Интеграция с доверенной третьей стороной иностранного государства

Оглавление

1 Введение

Настоящий документ содержит описание процесса взаимодействия при интеграции с Доверенной третьей стороной Республики Казахстан и Доверенной третьей стороной иностранного государства.

2 Определения и сокращения

В настоящем документе используются следующие основные понятия:

Сертификат – документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи установленным требованиям.

Список отозванных сертификатов (далее – СОС) – часть регистра сертификатов, содержащая сведения о сертификатах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования).

Удостоверяющий центр (далее – УЦ) – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность сертификата.

Доверенная третья сторона Республики Казахстан (далее – ДТС РК) – государственная техническая служба, осуществляющая подтверждение подлинности иностранной электронной цифровой подписи с использованием Программного комплекса «Доверенная третья сторона».

Протоколы сервера подтверждения и сертификации данных X.509 инфраструктуры открытых ключей в сети Интернет (Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, далее – RFC 3029) – протокол, на основе которого ДТС РК предоставляет услуги по подтверждению подлинности электронной цифровой подписи.

Доверенная третья сторона иностранного государства (далее – ДТС ИГ) – организация, наделенная в соответствии с законодательством иностранного государства правом осуществлять деятельность в автоматизированном режиме по проверке электронной цифровой подписи в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ.

Электронная цифровая подпись (далее – ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.

Квитанция проверки иностранной электронной цифровой подписи по RFC 3029 (далее – Квитанция) – электронный документ, удостоверенный ЭЦП ДТС РК и подтверждающий подлинность иностранной ЭЦП;

Сервис подтверждения подлинности документов, подписанных электронной цифровой подписью (Validation of Digitally Signed Document, далее – VSD) – сервис, осуществляющий проверку подлинности ЭЦП.

Средства криптографической защиты информации (далее – СКЗИ) – средства криптографической защиты информации – совокупность программно-технических средств, реализующих алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами и обеспечивающих применение электронной цифровой подписи и шифрования в информационных системах. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

SDK (software development kit) – комплект средств разработки, позволяющий создавать приложения для работы с VSD.

VSD–запрос – запрос сформированный к VSD согласно RFC-3029.

3 Схемы взаимодействия

Существует два вида схем взаимодействия ДТС РК и ДТС ИГ:

- Односторонняя схема взаимодействия;
- Двухсторонняя схема взаимодействия.

3.1 Односторонняя схема взаимодействия

Регламент взаимодействия сторон при односторонней схеме взаимодействия:

1. При необходимости, ДТС РК предоставляет ДТС ИГ SDK для формирования VSD-запроса согласно RFC-3029;
2. ДТС ИГ предоставляет ДТС РК свой сертификат, сертификаты УЦ (выпустившие сертификаты для службы и для подписи квитанций) и ссылки на СОС.
3. ДТС РК предоставляет ДТС ИГ свой сертификат, сертификат УЦ и ссылку на СОС;
4. ДТС ИГ предоставляет ДТС РК свой СЗКИ;
5. Если взаимодействие идет по протоколу https, ДТС ИГ и ДТС РК обмениваются ssl сертификатами.
6. ДТС РК предоставляет ДТС ИГ свой URL и необходимые политики (если имеются) для указания в VSD.
7. ДТС ИГ формирует VSD-запросы.
8. ДТС ИГ подписывает VSD-запрос (см. п.р. 3.3.2):
9. ДТС ИГ отправляет подписанные VSD-запросы ДТС РК, получает от него ответы и анализирует их.

3.2 Двухсторонняя схема взаимодействия

Регламент взаимодействия сторон при двухсторонней схеме взаимодействия:

1. ДТС РК и ДТС ИГ (далее – стороны) предоставляют SDK для формирования VSD-запросов.
2. Стороны обмениваются:
    a. Сертификатами;
    b. Сертификатами УЦ, выпустившими сертификаты;

c. Сертификатами УЦ, выпустившими сертификаты для подписи квитанций.

d. Сертификатами, которые будут посылать запросы;

e. Ссылками для скачивания COC для УЦ (перечисленных выше);

f. Ссылками на свой URL;

g. Сертификатами ssl, если взаимодействие происходит на основе https.

3. Стороны настраивают необходимые политики (добавление сертификатов в доверенные, настройка url для перенаправления запросов).

4. Стороны обмениваются валидной отсоединенной подписью в формате PKCS#7;

5. Стороны формируют VSD-запросы со вложенными квитанциями из пункта выше.

6. Стороны подписывают VSD-запросы (см. п.р. 3.3.2)

7. Стороны отправляют подписанные VSD-запросы, получают ответы и анализируют их.

3.3 Дополнительно

3.3.1 Если ДТС РК получает VSD-запрос, содержащий отсоединенную подпись, т.е. проверяемый электронный документ не включен в запрос к ДТС РК, тогда проверка подписи осуществляется не на основе содержимого электронного документа, а на основе хеша из вложенной квитанции на содержимое электронного документа. В этом случае, валидность подписи рекомендуется проверять на основе следующих проверок:

1) ответа от ДТС РК;

2) соответствия хеша, указанного в ответе от ДТС РК, хешу, подсчитанному на полученный электронный документ.

3.3.2 Формат подписанного VSD-запроса – присоединенная подпись pkcs#7 с подписанными атрибутами (signed attributes), в которой подписанными данными является VSD-запрос, подпись ставится ключами ИС.

3.3.3 В дополнение к RFC 3029, ДТС РК поддерживает следующий тип DVCSRequest:data:

```
DVCSRequest:data ::= CHOICE {
message OCTET_STRING,
messageImprint DigestInfo,
cers [0] IMPLICIT SEQ_OF_TargetEtcChain,
messageInfo [1] IMPLICIT MessageInfo
}
MessageInfo ::= SEQUENCE {
message OCTET_STRING,
externalData DigestInfos
}
```

3.3.4 ДТС РК использует следующие статусы ответов для DVCSResponse:

```
PKIStatus ::= INTEGER {
granted (0),
-- you got exactly what you asked for
rejection (2),
-- you don't get it, more information elsewhere in the message
}
```

3.3.5 CMS (Cryptographic Message Syntax) или PKCS#7 является криптографическим стандартом (RFC5652) представления криптографических данных в формате ASN.1. В стандарте описывается шесть типов данных: data, signedData, envelopedData, signedAndEnvelopedData, digestedData, и encryptedData.

Стандарт CMS описывает структуру криптографических сообщений, включающих в себя защищенные данные вместе со сведениями, необходимыми для их корректного открытия или использования. Например, в сообщении размещаются защищенные данные, информация об алгоритме хеширования и подписи, времени подписи,

сертификате открытого ключа, цепочке сертификации и т.д. Некоторые из указанных атрибутов носят опциональный характер, но приложение может само определить необходимость их наличия. У каждого алгоритма есть набор параметров, который должен быть согласован на обеих сторонах: для ГОСТ 34.10-2012, помимо открытого ключа, это модуль p, коэффициенты эллиптической кривой a и b и порядок циклической подгруппы точек эллиптической кривой q.