

Защита Web-сервера Microsoft MS IIS с помощью цифрового сертификата *thawte*

ПОШАГОВОЕ РУКОВОДСТВО по тестированию, установке и использованию цифрового сертификата *thawte* на Web-сервере MS IIS...

1. Обзор
2. Требования к системе
3. Создание пары из секретного ключа и запроса на подпись сертификата (CSR)
4. Создание резервной копии файла своего секретного ключа
5. Передача запроса тестового сертификата *thawte*
6. Установка тестового сертификата *thawte*
7. Запрос доверительного сертификата *thawte*
8. Установка доверительного сертификата *thawte*
9. Настройка сертификата для использования в MS IIS
10. Экспорт доверительного сертификата *thawte* с прикрепленным секретным ключом после установки
11. Полезные адреса URL
12. О роли *thawte*
13. Значение аутентификации
14. Способы связи с *thawte*
15. Глоссарий терминов

1. Обзор

В этом руководстве содержатся сведения по тестированию, приобретению, установке и использованию цифрового сертификата *thawte* на Web-сервере Microsoft MS IIS. Основное внимание в данном документе уделяется оптимальным методикам настройки, которые помогут обеспечить эффективное текущее управление ключами шифрования и цифровыми сертификатами.

Мы также остановимся на роли *thawte* как надежной третьей стороны, а также на деловых преимуществах цифровых сертификатов *thawte* за счет ориентированности на решение уникальных проблем сетевой защиты при обеспечении конфиденциальности для клиента.

Информация применима к следующим программным продуктам:

Microsoft IIS, версия 4.0
Microsoft IIS, версия 5.0
Microsoft IIS, версия 5.1
Microsoft IIS, версия 6.0

2. Требования к системе

Для каждой определенной версии MS IIS требуется установить самый последний пакет обновления.

Указания по установке пакета обновления:

- Если используется MS IIS 4.0, следует установить пакет обновления 6а.
- Если используется MS IIS 5.0 или MS IIS 5.1, следует установить пакет обновления 3.

Для получения последних пакетов обновления MS IIS обращайтесь на Web-узел технической поддержки Microsoft по следующему адресу:
[http://support.microsoft.com/default.aspx?scid=FH;\[LN\];sp&](http://support.microsoft.com/default.aspx?scid=FH;[LN];sp&)

ПОЛЕЗНЫЕ WEB-УЗЛЫ:

<http://support.microsoft.com/default.aspx?scid=fh;en-us;iis>
<http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis50>
<http://support.microsoft.com/default.aspx?scid=fh;EN-US;iis60>

3. Создание пары из секретного ключа и запроса на подпись сертификата (CSR)

Перед началом процесса получения сертификата требуется создать пару из **секретного ключа** и CSR вне Web-сервера. Эта операция выполняется с помощью консоли управления IIS (прежде чем создание пары из секретного ключа и CSR вне Web-сервера станет возможным, требуется установить IIS).

CSR является прежде всего открытым ключом, который Вы создаете на своем сервере, и который проверяет подлинность относящейся к компьютеру информации о Вашем Web-сервере и организации при выполнении запроса доверительного сертификата у *thawte*.

Для цифровых идентификаторов используется технология, которая называется "криптография с открытым ключом". Перед передачей запроса сертификата требуется создать на сервере секретный ключ и запрос сертификата (CSR). Открытый ключ, называемый также запросом на подпись сертификата (CSR), представляет собой ключ, которые требуется передать в *thawte*.

Секретный ключ должен храниться на сервере и ни при каких обстоятельствах не должен публиковаться в общедоступном домене. *thawte* не имеет доступа к Вашему секретному ключу. Он локально генерируется на сервере и не передается в *thawte*. Неприкосновенность цифрового идентификатора обеспечивается секретным ключом, которым распоряжаетесь и который знаете только Вы.

CSR невозможно сгенерировать без создания файла секретного ключа, а файл секретного ключа невозможно сгенерировать без создания файла CSR. Оба эти файла генерируются одновременно с помощью мастера на Web-сервере.

Обычно для создания пары из секретного ключа и CSR вне Web-сервера требуется ввести следующую информацию о своей организации:

- Название организации
- Организационные подразделения
- Код страны
- Область или штат
- Населенный пункт
- Общее имя*

Важное замечание

Термин "общее имя" применительно к X.509 употребляется для обозначения имени, которое служит наилучшим отличительным признаком сертификата и связывает его с Вашей организацией. В случае сертификатов Web-сервера SSL и 128-разрядных сертификатов SuperCerts введите точное имя своего хоста и имя домена, защиту которого требуется обеспечить. Они могут совпадать с именем корневого сервера или именем корпоративной локальной сети Вашей организации.

Пример. Если требуется обеспечить защиту `www.mydomain.com`, введите в это поле точное имя хоста (`www`) и имя домена. В случае ввода `mydomain.com` выданный Вам сертификат будет без ошибок работать только для этого имени домена. При доступе пользователей к домену с именем `www.mydomain.com` будет генерироваться ошибка

о Для создания пары из секретного ключа и CSR в MS IIS 4.0 выполните шаги, описание которых содержится по следующему адресу:

<http://www.thawte.com/support/keygen/index.html>

о Для создания пары из секретного ключа и CSR в IIS 5.0 или MS IIS 5.1 выполните шаги, описание которых содержится по следующему адресу:

<http://www.thawte.com/support/keygen/index.html>

о Для создания пары из секретного ключа и CSR в MS IIS 6.0 выполните шаги, описание которых содержится по следующему адресу:

<http://www.thawte.com/support/keygen/index.html>

Файл CSR, созданный при выполнении указанных выше шагов, сохраняется в текстовом формате и при просмотре выглядит приблизительно так, как показано в следующем примере:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2TCCAUICAQAwwZgxGzAJBgNVBAYTAiVMTMRAwDgYDVQQIEwdHZW9yZ2liMREwDwYDVQQ
HEwhDb2x1bWJ1czEzEjEzMBkGB1UEChMSQUZMQUUMgSW5jb3Jwb3JhdGVkMQswCQYDVQQLEwJJV
DEYMBYGA1UEAxMPd3d3LmFmbGFjbkuY29tMSAwHgYJKoZIhvcNAQkBFhFKR2FybW9uQGFMb
GFjLmNvbTCBnzANBqkqhkiG9w0BAQEFAAOBjgAWgYkCgYEAAsRqHZCLlrlxqqh8qs6hCC0KR9qEPX
2buwmA6GxegIcKpOi/IYY5+Fx3KZWXmta794nTPShh2lmRdn3iwxxQRKYqYKmp7wHCwtNm2taCRV
oboCQOuyZjS+DG9mj+bOrMK9rLME+9wz1f8i0FuArWhedDBnl2smOKQID45mWwB0hkCAwEAaAA
MA0GCSqGSIb3DQEBAUAA4GBAJNlxhOiv9P8cDjMsqyM0WXXWgagdRaGoa8tv8R/UOuBOS8/H
qu73umaB9vj6VHY7d9RKqDEIFc/xiXeDwoXNiF8quTm43pmY0Wcqnl1JZDGHMQkzzGtg502CLTHM
EIUGTdKpAK6rJcKucP0DKKEJKcmTySSnvgUu7m
-----END CERTIFICATE REQUEST-----
```

4. Создание резервной копии файла своего секретного ключа

Важное замечание

Затруднения, возникающие у пользователей при выполнении этого процесса, чаще всего связаны с секретными ключами, поскольку инструкции по экспорту секретного ключа отсутствуют в текущем мастере создания CSR. Главное затруднение возникает по той причине, что многие пользователи не знают, что секретный ключ генерируется одновременно с открытым ключом (поскольку секретный ключ не отображается пользователю).

В случае утраты или отсутствия доступа к секретному ключу, либо в случае потери пароля, который использовался при защите экспорта файла секретного ключа, выданный нами сертификат использовать невозможно. Во избежание таких ситуаций рекомендуется создать резервную копию файла секретного ключа на съемном носителе, а также памятку с паролем, который служит для защиты при экспорте файла секретного ключа.

Для создания резервной копии файла секретного ключа в MS IIS 4.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs5500>

Для создания резервной копии файла секретного ключа в MS IIS 5.0 или MS IIS 5.1 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs2065>

Для создания резервной копии файла секретного ключа в MS IIS 6.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22515>

6. Установка тестового сертификата *thawte*

Для установки сертификата в MS IIS 4.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs8385>

Для установки сертификата в MS IIS 5.0 или MS IIS 5.1 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7547>

Для установки сертификата в MS IIS 6.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22518>

После установки переходите к шагу 9 “Настройка сертификата для использования в MS IIS”.

Замечания относительно тестовых сертификатов *thawte*:

Тестовый сертификат обеспечивает шифрование, однако в начале каждого сеанса SSL с Вашим сервером при установленном тестовом сертификате отображается сообщение с предупреждением. Это сообщение извещает устанавливающего соединение пользователя о том, что сертификат не является доверительным сертификатом, а потому не может гарантировать неприкосновенность Web-узла.

Для браузера можно указать, что данный сертификат является доверительным, выбрав ссылку <http://www.thawte.com/roots/index.html> и выполнив инструкции, отображаемые в мастере по установке тестового корневого сертификата CA *thawte*.

7. Запрос доверительного сертификата *thawte*

Важное замечание

Для запроса доверительного сертификата у *thawte* требуется выполнить действия, указанные в шагах 3 и 4.

НЕ СЛЕДУЕТ, получив тестовый сертификат, затем передавать запрос на получение у *thawte* доверительного сертификата, используя **ТУ ЖЕ ПАРУ CSR и СЕКРЕТНОГО КЛЮЧА**. Процесс замены тестового сертификата на доверительный сертификат, для которого используется тот же секретный ключ/CSR, весьма непрост, поэтому его выполнение не рекомендуется.

Принятая в *thawte* практика выдачи сертификатов соответствует самым высоким стандартам. Мы уверены, что безупречные процедуры аутентификации и проверки подлинности абсолютно необходимы для обеспечения надежности в сети Интернет.

Заказ SSL-сертификатов *thawte* для Web-серверов и 128-разрядных сертификатов SuperCerts можно выполнить интерактивно по адресу <https://www.thawte.com/buy/>

В процессе запроса сертификата Вам будет предложено скопировать свой запрос на подпись сертификата (CSR) в текстовую область в интерактивной форме запроса.

Примечание. Скопировать и вставить CSR следует полностью - вместе с тире и полными строками операторов BEGIN и END.

В процессе заполнения запроса требуется указать всю запрашиваемую информацию и передать нам документы, подтверждающие Вашу подлинность или подлинность Вашей компании (например, регистрационное свидетельство компании). Дальнейшие подробные инструкции по получению SSL сертификата *thawte* для Web-сервера или 128-разрядного сертификата SuperCerts см. по адресу: <http://www.thawte.com/support/docs.html>

После завершения процесса заполнения интерактивного запроса *thawte* инициирует выполнение ряда шагов для проверки Вашей подлинности и сведений, которые Вы указали в CSR. Перед выдачей сертификата *thawte* подвергает серьезной проверке предоставленную информацию. Вследствие этого для проверки подлинности и сведений о компании перед выдачей сертификата может потребоваться несколько дней.

В этот период Вы можете отслеживать рассмотрение своего запроса:

<https://www.thawte.com/cgi/server/status.exe>

При возникновении вопросов в этот период можно обратиться к назначенному Вам представителю службы поддержки заказчиков. Сведения об этом представителе указаны на Вашей странице состояния по указанному выше адресу в разделе “*thawte* Contact Person” (лицо для контактов с *thawte*).

После проверки подлинности и CSR выдается сертификат. После выдачи сертификата указанное в запросе лицо для технических контактов получит сообщение электронной почты со ссылкой на адрес, с которого можно загрузить сертификат.

Скопируйте и вставьте сертификат в программу “Блокнот” вместе с тире и полными строками операторов BEGIN и END, как показано в примере ниже.

Сохраните выданный сертификат в файле с именем:
realcert_mydomain.crt

Примечание. Желательно присвоить сертификату имя, которое отличается от имени запрашиваемого ранее тестового сертификата.

Сертификат, созданный при выполнении указанных выше шагов, выглядит приблизительно так, как показано в следующем примере:

```
-----BEGIN CERTIFICATE-----
MIIDDDCCAnWgAwIbAgIDAMpQMA0GCSqGSIb3DQEBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcqUUVSVUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xZmZzAVBgnVBAstDIRFU1QgVEVTVCBURVNUMRww
GgYDVQQDEhNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTA0MDEyOTZyY2VydC5jb20x
MDIxOTEzMTkyMVoGZAxGTAxBgNVBAMTEHd3dy50ZXN0Y2VydC5jb20xZmZzAVBgnV
BAYTAIVTMRcwFQYDVQIEw5Ob3J0aCBDYXJvbnRlYXN0aW50aW50aW50aW50aW50aW50
aDEeMBwGA1UEChMVTXkgVGVzdCBDb25zdWx0aW50aW50aW50aW50aW50aW50aW50aW50
aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
znqA6BoMkpryFKNRdJHwPisa7KrdpaQiqdncJIZZ/SQBvhMZAyLtjeKXeZsoHvt
/aUcXRIEGZ0TvHvpCzblCtog4WO+Ten9eEwgjLGXdTN07WNZIVQKAQuQdEVGZzio
tBLDwsol2TAwlkrQ9XyzpLeN8Hes3Vza9qUnAgMBAAGjB5MAwGA1UdEwEB/wQC
MAAwMwYDVR0fBcwwKjAooCagJIYiaHR0cDovL3d3dy50aGF3dGUuY29tL3Rlc3Rj
ZXJ0LmNybDA0BgNVHSUELTAkBgggrBgEFBQcDAQYIKwYBBQUHAWIGCWCgsAGG+EIE
AQYKKwYBBAGCNwoDAzANBgkqhkiG9w0BAQQFAAOBgQAVqvhkJAAhPA7XPbDcxTz4
Vtr4Qi/wBFmnnvDotv4jSF3CXQRHT6wrlxUVlvpntncG3j2emtdu5yfr68jqwwLEP
I7Z44limQBjwMT/4/tkPqMy3cqas0+mYIehQBqF25DPypz7UIoQXFeXF9B/vffD2
9l/pXxEEus1Skv8XxJZkqA==
-----END CERTIFICATE-----
```

8. Установка доверительного сертификата *thawte*

После выдачи доверительного сертификата его можно загрузить со своей страницы состояния, нажав кнопку “Fetch Certificate” (Извлечь сертификат) (появляется только после выдачи сертификата).

За подробными инструкциями по загрузке доверительного сертификата обращайтесь к следующей статье базы знаний *thawte*:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7791>

Важное замечание

Этот сертификат привязывается к секретному ключу, который был создан ранее на шаге 3, и может быть 'прикреплен' только к этому ключу.

В случае утери секретного ключа, к которому привязан сертификат, или пароля, использовавшегося для защиты при экспорте файла секретного ключа, выданный сертификат становится непригодным для использования.

Для установки сертификата в MS IIS 4.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs8385>

Для установки сертификата в MS IIS 5.0 или MS IIS 5.1 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs7547>

Для установки сертификата в MS IIS 6.0 выполните шаги, описание которых содержится в следующих рекомендациях базы знаний:
<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22518>

9. Настройка сертификата для использования в MS IIS

Теперь, после установки сертификата, требуется активизировать сервер, а также, возможно, брандмауэр или маршрутизаторы, которые используются вместо него для защищенной связи.

С этой целью активизируйте порт SSL, который по умолчанию имеет номер 443, и назначьте уникальный IP-адрес сертификату на своем Web-сервере. Сертификат выдается только для того полного имени домена

(общего имени) и привязывается только к тому имени, для которого сертификат запрашивался.

Хотя сертификат и не привязывается к IP-адресу, назначенному Web-узлу, для каждого Web-узла с активизированным SSL требуется уникальный IP-адрес, т.к. SSL работает с виртуальными хостами с доступом по IP-адресам.

Назначенный Web-узлу IP-адрес можно изменить, и это никак не повлияет на сертификат при том условии, что IP-адрес будет уникальным.

Важное замечание

SSL не функционирует при использовании заголовков хостов, т.к. они содержатся в зашифрованных запросах. Такое поведение реализовано преднамеренно и не является ограничением IIS.

За дополнительными сведениями по данному вопросу обращайтесь к статье в базе знаний

Microsoft: [http://support.microsoft.com/default.aspx?scid=kb;\[LN\];Q187504](http://support.microsoft.com/default.aspx?scid=kb;[LN];Q187504)

Для активизации SSL на MS IIS 4.0 выполните следующие инструкции:

1. В группе программ "Сервер Интернета" откройте программу "Диспетчер ключей".
2. В окне "Диспетчер ключей" выберите ключ, для которого установлен сертификат.
3. Щелкните правой кнопкой мыши на этом ключе и выберите пункт "Свойства".
4. В окне "Привязки сервера" нажмите "Добавить".
5. В поле "IP-адрес" должен содержаться IP-адрес (набранный) требуемого Web-узла.

При наличии только одного Web-узла достаточно указать для IP-адреса значение по умолчанию "Все не назначенные".

6. В поле "Номер порта" щелкните на селективной кнопке рядом с полем "Номер порта" и добавьте 443. Затем нажмите "ОК".
7. Из меню "Компьютеры" выберите пункт "Выполнить изменения сразу" и на запрос "Выполнить все изменения сейчас?" выберите "Да".

Для включения SSL на MS IIS 5.0, MS IIS 5.1 и MS IIS 6.0 следуйте приведенным ниже инструкциям:

1. Поле IP-адреса на вкладке "Web-узел" должно содержать IP-адрес (набранный) соответствующего Web-узла. При наличии только одного Web-узла достаточно указать для IP-адреса значение по умолчанию "Все не назначенные".
2. Нажмите кнопку "Дополнительно" рядом с полем IP-адреса - проверьте, что в разделе "Несколько идентификаторов SSL для этого Web-узла" указан номер порта SSL.

Теперь имеется возможность безопасного доступа к данному компьютеру через <https://www.mydomain.com> и просмотра сведений сертификата.

После начала сеанса SSL в нижней строке инструментов браузера отображается символ в виде золотого висячего замка.

10. Экспорт доверительного сертификата *thawte* с прикрепленным секретным ключом после установки

Важное замечание

Рекомендуется создать на съемном диске резервную копию установленного сертификата с прикрепленным файлом секретного ключа, запомнив пароль, используемый для экспорта этого файла.

Данное действие является страховочной мерой, которая позволит в случае повреждения сервера вследствие непредвиденных обстоятельств иметь резервную копию сертификата и файла секретного ключа.

Для создания резервной копии сертификата с прикрепленным секретным ключом в MS IIS 4.0 обратитесь по следующему адресу URL:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs5500>

Для создания резервной копии сертификата с прикрепленным секретным ключом в MS IIS 5.0 или MS IIS 5.1 обратитесь по следующему адресу URL:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs1689>

Для создания резервной копии сертификата с прикрепленным секретным ключом в MS IIS 6.0 обратитесь по следующему адресу URL:

<http://kb.thawte.com/esupport/esupport/thawte/esupport.asp?id=vs22520>

11. Полезные адреса URL

Ряд распространенных затруднений, связанных с MS IIS, рассмотрен в разделе часто задаваемых вопросов:

<http://www.thawte.com/support/software/index.html>

Руководство по поиску и устранению неполадок MS IIS 4:

<http://kb.thawte.com/esupport/thawte/esupport.asp?id=vs12399>

Руководство по поиску и устранению неполадок MS IIS 5:

<http://kb.thawte.com/esupport/thawte/esupport.asp?id=vs6349>

Устранение распространенных неполадок в MS IIS при использовании SSL-сертификатов *thawte* для Web-сервера рассмотрены в разделе часто задаваемых вопросов:

<http://www.thawte.com/support/ssl/index.html>

Устранение распространенных неполадок в MS IIS при использовании 128-разрядных сертификатов SuperCerts *thawte* для Web-сервера рассмотрены в разделе часто задаваемых вопросов:

<http://www.thawte.com/support/sgc/index.html>

12. О роли *thawte*

thawte Technologies является центром сертификации (CA), который выдает сертификаты SSL для Web-серверов и 128-разрядные сертификаты SuperCerts организациям и частным лицам по всему миру. *thawte* проверяет, что заказавшая сертификат организация является зарегистрированной организацией и что лицо, заказавшее сертификат от имени этой организации, имеет соответствующие полномочия.

thawte также проверяет, что данная компания владеет соответствующим доменом. Цифровые сертификаты *thawte* полностью совместимы с серверами Apache и новейшим программным обеспечением Microsoft и Netscape, поэтому приобретение цифрового сертификата *thawte* для Web-сервера позволяет завоевать доверие заказчиков к Вашей системе и решает проблему неприкосновенности данных – при обращении к Вам по сети гарантируется высокая степень защиты.

13. 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 выявить 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.

14. 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

Тел.: +27 21 937 8902

Факс: +27 21 937 8967

15. 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 раскодировать 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), обеспечивающие 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.