

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
АВТОМАТИЧЕСКАЯ УСТАНОВКА МОДУЛЯ ИЗ MARKETPLACE	10
УСТАНОВКА МОДУЛЯ ВРУЧНУЮ.....	11
НАСТРОЙКА ПАРАМЕТРОВ АУТЕНТИФИКАЦИИ	12
УДАЛЕНИЕ МОДУЛЯ	15
Раздел 3. Визуальные компоненты модуля.....	16
УСТАНОВКА ШАБЛОНА ФОРМЫ АУТЕНТИФИКАЦИИ	16
УДАЛЕНИЕ ШАБЛОНА ФОРМЫ АУТЕНТИФИКАЦИИ	16
Раздел 4. Настройки браузеров	17
НАСТРОЙКА БРАУЗЕРА MICROSOFT INTERNET EXPLORER	17
НАСТРОЙКА БРАУЗЕРА GOOGLE CHROME	18
Раздел 5. Пример организации входа по сертификату на портал 1С Битрикс 20	
Раздел 6. Лицензионное соглашение	21

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 набор 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

Имеется два способа установки модуля: установка из 1С Bitrix Marketplace и скачивание архива модуля с репозитория www.trusdet.ru и установка его вручную.

Автоматическая установка модуля из Marketplace

Модуль «TrustedBitrix Start» версии 1.0.0 является бесплатным продуктом, поэтому клиенты смогут его установить 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**.

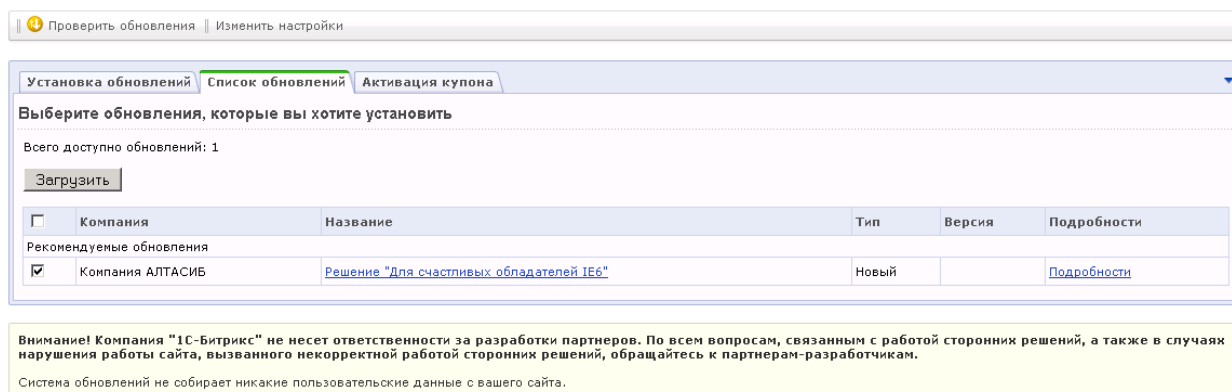
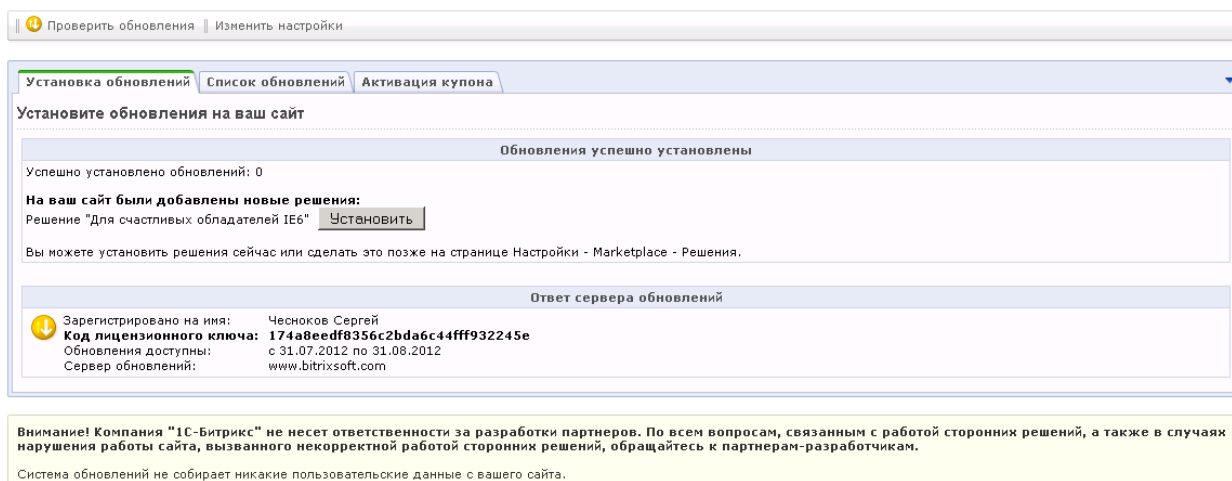


Рис. 2.1 Страница загрузки модуля из Marketplace

- В открывшемся окне ознакомьтесь с соглашением об использовании (содержание лицензионного соглашения представлено в п.7).
- После успешной загрузки модуля его можно установить (рис.2.2).



- После окончания установки новый модуль **Авторизация по сертификату** будет добавлен в общий список модулей (Рис. 2.):

Название	Версия	Дата обновления	Статус	Действие
Главный модуль Ядро продукта с технологией "SiteUpdate".	11.0.10	09.12.2011	Установлен	
AD/LDAP интеграция (ldap) Модуль для работы с Active Directory и LDAP.	11.0.0	03.10.2011	Установлен	Удалить
CRM (crm) Модуль дает возможность создания CRM	11.0.3	21.12.2011	Установлен	Удалить
DAV (dav) Модуль поддержки доступа к объектам и коллекциям	10.0.4	29.04.2011	Установлен	Удалить
Wiki (wiki) Модуль дает возможность ведения wiki-страниц на сайте.	11.0.4	06.12.2011	Установлен	Удалить
XMPP сервер (xmpp) Модуль позволяет использовать Jabber-клиенты для общения внутри корпоративного портала	11.0.0	19.10.2011	Установлен	Удалить
Авторизация по сертификату (TrustedBitrix) Модуль дает возможность авторизоваться по RSA-сертификату	1.0.0	13.04.2012	Установлен	Удалить

Рис. 2.3 Установленный модуль в списке

Установка модуля вручную

Чтобы установить модуль вручную выполните следующие действия:

- Необходимо скопировать архив с исходными текстами модуля **Авторизация по сертификату** (архив можно скачать с репозитория продуктов ООО «Цифровые технологии» <http://www.trusted.ru/support/downloads/?product=3357>) в каталог bitrix/modules/. При отображении общего списка модулей он будет присутствовать в нем под названием «**Авторизация по сертификату**» (рис. 2.4).

Название	Версия	Дата обновления	Статус	Действие
Главный модуль Ядро продукта с технологией "SiteUpdate".	11.0.10	09.12.2011	Установлен	
AD/LDAP интеграция (ldap) Модуль для работы с Active Directory и LDAP.	11.0.0	03.10.2011	Установлен	Удалить
CRM (crm) Модуль дает возможность создания CRM	11.0.3	21.12.2011	Установлен	Удалить
DAV (dav) Модуль поддержки доступа к объектам и коллекциям	10.0.4	29.04.2011	Установлен	Удалить
Wiki (wiki) Модуль дает возможность ведения wiki-страниц на сайте.	11.0.4	06.12.2011	Установлен	Удалить
XMPP сервер (xmpp) Модуль позволяет использовать Jabber-клиенты для общения внутри корпоративного портала	11.0.0	19.10.2011	Установлен	Удалить
Авторизация по сертификату (TrustedBitrix) Модуль дает возможность авторизоваться по RSA-сертификату	1.0.0	13.04.2012	Не установлен	Установить

Рис. 2.4 Отображение модуля в разделе установки

- Нажмите на кнопку **Установить** для запуска мастера установки. Мастер установки является многошаговым. На первом шаге для модуля организуются инфоблоки. Если модуль устанавливается впервые, то инфоблоки создаются заново. Если инфоблоки с данными были оставлены с предыдущих установок модуля, то можно выбрать вариант использования существующих. При успешной установке модуля должно появиться сообщение, представленное на рис. 2.5.

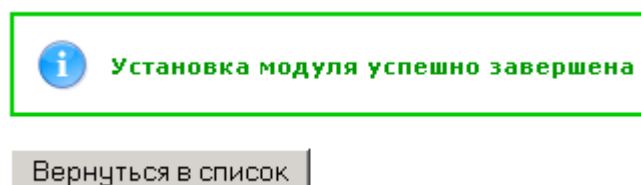


Рис. 2.5 Успешная установка модуля на портал

- После установки модуля (рис. 2.6), в левой панели меню должен появиться соответствующий пункт (рис. 2.7) через который можно выполнить переход к таблице настройки параметров аутентификации пользователей.

Название	Версия	Дата обновления	Статус	Действие
Главный модуль Ядро продукта с технологией "SiteUpdate".	11.0.10	09.12.2011	Установлен	
AD/LDAP интеграция (ldap) Модуль для работы с Active Directory и LDAP.	11.0.0	03.10.2011	Установлен	Удалить
CRM (crm) Модуль дает возможность создания CRM	11.0.3	21.12.2011	Установлен	Удалить
DAV (dav) Модуль поддержки доступа к объектам и коллекциям	10.0.4	29.04.2011	Установлен	Удалить
Wiki (wiki) Модуль дает возможность ведения wiki-страниц на сайте.	11.0.4	06.12.2011	Установлен	Удалить
XMPP сервер (xmpp) Модуль позволяет использовать Jabber-клиенты для общения внутри корпоративного портала	11.0.0	19.10.2011	Установлен	Удалить
Авторизация по сертификату (TrustedBitrix) Модуль дает возможность авторизоваться по RSA-сертификату	1.0.0	13.04.2012	Установлен	Удалить

Рис. 2.6 Установленный модуль Аутентификации по TLS

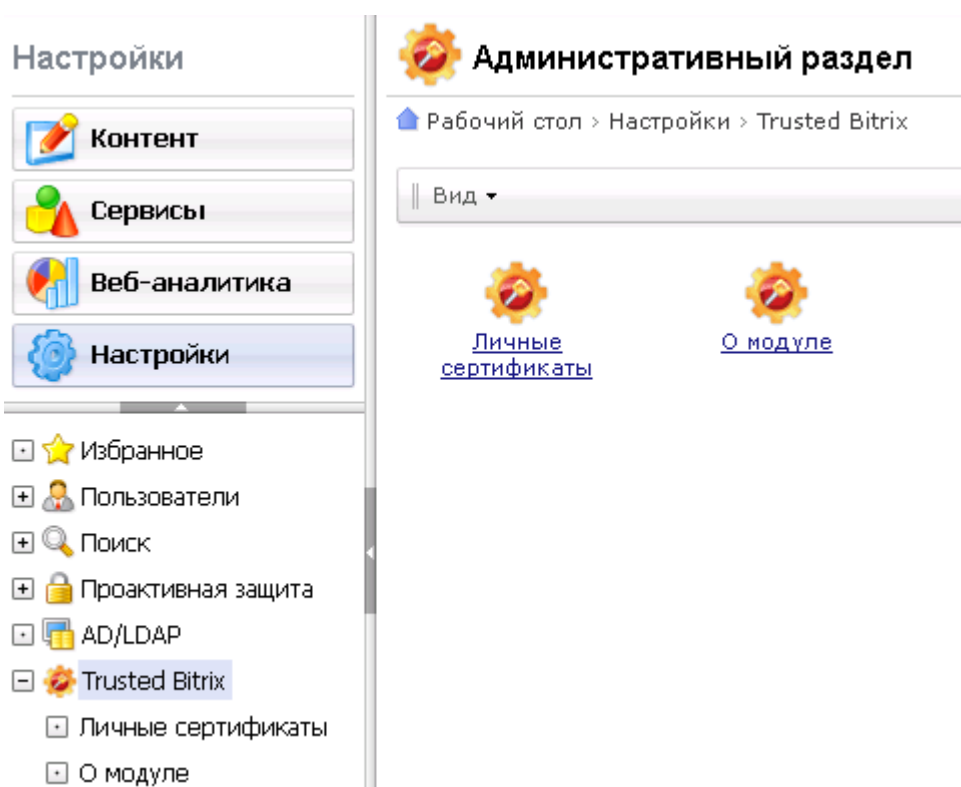


Рис. 2.7 Добавление пункта меню для доступа к настройкам модуля Trusted Bitrix

Настройка параметров аутентификации

Для только что установленного модуля необходимо выполнить настройку параметров авторизации пользователей портала. Для этого через пункт меню **Личные сертификаты** нужно перейти таблице личных сертификатов аутентификации пользователям сайта (рис. 2.8).

Список пользователей

Рабочий стол > Настройки > Trusted Bitrix > Личные сертификаты

Дополнительно

Найти: Компания

Найти Отменить

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.titov@example.com	(0) [+]
469	Александр	Сюгаев		a.syugaev@example.com	(0) [+]

Рис. 2.9 Таблица добавления сертификатов аутентификации пользователям

В колонке Сертификаты имеются ссылка на список привязанных к пользователю сертификатов (обозначается их количеством) и ссылка на добавление нового сертификата.

На странице добавления сертификата указывается кому назначается данный сертификат и предлагается выполнить выбор файла *.cer через диалог выбора файла (рис. 2.10). 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

Добавление нового сертификата

Тело сертификата: E:\Documents and Settings\... Обзор...

Активация сертификата: ☒

Сохранить Применить Отменить

*Поля, обязательные для заполнения.

Рис. 2.10. 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.

Важно! При удалении пользователя данные из хранилища сертификатов (сертификаты привязанные к ID пользователя) безвозвратно удаляются. При добавлении пользователя для него необходимо загрузить необходимые сертификаты.

Сертификаты пользователя отображаются списком (рис. 2.11) в котором также отображается их статус.

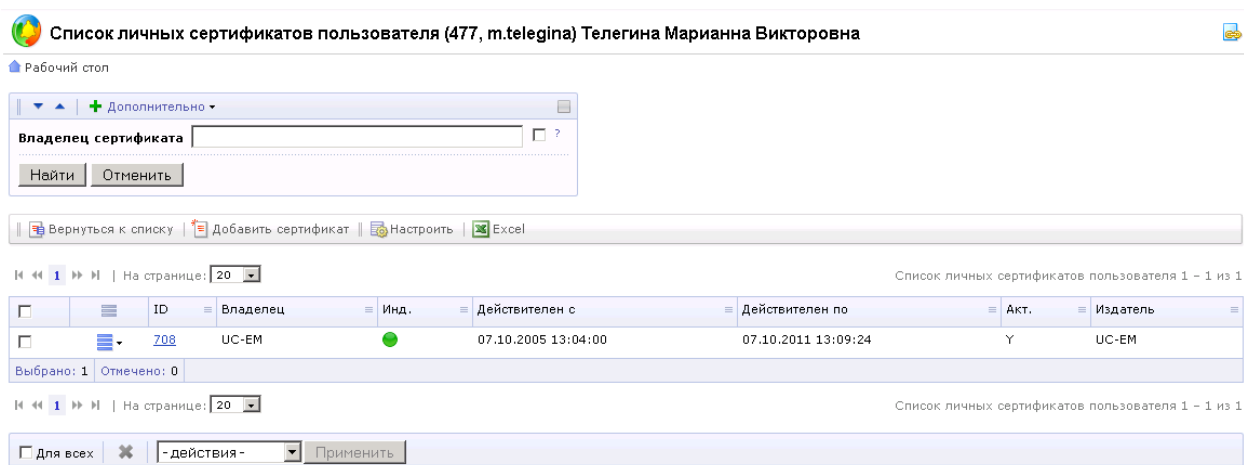


Рис. 2.11. Список сертификатов, привязанных к пользователю

Каждый из сертификатов аутентификации пользователей имеет определенные свойства. Эти свойства можно посмотреть и отредактировать вручную (рис. 2.12).

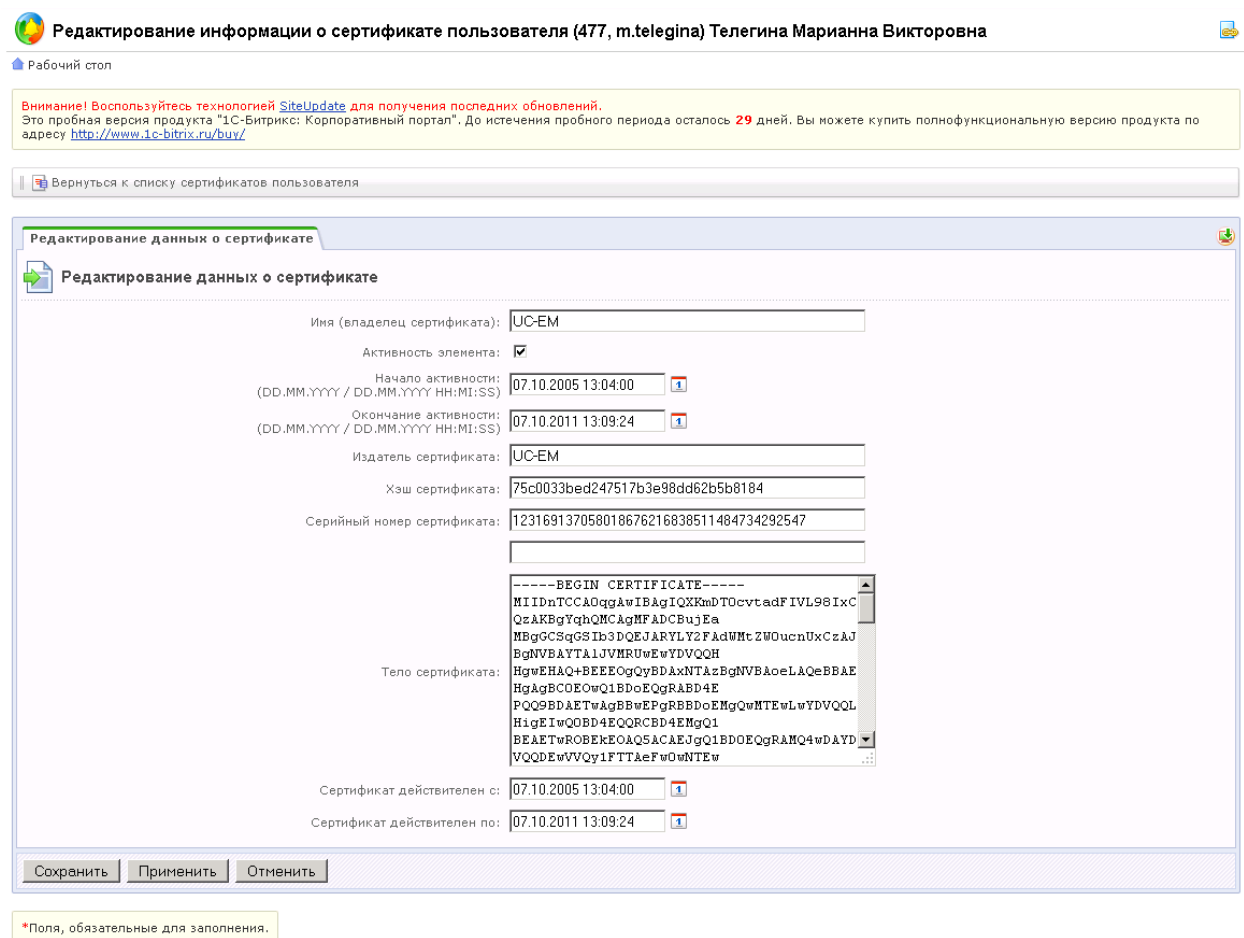


Рис. 2.12. Форма просмотра/редактирования свойств сертификата


Удаление модуля

Удаление модуля производится через страницу отображения списка установленных модулей, нажатием кнопки **Удалить** (рис. 2.8).

Название	Версия	Дата обновления	Статус	Действие
Главный модуль Ядро продукта с технологией "SiteUpdate".	11.0.10	09.12.2011	Установлен	
AD/LDAP интеграция (ldap) Модуль для работы с Active Directory и LDAP.	11.0.0	03.10.2011	Установлен	Удалить
CRM (crm) Модуль дает возможность создания CRM	11.0.3	21.12.2011	Установлен	Удалить
DAV (dav) Модуль поддержки доступа к объектам и коллекциям	10.0.4	29.04.2011	Установлен	Удалить
Wiki (wiki) Модуль дает возможность ведения wiki-страниц на сайте.	11.0.4	06.12.2011	Установлен	Удалить
XMPP сервер (xmpp) Модуль позволяет использовать Jabber-клиенты для общения внутри корпоративного портала	11.0.0	19.10.2011	Установлен	Удалить
Авторизация по сертификату (TrustedBitrix) Модуль дает возможность авторизоваться по RSA-сертификату	1.0.0	13.04.2012	Установлен	Удалить

Рис. 2.7 Удаление модуля

⚠ Важно! Удаление модуля с сервера сопровождается удалением всех установленных компонент и внесенных в хранилище сертификатов, если снять отметку Сохранять инфоблоки (рис. 2.8).

 **Внимание! Будет произведено удаление модуля Trusted Bitrix.**

Сохранить инфоблоки модуля и данные в них?

☒ Сохранить инфоблоки.

[Удаление модуля](#)

Рис. 2.8 Режим сохранения/удаления данных при удалении модуля

Раздел 3. Визуальные компоненты модуля

Установка шаблона формы аутентификации

В стандартную поставку модуля входят компоненты формы аутентификации стандартных шаблонов, таких как modern, classic и system.

Для установки компонента необходимо перейти на закладку **Разработка** в панели администратора, кликнуть двойным щелчком на стандартный компонент формы аутентификации. В окне *Параметры компонента* выбрать соответствующий шаблон сайта с суффиксом «.trusted» и нажать **Сохранить** (рис. 3.1).

Рис. 3.1 Выбор шаблона для модуля TrustedBitrixLogin

На главной странице в компоненте аутентификации должна появиться дополнительная ссылка **Вход по сертификату**.

Удаление шаблона формы аутентификации

Для удаления компонента необходимо перейти на закладку **Разработка** в панели администратора, кликнуть двойным щелчком на стандартный компонент формы аутентификации. В окне *Параметры компонента* выбрать соответствующий шаблон сайта без суффикса «.trusted» и нажать **Сохранить**.

Раздел 4. 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. 1.1):

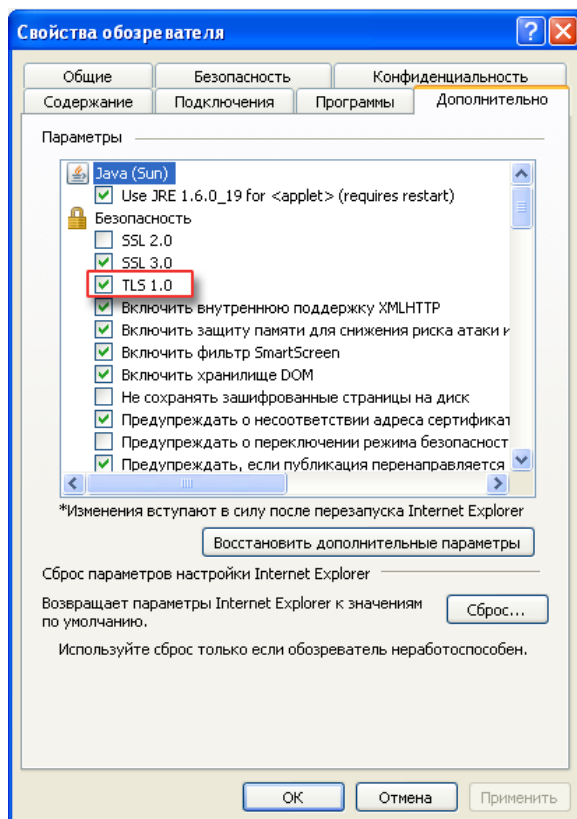



Рис. 1.1 Включение поддержки TLS в браузере

- Перейдите на закладку **Безопасность** и выберите раздел **Надежные узлы** . Нажмите на кнопку **Узлы** (рис. 1.2) и в появившемся диалоге *Надежные узлы* добавьте адрес того веб-ресурса на который выполняется вход по сертификату (рис. 1.3).

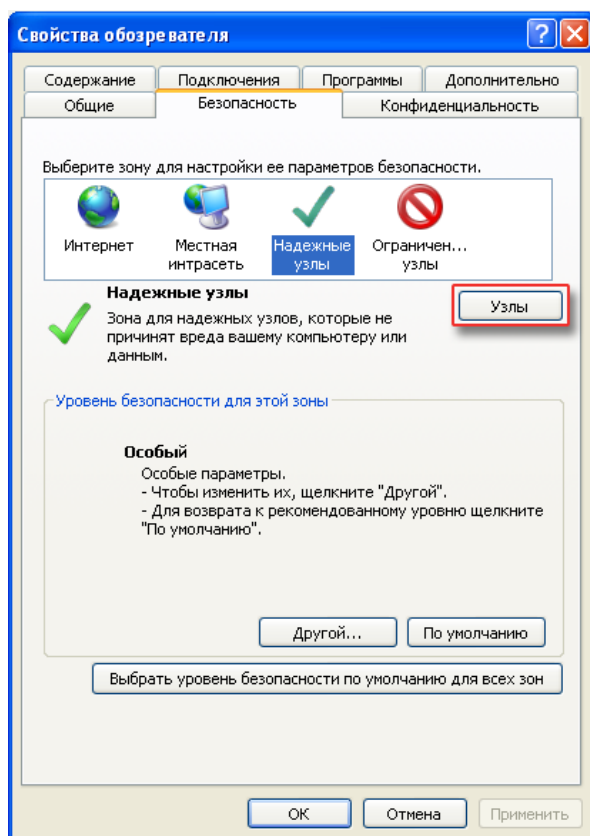


Рис. 1.2 Доступ к диалогу установки доверенных узлов

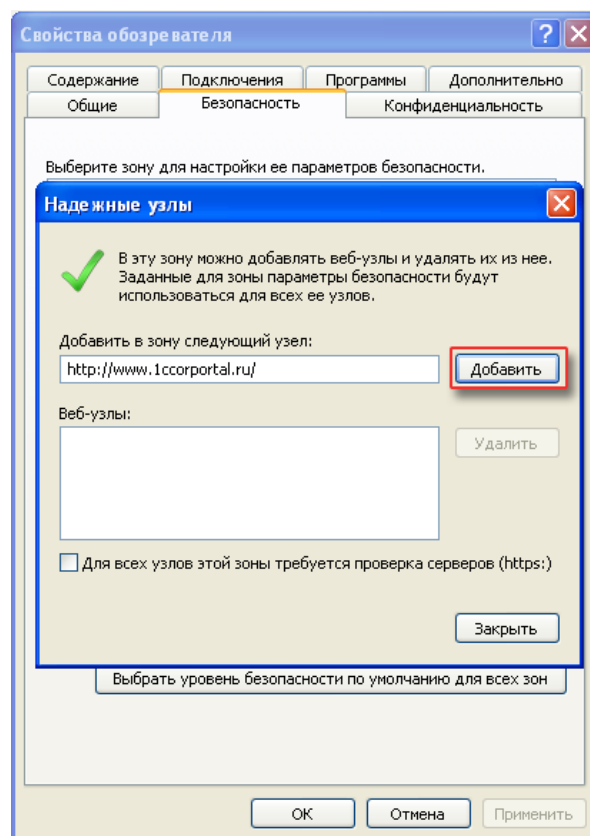


Рис. 1.3 Добавление ссылки на портал в доверенные узлы

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. 1.4)

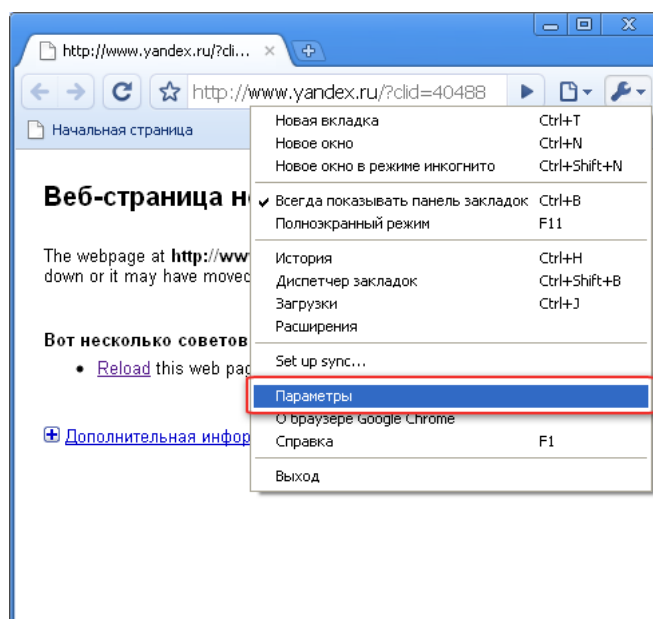


Рис. 1.4 Включение поддержки TLS в браузере

- В открывшемся окне *Параметры Google Chrome* на вкладке **Расширенные** включить режим **Использовать SSL 2.0** (Рис. 1.5):

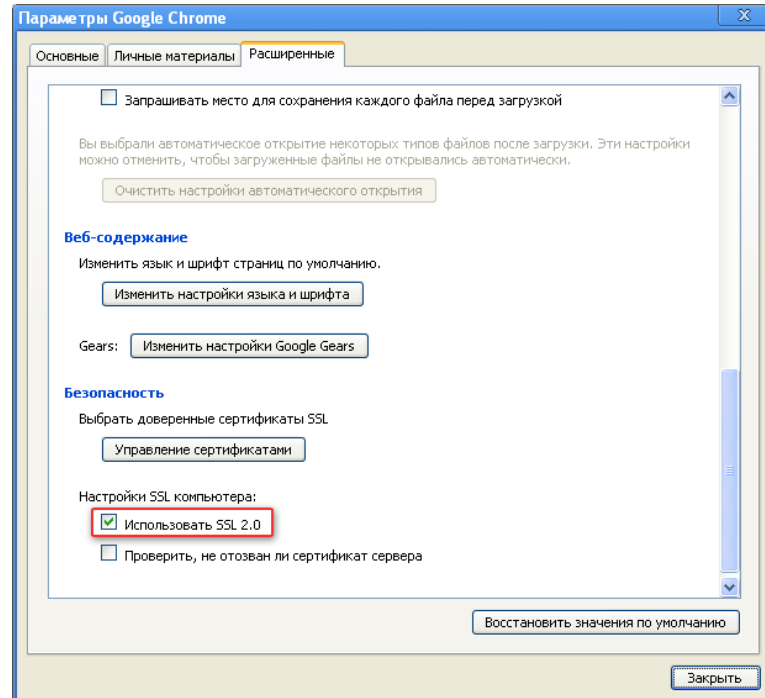


Рис. 1.5 Включение поддержки TLS в браузере

Раздел 5. Пример организации входа по сертификату на портал 1С Битрикс

Для входа по сертификату на главной странице портала необходимо нажать на ссылку «Вход по сертификату» в форме аутентификации (в данном случае справа вверху), появится окно с выбором сертификата, необходимо выбрать сертификат и нажать кнопку «ОК»

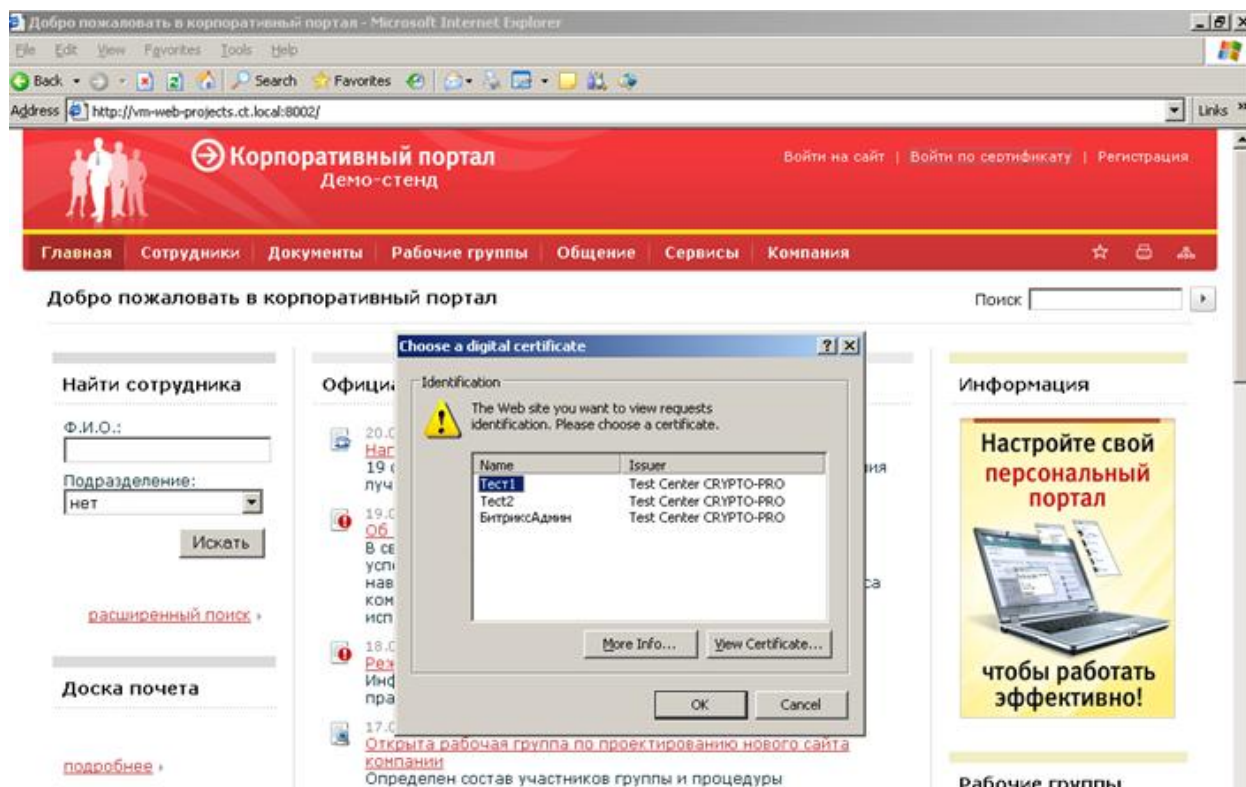


Рис. 3.1 Выбор сертификата аутентификации

Если аутентификация пройдена успешно, появится главное окно портала и панель пользователя.

Если предъявленный сертификат не имеет соответствующего контейнера с закрытым ключом, тогда соединение обрывается и пользователю показывается стандартная ошибка «404 Страница не найдена».

Если сертификат отсутствует в БД 1С-Битрикс пользователю будет выдано сообщение «Пользователь не аутентифицирован по сертификату».

Раздел 6. Лицензионное соглашение

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

НА ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ ДЛЯ ЭВМ

«Авторизация по сертификату»

Уважаемый Пользователь! Перед началом установки, копирования либо иного использования Модуля внимательно ознакомьтесь с условиями настоящего Соглашения, являющегося стандартной формой договора присоединения и заключаемого в письменной или иной форме, предусмотренной действующим законодательством Российской Федерации. Если вы не согласны с условиями настоящего Соглашения, вы не можете использовать Модуль. Установка, запуск или иное начало использования Модуля означает Ваше полное согласие со всеми условиями настоящего Соглашения и его надлежащее заключение в порядке, предусмотренном в пункте 3 статьи 1286 Гражданского Кодекса Российской Федерации. Настоящее Соглашение является юридически обязательным соглашением, если Вы не согласны принять на себя его условия, Вы не имеете права устанавливать Модуль и должны удалить все его компоненты со своего компьютера (ЭВМ).

Настоящее Лицензионное соглашение (далее – Соглашение) заключается между ООО «Цифровые технологии» (далее – Лицензиар) и Пользователем (любым физическим лицом, индивидуальным предпринимателем, юридическим лицом (далее – Пользователь) Программы для ЭВМ «Авторизация по сертификату» (далее – Модуль).

Основные термины настоящего Соглашения:

Модуль – программа для ЭВМ «Авторизация по сертификату» (как в целом, так и ее компоненты), исключительные имущественные права на которую на территории, определенной в п. 1.5. Соглашения, принадлежат Лицензиару;

Демо-версия Модуля – версия Модуля «Авторизация по сертификату», в которой установлено ограничение по сроку ее использования и которая предназначена исключительно для самостоятельного ознакомления Пользователем с функциональными возможностями Модуля на условиях настоящего Соглашения и не предназначена для продажи или иного отчуждения третьим лицам.

1. Предмет СОГЛАШЕНИЯ

1.1. В порядке и на условиях, предусмотренных настоящим Соглашением, Лицензиар предоставляет Пользователю право использования Модуля (простая неисключительная лицензия), реализуемое путем установки (инсталляции) и запуска Пользователем Модуля в соответствии с его технической документацией и условиями настоящего Соглашения.

1.2. Все положения настоящего Соглашения распространяются как на Модуль в целом, так и на его отдельные компоненты. Модуль лицензируется как единая программа для ЭВМ, его компоненты не могут быть разделены и использоваться на разных компьютерах (ЭВМ).

1.3. Настоящее Соглашение заключается до или непосредственно в момент начала использования Модуля и действует на протяжении всего срока действия исключительного права Лицензиара на Модуль, при условии надлежащего выполнения Пользователем условий настоящего Соглашения.

1.4. Лицензиар предоставляет Пользователю право использования Модуля на территории следующих стран Российская Федерация, Украина, Республика Беларусь, Республика Казахстан, Киргизская Республика, Республика Узбекистан, Туркменистан, Республика Таджикистан, Литовская Республика, Латвийская Республика, Эстонская Республика, Республика Молдова, Грузия, Республика Армения, Республика Азербайджан на условиях и в порядке, предусмотренных действующим законодательством Российской Федерации и настоящим Соглашением.

2. Авторские права

2.1. Модуль является результатом интеллектуальной деятельности и объектом авторских прав как программа для ЭВМ, которые регулируются и защищены законодательством Российской Федерации об интеллектуальной собственности и нормами международного права.

2.2. Модуль содержит коммерческую тайну и иную конфиденциальную информацию, принадлежащую Лицензиару. Любое использование Модуля в нарушение условий настоящего Соглашения рассматривается как нарушение прав Лицензиара и является достаточным основанием для лишения Пользователя предоставленных по настоящему Соглашению прав.

2.3. Лицензиар гарантирует, что обладает всеми правами использования Модуля, включая документацию к ней, необходимыми для предоставления Пользователю прав на использование Модуля по настоящему Соглашению.

2.4. В случае нарушения авторских прав предусматривается ответственность в соответствии с действующим законодательством Российской Федерации.

3. Условия использования МОДУЛЯ и ограничения

3.1. Настоящее Соглашение предоставляет право установки (инсталляции), запуска и использования законно приобретенной одной копии Модуля в рамках его функциональных возможностей на одном компьютере (ЭВМ).

3.2. Пользователь имеет право, уведомив Лицензиара, однократно уступить (передать) свои права и обязанности по настоящему Соглашению другому Пользователю в полном

объеме, кроме предусмотренного в настоящем пункте Соглашения права последующей уступки (передачи) прав по настоящему Соглашению другим Пользователям, что ограничивает возможность повторной передачи прав по настоящему Соглашению. Указанная уступка (передача) прав и обязанностей осуществляется при условии полного и безоговорочного согласия нового пользователя со всеми положениями и условиями настоящего Соглашения. Передавая права использования Модуля, Пользователь обязуется полностью уничтожить все копии Модуля, установленные на компьютерах Пользователя, включая резервные копии. Пользователь обязан предоставить полные данные нового Пользователя для перерегистрации на него прав использования Модуля в соответствии с настоящим Соглашением.

Уступка (передача) прав по настоящему Соглашению не может быть осуществлена (i) косвенно или через какое-либо третье лицо, а также (ii) в случае использования Пользователем Демо-версии Модуля, в отношении которой устанавливается полный запрет отчуждения первоначальным Пользователем.

3.3. Пользователь вправе изменять, добавлять или удалять любые файлы приобретенного Модуля только в случаях, предусмотренных Законодательством Российской Федерации об авторском праве.

3.4. Запрещается удалять любую информацию об авторских правах.

3.5. Запрещается любое использование Модуля, противоречащее действующему законодательству Российской Федерации.

4. Ответственность сторон

4.1. За нарушение условий настоящего Соглашения наступает ответственность, предусмотренная законодательством Российской Федерации.

4.2. Лицензиар не несет ответственности перед Пользователем за любой ущерб, любую потерю прибыли, информации или сбережений, связанных с использованием или с невозможностью использования Модуля, даже в случае предварительного уведомления со стороны Пользователя о возможности такого ущерба, или по любому иску третьей стороны.

5. Ограниченная гарантия

5.1. Лицензиар предоставляет Пользователю право получения Технической поддержки консультирования Пользователя по вопросам, связанным с функциональностью Модуля, особенностями установки и эксплуатации на стандартных конфигурациях поддерживаемых (популярных) операционных, почтовых и иных систем на условиях и в течение всего срока действия настоящего Соглашения, а также в соответствии с

действующим законодательством Российской Федерации без выплаты дополнительного вознаграждения.

5.2. Лицензиар предоставляет Пользователю право получения и использования в соответствии с настоящим Соглашением обновлений (новых версий) Модуля в течение всего срока действия настоящего Соглашения с момента приобретения прав на использование Модуля без выплаты дополнительного вознаграждения. Все обновления Модуля являются ее неотъемлемой частью и используются исключительно вместе с Модулем как единая программа для ЭВМ в порядке, предусмотренном в настоящем Соглашении, если иные условия использования таких обновлений не будут предусмотрены в отдельном лицензионном договоре.

5.3. Если при использовании Модуля будут обнаружены ошибки, Лицензиар обязуется исправить их в максимально короткие сроки и выпустить новую, исправленную версию Модуля. Стороны соглашаются, что точное определение срока устранения ошибки не может быть установлено, так как Модуль тесно взаимодействует с другими программами для ЭВМ сторонних разработчиков, операционной системой и аппаратными ресурсами компьютера Пользователя, и работоспособность и время устранения проблем в полной мере не зависят только от Лицензиара.

5.4. В случае несоблюдения любого из пунктов раздела 3 настоящего Соглашения, Пользователь автоматически теряет право на получение обновлений (новых версий) Модуля.

6. Действие, изменение и расторжение СОГЛАШЕНИЯ

6.1. Настоящее Соглашение заключено и подлежит толкованию в соответствии с законодательством Российской Федерации.

6.2. В случае нарушения Пользователем условий настоящего Соглашения по использованию Модуля Лицензиар имеет право в одностороннем порядке расторгнуть настоящее Соглашение, уведомив об этом Пользователя.

6.3. При расторжении настоящего Соглашения Пользователь обязан прекратить использование Модуля полностью и уничтожить все копии Модуля, установленные на компьютерах Пользователя, включая резервные копии и все компоненты Модуля.

6.4. Пользователь вправе расторгнуть настоящее Соглашение в любое время, полностью удалив Модуль

6.5. В случае если компетентный суд признает какие-либо положения настоящего Соглашения недействительными, Соглашение продолжает действовать в остальной части.

6.6. Настоящее Соглашение также распространяется на все обновления (новые версии) Модуля, предоставляемые Пользователю в течение срока его действия, если только при

обновлении Модуля Пользователю не будет предложено ознакомиться и принять отдельный лицензионный договор или дополнения к настоящему Соглашению.

7. Контактная информация Лицензиара

ООО «Цифровые технологии»

Контактные данные: <http://www.trusted.ru>