

# Защита при передаче данных в сети с помощью SSL

## ОЗНАКОМИТЕЛЬНОЕ РУКОВОДСТВО ПО СЕРТИФИКАТАМ SSL, *принципу их действия и п рименению...*

1. Обзор
2. Что такое SSL
3. Как определить, является ли Web-узел защищенным
4. Как выглядит сертификат SSL
5. Предупреждения браузера относительно безопасности
6. Как создается сеанс SSL
7. Открытые и секретные ключи
8. Применения SSL
9. Когда оправдано использование сертификатов SSL
10. Решения thawte на основе SSL-сертификатов
11. Проверка SSL-сертификатов на Вашем Web-сервере
12. Знак надежного Web-узла *thawte*
13. Полезные адреса URL
14. О роли thawte
15. Значение аутентификации
16. Способы связи с *thawte*
17. Глоссарий терминов

## 1. Обзор

*thawte* является ведущим поставщиком SSL-сертификатов по всему миру. Используя SSL-сертификат *thawte* на Web-сервере своей компании, Вы можете безопасно собирать важную информацию по сети и расширить коммерческие возможности, гарантируя своим заказчикам безопасность транзакций.

Цель данного руководства - ознакомить с защитой с помощью протокола SSL и с основными принципами его работы. Дополнительно руководство содержит обсуждение различных применений сертификатов SSL и, соответственно, их развертывания, а также сведения о том, как проверить SSL-сертификаты на Вашем Web-сервере.

## 2. Что такое SSL

Протокол защищенных сокетов (SSL) был разработан компанией Netscape в 1996 г. и быстро превратился в наиболее предпочтительный способ защиты при передаче данных через Интернет. SSL является составной частью большинства Web-браузеров и Web-серверов и использует систему шифрования по открытому и секретному ключу, разработанную RSA.

Для установления соединения SSL в соответствии с протоколом SSL требуется, чтобы на сервере был установлен цифровой сертификат. Цифровой сертификат - это электронный файл, который однозначно идентифицирует отдельных пользователей и серверы. Цифровые сертификаты выполняют роль цифрового паспорта или удостоверения, которое обеспечивает аутентификацию сервера перед установлением сеанса SSL. Обычно для подтверждения действительности цифровых сертификатов они подписываются независимыми и надежными сторонними организациями. Подписывающие сертификаты организации называются центрами сертификации (CA). Примером такой организации является *thawte*.

SSL обеспечивает безопасную связь путем объединения следующих двух элементов:

1] Аутентификация –

Цифровой сертификат привязан к определенному домену, и перед выдачей сертификата CA производит ряд проверок подлинности организации, запрашивающей сертификат. Таким образом, сертификат может быть установлен в домене, для которого он был аутентифицирован, что обеспечивает пользователям требуемый уровень гарантии. В различных программных продуктах используются различные уровни аутентификации.

2] Шифрование –

Шифрование - это процесс преобразования информации таким образом, чтобы она была понятна только назначенному получателю. Таким образом формируется основа для обеспечения неприкосновенности и конфиденциальности данных, которая требуется в электронной коммерции.

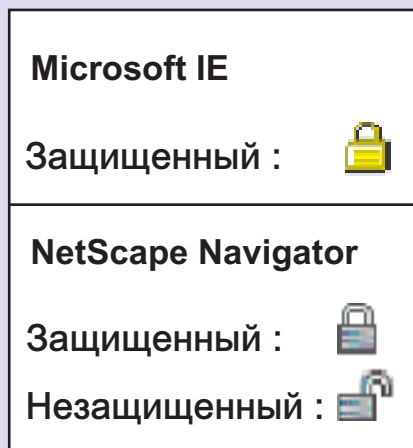
### Важное замечание

Наиболее распространенным применением SSL-сертификатов является защита данных при передаче между Web-браузерами и Web-серверами. Хотя SSL можно использовать для защиты связи между серверами, в этом руководстве работа SSL объясняется на примерах связи между браузером и сервером.

Для получения более полной информации об использовании SSL при связи между серверами обратитесь к представителю *thawte* по продажам.

### 3. Как определить, является ли Web-узел защищенным

Первой подсказкой для выяснения того, защищен ли Web-узел с помощью SSL-сертификата, является значок в виде висячего замка в строке состояния браузера. В браузерах IE для незащищенных страниц значок в виде висячего замка не отображается. Однако после установления сеанса SSL появляется значок в виде висячего замка. В браузере Netscape присутствуют значки “закрытого” и “открытого” висячего замка, обозначающие, соответственно, защищенный и незащищенный Web-узел.



Следующая подсказка содержится в строке адреса. Если между браузером и Web-сервером организовано защищенное соединение, часть “http:” адреса изменится на “https”, например: “<http://www.thawte.com>” изменится на “<https://www.thawte.com>”.

Дополнительно можно определить степень шифрования для отдельного сеанса SSL. В IE для выяснения степени шифрования поместите указатель мыши над значком в виде висячего замка.

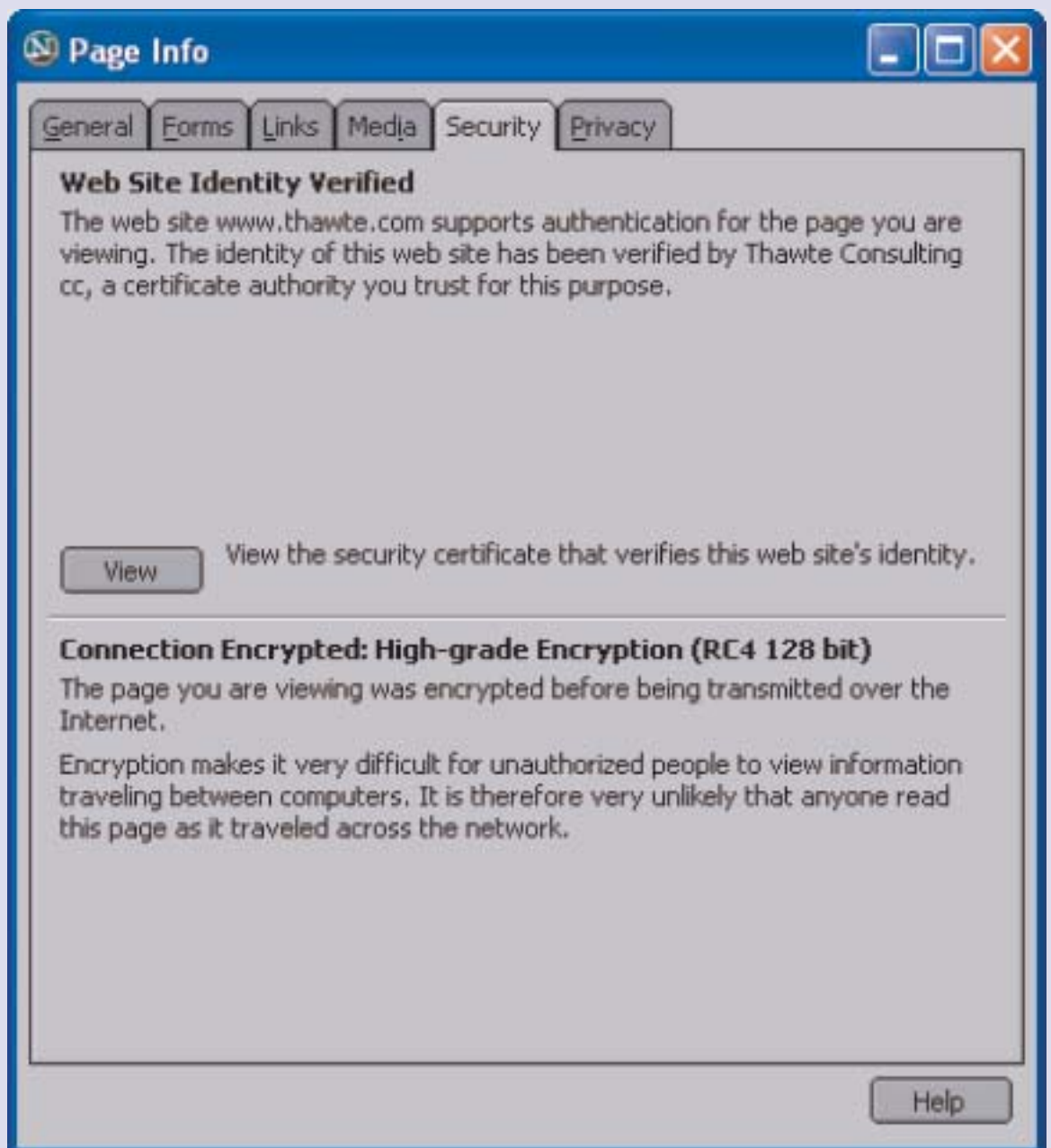
В Netscape дважды щелкните на значке в виде висячего замка для просмотра сертификата. Степень шифрования указана на первой вкладке сертификата.



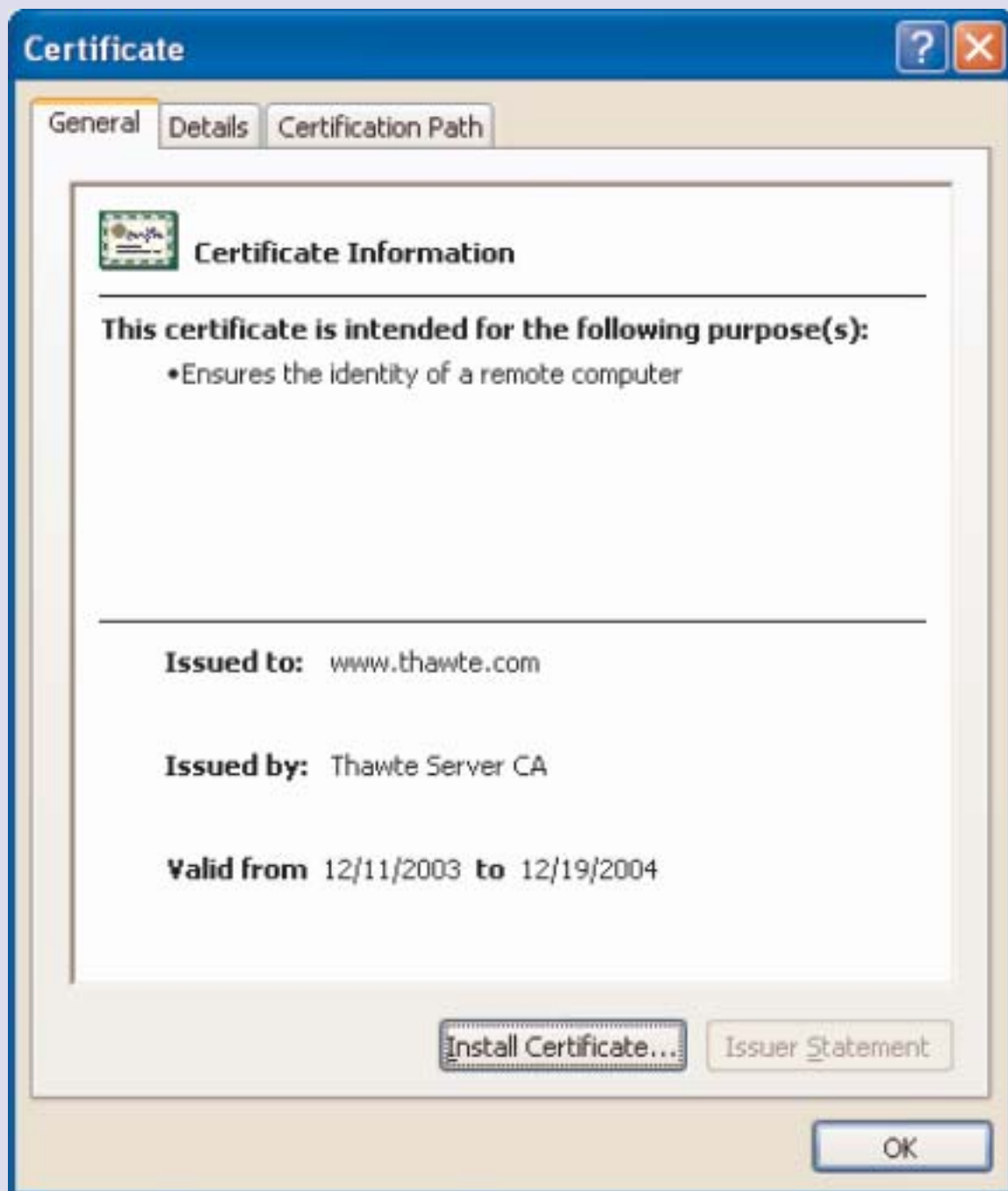
#### 4. Как выглядит сертификат SSL

Для просмотра сертификата Web-узла дважды щелкните на значке в виде закрытого висячего замка, который отображается в нижней строке состояния.

Цифровой сертификат при просмотре браузером Netscape 7.0:



Цифровой сертификат при использовании браузера IE 6.0:



SSL-сертификат для Web-сервера или выданный *thawte* сертификат SGC SuperCert позволяет заказчикам просматривать следующую информацию:

- Домен, для которого выдан сертификат. Заказчики могут убедиться, что SSL-сертификат для Web-сервера выдан именно для данного хоста и домена ([www.mydomain.com](http://www.mydomain.com)).
- Владелец сертификата. Служит дополнительной гарантией, поскольку заказчики могут видеть, с кем они имеют дело.
- Физическое местоположение владельца. Заказчики еще раз убеждаются, что имеют дело с действительной организацией.
- Срок действия сертификата. Эта информация весьма важна, т.к. демонстрирует пользователям, что Ваш цифровой сертификат еще действует.

## 5. Предупреждения браузера относительно безопасности

Браузер снабжен встроенной функцией защиты, которая отображает сообщение с предупреждением при попытке пользователя передать информацию на Web-узел с отсутствующим или ненадлежащим сертификатом.

Ниже приведен пример сообщения с предупреждением, отображаемым в Microsoft IE:



В предыдущем примере предупреждение о защите отображается, поскольку имя домена не соответствует имени домена Web-узла, к которому производится обращение, указывая на то, что Web-узел, на который установлен сертификат, не имеет прав на использование этого сертификата. Другие предупреждения о защите отображаются при истечении срока действия сертификата. В случае, если сертификат подписан неизвестным корневым сертификатом (корневым сертификатом, который не установлен по умолчанию в браузере), также отображается предупреждение.

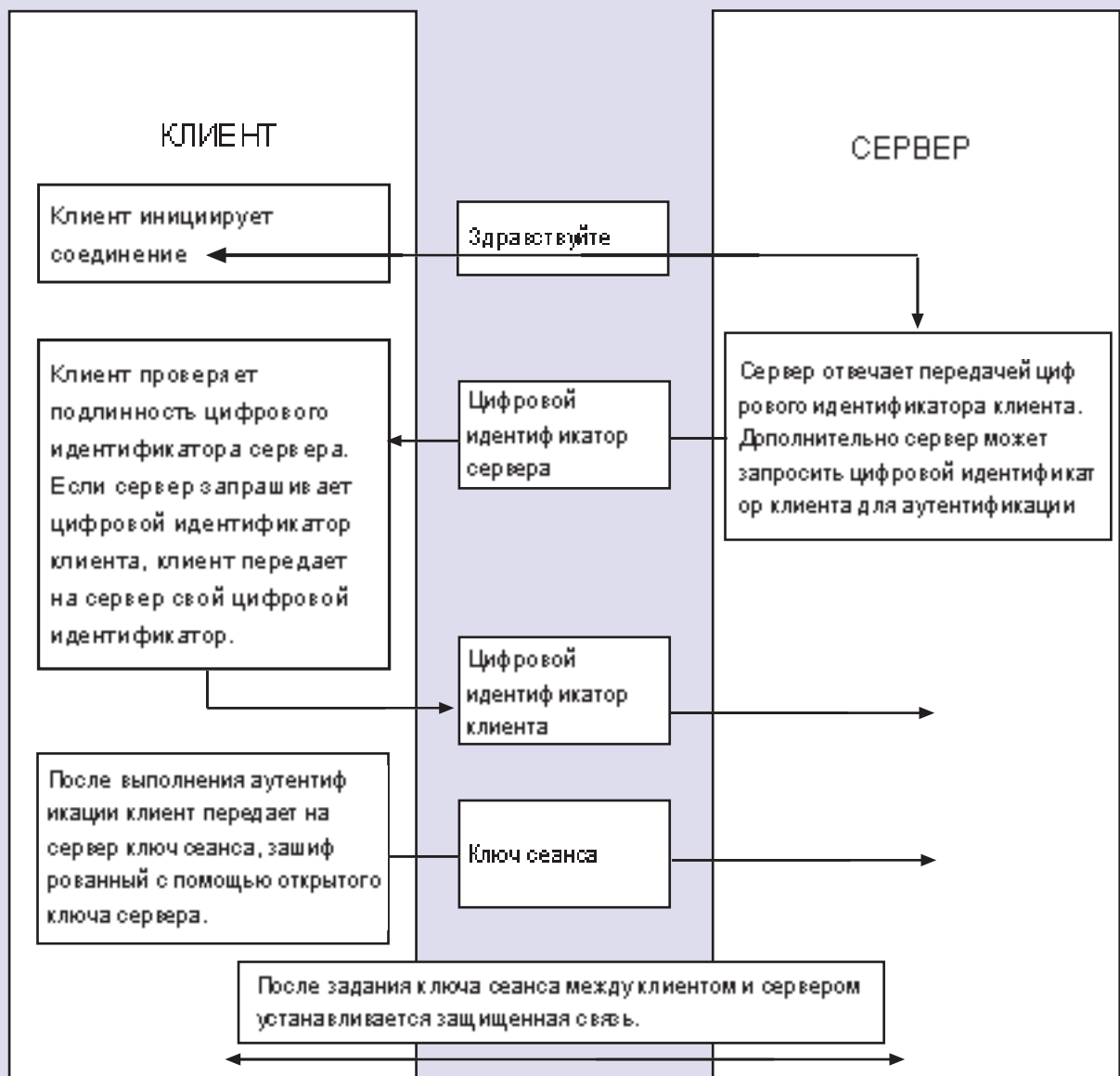
С другой стороны, при доступе пользователя к Web-узлу с действительным сертификатом пользователь информируется о том, что посещаемый им Web-узел имеет цифровой сертификат, выданный известным центром сертификации (CA), например, *thawte*, и все передаваемые пользователем данные будут зашифрованы. Проверив данный сертификат, пользователь может удостовериться, что Web-узел принадлежит действительной легальной компании, и ей принадлежит имя домена, к которому осуществляется доступ.



## 6. Как создается сеанс SSL

При установлении соединения с защищенным Web-сервером, например, с <https://www.thawte.com>, до создания защищенного соединения сервер должен удостоверить свою подлинность для Web-браузера с помощью цифрового сертификата.

На следующей схеме показаны этапы, которые выполняются при создании сеанса SSL:



При выполнении этого процесса Web-браузер производит следующие проверки:

- имя домена в сертификате соответствует домену, с которого этот сертификат передан
- срок действия сертификата не истек
- центр сертификации, которым подписан данный сертификат, является доверенным для данного Web-браузера

Процесс является непрерывным, т.е. пользователь не замечает выполнения указанных выше шагов. Сертификат служит доказательством того, что независимая и надежная сторонняя организация, например, *thawte*, удостоверилась в принадлежности данного домена реальной компании, поэтому домен является надежным. Действительный сертификат обеспечивает заказчикам конфиденциальность при защищенной передаче ими личной информации прошедшей аутентификацию стороне.

## 7. Открытые и секретные ключи

При запросе сертификата Вы генерируете на своем сервере пару ключей - открытый и секретный ключ. Когда пара ключей создается для коммерческого применения, секретный ключ устанавливается на сервер, и очень важно, чтобы посторонние не имели к нему доступа. С помощью секретного ключа создаются цифровые подписи, которые могут эффективно использоваться как электронная печать компании. Необходимо обеспечить максимальную защиту этого ключа. В случае утери секретного ключа дальнейшее использование сертификата невозможно. По этой причине в практике текущего управления ключами считается необходимым создать резервную копию секретного ключа.

Соответствующий открытый ключ устанавливается на Web-сервере как часть цифрового сертификата. Открытый и секретный ключ математически связаны, но не совпадают. Заказчики, которым требуется конфиденциальная связь (с использованием SSL), используют в своем сертификате открытый ключ для шифрования информации перед ее передачей Вам. Этот процесс происходит мгновенно и незаметно для пользователя. Эту информацию можно расшифровать только с помощью секретного ключа, установленного на Web-сервере. Заказчики будут защищены, т.к. любая информация, которую они передают на Ваш сервер, не может быть прочитана посторонними.

## 8. Применения SSL

Существуют две обширные области применения SSL-сертификатов:

### 1] Защита связи между браузером и Web-сервером

В настоящее время защита связи между браузером и Web-сервером является основным применением SSL-сертификатов и наиболее часто используется на Web-узлах электронной коммерции для защиты при передаче данных о платежах. В настоящий момент к данным, которые подлежат засекречиванию, относятся как финансовые данные, так и все сведения, позволяющие установить личность, включая идентификационные номера, номера социальной защиты, а также - все чаще - адреса электронной почты.

### 2] Защита связи между серверами

Все большее число компаний обращаются к SSL-сертификатам для защиты связи между серверами. Эта область применения предоставляет компаниям различные возможности повышения защищенности данных и конфиденциальности в сети. В настоящее время наиболее распространена защита связи между серверами электронной почты, хотя возможна и защита узлов FTP, серверов баз данных и приложений и других серверов.

## 9. Когда оправдано использование сертификатов SSL

Решение об использовании SSL-сертификатов принимается исходя из важности защиты передаваемых по сети данных. Например, если на Вашем Web-узле обрабатываются финансовые транзакции, не возникает никаких сомнений в необходимости использования SSL-сертификатов. В случае использования важных данных о заказчиках, например, номеров социальной защиты или идентификационных номеров, следует серьезно рассмотреть возможность использования SSL-сертификатов – особенно в том случае, если защита и конфиденциальность заказчиков или партнеров является одним из Ваших главных приоритетов.

С точки зрения коммерции использование SSL-сертификатов дает заказчикам и пользователям уверенность в отсутствии риска, связанного с передачей данных через сеть общего пользования. Сам этот факт обеспечивает целый ряд коммерческих преимуществ, большинство из которых вытекает из повышения надежности интерактивного взаимодействия с Вашей организацией. Если для Вашей деятельности требуются надежные отношения с заказчиками для упрощения электронных транзакций, использование SSL-сертификатов необходимо.

## 10. Решения *thawte* на основе SSL-сертификатов

### Сертификаты SSL123

SSL123 представляет собой сертификат с проверкой защищенного домена, который в зависимости от уровня шифрования, поддерживаемого браузером, может обеспечить шифрование с уровнем до 128 разрядов. Выдача данного сертификата занимает несколько минут. Он идеально подходит для коммерческих предприятий, которым требуется базовая защита связи между своими Web-узлами и интерактивными пользователями, а также выполнение задач общего назначения, например, защиты корпоративных локальных сетей. [Подробнее...](#)

### SSL-сертификаты для Web-сервера

SSL-сертификаты *thawte* для Web-сервера в зависимости от уровня шифрования, который поддерживается браузером клиента, могут обеспечить шифрование с уровнем до 128 разрядов. Эти сертификаты являются оптимальными для организаций, которые серьезно заботятся о сетевой коммерции и понимают важность и преимущества указания в сертификате достоверных сведений об организации. [Подробнее...](#)

### SGC SuperCerts

Сертификаты SGC SuperCert, выдаваемые *thawte*, позволяют клиентам применять 128-разрядное шифрование даже в случае использования следующих устаревших браузеров: IE 5.01 и Netscape 4.7x и более поздних версий, в которых возможности шифрования ограничены 40 или 56 разрядами. Эти сертификаты рекомендуются для защиты особо важной информации при предпочтительном применении 128-разрядного шифрования. [Подробнее...](#)

### Начальная программа PKI (SPKI)

Программа SPKI *thawte* оптимальна для компаний и организаций, которым требуется три и более цифровых сертификата в год для внутреннего применения на постоянной основе. Наша программа SPKI позволяет самостоятельно определять свои потребности в сертификации и предоставляет возможность существенной экономии.

[Подробнее...](#)

## 11. Проверка SSL-сертификатов на Вашем Web-сервере

Для практического ознакомления с SSL-сертификатами можно загрузить тестовый SSL-сертификат *thawte* и оценить его работу. Такие сертификаты действительны в течение 21 дня и позволяют познакомиться с процессом установки, а также обеспечить совместимость с конфигурацией своего Web-сервера. Бесплатные тестовые сертификаты предоставляются по адресу:

<http://www.thawte.com/ucgi/gothawte.cgi?a=w46840165367049000>

Вы также можете загрузить одно из пошаговых руководств, составленных специалистами *thawte*, где приведены процедуры запроса, настройки и установки SSL-сертификатов для двух наиболее распространенных платформ Web-серверов:

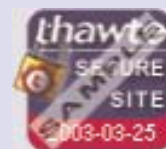
[Руководство для Apache](#) / [Руководство для Microsoft IIS](#)

Руководства по установке для других платформ Web-серверов предоставляются на нашем Web-узле технической поддержки

– [выберите эту ссылку](#).

## 12. Знак надежного Web-узла *thawte*

Все SSL-сертификаты *thawte* для Web-серверов и клиентские программы SGC SuperCert позволяют отображать на своих Web-узлах знак надежного узла *thawte*. Знак надежного узла *thawte* представляет собой защищенное изображение, которое является визуальным доказательством статуса надежности и обозначает, что Ваша подлинность подтверждена и пользователи могут безопасно и конфиденциально взаимодействовать с Вами.



Знак надежного узла *thawte* доступен в вариантах для различных языков и различного размера, что позволяет легко встраивать его в существующее оформление Web-узла. Подробнее см. страницу по адресу: <http://www.thawte.com/ssl123/index.html>

## 13. Полезные адреса URL

Подробнее о SSL-сертификатах *thawte* для Web-серверов см.:  
<http://www.thawte.com/ssl/index.html>

Устранение наиболее распространенных неполадок, возникающих при использовании SSL-сертификатов для Web-серверов, рассмотрено в базе знаний *thawte*:  
<http://kb.thawte.com>

Полезная информация содержится также в разделе часто задаваемых вопросов:  
<http://www.thawte.com/support/ssl/index.html>

Приобретение SSL-сертификатов для Web-сервера:  
<http://www.thawte.com/buy/>

## 14. О роли *thawte*

*thawte* является центром сертификации (CA), которые выдает различные цифровые SSL-сертификаты организациям и частным лицам по всему миру. *thawte* выполняет аутентификацию различного уровня в зависимости от продукта.

Цифровые сертификаты *thawte* полностью совместимы с наиболее распространенными Web-серверами и браузерами, поэтому приобретение цифрового сертификата *thawte* позволяет завоевать доверие заказчиков к Вашей системе и решает проблему неприкосновенности данных – при обращении к Вам по сети гарантируется высокая степень защиты.

## 15. Значение аутентификации

Информация является критически важным компонентом жизнедеятельности предприятия. Для обеспечения неприкосновенности и защиты данных важно точно знать, с кем Вы имеете дело, а также быть уверенным в том, что полученные данные являются подлинными. Аутентификация помогает установить надежные отношения между сторонами, участвующими во всех типах транзакций, позволяя выявлять целый ряд злоупотреблений, в том числе:

### Доступ путем обмана:

Низкая стоимость проектирования Web-узлов и простота копирования существующих страниц позволяет легко создавать незаконные Web-узлы, которые выглядят как созданные известными организациями. В действительности искусные аферисты незаконно узнают номера кредитных карт, создавая электронные витрины, внешне имитирующие легальные коммерческие предприятия.

### Несанкционированные действия:

Конкуренты или недовольные покупатели могут изменить Ваш Web-узел таким образом, что он будет неверно функционировать или отказывать в обслуживании потенциальным заказчикам.

### Несанкционированное разглашение:

При передаче информации о транзакции “открытым текстом” хакеры могут перехватить передаваемые данные для получения от Ваших заказчиков важной информации.

### Подмена данных:

Содержимое транзакции может быть перехвачено и изменено на пути передачи, как намеренно, так и случайно. Имена пользователей, номера кредитных карт и данные о денежных суммах, передаваемые “открытым текстом”, находятся под угрозой изменения.

## 16. Способы связи с *thawte*

С вопросами по содержанию этого руководства или продуктам и услугам *thawte* обращайтесь к консультанту по продажам:

Электронная почта: [sales@thawte.com](mailto:sales@thawte.com)

Тел.: +27 21 937 8902

Факс: +27 21 937 8967

## 17. Глоссарий терминов

### Асимметричное шифрование

Метод шифрования, в котором для шифрования и дешифрования сообщений используется пара из открытого и секретного ключа. Для передачи зашифрованного сообщения пользователь шифрует сообщение с помощью открытого ключа получателя. После получения сообщения оно дешифруется с помощью секретного ключа получателя. Функции шифрования и дешифрования, использующие для шифрования и дешифрования разные ключи, называются защитной однонаправленной функцией. Т.е. открытый ключ используется для шифрования сообщения, но не может использоваться для дешифрования этого сообщения. Не зная секретный ключ, практически невозможно декодировать информацию при использовании современных мощных алгоритмов шифрования.

### Центр сертификации

Центр сертификации (CA) - это организация (например, *thawte*), которая выдает реквизиты защиты и открытые ключи для шифрования сообщений, а также заведует этими данными.

### Запрос на подпись сертификата (CSR)

CSR представляет собой открытый ключ, который Вы создаете на своем сервере, и который проверяет подлинность относящейся к компьютеру информации о Вашем Web-сервере и организации при выполнении запроса сертификата у *thawte*.

### Секретный ключ

Секретный ключ - это цифровой код, используемый для дешифрования сообщений, зашифрованных соответствующим уникальным открытым ключом. Неприкосновенность данных шифрования обеспечивается секретным ключом, который не разглашается.

### Открытый ключ

Открытый ключ - это цифровой код, который позволяет шифровать сообщения, передаваемые держателю соответствующего уникального секретного ключа. Открытый ключ можно легко вычислить без ущерба для безопасности шифрования, и в то же время он повышает эффективность и удобство связи с использованием шифрования.

### Инфраструктура открытых ключей

Способ защищенного обмена информацией с организациями, целыми отраслями промышленности, странами и даже со всем миром. В PKI используется метод асимметричного шифрования для шифрования идентификаторов и документов или сообщений. (Другое название - метод "открытого/секретного ключа"). Начальной точкой PKI является центр сертификации (CA), например, *thawte*, который выдает и отзывает цифровые сертификаты (цифровые идентификаторы), которые обеспечивают подтверждение подлинности людей и организаций в общедоступных системах, например, в Интернет.

### Симметричная криптография

Метод шифрования, при котором для шифрования и дешифрования используется один и тот же ключ.

Этот подход имеет тот недостаток, что создает угрозу безопасности при распространении ключа, поскольку он должен быть передан и известен и отправителю, и получателю, но не должен раскрываться третьей стороне.