобы проверить, что сертификаты успешно созданы, запустите Панель управления Рутокен и перейдите на вкладку **Сертификаты.** В списке сертификатов должны быть сертификаты **BitLocker DRA** и **BitLocker.** Убедитесь, что сертификат **BitLocker** выбран в качестве сертификата по умолчанию.



7. При помощи mmc-консоли проверьте, зарегистрированы ли сертификаты в личном хранилище.

