

Установка и использование SSL-сертификатов

Руководство по правильной установке





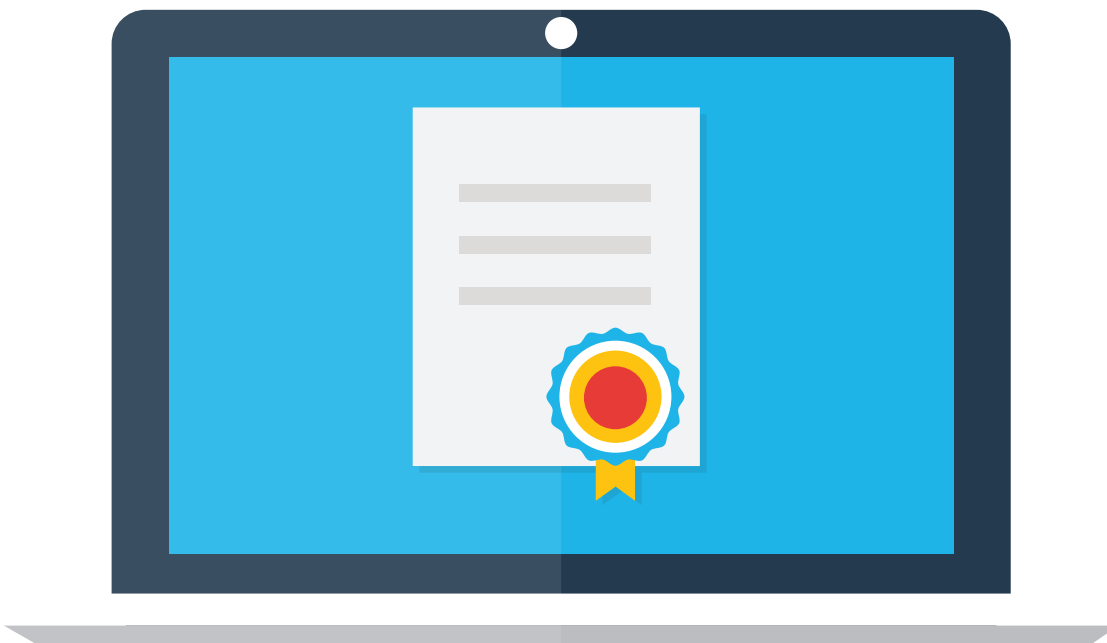
Итак, вы приобрели SSL-сертификат(ы).

Покупка сертификата — лишь первый шаг к обеспечению защиты веб-сайта. Часто сертификаты устанавливаются неправильно, страницы с конфиденциальной информацией остаются незащищенными, и данные форм публикуются в незашифрованном виде, делая многие веб-сайты уязвимыми для атак.

Учитывая это, компания Symantec подготовила следующие рекомендации, которые помогут вам правильно установить сертификаты с первого раза. Пользуясь этими рекомендациями, вы сможете избежать ошибок в сложных ситуациях и отказаться от сомнительных процедур, которые могут негативно повлиять на эффективность SSL-сертификатов. Помните, что SSL-сертификат — это средство повышения безопасности сайта для вас, ваших сотрудников и ваших клиентов.

Есть только один способ установки SSL-сертификата — правильный.

Итак, ваша организация осознала необходимость приобретения SSL-сертификата и предприняла необходимые шаги. Теперь вам нужно правильно установить сертификат. Если у потребителя возникает сомнение в безопасности вашего сайта, он не будет вести с вами дел.





Совет 1. Подготовка закрытого ключа и CSR-запроса



Перед установкой цифрового сертификата необходимо сгенерировать закрытый ключ и запрос на подпись сертификата (CSR) с использованием этого ключа на стороне сервера, где будет устанавливаться сертификат. Затем следует отправить CSR-запрос для получения сертификата. Для этого необходимо выполнить следующие действия.

Если вы используете серверы IIS 6 и более поздней версии или серверы Red Hat Linux, вы можете загрузить наше решение [Symantec SSL Assistant](#) и выполнить простые инструкции. Инструкции по генерированию CSR-запроса на других серверах смотрите на странице [Symantec CSR Generation](#). Чтобы подписаться на услуги для пользователей SSL-сертификатов Symantec, необходимо предоставить следующую информацию.

- Срок действия сертификата (1, 2 или 3 года)
- Количество серверов, находящихся в одном домене (до 5 серверов)
- Серверная платформа
- Название и адрес организации и подразделения
- Платежные реквизиты и контактное лицо для направления счета
- Обычное имя. Это имя узла и домена, например [www.mydomain.com](#) или [webmail.mydomain.com](#)
- Адрес электронной почты, по которому компания Symantec может связаться с вами для проверки информации
- Запрос на подпись сертификата (CSR), сгенерированный на сервере, безопасность которого необходимо обеспечить

После получения сертификата выполните действия, описанные в совете 3.

Если вашего сервера нет в списке или вам требуется дополнительная информация, ознакомьтесь с документацией по серверу или свяжитесь с поставщиком. Если вы не знаете, какое программное обеспечение используется на вашем сервере, обратитесь к ИТ-администратору.

В CSR-запрос, направляемый для регистрации, следует включить следующие верхний и нижний колонтитулы:

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



Совет 2. Правильная установка SSL-сертификата



Вы впервые устанавливаете SSL-сертификат и не уверены, как это сделать правильно? Не переживайте, это гораздо проще, чем может показаться. Ниже описывается установка сертификата Symantec на сервере.

Установка сертификатов на всех серверах следует одной логике.

Шаг 1. Сохранить сертификат.

Выполните инструкции, содержащиеся в электронном подтверждении: перейдите по указанному URL-адресу и сохраните SSL-сертификат на рабочем столе. Таким образом вы получите ваш сертификат и необходимые сертификаты промежуточного центра сертификации (ЦС).

Шаг 2. Установить или перенести сертификат в папку сертификатов.

Шаг 3. Настроить сертификат на веб-сайте.

Шаг 4. Указать путь к файлам сертификата.

[Щелкните здесь](#) для получения подробной информации и пошаговых инструкций для каждого типа серверов.

Чтобы максимально повысить эффективность SSL-сертификата, добавьте на свой веб-сайт знак безопасности Norton Secured. Это повысит уверенность потребителей в безопасности совершения операций на вашем сайте.

Чтобы добавить знак безопасности на свой веб-сайт, скопируйте необходимые строки на странице Symantec Norton Secured Seal в буфер обмена и вставьте в нужный файл; подробные инструкции доступны по ссылке в конце этого раздела. Там же представлена информация о том, как проверить правильность установки сертификата с помощью средства Certificate Installation Checker и указания доменного имени.

Теперь ваш SSL-сертификат установлен и готов к использованию.

У вас возникли проблемы?

Компания Symantec предлагает целый ряд учебных видеороликов об установке сертификатов на различные серверы. [Смотреть учебные ролики](#)

Проверка установки

Для проверки необходимо просто ввести URL-адрес сервера. [Проверить установку](#)

Генерировать знак безопасности

Инструкции по установке знака Norton Secured доступны на веб-сайте. [Генерировать знак](#)

Диагностика и устранение неполадок

Для диагностики проблем перейдите на страницу службы [технической поддержки Symantec](#)



Совет 3. Защита закрытых ключей с помощью лучших решений



Открытые и закрытые ключи являются составной частью процесса SSL-шифрования. Закрытый ключ безопасно хранится на вашем сервере и используется для шифрования всего содержимого веб-сайта. Открытый ключ, указанный в сертификате, также помогает идентифицировать ваш веб-сайт, например по доменному имени и названию организации.

Закрытые ключи — ценный актив, и доступ к ним следует предоставлять лишь небольшому числу доверенных партнеров и сотрудников. Вы можете себе представить, чтобы менеджер банка давал ключи от сейфа всем подряд? Разумеется, нет. Поэтому рекомендуем вам придерживаться следующих передовых методик.

- **Генерируйте закрытые ключи на доверенном сервере.** Не поручайте эту задачу сторонним организациям!
- **Защитите закрытые ключи паролем**, чтобы не допустить несанкционированного доступа к ним в системах резервного копирования.
- **Продлевайте сертификаты ежегодно** и всегда используйте новые закрытые ключи.

Размер закрытого ключа оказывает большое влияние на процедуру согласования криптографического соединения для установления защищенной связи. Использование слишком короткого ключа ненадежно, а использование слишком длинного ключа может привести к существенному замедлению операций.

Все более широкое применение находит криптографический алгоритм на основе эллиптических кривых (ECC), обеспечивающий высокий уровень безопасности при меньшей длине ключа. Компания Symantec предлагает ECC с размером ключей, составляющим лишь малую долю длины ключей RSA и DSA. При этом ключи ECC в 10 000 раз труднее взломать (по криптографической надежности 256-битный ключ ECC эквивалентен 3072-битному ключу RSA). Сертификаты ECC гарантируют более надежную защиту при меньшей загрузке сервера и помогут сократить время исполнения процессором криптографических операций сервера.

Дополнительные сведения о сертификатах ECC см. на стр. 7.



Совет 4. Устранение узких мест в цепочке



В большинстве случаев развертывания SSL-сертификата только на сервере недостаточно: для создания полной цепочки доверия необходимы три или более сертификата. Цепочка сертификатов включает в себя все сертификаты, необходимые для сертификации объекта, определяемого в конечном сертификате.

На практике в эту цепочку включаются сертификат конечного объекта, сертификаты промежуточного ЦС и корневого ЦС.

Процесс подтверждения подлинности и действительности нового сертификата предусматривает проверку всех сертификатов, начиная с универсальных доверенных корневых сертификатов и всех промежуточных сертификатов и заканчивая только что полученными сертификатами конечного объекта. Сертификат может быть доверенным только в том случае, если каждый сертификат в его цепочке был надлежащим образом выдан и удостоверен.

Часто пользователи правильно настраивают сертификат конечного объекта, но забывают включить сертификаты промежуточного ЦС. Проверить правильность установки промежуточных сертификатов можно [здесь](#).



Совет 5. Сертификаты RSA, ECC и значение длины ключа



Криптографический алгоритм на основе эллиптических кривых (ECC) обеспечивает более высокий уровень безопасности и производительности, чем используемые в настоящее время технологии шифрования.

Принцип метода шифрования ECC, одобренного правительством США и Агентством национальной безопасности США, заключается в использовании точек на эллиптической кривой для определения пар открытых/закрытых ключей. Эта технология устойчивее к методам грубой силы, которые часто используются злоумышленниками, а по быстродействию и требованиям к вычислительным ресурсам превосходит шифрование на базе RSA.

RSA — это алгоритм шифрования и цифровой подписи, который используется для обеспечения безопасности веб-сайтов уже почти двадцать лет. Он все еще остается действенным методом, однако минимальный допустимый размер ключа с течением времени увеличился ввиду необходимости обеспечения защиты от более сложных криптографических атак. Таким образом, технология ECC обеспечивает более высокую производительность, так как позволяет использовать ключ меньшего размера, и гарантирует непревзойденный уровень безопасности. Например, 256-битный ключ ECC обеспечивает такой же уровень защиты, что и 3072-битный ключ RSA. Это позволяет обеспечить необходимый уровень безопасности без ущерба для производительности.

Более того, благодаря меньшему размеру ключа для сертификата ECC снижается нагрузка на полосу пропускания. Все больше потребителей пользуются устройствами меньшего размера для совершения операций через Интернет, а сертификаты ECC помогают сделать этот процесс более удобным для них. Корневые сертификаты Symantec ECC поддерживаются тремя основными веб-браузерами с 2007 года, поэтому сертификаты Symantec ECC будут работать в вашей существующей инфраструктуре при условии использования современных веб-браузеров. Кроме того, они доступны без дополнительной оплаты.

Узнайте больше о [сертификатах ECC и гибкости алгоритма](#).



Совет 6. Всеобъемлющая защита по принципу Always On SSL



SSL-технологию необходимо использовать для шифрования всей информации на веб-сайте. Это можно обеспечить с помощью Always On SSL — экономически эффективной меры обеспечения безопасности веб-сайтов, которая поможет защитить конечного пользователя на протяжении всего процесса взаимодействия с веб-сайтом, значительно повысив безопасность поиска информации, обмена данными и совершения покупок через Интернет.

Компании, которые по-настоящему серьезно подходят к вопросу защиты клиентов и собственной репутации, делают выбор в пользу защиты на уровне Always On SSL при использовании SSL-сертификатов от надежного центра сертификации, такого как Symantec. Реализация защиты на уровне Always On SSL не составит затруднений и обеспечит проверку подлинности веб-сайта и шифрование всей информации, которой пользователь обменивается с веб-сайтом (включая cookie-файлы), чтобы защитить данные от несанкционированного просмотра, изменения или использования.

Организация Online Trust Alliance настоятельно рекомендует использовать Always On SSL для всех веб-сайтов. По мнению этой организации, «Always On SSL — испытанная временем действенная мера безопасности, которую необходимо использовать на всех веб-сайтах, поддерживающих обмен конфиденциальной информацией или доступ к ней».

Многие из самых успешных в мире компаний признали эффективность механизмов Always On SSL для защиты от побочного подключения и взлома за счет использования уязвимостей, таких как Firesheep, или внедрения вредоносного кода.

Always On SSL поможет укрепить доверие пользователей к вашему веб-сайту, вселяя в них уверенность в том, что вы серьезно относитесь к обеспечению их безопасности и защите конфиденциальности и делаете все возможное для защиты их данных в Интернете.



Совет 7. Привязка открытых ключей — вопрос доверия



Привязка открытых ключей (больше известная как HTTP-расширение для механизма привязки открытых ключей) дает операторам веб-сайтов возможность ограничить список центров сертификации, которым разрешено выдавать сертификаты для их серверов.

По сути, механизм привязки открытых ключей связывает сервер с заданным сертификатом или открытым ключом. После того как открытый ключ становится видимым для веб-сервера, он ассоциируется с этим веб-сервером, или «привязывается» к нему.

По мнению экспертов организации CA Security Council, привязка открытых ключей позволяет владельцам веб-сайтов продемонстрировать, что их SSL-сертификат имеет одну или несколько из следующих характеристик:

- имеет заданный открытый ключ;
- подписан центром сертификации с помощью этого открытого ключа;
- имеет иерархическую структуру доверительных отношений с центром сертификации на основе этого открытого ключа

Если сертификат для домена владельца сертификата выдан центром сертификации, не включенным в список (т. е. непривязанным), браузер, который поддерживает привязку открытых ключей, отображает диалоговое окно с предупреждением системы безопасности. Владельцы веб-сайтов могут привязывать несколько ключей от разных центров сертификации, которые будут восприниматься этими браузерами как действительные.

Владелец сертификата уверен в том, что выбранные центры сертификации не допустят ошибочной выдачи сертификата для его домена. Эти ЦС часто ограничивают список лиц, имеющих право запрашивать сертификат для определенных доменов владельца, что обеспечивает дополнительную защиту от ошибочной выдачи сертификатов несанкционированным лицам.

Организация CA Security Council утверждает, что, к сожалению, механизм привязки публичных ключей, объявленный компанией Google в 2011 году, не масштабируется, поскольку он требует добавления к браузеру открытых ключей для каждого домена. В настоящее время идет работа над документацией о создании масштабируемого механизма привязки открытых ключей с помощью рабочих предложений Инженерного совета Интернета (IETF RFC).

Согласно этому предложению, привязка открытых ключей будет определяться посредством HTTP-заголовка, отправляемого от сервера к браузеру. Варианты заголовка могут содержать такую информацию, как алгоритм ключа SHA-1 и (или) SHA-256, максимальная продолжительность использования механизма, возможность поддержки поддоменов и жесткость привязки.



Совет 8. Защита от несанкционированного доступа к информации с помощью совершенной прямой секретности



Как вы отнесетесь к тому, что злоумышленник, записывавший передаваемые вами данные, получит возможность расшифровать их в будущем? Разумеется, отрицательно. Однако вы можете оказаться в такой ситуации, совершенно не зная об этом.

Возьмем, к примеру, алгоритм RSA. Он используется для генерации открытых ключей для шифрования и дешифрования сообщений. Продолжительное использование ключей, допускающих повторное применение, может привести к тому, что сохраненные зашифрованные данные станут доступными в будущем, если эти ключи будут взломаны. Во многих случаях злоумышленник, имея ваш закрытый ключ и сохраненную SSL-информацию, может использовать этот ключ для дешифровки всех сеансовых ключей, использованных во время процедур согласования SSL-соединения, которые были сохранены, и затем дешифровать данные всех сохраненных сеансов с помощью этих ключей. Этот сценарий дает основания для беспокойства. Однако решение, основанное на совершенной прямой секретности, поможет избежать этих неприятностей.

При использовании этого решения создаются одноразовые временные сеансовые ключи, которые отменяются после использования. Более того, при правильной реализации совершенной прямой секретности — с использованием криптографического алгоритма на основе эллиптических кривых (см. ECC в совете 5) — она обеспечивает более высокий уровень безопасности и эффективности, чем алгоритмы RSA.

При использовании совершенной прямой секретности отсутствует связь между закрытым ключом на стороне сервера и ключом каждого сеанса. Если и клиент, и сервер поддерживают совершенную прямую секретность, они используют протокол Диффи-Хеллмана (названный по имени его авторов), который предусматривает безопасный обмен случайными числами между обеими сторонами для получения общего секретного ключа. Это сложный алгоритм, который предотвращает доступ злоумышленника к секретному ключу, даже если он имеет возможность просматривать все передаваемые данные.

Дополнительные сведения см. в инфографике Symantec.

[Посмотреть инфографику](#)



Совет 9. Строгая безопасность передачи информации по протоколу HTTP — гарантия вашей защиты



Обеспечение высочайшего уровня безопасности операций в Интернете имеет огромное значение. Иногда для достижения необходимого уровня защиты требуется принимать меры, выходящие за рамки обычных стандартов.

Взломщики могут использовать «атаки посредника» в беспроводных сетях, такие как SSL-стриппинг, для перехвата запросов, отправляемых браузером на сайты, использующие HTTPS, чтобы получить запрошенные страницы по протоколу HTTP. Это означает, что соединение уже не является шифрованным, и злоумышленник может перехватить информацию, которую пользователь вводит на веб-сайте, считая его защищенным. Пользователь может не заметить этого изменения, поскольку не всегда обращает внимания на адресную строку браузера при переходе на новую страницу веб-сайта. Браузеры не способны определять должный уровень защиты передаваемой информации, поэтому не отправляют уведомлений пользователю, если веб-сайт загружается по нешифрованному соединению.

Предотвратить это можно с помощью механизма HTTP Strict Transport Security (HSTS), который разрешает серверам отправлять сообщение веб-браузеру с требованием об обязательном шифровании всех подобных соединений. Браузеры принимают соответствующие меры для того, чтобы страницы, посещаемые пользователями, оставались зашифрованными надлежащим образом. Это обеспечивает надежную защиту вашей организации и ваших потребителей от атак злоумышленников.

Чтобы активировать механизм HSTS, необходимо задать единый заголовок ответа на ваших веб-сайтах. После этого браузеры, поддерживающие HSTS (например, Chromium, Google Chrome, Firefox, Opera и Safari), обеспечат выполнение ваших инструкций. После активации механизм HSTS не допустит установления незащищенного соединения с вашим веб-сайтом. Это обеспечивается за счет автоматического преобразования открытого текста в зашифрованный.

Браузер Internet Explorer пока не поддерживает механизм HSTS, но компания Microsoft уже объявила о том, что это будет реализовано в браузере Internet Explorer 12.

© Symantec Corporation, 2015. Все права защищены. Symantec, логотипы Symantec, Checkmark и Norton Secured являются товарными знаками или зарегистрированными товарными знаками корпорации Symantec или ее дочерних компаний в США и других странах. Другие наименования могут быть товарными знаками соответствующих владельцев.