ОФИЦИАЛЬНЫЙ САЙТ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» ДЛЯ РАЗМЕЩЕНИЯ ИНФОРМАЦИИ О РАЗМЕЩЕНИИ ЗАКАЗОВ НА ПОСТАВКИ ТОВАРОВ, ВЫПОЛНЕНИЕ РАБОТ, ОКАЗАНИЕ УСЛУГ (WWW.ZAKUPKI.GOV.RU)

Общая схема настройки двухсторонней аутентификации с Подсистемой интеграции (начиная с версии 3.4) между смежной системой размещения сведений о закупках товаров, работ, услуг в соответствии с положениями Федерального закона от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и внешними системами

На 6 листах

АННОТАЦИЯ

Данный документ содержит общую схему настройки двухсторонней аутентификации с Подсистемой интеграции между смежной системой размещения сведений о закупках товаров, работ, услуг в соответствии с положениями Федерального закона от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и внешними системами.

СОДЕРЖАНИЕ

1 СХЕМА ДВУХСТРОННЕЙ АУТЕНТИФИКАЦИИ

1.1 Общая информация

Передача информации осуществляется по защищенным телекоммуникационным каналам связи по специализированному адресу (https:// int223.zakupki.gov.ru/223/integration/integration/upload) по протоколу HTTPS. При этом используется криптографический протокол TLS. Соединение устанавливается по протоколу TLS в режиме двухсторонней аутентификации с дополнительной проверкой сертификата электронной подписи (далее ЭП).

Для обеспечения двухсторонней аутентификации с применением электронной подписи необходимо:

- Внешней системе размещения закупок (далее ВСРЗ) получить сертификаты электронной подписи в удостоверяющих центрах, аккредитованных согласно требованиям Федерального закона № 63-ФЗ. Полученные сертификаты должны использоваться ВСРЗ для подписания пакетов данных, передаваемых в Смежную систему размещения сведений 223-ФЗ;
- ВСРЗ обеспечить своих заказчиков файлами, содержащими открытый ключ электронной подписи, используемой для интеграции со Смежной системой размещения сведений 223-ФЗ.

В Смежную систему размещения сведений в рамках Закона 223-ФЗ информация передается с использованием метода POST (<Content-Type: multipart/form-data>), используя следующие параметры:

- login - имя пользователя, осуществляющего загрузку сведений;
- password – пароль пользователя, осуществляющего загрузку сведений;
- document (тип – файл, обязательный) – передаваемый XML-документ.

(см. ТФФ v 1.5)

Примечание: исключить из POST-запроса параметр “signature”.

1.2 Схема работы сервера на стороне ООС

1. Клиент делает hello-запрос на сервер.
2. Сервер отвечает на запрос, шлет сертификат, удостоверяющий подлинность сервера.

3. Сервер запрашивает у клиента его сертификат, пересылая ему список принимаемых им удостоверяющих центров.
4. Клиент находит среди сертификатов такой, который был выдан одним из удостоверяющих центров, принимаемых сервером, и передает его.
5. Сервер проверяет соответствие полученного сертификата и сертификата удостоверяющего центра, и в случае успеха, аутентификация успешна.

Далее после успешной установки соединения, на уровне приложения интеграции должна выполнятся проверка на валидность и неотозванность сертификата по сервису Информационной системы головного удостоверяющего центра.

В случае успешной проверки, в рамках установленного соединения, производится передача сведений, с использование логина и пароля пользователя, указанные в его личном кабинете (ЛК).

1.3 Проверки, выполняемые на сервере

1. Проверка сертификата на соответствие требованиям ГОСТ Р 34.10-2001.
2. Проверка на доверие к сертификату электронной подписи. Для этого у сертификата проверяется вся цепочка корневых сертификатов удостоверяющих центров, выдавших данный сертификат. Проверка считается пройденной, если все корневые сертификаты находятся в перечне доверительных корневых сертификатов Смежной системы размещения сведений 223-ФЗ и срок их действия не истек.
3. Проверка сертификата электронной подписи на валидность и неотозванность. Проверка включает в себя проверку сертификата в ИС ГУЦ.

После успешных проверок осуществляется проверка на право загрузки сведений, переданных от ВСРЗ, в ЛК организации, зарегистрированной в Смежной системе размещения сведений 223-ФЗ.

1.4 Документы и полезные ссылки

О том как запрашивается сертификат информация представлена в документе "Спецификация TLS 1.0" http://tools.ietf.org/html/rfc2246, пункт 7.4.4. Certificate request.

Информация по настройке двухсторонней аутентификации - https://www.simple-talk.com/dotnet/.net-framework/tlsssl-and-.net-framework-4.0/

Сертификат должен соответствовать ГОСТ Р 34.10-2001.

Состав полей определяется законом № 63-ФЗ и описывается документами:

http://zakupki.gov.ru/223/ppa/public/information/forCustomersAndSuppliers.html?rubricId=101 - (Федеральный закон от 06_04_2011 № 63-ФЗ);

http://zakupki.gov.ru/223/ppa/public/information/forCustomersAndSuppliers.html?rubricId=50 - (Приказ ФСБ РФ от 27_12_2011 № 795);

http://zakupki.gov.ru/223/ppa/public/information/forCustomersAndSuppliers.html?rubricId=100 - (Методические рекомендации к составу СКП ЭП).