

TrustedBitrix

Руководство пользователя

01.08.2012



ООО «Цифровые технологии»

TrustedBitrix. Руководство пользователя. Версия 1.0.

Дата сборки документа 01.08.2012.

Этот документ является составной частью технической документации ООО «Цифровые технологии».

Сайт справки по продуктам ООО «Цифровые технологии» <http://www.trusted.ru>

© 2012-2013 ООО «Цифровые технологии». Все права защищены.

Контактная информация

ООО «Цифровые технологии»

<http://www.trusted.ru>


Содержание

Введение	4
Раздел 1. Технология аутентификации по протоколу TLS	5
ПРИНЦИПЫ АУТЕНТИФИКАЦИИ ПО ПРОТОКОЛУ TLS	5
НЕОБХОДИМЫЕ ЭЛЕМЕНТЫ АУТЕНТИФИКАЦИИ ПО TLS	6
АЛГОРИТМ АУТЕНТИФИКАЦИИ.....	7
ГЕНЕРАЦИЯ СЕРТИФИКАТОВ ЧЕРЕЗ OPENSSL И НАСТРОЙКА TLS.....	7
Раздел 2. Установка модуля TrustedBitrixLogin.....	10
УСТАНОВКА МОДУЛЯ ИЗ MARKETPLACE.....	10
НАСТРОЙКА ПАРАМЕТРОВ МОДУЛЯ.....	11
АДМИНИСТРИРОВАНИЕ ХРАНИЛИЩА СЕРТИФИКАТОВ	12
УДАЛЕНИЕ МОДУЛЯ.....	14
Раздел 3. Настройки браузеров.....	16
НАСТРОЙКА БРАУЗЕРА MICROSOFT INTERNET EXPLORER	16
НАСТРОЙКА БРАУЗЕРА GOOGLE CHROME	17
Раздел 4. Коды ошибок модуля.....	19

Введение

Руководство предназначено для пользователей, администраторов и редакторов сайта на базе систем *"1С-Битрикс: Управление сайтом"*, *"1С-Битрикс: Корпоративный портал"*, *"1С-Битрикс: Портал органов государственной власти"*. В руководстве описаны основные действия по установке и настройке модуля TrustedBitrixLogin для взаимодействия с ПО TrustedTLS.

Решение с использованием модуля TrustedBitrixLogin рекомендуется для компаний, имеющих широкую локальную сеть и не использующих сертифицированные средства криптографической защиты, в то время как сотрудники должны иметь доступ к удаленным веб-ресурсам (например, порталам 1С Битрикс), вход на которые выполняется строго по ГОСТ-сертификатам.

 **Важно!** Работа с модулем аутентификации требует установки на клиентском рабочем месте дополнительного ПО – криптопровайдера КриптоПро CSP в случае необходимости использования ГОСТ алгоритмов. На сервере должны быть установлены продукты КриптоАРМ, КриптоПро CSP и TrustedTLS.

Раздел 1. Технология аутентификации по протоколу TLS

Принципы аутентификации по протоколу TLS

TLS (что есть Transport Layer Security), он же ранее известный как SSL (Secure Sockets Layer), на данный момент является стандартом де-факто для защиты протоколов транспортного уровня от различных методов вмешательства извне.

Функционирует TLS поверх транспортного протокола, например (и зачастую) TCP. Он работает с двумя потоками данных, вне зависимости от их природы, - входящим и исходящим, и каждый из них преобразует соответствующим образом в зашифрованный поток (точнее в «измененный», поскольку TLS разрешает и отсутствие шифрования передаваемых данных).

Работа протокола разделяется на два этапа: обмен ключами, и дальнейший обмен данными.

Первый этап проходит без каких-либо «полезных» данных, передаваемых от клиента к серверу и обратно, и служит для идентификации клиента и сервера, а также выбора алгоритмов и инициализации ключей для дальнейшего шифрования. На втором этапе идет просто обмен данными через установленное логическое соединение, где каждый пакет полезных данных шифруется (если шифрование включено), защищается при помощи MAC, и передается другой стороне через нижележащий протокол (TCP).

Инициализируется общение между клиентом и сервером сообщением *ClientHello*, которое посылается клиентом серверу. В этом сообщении клиент перечисляет поддерживаемые им «алгоритмы защиты» (в порядке предпочтения), а также передает некоторые другие параметры (поддерживаемые алгоритмы сжатия данных, 28 байт случайных данных, которое потом будут использованы для генерации общего секрета, идентификатор сессии при желании ее восстановления). Каждый «алгоритм защиты», вернее *Cipher Suite* («набор алгоритмов»), на самом деле идентифицирует три алгоритма:

- 1) алгоритм обмена ключами, благодаря которому у клиента и сервера после преобразований появляются общие 48 байт разделенного секрета, которые позже используются для генерации ключей ко всем остальным алгоритмами (шифрования и MAC);
- 2) блочный или поточный алгоритм шифрования, используемые для шифрования данных;
- 3) MAC - алгоритм, используемый для подсчета MAC-кода сообщения (идентифицируется хеш-алгоритмом, поскольку в стандарте RFC 5246 описан только HMAC).

Получив это сообщение, сервер выбирает набор шифров, который будет использоваться, согласно своей таблице предпочитаемых *Cipher Suites*, и отправляет клиенту в сообщении *ServerHello*. Кроме выбранного набора, сервер также посылает свои сгенерированные случайные данные и идентификатор сессии. Сразу после этого сообщения сервер, в

зависимости от выбранного набора алгоритмов, посылает (или не посылает) следующие сообщения: Certificate, ServerKeyExchange, CertificateRequest.

В сообщении Certificate сервер посылает свой X.509 сертификат, который удостоверяет аутентичность сервера, а в CertificateRequest - сервер требует от клиента также прислать свой сертификат, чтобы доверить его аутентичность.

Кроме сертификата, сервер также (в пакете ServerKeyExchange) присылает цифровую подпись данных, посылаемых в этом пакете, что позволяет убедиться, что данный пакет действительно прислан сервером, который владеет секретным ключом к присланному сертификату.

Сертификат x.509 - есть привязка некоторого открытого ключа к некоторой сущности (человеку, организации, или, как в данном случае - серверу), которая владеет секретным ключом, соответствующим этому открытому. Сертификаты бывают самозаверенные (self-signed), когда человек сам его подписывает, и заверенные центром сертификации. Основной вопрос, который возникает при встрече с таким сертификатом — доверие к нему, и тут можно полагаться или на свои личные данные (как в случае самозаверенными сертификатами - кто угодно может генерировать такой сертификат), или на доверенные центры, которые налагают свою подпись на сертификат, тем самым как бы доказывая, что они проверили, и этот сертификат действительно соответствует тому-то и тому-то.

Сервер присылает свой сертификат, и клиент проверяет, действительно ли он доверяет этому сертификату, и в случае отрицательного ответа прерывает сеанс связи. Если сервер потребовал сертификат у клиента, клиент обязан предъявить свой сертификат, иначе связь уже будет прервана сервером.

После получения этого всего клиент посылает свой пакет Certificate (при надобности), ClientKeyExchange, CertificateVerify (цифровая подпись, сгенерированная сертификатом клиента).

После этого, при прошедших взаимных проверках, считается, что клиент и сервер обладают общим секретом, размерностью в 48 байт. Из этого разделенного секрета, при помощи переданных перед этим случайных данных, и некоторых констант, по некоторым правилам, генерируются ключи для алгоритмов шифрования и проверки MAC-кода (это стоило написать раньше, в общем MAC-код это что-то вроде хеша, но который успешно можно проверить только обладая дополнительно некоторым ключом), и далее идет обмен данным как предусмотрено протоколом уровня приложения.

Необходимые элементы аутентификации по TLS


Что необходимо настроить для использования TLS:

1. *Обмен сертификатами.* Если сервер присылает сертификат, который не заверен корневым центром сертификации, известным вашему компьютеру, ваше устройство, в зависимости от настроек, как правило, спросит «а доверяете ли вы такому-то

сертификату?», если бездумно ответить «да!», то можно перечеркнуть всю безопасность, предлагаемую протоколом TLS.

2. *Сертификат сервера.* Как узнать, что сертификат соответствует этому сайту? Это можно определить, потому как для TLS сертификатов в поле common name (CN=) прописывается имя сайта, которому он соответствует, и которое браузер должен проверять, и в результате несоответствия говорить про ошибку проверки.

3. *Сертификат клиента.* Этот сертификат каким-то образом должен быть сохранен на сервер в списке доверяемых, или authority, выписавшая этот сертификат, должна быть доверяемой на сервере.

 **Важно!** Быстродействие установления TLS соединения значительно отличается от обычного входа. Инициализация протокола требует трех посылок данных туда и назад (т.е. это уже 3 пинга), еще достаточно времени требует генерирование цифровой подписи (мы рассматриваем сторону сервера), а также разворачивание ключей для симметричных алгоритмов шифрования, что в сумме может занять более полсекунды (кстати, надо заметить, что генерирование DSA-подписи при равном размере с RSA-ключом, происходит раза в 2-4 быстрее).

Алгоритм аутентификации

Технология заключается в установлении принудительной двухсторонней аутентификации по сертификатам сервера и клиента и дальнейшей проверки открытого сертификата клиента в таблице ассоциации сертификатов аутентификации и пользователей в БД 1С-Битрикс и дальнейшей аутентификации пользователя в системе, а также реагирования на события входа по логину/паролю.

При установке соединения происходит проверка сертификата по СОС из УЦ. Если проверка не проходит, то соединение не устанавливается и пользователь видит стандартную ошибку 404.

После прохождения проверки по СОС из УЦ, проверяется наличие сертификата пользователя в таблице ассоциации сертификатов аутентификации и пользователей в БД 1С-Битрикс.

Генерация сертификатов через OpenSSL и настройка TLS

После установки OpenSSL на машину где будут генерироваться сертификаты для клиентского рабочего места и сервера, необходимо внести в файл конфигурации (/etc/ssl/openssl.cnf) следующие изменения:

[CA_default]

Это каталог для работы с ssl

dir = .

Каталог сохранения сертификатов

certs = \$dir/ssl.crt

Каталог листов "отзыва подписей"

```
crl_dir = $dir/ssl.crl  
# Здесь index file для индексирования запросов на подпись  
database = $dir/index.txt  
# Каталог записи новых сертификатов  
new_certs_dir = $dir/ssl.crt  
# Корневой сертификат  
certificate = $dir/nemesida-ca.pem  
# Серийный номер запроса  
serial = $dir/serial  
# Текущий лист отзывов подписей  
crl = $dir/ssl.crl/nemesida.pem  
# Секретный ключ для основного сертификата  
private_key = $dir/ssl.key/nemesida-ca.key  
RANDFILE = $dir/ssl.key/.rand #
```

Далее необходимо создать корневой сертификат. Для удобства, можно перейти в каталог с конфигурацией Apache, где располагаются подкаталоги с искомыми сертификатами:

```
# cd /usr/local/etc/apache
```

Корневой сертификат является корнем дерева подписей. Секретный ключ (он нужен для того, чтобы можно было воспользоваться вашим корневым сертификатом для подписи остальных) и сертификат создаются одной командой:

```
# openssl req -config /etc/ssl/openssl.cnf -new -x509 -keyout ssl.key/nemesida-ca.pem -  
out nemesida-ca.pem -days 3650
```

При генерации будет запрошен пароль - введите и запомните его. Все остальные поля можно заполнить по своему усмотрению. Снимите пароль с ключа:

```
# openssl rsa -in ssl.key/nemesida-ca.pem -out nemesida-ca.key
```

Выполните следующую команду, чтобы сформировать сам сертификат:

```
# openssl x509 -in nemesida-ca.pem -out nemesida-ca.crt
```

В результате проделанных действий корневой сертификат должен быть создан и подписан сам собой.

Следует создать два файла с некоторой индексной информацией. Создайте индексный файл (ключевое слово database из openssl.cnf):

```
# touch index.txt
```

Создайте файл серийных номеров (ключевое слово serial из openssl.cnf):

```
# echo '01' > serial
```


Этот файл должен содержать две цифры (обязательно). Если вы ранее не создавали никаких сертификатов кроме корневого, файл должен содержать 01.

Далее требуется создать сертификат сервера. Создание сертификатов сервера состоит из процедуры создания запроса на подпись, а затем подписи этого запроса в отличии от создания самоподписанного корневого сертификата. Создайте запрос на подпись нового сертификата и секретный ключ к нему:

```
# openssl req -config /etc/ssl/openssl.cnf -new -keyout ssl.key/nemesida.pem -out  
ssl.csr/nemesida.pem
```

Вводя данные, учтите, что поле Common Name должно содержать полностью определённое доменное имя (FQDN) того сайта, где вы будете использовать https-протокол, чтобы браузеры не выдавали предупреждения о несоответствии имени. Снимите пароль с ключа:

```
# openssl rsa -in ssl.key/nemesida.pem -out nemesida.key
```

Подпишите запрос (подписка запроса и есть создание нового сертификата) своим корневым сертификатом:

```
# openssl ca -config /etc/ssl/openssl.cnf -policy policy_anything -out  
ssl.crt/nemesida.pem -infiles ssl.csr/nemesida.pem
```

Подготовьте сертификат к использованию:

```
# openssl x509 -in ssl.crt/nemesida.pem -out ssl.crt/nemesida.crt
```

Создание клиентского сертификата производится аналогично. Не забудьте указать назначение сертификата – в одном случае «Подтверждение подлинности сервера», в другом – «Подтверждение подлинности клиента».

В файле httpd.conf (в конфигурации 1С Битрикс) прописываем:

```
NameVirtualHost *:443  
DocumentRoot "/home/nemesida/www"  
ServerName nemesida.ru  
ScriptAlias /cgi-bin/ /home/nemesida/cgi-bin/  
SSLEngine on  
SSLCertificateFile /usr/local/etc/apache/ssl.crt/nemesida.crt  
SSLCertificateKeyFile /usr/local/etc/apache/ssl.key/nemesida.key  
SSLCACertificateFile /usr/local/etc/apache/nemesida-ca.crt  
SSLCARevocationFile /usr/local/etc/apache/ssl.crl/nemesida.crl  
SSLOptions +StdEnvVars
```

После внесения изменений перезапустите Apache и проверьте вход по https.

Раздел 2. Установка модуля TrustedBitrixLogin

Установка модуля из Marketplace

Модуль «**TrustedBitrix Start**» версии 1.0.0 является бесплатным продуктом, поэтому клиенты смогут свободно установить его из Marketplace следующим образом:

Перейдите на административную часть сайта и выберите на вкладке **Настройки** пункт **MarketPlace**.

В разделе **Решения для сайтов -> Безопасность** представлена информация о модуле **Авторизация по сертификату** (*trusted.tBitrixStart*). Перейдите по ссылке **Установить**.

В открывшемся окне ознакомьтесь с соглашением об использовании (содержание лицензионного соглашения).

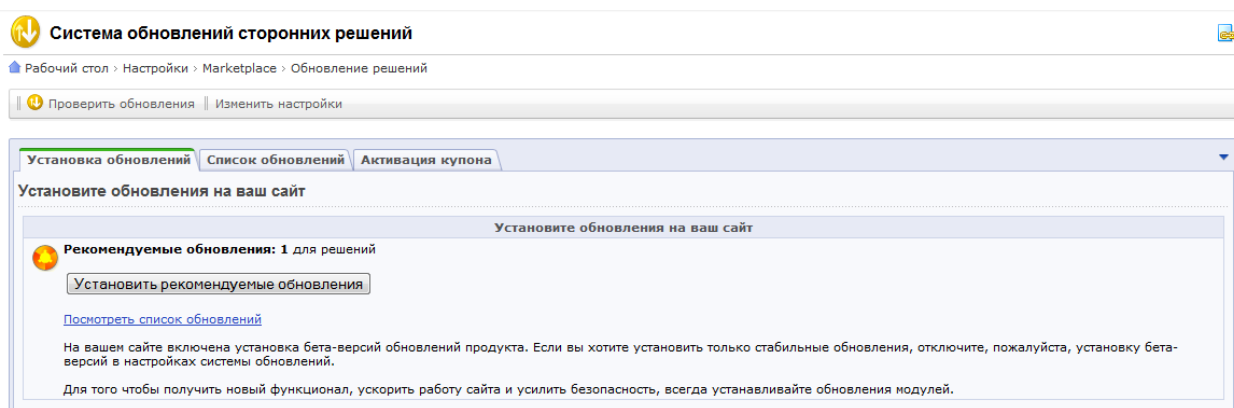


Рис. 2.1 Инициализация загрузки модуля на портал

После выбора действия по установке рекомендуемого обновления, исходный код модуля будет загружен на портал (рис.2.1).

После успешной загрузки модуля его можно установить (рис.2.2).

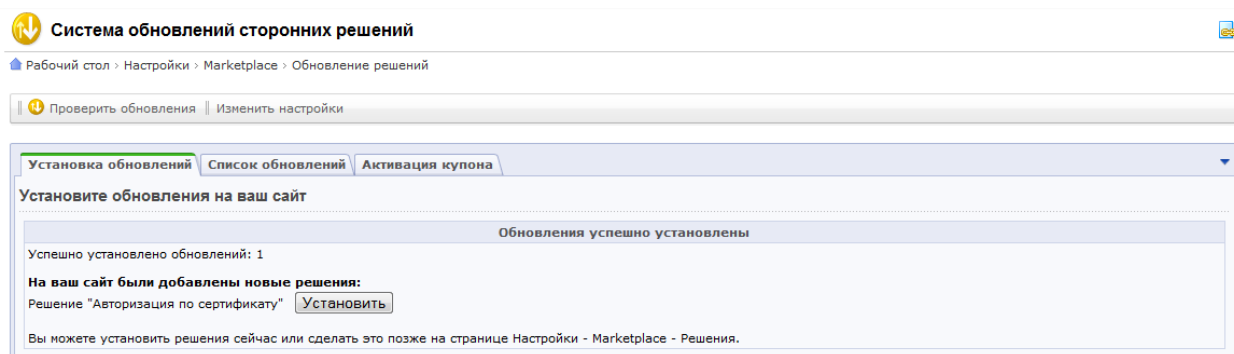


Рис. 2.2. Установка решения на портал

Установка модуля заключается в последовательном прохождении двух шагов мастера. На первом шаге предлагается выбор варианта организации инфоблоков хранилищ (рис.2.3):

- в первом случае создаются новые инфоблоки с неизменными именами и заданными пользовательскими свойствами. Если инфоблоки модуля были созданы и использовались ранее, то произойдет уничтожения существующих в них данных.

- во втором случае инфоблоки не создаются, а используются существующие. Имена инфоблоков будут отражены в полях просмотра и остаются неизменными.



Рис. 2.3. Установка решения на портал

На следующем шаге мастера установки (рис.2.3) должно появиться сообщение о завершении установки и регистрации модуля на портале. После щелчка по кнопке **Вернуться в список** будет выполнен переход в список установленных решений (рис. 2.5).

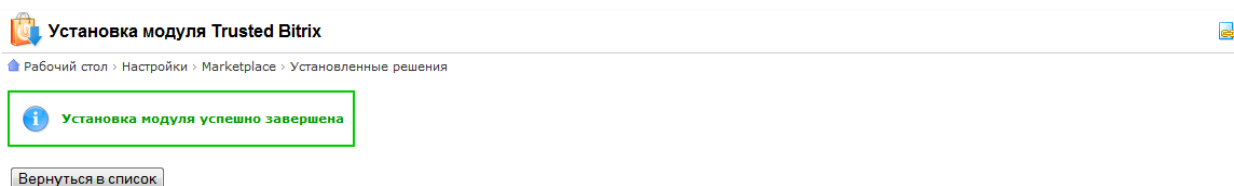
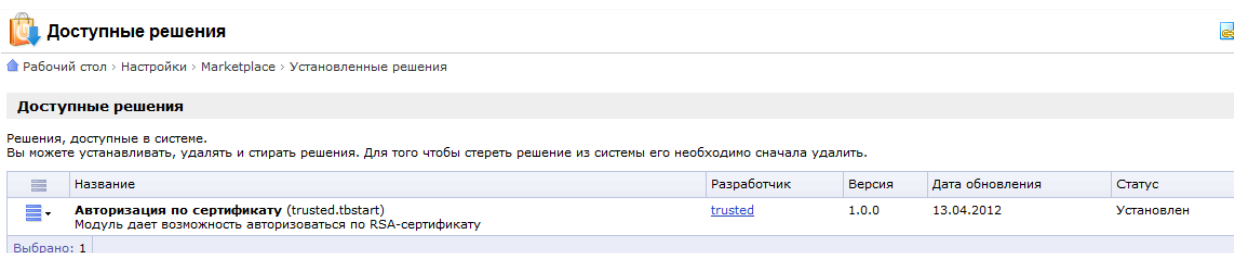


Рис. 2.4. Завершение установки



Название	Разработчик	Версия	Дата обновления	Статус
Авторизация по сертификату (trusted.tbstart) Модуль дает возможность авторизоваться по RSA-сертификату	trusted	1.0.0	13.04.2012	Установлен

Рис. 2.5. Список установленных решений

Присутствие записи о решении в списке со статусом «Установлен», говорит о том, что модуль готов к использованию при условии настройки доступа по протоколу TLS.

Настройка параметров модуля

После установки модуля необходимо удостовериться в возможности входа на сайт по протоколу TLS и после этого можно активировать модуль. Для активации перейдите в раздел **Настройки, Настройки продукта, Настройки модулей, Авторизация по сертификату**.



В настройках модуля по умолчанию выставлен HTTPS порт 443 и отсутствует отметка пункта «Активировать авторизацию по сертификату». Для того чтобы при входе на портал по HTTPS у пользователя запрашивался сертификат требуется отметить этот пункт.

⚠ Важно! Если вход по протоколу TLS не настроен, то при активации модуля может возникнуть критическая ошибка блокирующая корректное отображение страниц портала.

Администрирование хранилища сертификатов

Чтобы начать работу с модулем необходимо иметь сертификаты пользователей для их занесения в хранилище. Пользователи должны быть предварительно зарегистрированы на портале с необходимыми правами.

Через пункт меню **Личные сертификаты** нужно перейти таблице зарегистрированных пользователей портала (рис. 2.6).

 **Список пользователей** 

Рабочий стол > Настройки > Trusted Bitrix > Личные сертификаты

На странице: 20

Пользователи 1 – 20 из 477

ID	Имя	Фамилия	Компания	E-Mail	Сертификаты
477	Марианна	Телегина		m.telegina@example.com	(0) [+]
476	Ольга	Немцова		o.nemcova@example.com	(0) [+]
475	Софья	Михайлова		s.mihajlova@example.com	(0) [+]
474	Алевтина	Ляхович		a.lyahovich@example.com	(0) [+]
473	Наталья	Ломова		n.lomova@example.com	(0) [+]
472	Александр	Холзаков		a.holzakov@example.com	(0) [+]
471	Виктор	Трапезников		v.trapeznikov@example.com	(0) [+]
470	Дмитрий	Титоров		d.titorov@example.com	(0) [+]
469	Александр	Сюгаев		a.syugaev@example.com	(0) [+]

Рис. 2.6 Таблица со списком пользователей портала

В колонке Сертификаты имеются ссылка на список привязанных к пользователю сертификатов (обозначается их количеством) и ссылка на добавление нового сертификата. Переход по второй ссылке приводит к открытию формы добавления нового сертификата.

На форме добавления сертификата указывается кому назначается данный сертификат и предлагается выполнить выбор файла *.cer через диалог выбора файла (рис. 2.7). При включении отметки **Активация сертификата**, добавленный элемент немедленно активируется, и пользователь может использовать загруженный сертификат для входа. При отсутствии отметки сертификат будет добавлен в хранилище, но вход по нему будет временно блокирован.

Добавление сертификата пользователю (477, m.telegina) Телегина Марианна Викторовна

Рабочий стол

Вернуться к списку сертификатов пользователя

Добавление нового сертификата

Тело сертификата: E:\Documents and Settings\m.telegina\Рабочий стол\Сертификат.cer Обзор...

Активация сертификата: ☒

Сохранить Применить Отменить

*Поля, обязательные для заполнения.

Рис. 2.7. Форма загрузки сертификата аутентификации

С каждым пользователем в хранилище может быть связано сколько угодно сертификатов. По любому из них, при соблюдении условий активности и валидации он может авторизоваться на сайте. **В данной бесплатной версии модуля могут использоваться сертификаты, сгенерированные на RSA-алгоритмах. ГОСТ-сертификаты не будут загружаться в хранилище сертификатов.**

Важно! При удалении пользователя данные из хранилища сертификатов (сертификаты привязанные к ID пользователя) безвозвратно удаляются. При добавлении пользователя для него необходимо загрузить необходимые сертификаты. Также удаляются сертификаты, не привязанные к пользователю и дублирующие друг друга.

Сертификаты пользователя отображаются списком (рис. 2.8) в котором также отображается их статус.

Список личных сертификатов пользователя (477, m.telegina) Телегина Марианна Викторовна

Рабочий стол

Дополнительно

Владелец сертификата

Найти Отменить

Вернуться к списку Добавить сертификат Настроить Excel

На странице: 20

Список личных сертификатов пользователя 1 - 1 из 1

	ID	Владелец	Инд.	Действителен с	Действителен по	Акт.	Издатель
<input type="checkbox"/>	708	UC-EM	●	07.10.2005 13:04:00	07.10.2011 13:09:24	Y	UC-EM

Выбрано: 1 Отмечено: 0



На странице: 20

Список личных сертификатов пользователя 1 - 1 из 1

Для всех -действия- Применить


Рис. 2.8. Список сертификатов, привязанных к пользователю

Каждый из сертификатов аутентификации пользователей имеет определенные свойства. Эти свойства можно посмотреть и отредактировать вручную (рис. 2.9).

 Редактирование информации о сертификате пользователя (477, m.telegina) Телегина Марианна Викторовна 

Рабочий стол

Внимание! Воспользуйтесь технологией SiteUpdate для получения последних обновлений.
 Это пробная версия продукта "1С-Битрикс: Корпоративный портал". До истечения пробного периода осталось 29 дней. Вы можете купить полнофункциональную версию продукта по адресу <http://www.1c-bitrix.ru/buy/>


 Вернуться к списку сертификатов пользователя


Редактирование данных о сертификате

Редактирование данных о сертификате

Имя (владелец сертификата): UC-EM

Активность элемента: ☒

Начало активности: (DD.MM.YYYY / DD.MM.YYYY HH:MI:SS) 07.10.2005 13:04:00 

Окончание активности: (DD.MM.YYYY / DD.MM.YYYY HH:MI:SS) 07.10.2011 13:09:24 


Издатель сертификата: UC-EM


Хэш сертификата: 75c0033bed247517b3e98dd62b5b8184

Серийный номер сертификата: 123169137058018676216838511484734292547

Тело сертификата:

```
-----BEGIN CERTIFICATE-----
MIIDnTCCA0ggAwIBAgIQXKmDT0cvtdFIVL96IxC
QzAKBgYqhQMCAGMFADCBujEa
MBgGCSqGSIb3DQEJARYLY2FAdWMtZW0ucnUxCzAJ
BgNVBAYTA1JVMRUEwEwYDVQQH
HgWEHAQ+BEEEOQyBDxNTAzBgNVBAoELAQeBBAE
HgAgBCOEOWQ1BD0EQgRABD4E
PQQ9BDAETwAgBBwEPgRBBDoEMgQwMTEwLwYDVQQL
HigETwQOB4EQQRCD4EMgQ1
BEAETwROBEKEOAQ5ACAEJgQ1BD0EQgRAMQ4wDAYD
VQOQEWVQy1FTTAeFw0wNTEw
```

Сертификат действителен с: 07.10.2005 13:04:00 



Сертификат действителен по: 07.10.2011 13:09:24 

*Поля, обязательные для заполнения.

Рис. 2.9. Форма просмотра/редактирования свойств сертификата

Удаление модуля

Для удаления модуля нужно открыть страницу со списком установленных решений (рис.2.10).

 Доступные решения 

Рабочий стол > Настройки > Marketplace > Установленные решения


Доступные решения					
Решения, доступные в системе. Вы можете устанавливать, удалять и стирать решения. Для того чтобы стереть решение из системы его необходимо сначала удалить.					
	Название	Разработчик	Версия	Дата обновления	Статус
	Авторизация по сертификату (trusted.tbstart) Модуль дает возможность авторизоваться по RSA-сертификату	trusted	1.0.0	16.08.2012	Установлен
Выбрано: 1					

Рис. 2.10. Список установленных решений

Из контекстного меню элемента списка нужно выбрать команду **Удалить**, после чего запустится мастер удаления. На первом шаге мастера можно выбрать: удалить или оставить инфоблоки с данными о сертификатах и пользователях (рис. 2.11).

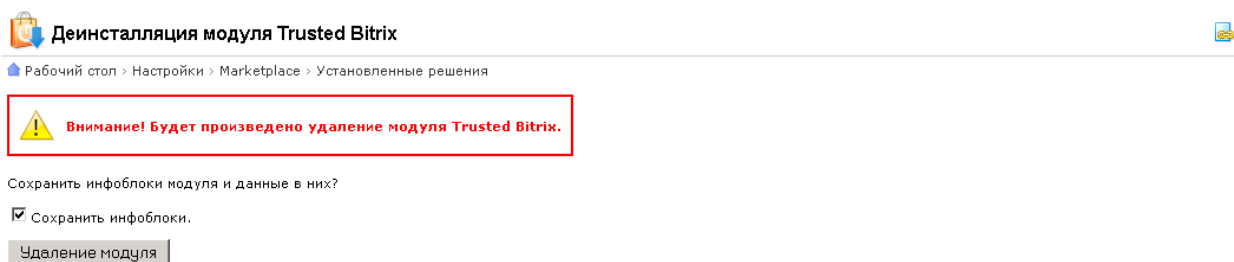


Рис. 2.11 Мастер удаления модуля

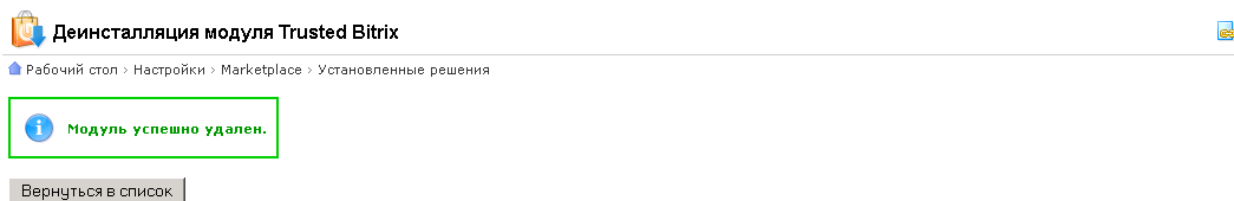


Рис. 2.12 Завершение работы мастера удаления модуля

Раздел 3. Настройки браузеров

⚠ Важно! В данный момент разработчиками в решении по аутентификации и защите информационного канала поддерживаются два типа браузеров – Microsoft Internet Explorer и Google Chrome. Если на клиентском рабочем месте установлены эти браузеры и вход на портал осуществляется по сертификату, то решение гарантирует корректную работу TLS по ГОСТ алгоритмам, предоставляемым СКЗИ КриптоПро CSP. Обычный вход на портал (по логину/паролю) пользователь может осуществлять, используя любой из доступных браузеров.

Настройка браузера Microsoft Internet Explorer

Для настройки браузера Microsoft Internet Explorer выполните следующее (инструкции приведены для 8 версии браузера):

- Найдите в строке меню закладку **Сервис** и выберите пункт **Свойства обозревателя**. На экране должно появиться окно *Свойства обозревателя*.
- Перейдите в окне *Свойства обозревателя* на закладку *Дополнительно* и убедитесь, что в списке параметров браузера отмечен пункт **TLS 1.0** (рис. 3.1):

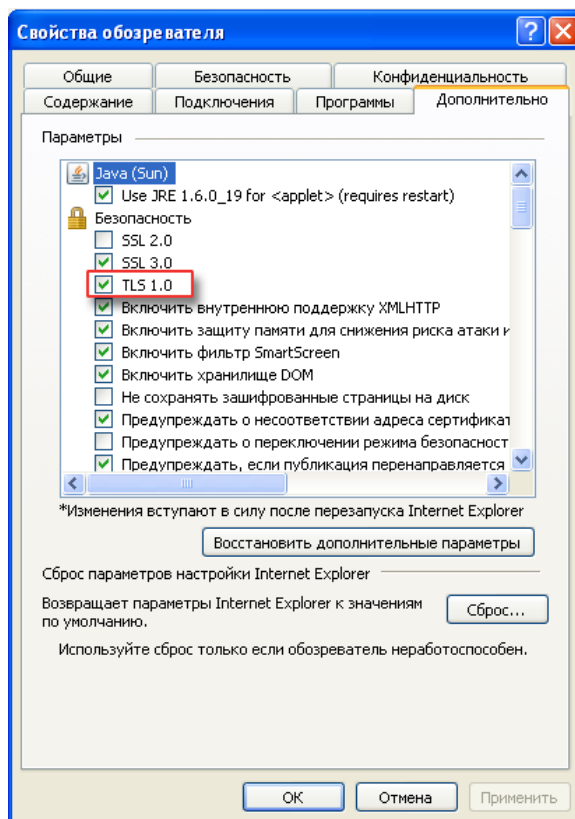



Рис. 3.1 Включение поддержки TLS в браузере

- Перейдите на закладку **Безопасность** и выберите раздел **Надежные узлы** . Нажмите на кнопку **Узлы** (рис. 3.2) и в появившемся диалоге *Надежные узлы* добавьте адрес того веб-ресурса на который выполняется вход по сертификату (рис. 3.3).

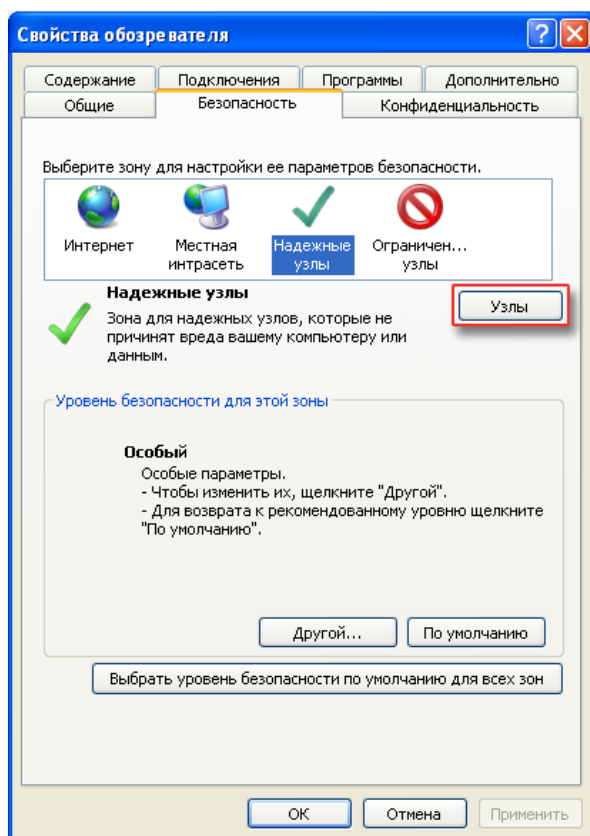


Рис. 3.2 Доступ к диалогу установки доверенных узлов

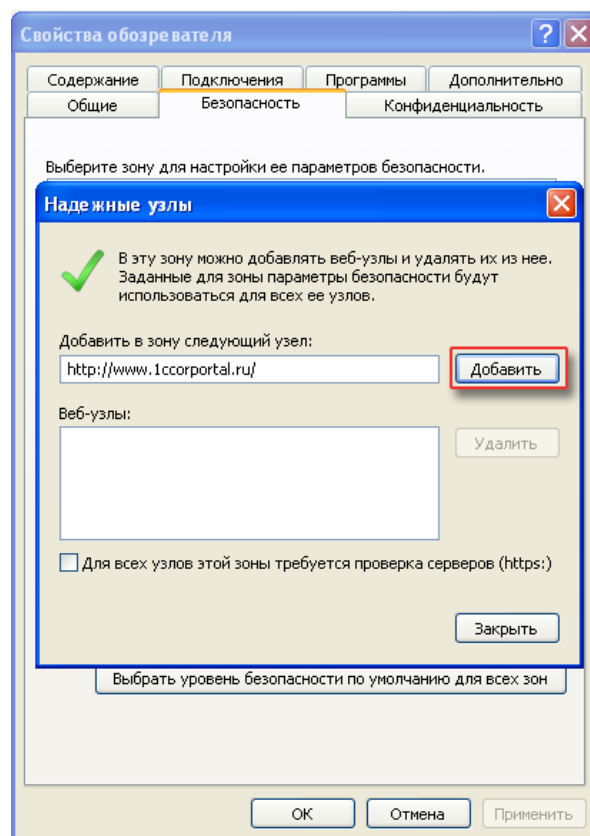


Рис. 3.3 Добавление ссылки на портал в доверенные узлы

Настройка браузера Google Chrome

Для настройки браузера Google Chrome выполните следующее (инструкции приведены для 5 версии браузера):

- Откройте меню **Настройка** и выберите пункт **Параметры** (рис. 3.4)

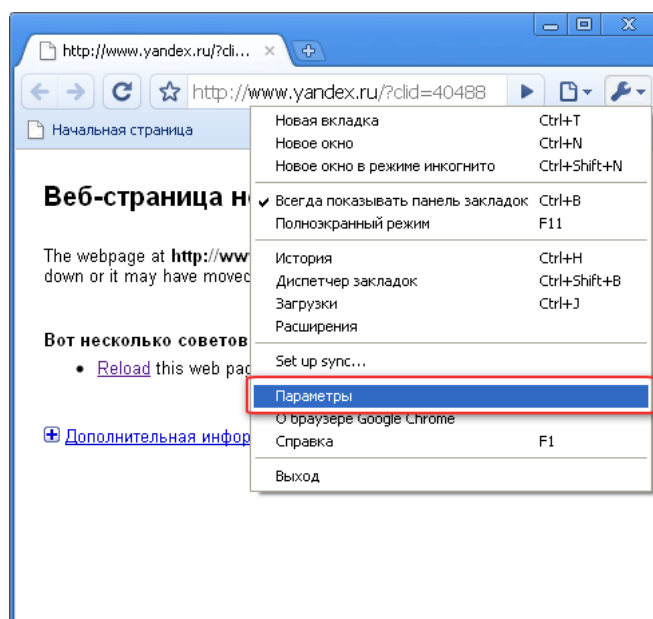


Рис. 3.4 Включение поддержки TLS в браузере

- В открывшемся окне *Параметры Google Chrome* на вкладке **Расширенные** включите режим **Использовать SSL 2.0** (Рис. 3.5):

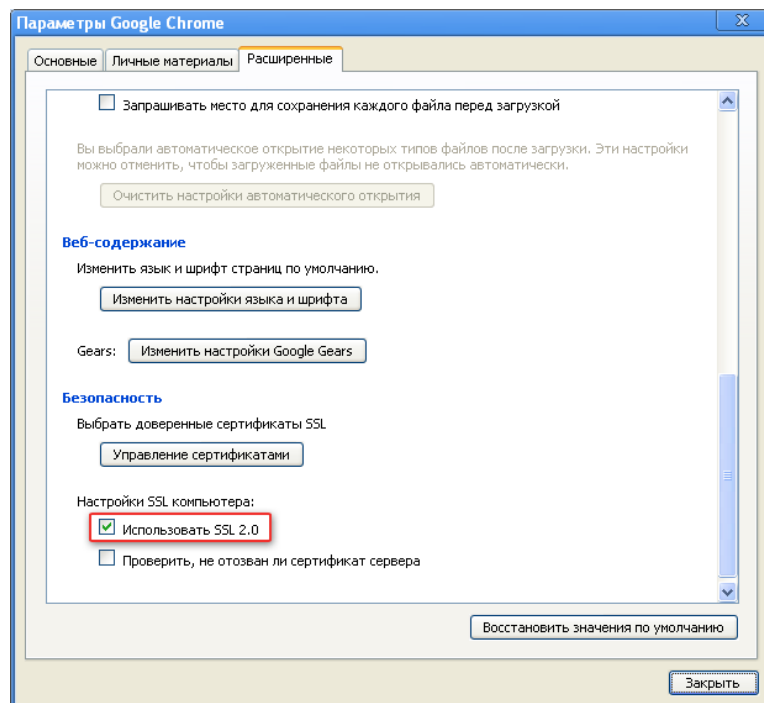


Рис. 3.5 Включение поддержки TLS в браузере

Раздел 4. Коды ошибок модуля

В таблице приводятся коды ошибок и сообщения, появляющиеся при возникновении критических ошибок и блокирующих дальнейшую работу модуля.

№	Код ошибки	Текст сообщения
1	Error #1	В системе не установлен необходимый модуль IBlock
2	Error #2	Ошибка удаления инфоблока или типа инфоблока MAPPING_STORY
3	Error #3	Ошибка удаления инфоблока или типа инфоблока CERT_STORY
4	Error #4	Ошибка создания типа инфоблока MAPPING_STORY
5	Error #5	Ошибка создания типа инфоблока CERT_STORY
6	Error #6	Ошибка создания инфоблока MAPPING_STORY
7	Error #7	Ошибка создания инфоблока CERT_STORY
8	Error #8	Ошибка создания свойств инфоблока MAPPING_STORY
9	Error #9	Ошибка создания свойств инфоблока CERT_STORY
10	Error #10	Не завершена установка модуля trusted.tbstart
11	Error #11	Инфоблок хранилища не обнаружен
12	Error #12	Не удалось изменить свойства инфоблока
13	Error #13	Не удалось удалить элемент инфоблока
14	Error #14	Ошибка добавления сертификата в инфоблок CERT_STORY
15	Error #15	Ошибка добавления привязки в инфоблоке MAPPING_STORY
16	Error #16	Ошибка удаления сертификата из хранилища CERT_STORY
17	Error #17	Ошибка активации сертификата
18	Error #18	Ошибка деактивации сертификата
19	Error #19	Ошибка проверки корректности сертификата
20	Error #20	Ошибка получения опций, установленных по умолчанию