**ИНТЕГРАЦИЯ JBOSS 6.1.0 Final (“Neo”) и JTLS 2.0**

**Предустановленные компоненты:**

1. *OS*: Windows 7 (x64)
2. *JBoss*: версия 6.1.0 Final от 2011-08-16, <http://jbossas.jboss.org/downloads> для ***localhost***
3. *Java*: JDK 1.6.0\_43
4. *Провайдеры*: JCP и JTLS версии 2.0, установленные в JDK
5. *Сняты ограничения для JCP*: <https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/44/6/snjatie-ehksportnykh-ogrnichenijj>
6. *Ключи сервера*: хранилище сертификатов *keystore* формата *CertStore* и ключевой контейнер *jboss* с сертификатом для аутентификации сервера формата *HDImageStore*. Пароли хранилища и серверного контейнера совпадают.
7. *Клиент (браузер) для проверки подключения к серверу*: браузер IE с установленным CSP 4.0. При требовании сервером jboss клиентского сертификата в реестр системы предварительно должен быть установлен действительный тестовый *клиентский* сертификат с привязкой к ключу и доступный пользователю браузера.
8. *Дополнительная документация*: <https://developer.jboss.org/thread/196715> и <http://docs.jboss.org/jbossweb/3.0.x/ssl-howto.html>
9. **Настройка ГОСТ TLS**

У *jboss* этой версии (устарела) очень много общего с *tomcat*, поэтому настройка для него производится, как и для *tomcat*, с помощью *connector’а*:

*<Connector*

*protocol="HTTP/1.1"*

*SSLEnabled="true"*

*port="****${jboss.web.https.port}****"*

*address="****${jboss.bind.address}****"*

*scheme="https"*

*clientAuth="****true****"*

*secure="true"*

*minSpareThreads="5"*

*maxSpareThreads="75"*

*enableLookups="false"*

*disableUploadTimeout="true"*

*acceptCount="100"*

*maxThreads="200"*

*sslProtocol="****GostTLS****"*

*sslEnabledProtocols="****GostTLS****"*

*ciphers="****TLS\_CIPHER\_2001****"*

*keystoreProvider="****JCP****"*

*keystoreType="****HDImageStore****"*

*keystoreFile="****your\_path\_to\_cert\_store****"*

*keystorePass="****tomcat7****"*

*truststoreProvider="****JCP****"*

*truststoreType="****CertStore****"*

*truststoreFile="* ***your\_path\_to\_cert\_store*** *"*

*truststorePass="****tomcat7****"*

*/>*

Этот коннектор нужно добавить в файл *<корень\_jboss>\server\default\deploy\jbossweb.sar\server.xml* следом за, например, *http*-коннектором:

*<Connector protocol="AJP/1.3" port="${jboss.web.ajp.port}" address="${jboss.bind.address}"*

*redirectPort="${jboss.web.https.port}" />*

**Жирным** выделены основные настройки, смысл которых понятен из названия (по аналогии с *tomcat*).

В новом коннекторе порт задается сервером, указаны протокол (*GostTLS*), используемые сайфер-сюиты (*TLS\_CIPHER\_2001*), провайдер (*JCP*), путь к хранилищу доверенных сертификатов (*your\_path\_to\_cert\_store)* формата *CertStore*, чей пароль совпадает с паролем к серверному контейнеру.

Список ciphers может быть расширен так:

*ciphers="TLS\_CIPHER\_2001,TLS\_CIPHER\_2012"*

В папку пользователя (*C:/Users/<user>/AppData/Crypto Pro*) сервера *jboss* следует поместить сам ключевой контейнер, который и будет использоваться сервером. Ключевой контейнер должен быть доступен пользователю, под управлением которого запускается сервер. Сертификат в контейнере должен быть действителен и содержать OID политики использования для аутентификации сервера (расширенное использование ключа).

В указанном коннекторе требуется авторизация клиента по сертификату (*clientAuth=”true”*). Как в случае настройки сервера *tomcat* с аутентификацией клиента, доверенное хранилище *your\_path\_to\_cert\_store* указывается дважды.

Далее в корневой папке сервера следует найти папку *bin*, перейти в нее, открыть файл *run.bat*, отыскать в нем строку «*set JAVA\_OPTS»* и расширить ее, дописав параметр *-Dcom.sun.security.enableCRLDP=true*:

*set JAVA\_OPTS=-Dprogram.name=%PROGNAME% -Dlogging.configuration=file:%DIRNAME%logging.properties* ***-Dcom.sun.security.enableCRLDP=true*** *%JAVA\_OPTS%*

Это сделано по той причине, что в *cpSSL* по умолчанию включена проверка цепочки сертификатов клиента по *CRLDP*. Без этого параметра в логах сервера будет ошибка:

*GeneralSecurityException: [PKIX] Online verification of certificate status is enabled but com.sun.security.enableCRLDP=false, com.ibm.security.enableCRLDP=false*

Если нужно отключить проверку цепочки, то следует запустить панель *JCP*, перейти на закладку *«Настройки сервера» («Server settings»)* и убрать галочку *«Проверка статуса…».*

1. **Проверка подключения**

Ранее была произведена настройка с требованием сертификата клиента, поэтому после запуска сервера (в одну строку):

*C:\software\jboss-6.1.0.Final\bin >run.bat*

Если требуется проверить подключение в локальной сети с другой машины, то запускать следует командой:

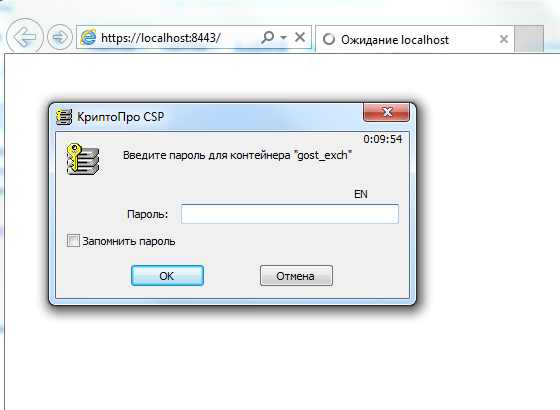
*C:\software\jboss-6.1.0.Final\bin >run.bat -b 0.0.0.0*

Примечание*: Use the option -b 0.0.0.0 when starting jboss (run.sh or run.bat) this binds the port to all network interfaces. Default is localhost thats why you can't reach the server over the network.*

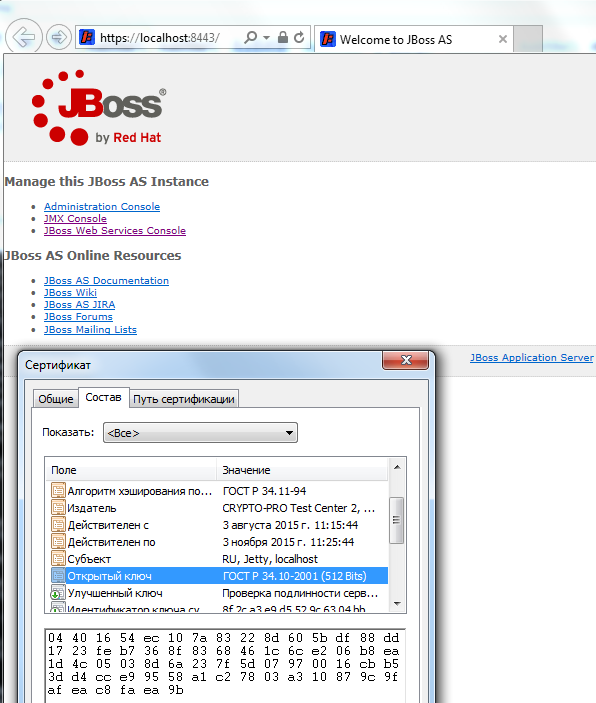
и перехода в *IE* по адресу:

[*https://localhost:8443/*](https://localhost:8443/TestService/Test)

будет предложено выбрать сертификат пользователя, и после ввода пароля к контейнеру пользователя:

****

откроется дефолтная страница сервера (из списка сайфер-сюит сервером была выбрана *TLS\_CIPHER\_2001*):



Чтобы *IE* не сообщал об ошибке перехода на не доверенный сайт, *CN* имя в сертификате соответствует имени хоста, т.е. *localhost*.

**ИНТЕГРАЦИЯ JBOSS EAP 6.4.0 (7) и JTLS 2.0**

Благодарность пользователю *dzevakhin*

за указания по настройке *JBoss 7* и *JTLS 1.0*

*<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">*

*...*

*<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">*

*<ssl name="ssl" key-alias="${keyStoreAlias}" password="${keyStorePassword}" certificate-key-file="${keyStore}" cipher-suite="****TLS\_CIPHER\_2001****" protocol="****GostTLS****" verify-client="true" ca-certificate-file="${trustStore}"/>*

*</connector>*

*</subsystem>*

JCP-388

*Выполнить настройку не удалось из-за изменений в коннекторе - connector -> ssl, а также невозможности явно задать сайфер-сюиту (cipher-suite), протокол (protocol) и провайдер - они зафиксированы в коде, protocol должен содержать TLSv1 и т.п., cipher-suite – ALL, при этом список сайфер-сюит уже не связан с реализуемыми провайдером cpSSL.*