Приложение 1 к типовым требованиям к программе и методике

квалификационных испытаний корректности встраивания СКЗИ

в прикладное программное обеспечение

**Методические рекомендации по проведению проверок корректности функционирования прикладных программных комплексов Банка России со встроенными средствами криптографической защиты информации с использованием контрольных примеров с преднамеренными искажениями**

АННОТАЦИЯ

Настоящий документ определяет перечень базовых экспериментов, по результатам которых можно сделать вывод о корректности или некорректности встраивания средств криптографической защиты информации (СКЗИ) в прикладное программное обеспечение (ППО) и основан на «Типовых требованиях к программе и методике квалификационных испытаний корректности встраивания СКЗИ в прикладное программное обеспечение», рекомендации по их проведению, а также включает в себя рекомендации по моделированию нештатных ситуаций.

### Перечень базовых экспериментов

В данном разделе приведен перечень базовых экспериментов, который указывает объем и полноту проводимых проверок.

* 1. **Эксперименты с инициализацией СКАД «Сигнатура»**
     1. Попытка инициализации системы криптографической авторизации документов (СКАД) «Сигнатура» в экспериментах с участием списка отозванных сертификатов (СОС), необходимого для проверки собственного сертификата, для случая, когда срок действия СОС истек;
     2. Попытка инициализации СКАД «Сигнатура» при отсутствии персонального справочника сертификатов (local.pse) (ПСП);
     3. Попытка инициализации СКАД «Сигнатура» при отсутствии локального справочника сертификатов (local.gdbm) (ЛСС);
     4. Попытка инициализации СКАД «Сигнатура» с использованием закрытого ключа, не соответствующего расширенной области применения ключа.
  2. **Эксперименты с подключением к СКЗИ «Янтарь АСБР»**

#### Попытка подключения к несуществующей сессии СКЗИ «Янтарь»;

#### Попытка подключения к сессии СКЗИ «Янтарь», в которую не загружен закрытый ключ;

#### Попытка авторизации на СКЗИ «Янтарь» с небезопасным (длина менее 8 символов) паролем;

#### Попытка авторизации на СКЗИ «Янтарь» с неверным паролем;

#### Попытка подключения к сессии СКЗИ «Янтарь», в которую загружен ключ, не соответствующий расширенной области применения ключа.

* 1. **Эксперименты с установкой КА**
     1. Формирование кода аутентификации (КА) в штатной ситуации;
     2. Попытка формирования КА, сформированного на закрытом ключе, не соответствующем расширенной области применения ключа.
  2. **Эксперименты с проверкой КА**
     1. Проверка КА в штатной ситуации;
     2. Попытка проверки при искажении КА или подписанных данных;
     3. Попытка проверки КА при отсутствии КА.

Примечание.

При наличии в электронном сообщении (ЭС) двух КА следует моделировать все варианты искажений, приводящие к тому, что:

* недействителен первый КА, второй действителен;
* недействителен второй КА, первый действителен;
* недействительны оба КА;
* нарушено число требуемых КА (отсутствует один или оба КА).
  + 1. Попытка проверки КА с использованием несобственного сертификата для каждого из следующих условий:
       1. срок действия сертификата истек;
       2. сертификат является отозванным;
       3. сертификат отсутствует в справочнике сертификатов;
       4. сертификат имеет нарушенную целостность.
    2. Попытка проверки КА, сформированного на закрытом ключе, не соответствующем расширенной области применения ключа.
    3. Попытка проверки КА в экспериментах с участием СОС, необходимого для проверки несобственного сертификата, в случае, когда:
       1. срок действия СОС истек;
       2. СОС отсутствует;
       3. отсутствует сертификат, необходимый для проверки СОС;
       4. нарушена целостность СОС.
  1. **Эксперименты с шифрованием** 
     1. Попытка шифрования ЭС в штатной ситуации;
     2. Попытка шифрования ЭС с использованием сертификата открытого ключа получателя для каждого из следующих условий:
        1. срок действия сертификата истек;
        2. сертификат является отозванным;
        3. сертификат отсутствует в справочнике сертификатов;
        4. сертификат имеет нарушенную целостность.
     3. Попытка шифрования ЭС с участием СОС для каждого из следующих условий:
        1. срок действия СОС истек;
        2. отсутствует сертификат, необходимый для проверки СОС;
        3. СОС отсутствует в справочнике сертификатов отправителя;
        4. нарушена целостность СОС.
     4. Попытка шифрования ЭС с использованием закрытого ключа без функции шифрования;
     5. Попытка шифрования с использованием закрытого ключа, не соответствующего расширенной области применения ключа.
  2. **Эксперименты с расшифрованием**
     1. Попытка расшифрования ЭС в штатной ситуации;
     2. Попытка расшифрования ЭС при искажении подписанных данных;
     3. Попытка расшифрования ЭС с использованием сертификата открытого ключа отправителя для каждого из следующих условий:
        1. срок действия сертификата истек;
        2. сертификат является отозванным;
        3. сертификат отсутствует в справочнике сертификатов;
        4. нарушена целостность сертификата.
     4. Попытка расшифрования ЭС с участием СОС для каждого из следующих условий:
        1. срок действия СОС истек;
        2. отсутствует сертификат, необходимый для проверки СОС;
        3. СОС отсутствует в справочнике сертификатов получателя;
        4. нарушена целостность СОС**.**
     5. Попытка расшифрования ЭС, зашифрованного с использованием закрытого ключа, не соответствующего открытому ключу получателя;
     6. Попытка расшифрования ЭС, зашифрованного с использованием закрытого ключа, не соответствующего расширенной области применения ключа.

### Рекомендации по проведению базовых экспериментов

В данном разделе приведены рекомендации по проведению базовых экспериментов с указанием корректной реакции СКЗИ на условия проводимых экспериментов. Для корректного проведения базовых экспериментов, рекомендуется использовать «Программу моделирования кодов ошибок СКАД «Сигнатура»» и «Программу моделирования кодов ошибок СКЗИ «Янтарь АСБР»» в прикладном программном обеспечении. Данная программа предназначена для организации экспериментального тестирования при проведении работ по проверке корректности встраивания СКЗИ в прикладное программное обеспечение. Эта программа предназначена для использования на стендах тестирования. Данную программу нельзя применять на автоматизированных рабочих местах, используемых в реальной работе ППО.

### Рекомендации по проведению экспериментов с инициализацией СКЗИ

#### Попытка инициализации СКАД «Сигнатура» в экспериментах с участием СОС, необходимого для проверки собственного сертификата, для случая, когда срок действия СОС истек.

Данный эксперимент моделируется переводом времени таким образом, чтобы для времени проведения эксперимента были справедливы следующие соотношения:

#### на момент проведения эксперимента действителен закрытый ключ пользователя, выполняющего инициализацию;

#### на момент проведения эксперимента были недействителен хотя бы один из СОС, выпущенных вышестоящими Центром Сертификации (ЦС).

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700034***,*** которому соответствует текстовое описание «Ошибка проверки сертификата» («Verify Certificate Error»).

#### Попытка инициализации СКАД «Сигнатура» при отсутствии персонального справочника сертификатов (local.pse).

Данный эксперимент моделируется удалением файла local.pse. Данное действие можно сделать с использованием стандартных средств Windows.

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070002D, которому соответствует текстовое описание «Ошибка доступа к ПСП» («Open PSE Error»).

#### Попытка инициализации СКАД «Сигнатура» при отсутствии локального справочника сертификатов (local.gdbm).

Данный эксперимент моделируется удалением файла local.gdbm. Данное действие можно сделать с использованием стандартных средств Windows.

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700030, которому соответствует текстовое описание «Ошибка проверки целостности ПСП» («Verifying PSE integrity error»).

#### Попытка инициализации СКАД «Сигнатура» с использованием закрытого ключа, не соответствующего расширенной области применения ключа.

Для проведения данного эксперимента необходимо инициализировать СКЗИ с помощью закрытого ключа, расширенная область применения ключа которого не соответствует требуемому значению.

В связи с тем, что СКЗИ при загрузке ключевой информации не проверяет соответствие объектных идентификаторов закрытого ключа требуемым значениям, данная проверка должна проводиться на уровне ППО.

#### Рекомендации по проведению экспериментов с подключением к СКЗИ «Янтарь» и авторизации на СКЗИ «Янтарь».

#### Попытка подключения к несуществующей сессии СКЗИ «Янтарь»

Для проведения данного эксперимента необходимо передать в функции авторизации некорректный идентификатор сессии СКЗИ «Янтарь» (например, её символьное имя или идентификатор закрытого ключа).

Корректной реакцией СКЗИ для данного эксперимента является код возврата E0700081, которому соответствует текстовое описание «Сессия криптосервера не найдена» («Cryptoserver session with specified cert not found»).

#### Попытка подключения к сессии СКЗИ «Янтарь», в которую не загружен закрытый ключ

Для проведения данного эксперимента следует вызвать функцию авторизации СКЗИ «Янтарь» с корректными параметрами в тот момент, когда администратор КС еще не загрузил в сессию закрытый ключ.

Корректной реакцией СКЗИ для данного эксперимента является код возврата A02000AA, которому соответствует текстовое описание «Сессия заблокирована» («Session blocked»).

#### Попытка авторизации на криптосервере с небезопасным паролем

Для проведения данного эксперимента необходимо передать в функции авторизации некорректный пароль для сессии криптосервера, длина которого менее 8 символов.

Корректной реакцией СКЗИ для данного эксперимента является код возврата E02000AC, которому соответствует текстовое описание «Небезопасные данные аутентификации» («Unsecure authentication credentials»).

#### Попытка авторизации на криптосервере с неверным паролем

Для проведения данного эксперимента необходимо передать в функции авторизации некорректный пароль для сессии криптосервера, длина которого не менее 8 символов.

Корректной реакцией СКЗИ для данного эксперимента является код возврата E02000A9,которому соответствует текстовое описание «Доступ запрещен» («Access denied»).

#### Попытка подключения к сессии криптосервера, в которую загружен ключ, не соответствующий расширенной области применения ключа

Для проведения данного эксперимента необходимо подключиться к сессии криптосервера, в которую загружен ключ, расширенная область применения ключа которого не соответствует требуемому значению.

В связи с тем, что СКЗИ при загрузке ключевой информации не проверяет соответствие объектных идентификаторов закрытого ключа требуемым значениям, данная проверка должна проводиться на уровне ППО.

#### Рекомендации по проведению экспериментов с установкой КА

В перечне базовых экспериментов содержится два эксперимента с установкой КА:

1. Формирование КА в штатной ситуации;
2. Попытка формирования КА, сформированного на закрытом ключе, не соответствующем расширенной области применения ключа.

Оба эксперимента надо проводить в момент времени, когда все необходимые для установки КА объекты находятся в штатном состоянии. В обоих экспериментах СКЗИ отрабатывает штатно, и возвращает код возврата 0, которому соответствует текстовое описание «ОК». При этом во втором эксперименте проверка соответствия OID закрытого ключа требуемым значениям должна проводиться ППО.

#### Рекомендации по проведению экспериментов с проверкой КА

В настоящем разделе приведены рекомендации по проведению экспериментов с проверкой КА, а также описание кодов возврата СКЗИ и соответствующих им текстовых описаний. При этом код возврата СКЗИ указывается в формате «числовое значение кода возврата функции СКЗИ» или «числовое значение кода возврата функции СКЗИ : результат проверки КА», так как функция проверки подписи СКЗИ может возвращать информацию о результатах проверки отдельных КА. При этом если КА несколько, то результаты работы СКЗИ будут указаны в формате «числовое значение кода возврата функции СКЗИ: результат проверки первого КА : результат проверки второго КА : …».

При описании рекомендации по проведению экспериментов предполагается, что на момент проведения испытаний всегда действителен закрытый ключ пользователя, выполняющего проверки.

#### Проверка КА в штатной ситуации

Данный эксперимент необходимо проводить в момент времени, когда все необходимые для проверки КА объекты (сертификаты и СОС) находятся в штатном состоянии. В данном эксперименте СКЗИ возвращает код возврата 0, которому соответствует текстовое описание «ОК».

#### Попытка проверки при искажении КА или подписанных данных.

Данный эксперимент необходимо проводить в момент времени, когда все необходимые для проверки КА объекты (сертификаты и СОС) находятся в штатном состоянии.

Для моделирования рассматриваемой нештатной ситуации необходимо внести искажения в подписанные данные или КА в соответствии с рекомендациями раздела «Попытка проверки при искажении КА или подписанных данных.», и получить следующие коды возврата:

#### E0700019 : E0700042, которому отвечает текстовое сообщение «Ошибка проверки КА. Подпись недостоверна» («Sign Verify Error. Invalid Signature»)

Примечание. В данном случае текстовое описание состоит из двух предложений – первое соответствует коду E0700019, а второе – коду E0700042.

#### E070001A, которому соответствует текстовое описание «Сообщение не подписано или формат искажен» («Message not signed or damaged»)

#### Попытка проверки КА при отсутствии КА.

Данный эксперимент рекомендуется проводить в момент времени, когда все сертификаты и СОС, необходимые для проверки рабочего сертификата пользователя, находятся в штатном состоянии. Причем проверка на отсутствие КА должна проводиться средствами ППО. Соответственно, данный эксперимент не требует участия СКЗИ.

#### Попытка проверки КА с использованием несобственного сертификата, находящегося в нештатном состоянии

Рекомендации по моделированию нештатных состояний для несобственного сертификата приведены в разделе «Моделирование нештатных разделов сертификатов». Поэтому в настоящем разделе приведены только описания реакции СКЗИ на условия экспериментов для различных нештатных состояний несобственного сертификата.

#### срок действия сертификата истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700036, которому соответствует текстовое описание «Ошибка проверки КА. Сертификат истек» («Sign verify Error. Certificate expired»).

#### сертификат является отозванным

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700039, которому соответствует текстовое описание «Ошибка проверки КА. Сертификат отозван» («Sign verify Error. Certificate revoked»).

#### сертификат отсутствует в справочнике сертификатов

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700046, которому соответствует текстовое описание «Ошибка проверки КА. Сертификат не найден» («Sign verify Error. Certificate not found»).

#### сертификат имеет нарушенную целостность

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700037, которому соответствует текстовое описание «Ошибка проверки КА. Сертификат поврежден» («Sign verify Error. Certificate damaged»).

#### Попытка проверки КА, сформированного на закрытом ключе, не соответствующем расширенной области применения ключа.

Для проведения данного эксперимента необходимо, чтобы в сертификате подписанта поле OID отличалось от требуемого.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700041, которому соответствует текстовое описание «Использование сертификата не по назначению» («Invalid Certification Usage»).

Примечание. Указанный выше код возврата можно получить только при использовании при проверке КА флага FLAG\_VERIFY\_EXTKEYUSAGE. В большинстве прикладных систем данный флаг при проверке КА не устанавливается, и проверка объектных идентификаторов сертификата подписанта на соответствие требуемым выполняется прикладным уровнем.

#### Попытка проверки КА в экспериментах с участием СОС, необходимого для проверки несобственного сертификата и находящегося в нештатном состоянии

Рекомендации по приведению СОС в нештатное состояние описаны в разделе «Рекомендации по моделированию нештатных состояний СОС». Поэтому в настоящем разделе приведены только описания реакции СКЗИ на условия экспериментов для различных нештатных состояний СОС.

#### срок действия СОС истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E070003C, которому соответствует текстовое описание «Ошибка проверки КА. СОС издателя недействителен по времени» («Sign verify Error. CRL expired»).

#### СОС отсутствует

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E070003B, которому соответствует текстовое описание «Ошибка проверки КА. Отсутствует СОС издателя» («Sign verify Error. CRL missing»).

#### отсутствует сертификат, необходимый для проверки СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E0700035, которому соответствует текстовое описание «Ошибка проверки КА. Сертификат не найден» («Sign verify Error. Certificate not found»).

#### нарушена целостность СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700019 : E070003D, которому соответствует текстовое описание «Ошибка проверки КА. Недостоверна подпись CRL издателя» («Sign verify Error. CRL damaged»).

#### Рекомендации по проведению экспериментов с шифрованием

#### Попытка шифрования ЭС в штатной ситуации.

Данный эксперимент необходимо проводить в момент времени, когда все необходимые для успешного шифрования объекты (сертификаты и СОС) находятся в штатном состоянии. В данном эксперименте СКЗИ возвращает код возврата 0, которому соответствует текстовое описание «ОК».

#### Попытка шифрования ЭС с использованием сертификата открытого ключа получателя, находящегося в нештатном состоянии

Эксперименты с шифрованием ЭС с использованием сертификата открытого ключа получателя для следующих условий:

#### срок действия сертификата истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700036, которому соответствует текстовое описание «Сертификат истек» («Certificate expired»).

#### сертификат является отозванным

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700039, которому соответствует текстовое описание «Сертификат отозван» («Certificate revoked»).

#### сертификат отсутствует в справочнике сертификатов

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700046, которому соответствует текстовое описание «Сертификат не найден» («Certificate not found»).

#### сертификат имеет нарушенную целостность

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700037, которому соответствует текстовое описание «Сертификат поврежден» (Certificate damaged»).

#### Попытка шифрования ЭС с участием СОС, необходимого для проверки сертификата получателя и находящегося в нештатном состоянии

В настоящем разделе приведены описания реакции СКЗИ на условия экспериментов для различных нештатных состояний СОС.

#### срок действия СОС истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003C, которому соответствует текстовое описание «СОС издателя недействителен по времени» («CRL expired»).

#### СОС отсутствует

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003B, которому соответствует текстовое описание «Отсутствует СОС издателя» («CRL missing»).

#### отсутствует сертификат, необходимый для проверки СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700035, которому соответствует текстовое описание «Сертификат не найден» («Certificate not found»).

#### нарушена целостность СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003D, которому соответствует текстовое описание «Недостоверна подпись CRL издателя» («CRL damaged»).

#### Попытка шифрования ЭС с использованием закрытого ключа без функции шифрования.

Для проведения данного эксперимента для СКАД необходимо проинициализировать закрытый ключ, не имеющий функции шифрования, а для СКЗИ «Янтарь АСБР» необходимо подключиться к сессии криптосервера, рабочий ключ которой не имеет функции шифрования, и затем сделать попытку шифрования ЭС.

При этом данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700008, которому соответствует текстовое описание «Неправильное использование сертификата» («Wrong Certificate Usage»).

#### Попытка шифрования с использованием закрытого ключа, не соответствующего расширенной области применения ключа.

Для проведения данного эксперимента необходимо проинициализировать СКАД «Сигнатура» с использованием закрытого ключа (подключиться к сессии СКЗИ «Янтарь АСБР», в которую загружен закрытый ключ), который имеет расширенную область применения ключа, не совпадающую с требуемой, и затем попытаться выполнить шифрование сообщения.

При этом данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

В данной ситуации СКЗИ отрабатывает штатно, и проверка соответствия OID закрытого ключа требуемым значениям должна проводиться ППО.

#### Рекомендации по проведению экспериментов с расшифрованием

#### Попытка расшифрования ЭС в штатной ситуации.

Данный эксперимент необходимо проводить в момент времени, когда все необходимые для успешного шифрования объекты (сертификаты и СОС) находятся в штатном состоянии. В данном эксперименте СКЗИ возвращает код возврата 0, которому соответствует текстовое описание «ОК».

#### Попытка расшифрования ЭС при искажении подписанных данных.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

При этом необходимо предварительно внести искажения в зашифрованный текст в соответствии с рекомендациями раздела «Рекомендации по внесению изменений в зашифрованный текст», позволяющие получить следующие коды возврата СКЗИ (и соответствующие им текстовые описания):

1. Для простого формата зашифрованного текста:
   * E0700083, которому соответствует текстовое описание «Сообщение не зашифровано или формат сообщения искажен» («Message is not encrypted or damaged»).
2. Для зашифрованного текста в формате PKCS#7:
   * E0700027, которому соответствует текстовое описание «Ошибка выполнения расшифрования зашифрованного сообщения» («Error PKCS#7 decrypt»);
   * E0700083, которому соответствует текстовое описание «Сообщение не зашифровано или формат сообщения искажен» («Message is not encrypted or damaged»).

#### Попытка расшифрования ЭС с использованием сертификата открытого ключа отправителя для каждого из следующих условий:

Сертификат отправителя зашифрованного ЭС является несобственным по отношению к сертификату пользователя, поэтому для приведения сертификата отправителя в нештатное состояние надо использовать рекомендации, изложенные в разделе «Моделирование нештатных состояний сертификатов».

#### срок действия сертификата истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700036, которому соответствует текстовое описание «Сертификат истек» («Certificate expired»).

#### сертификат является отозванным

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700039, которому соответствует текстовое описание «Сертификат отозван» («Certificate revoked»).

#### сертификат отсутствует в справочнике сертификатов

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700025, которому соответствует текстовое описание «Не найден отправитель зашифрованного сообщения» («No decrypt sender cert found»).

#### сертификат имеет нарушенную целостность

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700037, которому соответствует текстовое описание «Сертификат поврежден» (Certificate damaged»).

#### Попытка расшифрования ЭС с участием СОС, необходимого для проверки сертификата отправителя и находящегося в нештатном состоянии

Рекомендации по приведению СОС в нештатное состояние описаны в разделе «Моделирование нештатных состояний СОС».

#### срок действия СОС истек

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003C, которому соответствует текстовое описание «СОС издателя недействителен по времени» («CRL expired»).

#### СОС отсутствует

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003B, которому соответствует текстовое описание «Отсутствует СОС издателя» («CRL missing»).

#### отсутствует сертификат, необходимый для проверки СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E0700035, которому соответствует текстовое описание «Сертификат не найден» («Certificate not found»).

#### нарушена целостность СОС

Корректной реакцией СКЗИ на условия данного эксперимента является код возврата E070003D, которому соответствует текстовое описание «Недостоверна подпись CRL издателя» («CRL damaged»).

#### Попытка расшифрования ЭС, зашифрованного с использованием закрытого ключа, не соответствующего открытому ключу получателя

Для проведения данного эксперимента необходимо выполнить попытку расшифрования ЭС с использованием открытого ключа, который отсутствует в списке получателей зашифрованного сообщения. При этом данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

Корректной реакцией СКЗИ на условия данного эксперимента для простого формата шифртекста является код возврата E0700028, которому соответствует текстовое описание «Ошибка выполнения расшифрования» («Decrypt error»).

Для формата шифртекста PKCS#7 корректной реакцией является код возврата E0700026 с соответствующим ему текстовым описание «Не найден сертификат получателя зашифрованного сообщения» («No decrypt recipient cert found»).

#### Попытка расшифрования ЭС, зашифрованного с использованием закрытого ключа, не соответствующего расширенной области применения ключа.

Для проведения данного эксперимента необходимо, чтобы в сертификате подписанта поле OID отличалось от требуемого.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта, а также все необходимые для его проверки сертификаты ЦС и СОС находятся в штатном состоянии.

При проведении данного эксперимента СКЗИ отрабатывает штатно, и проверка соответствия расширенной области применения закрытого ключа отправителя требуемым объектным идентификаторам должна проводиться средствами ППО.

1. **Рекомендации по моделированию нештатных ситуаций**

Настоящий раздел содержит рекомендации по моделированию нештатных ситуаций для базового перечня экспериментов.

#### Рекомендации по моделированию искажений в СОС и сертификатах

#### Моделирование искажений в сертификатах пользователей

Для моделирования искажений в сертификатах пользователей необходимо использовать НЕХ-редактор (для примера используется ХVI32), а также распечатанный сертификат или сохраненная в файл распечатка сертификата. Распечатать сертификат можно следующим образом: выбрать в справочнике сертификатов требуемый сертификат → в открывшемся окне выбрать вкладку «Состав» → «Распечатать». Для сохранения сертификата в файл: выбрать в справочнике сертификатов требуемый сертификат → в открывшемся окне выбрать вкладку «Состав» → «Сохранить в файл».

Далее необходимо открыть сохраненный файл (или взять распечатанный сертификат) и найти в нем поля «Серийный номер» (SerialNumber) и «КА» (Signature).

Запустить НЕХ-редактор и открыть в нем файл local.gdbm. Появится окно, представленное на Рисунок 1

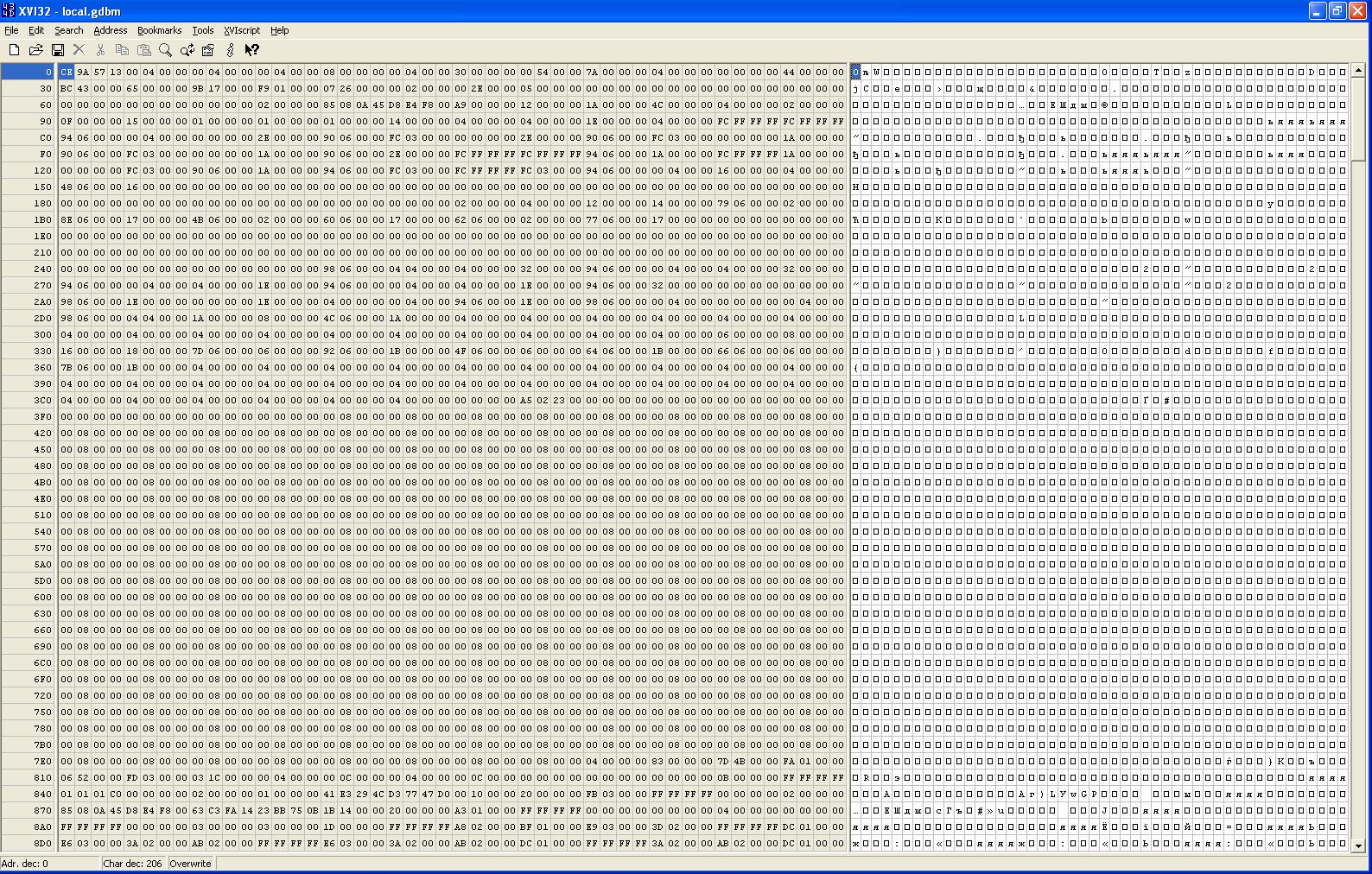


Рисунок 1

В левом окне отображается содержимое файла в шестнадцатеричном формате, в правом – как обычного текстового файла. Из пункта меню Search выбрать пункт Find. Откроется окно поиска (Рисунок 2), в которое нужно будет ввести номер ключа из сертификата в шестнадцатеричном формате (в данном примере достаточно ввести 10 шестнадцатеричных символов, чтобы в результате поиска был найден единственный номер).

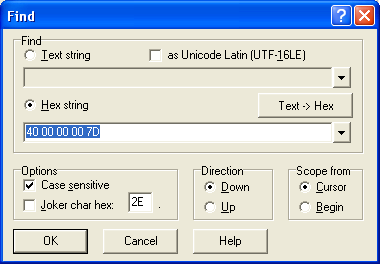


Рисунок 2

Будет найдена позиция в файле, с которой начинается номер сертификата. В левом нижнем углу программы отображается номер позиции в файле, на которой в настоящий момент находится курсор (в данном примере – номер позиции 4С5С) (Рисунок 3).

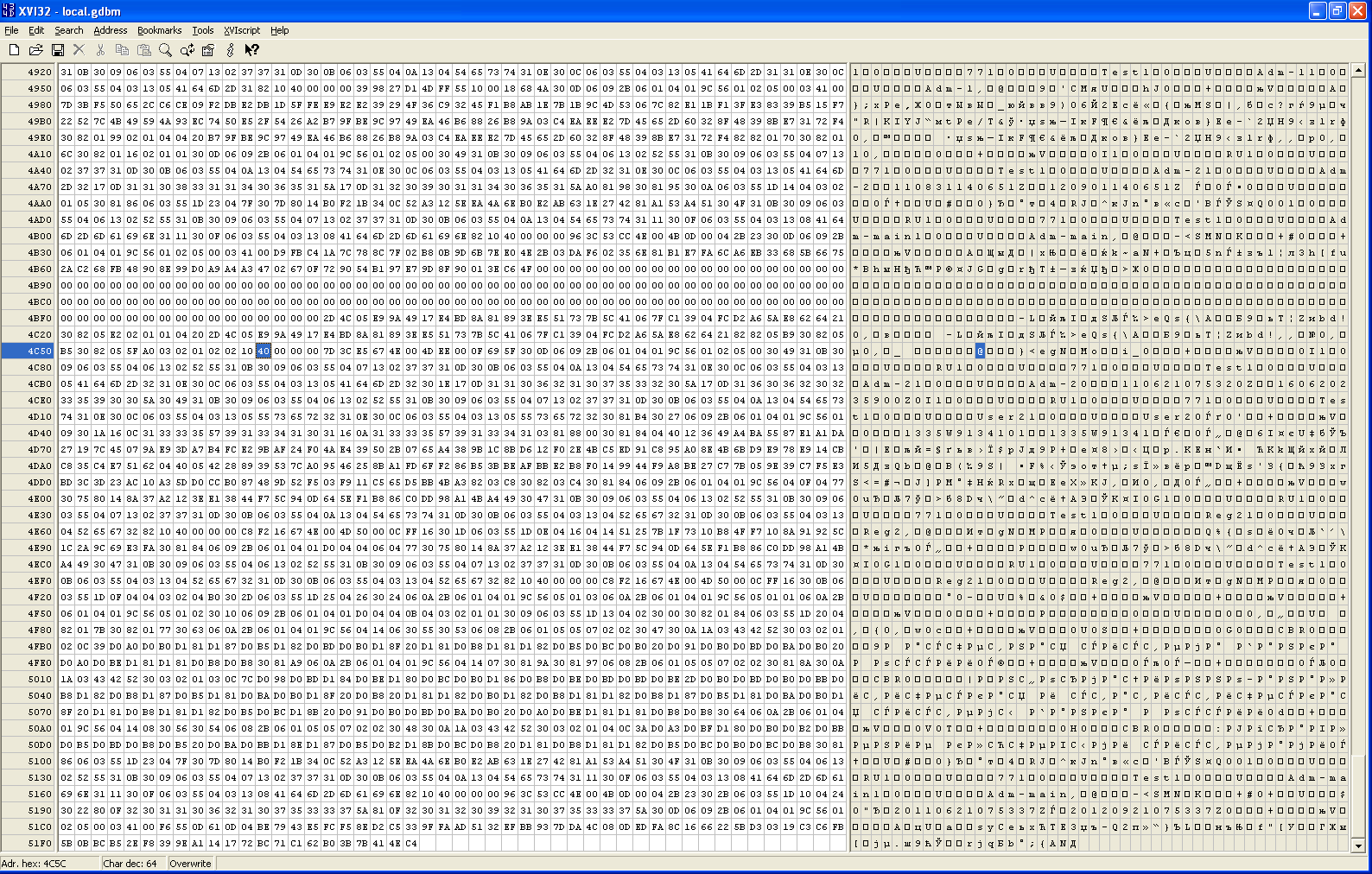


Рисунок 3

Затем аналогичным образом находятся последние байты поля «КА», значение которых известно из распечатки сертификата (Рисунок 4).

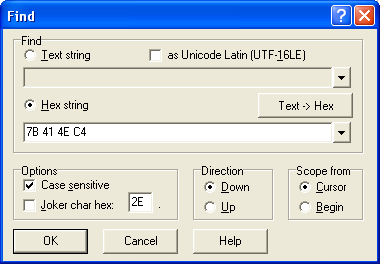


Рисунок 4

Будет найдена позиция в файле, с которой начинается введенная строка. В данном примере это 5202 (номер байта со значением 7B). Соответственно, последний байт подписи сертификата (содержащий C4), будет иметь номер 5205 (Рисунок 5).

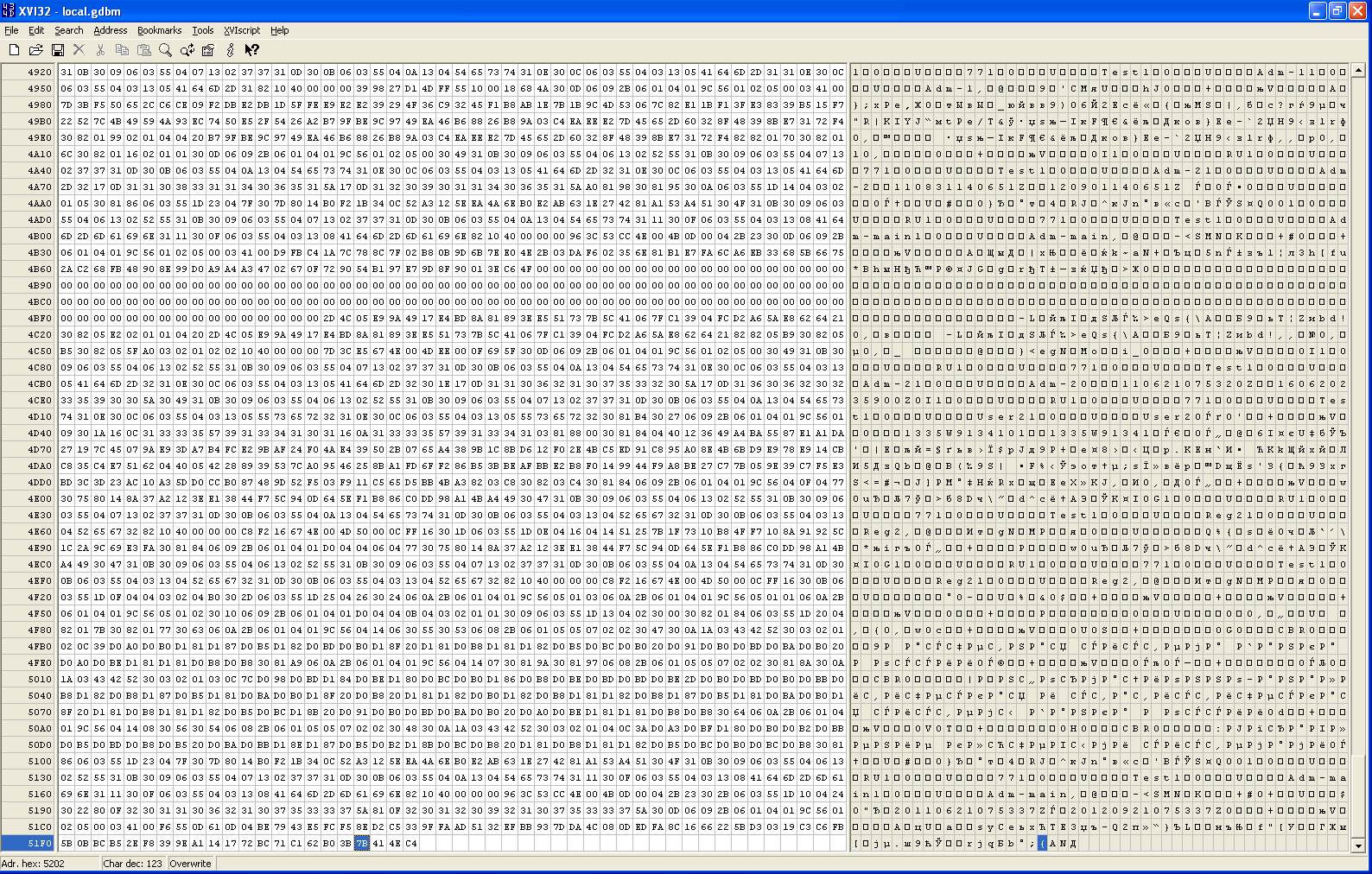


Рисунок 5

Таким образом, найдены одни из первых байтов искомого сертификата и одни из последних его байтов, то есть, найден промежуток local.gdbm, содержащий байты с номерами от 4C5C до 5205, гарантированно являющийся частью искомого сертификата (но не всем сертификатом). Для внесения искажений необходимо установить курсор на байт, который нужно исказить, затем ввести новое значение байта и сохранить изменения.

Однако, из-за особенностей DER-кодировки, в которой хранятся сертификаты в local.gdbm, искажение произвольного байта в этом промежутке не обязательно приведет к искажению какого-либо поля сертификата. Поэтому необходимо найти конкретные поля сертификата и вносить в них искажения.

Все шестнадцатеричные поля сертификата (которые указываются в формате XX:XX:XX:…:XX) могут быть найдены в указанном промежутке таким же образом, каким выполнялся поиск номера сертификата.

Для поиска текстовых полей (например, начало и конец времени действия сертификата) необходимо в окне поиска указать, что поиск ведется по тексту и ввести искомую строку (Рисунок 6).

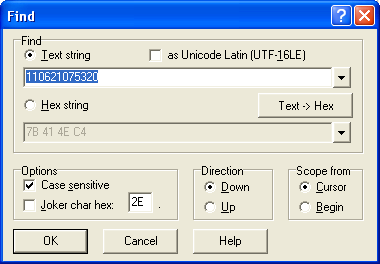


Рисунок 6

В случае поиска по времени необходимо вводить дату без пробелов в формате год-месяц-день-часы-минуты-секунды. При этом год вводить в формате двух цифр, а не четырех. В данном примере искомый сертификат действует с 21 июня 2011 года, 7 часов 53 минут 20 секунд. Поэтому в строку поиска нужно ввести 110621075320 (см. Рисунок 6).

#### Моделирование искажений в списках отозванных сертификатов

Моделирование искажений в СОС происходит аналогично моделированию искажений в сертификатах пользователей. В распечатке сертификата необходимо найти поля «Дата выпуска» (LastUpdate) (или «Следующий выпуск» (NextUpdate)) и «КА» и найти с помощью НЕХ-редактора часть списка отозванных сертификатов, в которую внести искажения.

#### Рекомендации по проведению экспериментов с искажением КА или подписанных данных

#### Внесение искажений в КА в простом формате и описание реакции СКЗИ на искажения

Для внесения искажений в КА в простом формате необходимо выбрать искажаемое поле (в соответствии с приведенной ниже таблицей), определить диапазон номеров байтов, в которых находится данное поле, и изменить его значение с помощью HEX-редактора.

Таблица 1. Описание простого формата КА для одного КА

|  |  |
| --- | --- |
| **Название поля** | **Размер поля в байтах** |
| Метка | 7 |
| КА | 64 |
| Идентификатор ключа подписанта | 12 |
| Время выполнения КА | 4 |
| Метка КА | 3 |
| Расширение | 3 |
| Количество подписей | 1 |
| Размер подписанных данных | 4 |

В случае наличия нескольких КА файл с КА будет иметь следующую структуру (для iКА):

Таблица 2. Описание простого формата КА для нескольких КА

|  |  |
| --- | --- |
| **Название поля** | **Размер поля в байтах** |
| Метка 1-го КА | 7 |
| КА\_1 | 64 |
| Идентификатор ключа подписанта КА\_1 | 12 |
| Время выполнения КА\_1 | 4 |
| Метка 2-го КА | 7 |
| КА\_2 | 64 |
| Идентификатор ключа подписанта КА\_2 | 12 |
| Время выполнения КА\_2 | 4 |
| … | … |
| Метка i-го КА | 7 |
| КА\_i | 64 |
| Идентификатор ключа подписанта КА\_i | 12 |
| Время выполнения КА\_i | 4 |
| Метка КА | 3 |
| Расширение | 3 |
| Количество подписей | 1 |
| Размер подписанных данных | 4 |

При описании реакции СКЗИ на искажения для одинарного (Таблица 3) и двойного КА (Таблица 4), необходимо отметить, что функция проверки подписи СКЗИ в случае возникновения нештатной ситуации, отвечающей коду возврата E0700019 (VCERT\_E\_VERIFY) дополнительно возвращает массив результатов проверки подписи, который содержит результаты проверки для каждого КА в отдельности.

Таблица 1. Описание реакции СКЗИ на искажения в случае одинарного КА

|  |  |  |
| --- | --- | --- |
| **Название поля** | **Код возврата СКЗИ** | **Результат проверки КА** |
| Метка | E0700019 | E0700042 |
| КА | E0700019 | E0700042 |
| Идентификатор ключа подписанта | E0700019 | E0700046 |
| Время выполнения КА | E0700019 | E0700042 |
| Метка КА | E070001A | - |
| Расширение | 0 | 0 |
| Количество подписей | E070001A | - |
| Размер подписанных данных | E070001A | - |
| Искажение подписанных данных без изменения размера | E0700019 | E0700042 |
| Искажение подписанных данных с изменением размера | E070001A**Ошибка! Закладка не определена.** | - |
| Искажение размера КА | E070001A | - |

Таблица 2. Описание реакции СКЗИ на искажения в случае двойного КА

|  |  |  |  |
| --- | --- | --- | --- |
| **Название поля** | **Код возврата СКЗИ** | **Результат проверки КА1** | **Результат проверки КА2** |
| Метка КА1 | E0700019 | E0700042 | 0 |
| КА1 | E0700019 | E0700042 | 0 |
| Идентификатор ключа подписанта КА1 | E0700019 | E0700046 | 0 |
| Время выполнения КА | E0700019 | E0700042 | 0 |
| Метка КА2 | E0700019 | 0 | E0700042 |
| КА2 | E0700019 | 0 | E0700042 |
| Идентификатор ключа подписанта КА2 | E0700019 | 0 | E0700046 |
| Время выполнения КА2 | E0700019 | 0 | E0700042 |
| Метка КА | E070001A | - | - |
| Расширение | 0 | 0 | 0 |
| Количество подписей | E070001A | - | - |
| Размер подписанных данных | E070001A | - | - |
| Искажение подписанных данных без изменения размера | E0700019 | E0700042 | E0700042 |
| Искажение подписанных данных с изменением размера | E070001A | - | - |
| Искажение размера КА | E070001A | - | - |

Приведенным в таблицах 3 и 4 кодам возврата соответствуют следующие текстовые описания:

- 0 – ОК;

- E0700019 – ошибка проверки КА;

- E070001A - сообщение не подписано или формат искажен;

- E0700042 – подпись недостоверна;

- E0700046 – сертификат не найден.

#### Внесение искажений в КА в простом формате, закодированном в base64

Во многих системах Банка России используется формат сообщений УФЭБС, в котором КА кодируются с помощью кодировки base64. Для подготовки тестовых сообщений при проведении экспериментов с искажениями, в настоящем разделе указаны номера символов, искажение которых приводит к гарантированному искажению конкретного поля раскодированного КА в простом формате.

Одинарный КА в простом формате имеет размер 98 байт, соответственно, в кодировке base64 данный КА имеет размер в 132 символа.

Таблица 3. Соответствие полей одинарного КА в простом формате номерам символов в кодировке base64

|  |  |  |
| --- | --- | --- |
| **Название поля** | **Размер поля в байтах** | **Диапазон номеров символов в кодировке base64** |
| Метка | 7 | 1-9 |
| КА | 64 | 11- 94 |
| Идентификатор ключа подписанта | 12 | 96 - 110 |
| Время выполнения КА | 4 | 112 - 116 |
| Метка КА | 3 | 117-120 |
| Расширение | 3 | 121-124 |
| Количество подписей | 1 | 125 |
| Размер подписанных данных | 4 | 127-130 |

Примечание. Символы 10, 95, 111, 126 и 131 пропущены, так как их произвольное искажение не гарантирует искажение конкретных полей КА в простом формате. Это связано с тем, что исходные данные кодируются в base64 группами по 3 байта, причем каждая группа в base64 представляется 4-мя символами.

#### Внесение искажение в КА в формате PKCS#7

СКАД «Сигнатура» и СКЗИ «Янтарь АСБР» поддерживают возможность формирования КА в формате PKCS#7, описанном в RFC 2315. В общем случае, для внесения целенаправленных искажений в КА в формате PKCS#7 понадобится утилита dumpasn1.exe, так как КА в формате PKCS#7 представляется в кодировке ASN.1, а также необходим HEX-редактор для внесения искажений. При этом сам алгоритм внесения искажений следующий:

* 1. раскодировать КА, используя утилиту dumpasn1.exe;
  2. выбрать поле, подлежащее искажению (например, дата формирования КА, серийный номер сертификата подписанта, хэш-значение подписанных данных, подписанные данные (в случае присоединенного КА) и т.п.);
  3. открыть файл с КА в HEX-редакторе и найти выбранное на предыдущем шаге поле по значению;
  4. внести искажение в выбранное поле.

#### Внесение искажений в КА в формате PKCS#7, закодированном в base64

Особенностью КА в формате PKCS#7 является то, что длина КА не является фиксированной. Поэтому невозможно заранее сказать, какие конкретно номера символов будут соответствовать различным полям КА (в том числе, полю «messageDigest»).

Однако, код возврата E070001A можно получить, исказив длину контейнера с КА в формате PKCS#7. Это можно сделать, внеся изменения в третий или четвертый байт файла, содержащего КА, то есть изменив четвертый или пятый символ в КА в кодировке base64.

При этом единственно возможным надежным способом получения остальных кодов возврата является раскодирование КА из base64, внесение искажений в КА и его последующее обратное кодирование в base64.

#### Рекомендации по внесению искажений в зашифрованный текст

#### Внесение искажение в зашифрованный текст в простом формате

Описание простого формата криптоконтейнера СКАД «Сигнатура» и СКЗИ «Янтарь АСБР» приведено в таблице 6.

Таблица 6. Описание формата криптоконтейнера СКЗИ

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Название поля** | **Размер поля в байтах** | |
| **1** | Зашифрованные данные | **—** | |
| Структура заголовка | | | |
| **2** | Признак зашифрованного блока памяти на асимметричных ключах "s" | **1** | **31** |
| **3** | Серия ключа отправителя. Например, "GNFSDR" | **6** |
| **4** | Размер зашифрованных данных в байтах | **4** |
| **5** | Имитовставка зашифрованных данных | **4** |
| **6** | Синхропосылка зашифрованных данных | **8** |
| **7** | Дополнительная синхропосылка № 2 | **8** |
| Повторяющаяся структура зашифрованного ключа получателя, когда серия отправителя совпадает с серией получателя | | | |
| **8** | Номер ключа получателя. Например, "0002" | **4** | **48** |
| **9** | Дополнительная синхропосылка №1 | **8** |
| **10** | Зашифрованный ключ получателя | **32** |
| **11** | Имитовставка зашифрованного ключа получателя | **4** |
| Повторяющаяся структура зашифрованного ключа получателя, когда серия отправителя НЕ совпадает с серией получателя | | | |
| **12** | Номер ключа получателя в числовом виде. С переставленными байтами и маской 0x80 в первом байте. Например, 0x80:0x02 | **2** | **48** |
| **13** | Серия ключа получателя. Например, "VLYFGN" | **6** |
| **14** | Дополнительная синхропосылка №1 | **4** |
| **15** | Зашифрованный ключ получателя | **32** |
| **16** | Имитовставка зашифрованного ключа получателя | **4** |
| Завершающая структура данных | | | |
| **17** | Номер ключа отправителя. Например, "0001" | **4** | **6** |
| **18** | Количество получателей | **2** |

В СКАД «Сигнатура» идентификатор ключа шифрования имеет длину в 10 символов. Термину «номер ключа» соответствуют первые четыре символа, а термину «серия ключа» - последние 6 символов.

Рассмотрим теперь реакцию СКЗИ на всевозможные искажения полей криптоконтейнера (считаем, что расшифрование выполняет пользователь, серию ключа которого не совпадает с серией ключа отправителя и шифрование происходило в один адрес).

Таблица 7. Описание кодов возврата СКЗИ при искажении криптоконтейнера

|  |  |  |
| --- | --- | --- |
| **№** | **Название поля** | **Код возврата СКЗИ** |
| **1** | Зашифрованные данные (без изменения размера) | **E0700028** |
| **2** | Признак зашифрованного блока памяти на асимметричных ключах "s" | **E0700083** |
| **3** | Серия ключа отправителя. Например, "GNFSDR" | **E0700025** |
| **4** | Размер зашифрованных данных в байтах | **E0700083** |
| **5** | Имитовставка зашифрованных данных | **E0700028** |
| **6** | Синхропосылка зашифрованных данных | **E0700028** |
| **7** | Дополнительная синхропосылка № 2 | **E0700028** |
| **8** | Номер ключа получателя. Например, "0002" | **0** |
| **9** | Дополнительная синхропосылка №1 |
| **10** | Зашифрованный ключ получателя |
| **11** | Имитовставка зашифрованного ключа получателя |
| **12** | Номер ключа получателя в числовом виде. С переставленными байтами и маской 0x80 в первом байте. Например, 0x80:0x02 | **E0700028** |
| **13** | Серия ключа получателя. Например, "VLYFGN" | **E0700028** |
| **14** | Дополнительная синхропосылка №1 | **E0700028** |
| **15** | Зашифрованный ключ получателя | **E0700028** |
| **16** | Имитовставка зашифрованного ключа получателя | **E0700028** |
| Завершающая структура данных | | |
| **17** | Номер ключа отправителя. Например, "0001" | **E0700025** |
| **18** | Количество получателей | **E0700083** |

Приведенным в таблице 7 кодам возврата СКЗИ соответствуют следующие текстовые описания:

1. 0 – ОК;
2. E0700025 – не найден отправитель зашифрованного сообщения;
3. E0700028 – ошибка выполнения расшифрования;
4. E0700083 - сообщение не зашифровано или формат сообщения искажен.

Первый код возврата можно получить при расшифровании в штатной ситуации, а второй – в ситуации, когда сертификат отправителя сообщения не найден в справочнике сертификатов получателя. Поэтому остается смоделировать только два кода возврата СКЗИ - E0700028 и E0700083, получить которые возможно, исказив зашифрованные данные без изменения размера криптоконтейнера и с изменением размера соответственно.

#### Внесение искажение в зашифрованный текст в простом формате, закодированный в base64

Из таблицы 6 следует, что для внесения искажений в конкретные поля файла-криптоконтейнера (за исключением зашифрованных данных) в формате base64 с целью получить определённый код возврата необходимо выполнить конвертацию данных криптоконтейнера в стандартное представление, произвести искажение данных в этом виде, а затем выполнить обратную конвертацию. Это связано с тем, что первое поле криптоконтейнера, содержащее зашифрованные данные, не имеет фиксированного размера. Поэтому указать номера символов, требующих искажения для получения того или иного результата, не представляется возможным.

В то же время, необходимые коды возврата E0700028 и E0700083 можно получить, искажая только зашифрованные данные.

Внести искажения в зашифрованный текст без размера криптоконтейнера можно, исказив лишь первый символ криптоконтейнера в кодировке base64.

Для внесения искажений в зашифрованный текст с изменением размера криптоконтейнера необходимо удалить (или добавить) из криптоконтейнера 4 символа в кодировке base64, поскольку это минимальное число символов в base64, раскодируемое в целое число байт.

#### Внесение искажение в зашифрованный текст в формате PKCS#7

Общий алгоритм внесения искажений в зашифрованный текст в формате PKCS#7 полностью повторяет алгоритм внесения искажений в КА в формате PKCS#7. На примере будет показано, как можно получить наиболее вероятные коды возврата - E0700083, E0700025, E0700026 и E0700027.

Кодам возврата E0700026 и E0700027 соответствуют следующие текстовые описания:

1. E0700026 – не найден сертификат получателя зашифрованного сообщения («No decrypt recipient cert found»);
2. E0700027–ошибка выполнения расшифрования зашифрованного сообщения («Error PKCS#7 decrypt»).

Код возврата E0700083 можно получить, исказив длину контейнера с зашифрованными данными в формате PKCS#7. То есть, как для получения кода возврата E070001A в операции проверки КА, необходимо исказить третий или четвертый байты файла с зашифрованными данными.

Коду возврата E0700025 соответствует также нештатная ситуация «попытка расшифрования сообщения в случае, когда сертификат отправителя отсутствует в справочнике сертификатов получателя».

Код возврата E0700026 соответствует нештатной ситуации «попытка расшифрования ЭС, зашифрованного с использованием закрытого ключа, не соответствующего открытому ключу получателя».

Для получения кода возврата E0700027, необходимо с помощью утилиты dumpasn1.exe раскодировать зашифрованные данные, и найти в раскодированном файле начало блока, содержащего непосредственно шифртекст (Рисунок 7).

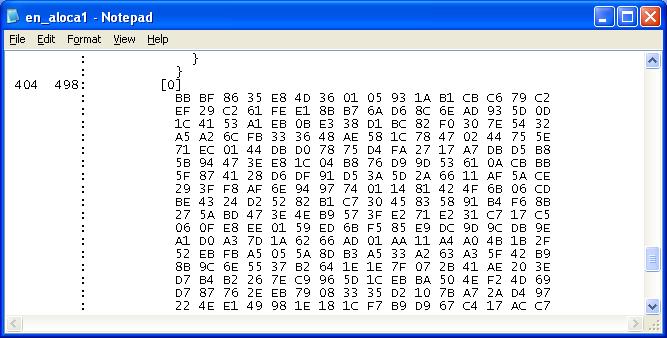


Рисунок 7

Далее необходимо с помощью НЕХ-редактора выполнить поиск в исходном файле с зашифрованными данными по первым байтам шифртекста (Рисунок 8).



Рисунок 8

Курсор в этом случае будет установлен на первый байт шифртекста (Рисунок 9), который и необходимо исказить для получения кода возврата E0700027.

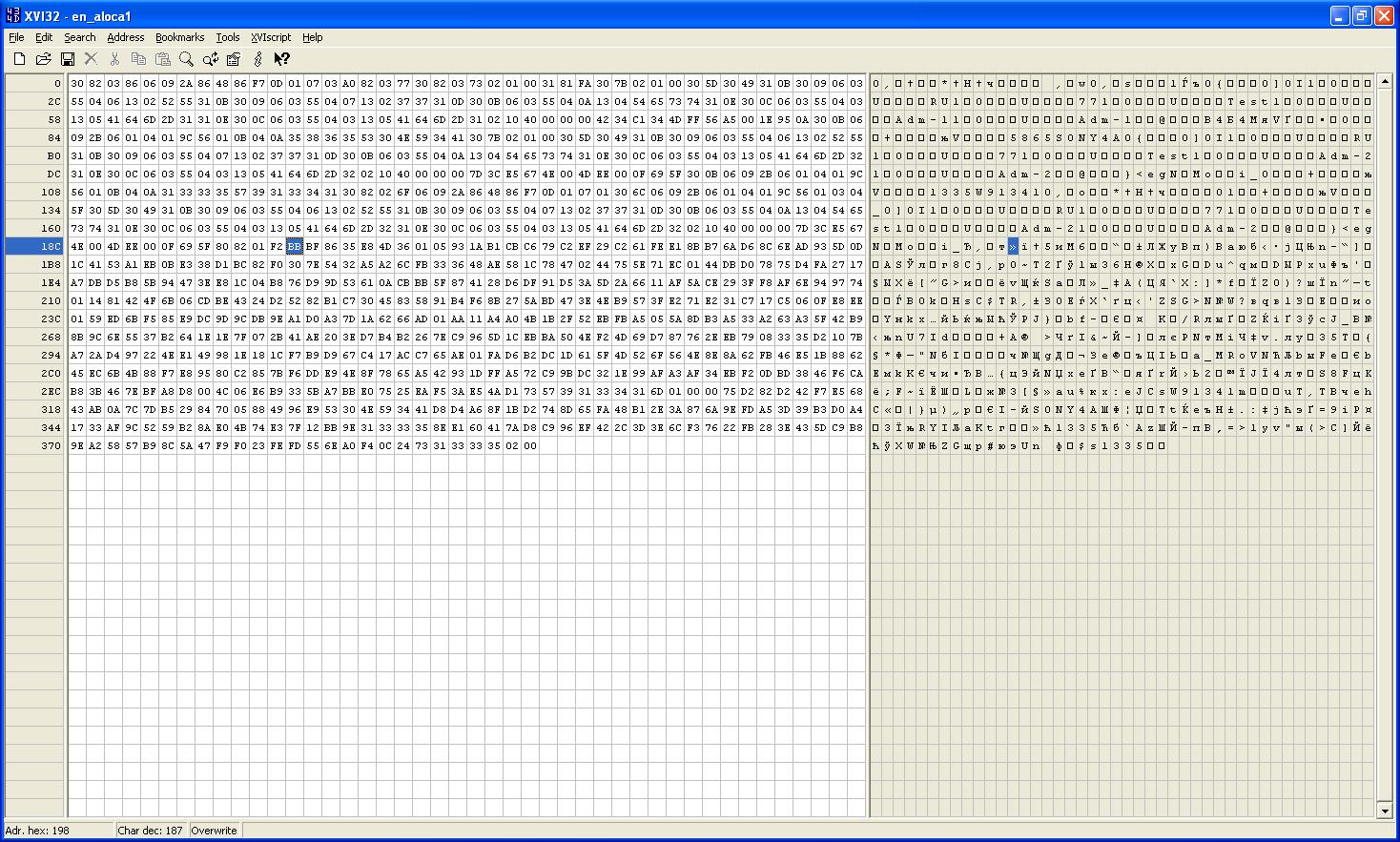


Рисунок 9

#### Внесение искажение в зашифрованный текст в формате PKCS#7, закодированный в base64

В общем случае размер зашифрованных данных в формате PKCS#7 не является фиксированным. Поэтому невозможно заранее сказать, какие конкретно номера символов будут соответствовать различным полям шифртекста.

Однако, код возврата E0700083 можно получить, исказив длину контейнера с зашифрованными данными в формате PKCS#7. Это можно сделать, внеся изменения в третий или четвертый байт файла, содержащего зашифрованные данные, то есть, изменив четвертый или пятый символ в КА в кодировке base64.

При этом единственно возможным надежным способом получения остальных кодов возврата является раскодирование шифртекста из base64, внесение искажений в шифртекст и его последующее обратное кодирование в base64.

#### Моделирование нештатных состояний сертификатов

В настоящем разделе изложены рекомендации по моделированию нештатных ситуаций с несобственными сертификатом при проверке КА и шифровании/расшифровании.

Существует четыре нештатные ситуации, связанные с состоянием несобственного сертификата.

#### срок действия несобственного сертификата истек.

Данный эксперимент проводится путем изменения времени на такой момент времени, в который:

* 1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
  2. Истек сертификат подписанта, причем все необходимые для проверки сертификата подписанта сертификаты ЦС и СОС находятся в штатном состоянии.

#### несобственный сертификат является отозванным.

Моделирование отзыва сертификата осуществляется штатными средствами программ «Центр сертификации», «Центр регистрации» и «Справочник сертификатов». С помощью указанных программ, в соответствии с руководством пользователя, выполняется следующая последовательность действий: Центр Регистрации (ЦР) направляет в ЦС запрос на отзыв выбранного сертификата, ЦС на основе данного запроса издает новый СОС, ЦР помещает данный СОС в сетевой справочник или передает абоненту (программе «Справочник сертификатов»). Средствами программы «Справочник сертификатов» СОС с отозванным сертификатом помещается в локальный справочник.

Данный эксперимент нужно проводить в такой момент времени, в который:

* 1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
  2. Все необходимые для проверки сертификата подписанта сертификаты ЦС и СОС находятся в штатном состоянии.

#### сертификат отсутствует в справочнике сертификатов;

Для проведения данного эксперимента необходимо удалить несобственный сертификат из справочника сертификатов пользователя. Удаление сертификата из локального справочника возможно средствами программы «Справочник сертификатов», работающей в режиме Администратора (режим по умолчанию). Для этого средствами графического интерфейса данной программы выделяется сертификат, подлежащий удалению, и нажимается клавиша DEL

Данный эксперимент нужно проводить в такой момент времени, в который действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя.

#### сертификат имеет нарушенную целостность.

Для проведения данного эксперимента необходимо исказить несобственный сертификат в справочнике сертификатов пользователя. Для искажения сертификата, необходимо исказить поле КА сертификата подписанта, так как искажение других полей сертификата может привести к реакции СКЗИ на нарушение целостности сертификата, соответствующей другим нештатным ситуациям.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. Действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. Сертификат подписанта действителен по времени, а все необходимые для проверки сертификата подписанта сертификаты ЦС и СОС находятся в штатном состоянии.

#### Моделирование нештатных состояний СОС

Эксперименты с участием СОС для операций проверки КА и шифрования/расшифрования проводятся только в иерархической системе управления сертификатами. Это требование обусловлено тем, что если при проведении экспериментов с СОС не использовать иерархическую систему управления сертификатами, то в проверке цепочки сертификатов для рабочего сертификата пользователя и для любого несобственного сертификата будут участвовать одни и те же СОС. При условии использования иерархической ключевой системы эксперименты с участием СОС для операций проверки КА и шифрования/расшифрования возможно провести при условии, что несобственный сертификат пользователя, необходимый для выполнения криптографической операции, будет находиться в другой ветке иерархической системы управления сертификатами по отношению к рабочему сертификату пользователя.

#### Рекомендации по моделированию нештатных состояний СОС

В настоящем разделе изложены рекомендации по моделированию нештатных ситуаций с СОС при проверке КА и шифровании/расшифровании.

Существует 4 нештатные ситуации, связанные со списками отозванных сертификатов:

#### срок действия СОС истек;

Данная нештатная ситуация моделируется переводом времени на такой момент времени, в который:

1. действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. сертификат подписанта действителен по времени, также все необходимые для проверки сертификата подписанта сертификаты ЦС находятся в штатном состоянии, и хотя бы один из СОС, выпущенных подчиненными ЦС, истек по времени.

#### СОС отсутствует;

Для проведения данного эксперимента необходимо удалить из справочника сертификатов пользователя хотя бы один СОС, участвующих в проверке сертификата подписанта и не участвующих при этом в проверке рабочего сертификата пользователя. Удаление СОС из локального справочника возможно средствами программы «Справочник сертификатов», работающей в режиме Администратора. Для этого средствами графического интерфейса данной программы выделяется СОС, подлежащий удалению, и нажимается клавиша DEL.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. сертификат подписанта действителен по времени, также все необходимые для проверки сертификата подписанта сертификаты ЦС и оставшиеся СОС находятся в штатном состоянии.

#### отсутствует сертификат, необходимый для проверки СОС

Для проведения данного эксперимента необходимо удалить из справочника сертификатов получателя хотя бы один сертификат ЦС, участвующий в проверке сертификата подписанта и не участвующий при этом в проверке рабочего сертификата пользователя. Удаление сертификата из локального справочника возможно средствами программы «Справочник сертификатов», работающей в режиме Администратора. Для этого средствами графического интерфейса данной программы выделяется сертификат, подлежащий удалению, и нажимается клавиша DEL.

Данный эксперимент нужно проводить в такой момент времени, в который:

1. действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. сертификат подписанта действителен по времени, также все необходимые для проверки сертификата подписанта СОС и оставшиеся сертификаты ЦС находятся в штатном состоянии.

#### нарушена целостность СОС.

Для проведения данного эксперимента необходимо исказить в справочнике сертификатов получателя хотя бы один из СОС, участвующих в проверке сертификата подписанта и не участвующих при этом в проверке рабочего сертификата пользователя. Для внесения искажений необходимо использовать описанную в разделе «Рекомендации по моделированию нештатных состояний СОС» методику, причем необходимо искажать поле КА СОС. При этом необходимо учитывать, что искажение других полей СОС может привести к реакции СКЗИ на нарушение целостности СОС, которая соответствующей другим нештатным ситуациям. Искажение же поля КА позволяет получить код возврата, в точности отвечающий нештатной ситуации «нарушении целостности СОС».

Данный эксперимент нужно проводить в такой момент времени, в который:

1. действителен закрытый ключ пользователя и все сертификаты ЦС и СОС, участвующие в проверке рабочего сертификата пользователя;
2. сертификат подписанта действителен по времени, также все необходимые для проверки сертификата подписанта сертификаты ЦС и оставшиеся СОС находятся в штатном состоянии.