**ИНТЕГРАЦИЯ Tomcat 6/7/8 (до версии 8.5) и JTLS**

<https://www.cryptopro.ru/forum2/default.aspx?g=posts&t=877>

1) устанавливаем JVM

2) устанавливаем JCP (включая модули шифрования)

3) устанавливаем JTLS

4) снимаем экспортные ограничения (<https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/44/6/snjatie-ehksportnykh-ogrnichenijj>)

5) проверяем конфигурацию: *<JRE/bin/java> -cp samples.jar ComLine.CheckConfFull*

6) устанавливаем *tomcat*

**Внимание**! *Если используется tomcat версии 8.5 и выше, то см. инструкцию How\_to\_set\_gost\_tls\_tomcat9.docx в папке Tomcat9.*

1. **Односторонняя аутентификация**

1) Настройки коннектора:

*Connector port="8443" maxHttpHeaderSize="8192"*

*protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"*

*maxThreads="150" minSpareThreads="25" maxSpareThreads="75"*

*enableLookups="false" disableUploadTimeout="true"*

*acceptCount="100" scheme="https" secure="true"*

*clientAuth="false"*

*algorithm="GostX509"*

*keystoreProvider="JCP"*

*sslProtocol="GostTLS"*

*keystoreType="HDImageStore"*

*keyalg="GOST3410"*

*sigalg="GOST3411withGOST3410EL"*

*keystoreFile="C:\store.store"*

*keystorePass="123"*

Для последних версий (до tomcat 8.5) *tomcat* может потребоваться дополнительно:

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

*sslEnabledProtocols="TLSv1"*

2) настраиваем *tomcat* под свою учетную запись (*Windows*) (*Панель управления -> Администрирование -> Службы и приложения -> Службы -> Apache Tomcat свойства -> вход в систему: с учетной записью (указать имя и пароль)*) или следуем инструкциям в руководстве.

3) генерируем ключ (аутентификация сервера) с помощью контрольной панели JCP, там же сохраняем запрос в формате BASE64, по сохраненному запросу получаем сертификат на <http://www.cryptopro.ru/certsrv/>, там же получаем корневой сертификат, с помощью контрольной панели устанавливаем полученный сертификат в контейнер (для того, чтобы записать цепочку сертификатов, можно воспользоваться ComLine.Certs), хотя цепочку можно и не записывать, устанавливаем на контейнер пароль "123" с помощью контрольной панели, создаем хранилище сертификатов C:/store.store и устанавливаем на него пароль "123" (важно, чтобы пароль на контейнер совпадал с паролем на хранилище), в хранилище сертификатов записываем корневой сертификат.

4) запускаем *tomcat,* получаем соединение с односторонней аутентификацией:

a) проверяем *csptest (*входит в состав Крипто-Про CSP*) (в ОС семейства Unix/Linux - "csptestf").* Для использования csptest нужно установить Крипто-Про CSP*:*

*csptest -tlsc -port 8443 -v -file index.jsp -nocheck*

*CSP (Type:75) v3.6.4070 KC1 Release Ver:3.6.4956 OS:Windows CPU:IA32 FastCode:READY,DISABLED (CContextG28147EncryptECB; CContextG28147DecryptECB; CContextG28147EncryptCBC; CContextG28147DecryptCBC; CContextG28147G*

*D:\Program Files\Crypto Pro\CSP\csptest.exe -tlsc -port 8443 -v -file index.jsp -nocheck*

*ClientHello: RecordLayer: SSL, Len: 85*

*Cipher Suites: (81 00 00) (80 00 00) (32 00 00) (04 00 00) (05 00 00) (0a 00 00) (80 00 01) (c0 00 07) (80 00 03) (09 00 00) (40 00 06) (64 00 00) (62 00 00) (03 00 00) (06 00 00) (80 00 02) (80 00 04) (13 00 00) (12 00 00) (63 00 00)*

*87 bytes of handshake data sent*

*535 bytes of handshake data received*

*210 bytes of handshake data sent*

*6 bytes of handshake data received*

*25 bytes of handshake data received*

*Handshake was successful*

*Server certificate:*

*Subject: C=RU, O=CryptoPro, CN=TC*

*Valid : 19.05.2008 - 19.05.2009*

*Issuer : E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPTO-PRO*

*Protocol: TLS1*

*Cipher: 0x661e*

*Cipher strength: 256*

*Hash: 0x801e*

*Hash strength: 256*

*Key exchange: 0xaa25*

*Key exchange strength: 512*

*Header: 5, Trailer: 4, MaxMessage: 16379*

*HTTP request: GET /index.jsp HTTP/1.0*

*User-Agent: Webclient*

*Accept:\*/\**

*Sending plaintext: 62 bytes*

*71 bytes of application data sent*

*8597 bytes of (encrypted) application data received*

*Decrypted data: 8588 bytes*

*11 bytes of (encrypted) application data received*

*Sending Close Notify*

*11 bytes of handshake data sent*

*1 connections, 8588 bytes in 0.219 seconds;*

*Total: SYS: 0.063 sec USR: 0.016 sec UTC: 0.328 sec*

*[ErrorCode: 0x00000000]*

б) если удалось подключиться через *csptest*, заходим через IE (<https://localhost:8443/>) – ОК.

1. **Двусторонняя аутентификация**

1) Настройки коннектора:

*Connector port="8443" maxHttpHeaderSize="8192"*

*protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"*

*maxThreads="150" minSpareThreads="25" maxSpareThreads="75"*

*enableLookups="false" disableUploadTimeout="true"*

*acceptCount="100" scheme="https" secure="true"*

*clientAuth="true"*

*algorithm="GostX509"*

*keystoreProvider="JCP"*

*sslProtocol="GostTLS"*

*keystoreType="HDImageStore"*

*keyalg="GOST3410"*

*sigalg="GOST3411withGOST3410EL"*

*keystoreFile="C:\store.store"*

*keystorePass="123"*

*truststoreFile="C:\store.store"*

*truststorePass="123"*

Для последних версий (до tomcat 8.5) *tomcat* может потребоваться дополнительно:

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

*sslEnabledProtocols="TLSv1"*

2) пп (2)-(3) см. выше.

3) генерируем ключ (*аутентификация клиента*) на <http://www.cryptopro.ru/certsrv/> с помощью средств CSP,

устанавливаем сертификат со ссылкой на закрытый ключ, там же получаем корневой сертификат и устанавливаем его.

4) Запускаем *tomcat* получаем соединение с двусторонней аутентификацией:

a) проверяем *csptest (*входит в состав Крипто-Про CSP*) (в ОС семейства Unix/Linux - "csptestf").* Для использования csptest нужно установить Крипто-Про CSP:

*csptest -tlsc -port 8443 -v -file index.jsp -nocheck*

*CSP (Type:75) v3.6.4070 KC1 Release Ver:3.6.4956 OS:Windows CPU:IA32 FastCode:READY,DISABLED (CContextG28147EncryptECB; CContextG28147DecryptECB; CContextG28147EncryptCBC; CContextG28147DecryptCBC; CContextG28147G*

*D:\Program Files\Crypto Pro\CSP\csptest.exe -tlsc -port 8443 -v -file index.jsp -nocheck*

*ClientHello: RecordLayer: SSL, Len: 85*

*Cipher Suites: (81 00 00) (80 00 00) (32 00 00) (04 00 00) (05 00 00) (0a 00 00) (80 00 01) (c0 00 07) (80 00 03) (09 00 00) (40 00 06) (64 00 00) (62 00 00) (03 00 00) (06 00 00) (80 00 02) (80 00 04) (13 00 00) (12 00 00) (63 00 00)*

*87 bytes of handshake data sent*

*1232 bytes of handshake data received*

*Trying to create new credential*

*Issuer 0: C=??, O=?????????, CN=???*

*Issuer 1: DC=??, DC=?????????, CN=?????????? ????*

*Issuer 2: C=??, CN=?????????*

*Issuer 3: E=?????????????????, C=??, L=??????, O=??? ??????-???, CN=?? ??????????*

*Issuer 4: DC=??, DC=?????????, CN=?????????? ??????? ??*

*Issuer 5: E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPTO-PRO*

*Issuer 6: DC=??, DC=??, CN=???????*

*Issuer 7: C=??, O=?????????, CN=??????????*

*Issuer 8: C=??, O=?????????, CN=????????*

*Issuers: 9, Lenght: 706 bytes*

*Client certificate:*

*Subject: CN=cln*

*Valid : 19.05.2008 - 19.05.2009*

*Issuer : E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPTO-PRO*

*new schannel credential created*

*814 bytes of handshake data sent*

*6 bytes of handshake data received*

*25 bytes of handshake data received*

*Handshake was successful*

*Server certificate:*

*Subject: C=RU, O=CryptoPro, CN=TC*

*Valid : 19.05.2008 - 19.05.2009*

*Issuer : E=info@cryptopro.ru, C=RU, O=CRYPTO-PRO, CN=Test Center CRYPTO-PRO*

*Protocol: TLS1*

*Cipher: 0x661e*

*Cipher strength: 256*

*Hash: 0x801e*

*Hash strength: 256*

*Key exchange: 0xaa24*

*Key exchange strength: 512*

*Header: 5, Trailer: 4, MaxMessage: 16379*

*HTTP request: GET /index.jsp HTTP/1.0*

*User-Agent: Webclient*

*Accept:\*/\**

*Sending plaintext: 62 bytes*

*71 bytes of application data sent*

*8597 bytes of (encrypted) application data received*

*Decrypted data: 8588 bytes*

*11 bytes of (encrypted) application data received*

*Sending Close Notify*

*11 bytes of handshake data sent*

*1 connections, 8588 bytes in 1.813 seconds;*

*Total: SYS: 0.063 sec USR: 0.094 sec UTC: 1.859 sec*

*[ErrorCode: 0x00000000]*

б) если удалось подключиться через *csptest*, заходим через IE (<https://localhost:8443/>) – ОК. Для использования ГОСТ TLS в IE нужно установить Крипто-Про CSP.

*Tomcat* может использовать библиотеки *Apache Portable Runtime (APR)* для повышения производительности. *APR* использует платформо-зависимую реализацию SSL, которая не может работать с российскими ГОСТ алгоритмами и *Java* настройками типа *keystoreFile* и выдаст ошибку. Для предотвращения авто конфигурации через *APR* и задания *Java* коннектора, независимо от того загружены *ARP* библиотеки или нет, необходимо в описании коннектора явно задать имя класса реализации в атрибуте протокола *protocol = "org.apache.coyote.http11.Http11NioProtocol".*