127 018, Москва, Сущевский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро JTLS

Версия 2.0 R2

Инструкция по использованию

ЖТЯИ.00091-02 91 02-01

Листов 7

2018

Оглавление

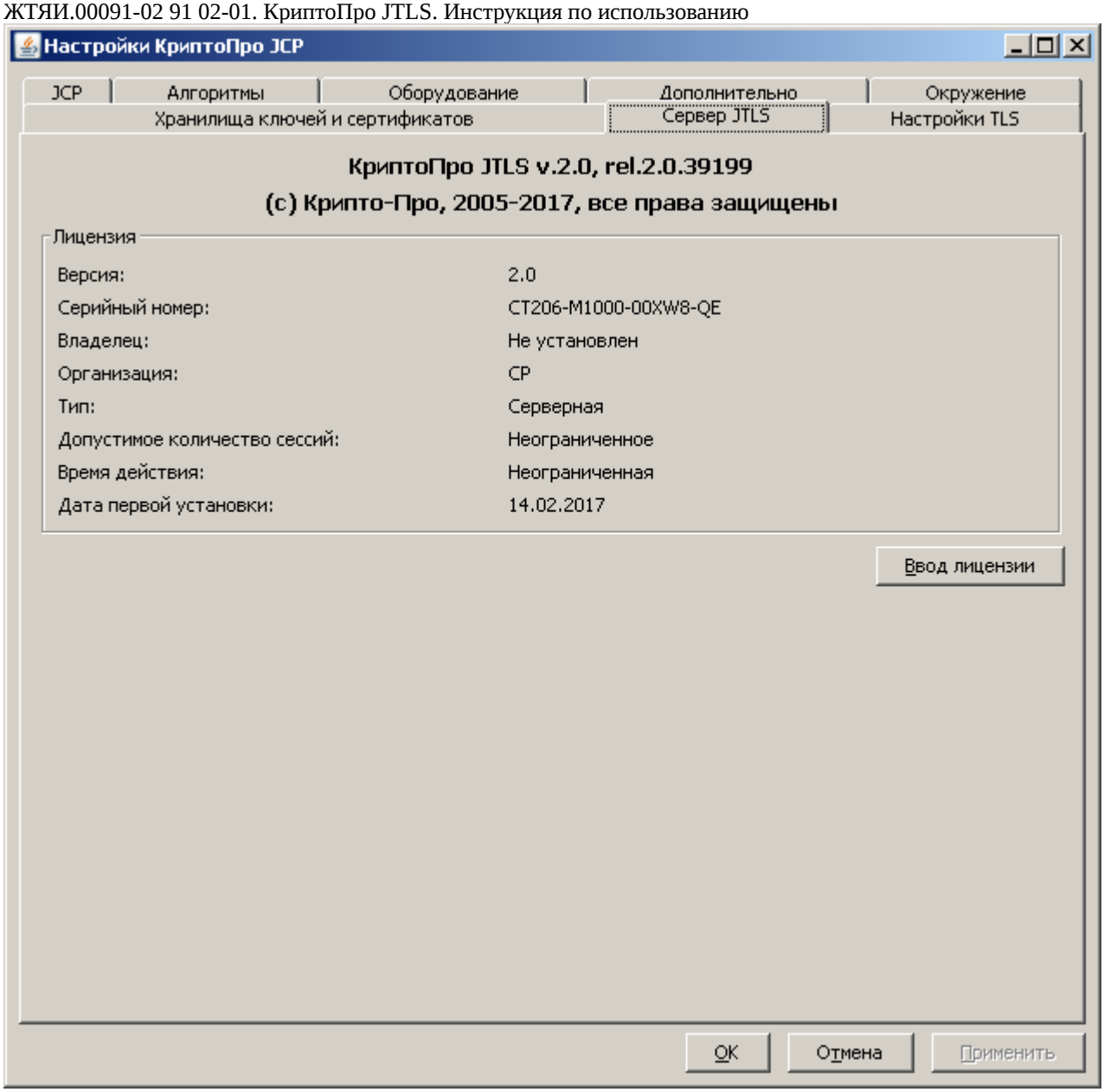
1. Введение

«КриптоПро JTLS» версия 2.0 R2 является программным комплексом защиты информации, разработанным на основе «КриптоПро JCP» версия 2.0 R2 и реализующим протоколы SSL и TLS в соответствии с российскими криптографическими алгоритмами.

Основные функции, реализуемые «КриптоПро JTLS» версия 2.0 R2:

- Две схемы аутентификации с использованием обмена ключей по алгоритму Диффи-Хэллмана и хэширования в соответствии с ГОСТ Р 34.11-94.
  - односторонняя - анонимный клиент, аутентифицируемый сервер;
  - двухсторонняя - аутентифицируемые клиент и сервер.

  В случае аутентификации клиента на ключе подписи применяются алгоритмы выработки электронной подписи в соответствии с ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012 и проверки в соответствии с ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.
- шифрование соединения в соответствии с ГОСТ 28147-89;
- имитозащита передаваемых данных в соответствии с ГОСТ 28147-89.



2. Контрольная панель

Основной набор закладок контрольной панели «КриптоПро JCP» версия 2.0 R2 описан в «Руководстве администратора». После установки модуля «КриптоПро JTLS» версия 2.0 R2 на контрольной панели появятся соответствующие закладки.

2.1. Закладка "Сервер JTLS"

Рисунок 1. Внешний вид панели "Лицензия" (временная лицензия)

Данная панель содержит информацию о серверной лицензии «КриптоПро JTLS» версия 2.0 R2. Работа с данной панелью аналогична работе с закладкой "JCP" (панель "Лицензия").

2.2. Закладка "Настройки TLS"

Рисунок 2. Внешний вид панели "Настройки TLS"

Данная панель содержит настройки сервера:

- Аутентификация клиента:
  - не требуется (по умолчанию)
  - желательна
  - требуется
- Размер кэша сессий (количество сессий; по умолчанию 0 - неограниченное)
- Время хранения сессий в кэше (по умолчанию 24 часа; если размер кэша сессий не задан (=0), то "старые" сессии удаляться не будут).
- Возможность полного отключения проверки цепочки сертификатов на отзыв, включение проверки с условием загрузки COC из сети по CRLDP сертификата, включение проверки с условием загрузки COC из папки (задается абсолютный путь к папке с COC).
- Отключение, включение и требование поддержки расширения Renegotiation Indication (RFC 5746). Задание данных настроек с помощью параметров *-Dru.CryptoPro.ssl.allowUnsafeRenegotiation=<value>* *-Dru.CryptoPro.ssl.allowLegacyHelloMessages=<value>* в приложении имеет приоритет выше и переопределяет настройки JTLS. Пары указанных свойств образуют следующие группы:

Режим	**Allow Legacy Hello Messages**	**Allow Unsafe Renegotiation**	**Аналогия с CSP TLS**
Строгий (strict)	false	false	Требуем RFC 5746: наличие RI обязательно, проверка выполняется
Безопасный (interoperable)	true (SUN default)	false	Поддерживаем RFC 5746(по умолчанию в CryptoPro CSP 4.0): наличие RI необязательно, проверка может выполняться
Небезопасный (insecure)	true	true	Не поддерживаем RFC 5746 (по умолчанию в CryptoPro CSP): наличие RI необязательно, проверка не выполняется

- Запрет отправки клиентом расширения Renegotiation Indication.

3. Настройка параметров провайдера с помощью Preferences

В некоторых случаях может потребоваться настройка Java TLS путем редактирования параметров провайдера, хранящихся в Preferences.

Доступ к ним преимущественно можно получить тремя способами:

1) программно, с помощью Preferences.systemRoot() или Preferences.userRoot(), перечисления путей к узлам и задания новых значений;
2) вручную, редактируя параметры в соответствующих разделах (SOFTWARE\JavaSoft\Prefs\ru или SOFTWARE\Wow6432Node\JavaSoft\Prefs\ru компьютера HKEY_LOCAL_MACHINE или пользователя HKEY_CURRENT_USER) реестра ОС Windows или файлы вида prefs.xml в соответствующих папках .systemPrefs/ru (например, /etc/.java/.systemPrefs/ru) или .userPrefs (/home/user/.userPrefs/ru) ОС *nix;
3) с помощью класса ru.CryptoPro.JCP.Util.SetPrefs, находящегося в модуле JCP и предоставляющего возможности для добавления и редактирования, например:

```
java ru.CryptoPro.JCP.Util.SetPrefs -user -node ru/CryptoPro/JCP -key
JCP_any_param -value any_value
```

```
java ru.CryptoPro.JCP.Util.SetPrefs -system -node ru/CryptoPro/JCP/Key -key
JCP_any_param -value any_value
```

Таблица: Основные параметры Java TLS

Описание	Путь	Ключ	Соответствует
Путь к папке CRL	ru/CryptoPro/ssl	CRL_location_default	Закладка «Настройки TLS», загрузка CRL из папки
Аутентификация клиента, число (0-2)	ru/CryptoPro/ssl	Client_auth_default	Закладка «Настройки TLS», аутентификация клиента
Проверка цепочки сертификатов на отзыв, true или false	ru/CryptoPro/ssl	Enable_CRL_revocation_off-line_default	Закладка «Настройки TLS», проверка цепочки сертификатов на отзыв
Запрет для клиента отправлять расширение Renegotiation Indication, true или false	ru/CryptoPro/ssl	disable_client_ri	Закладка «Настройки TLS», запрет для клиента отправлять расширение Renegotiation Indication
Размер кеша сессий, число	ru/CryptoPro/ssl	Session_cache_size_default	Закладка «Настройки TLS», размер кеша сессий
Время хранения сессий в кеше, часы	ru/CryptoPro/ssl	Session_time_default	Закладка «Настройки TLS», время хранения сессий в кеше
Алгоритм работы с Renegotiation Indication, число (0-2)	ru/CryptoPro/ssl	RI_support	Закладка «Настройки TLS», Renegotiation Indication