Сертификаты

Цифровой сертификат — это файл, содержащий открытый ключ и цифровую подпись. Его можно представить как цифровую версию удостоверения личности. Но на самом деле он обладает гораздо большими возможностями, чем просто обеспечение аутентификации.

Одна из характеристик, к которой мы постоянно стремимся в сфере ИТ-безопасности, — это надёжность. Всякий раз, когда мы предоставляем кому-то доступ к системе, мы полагаемся на то, что человек, использующий это имя пользователя и пароль, действительно является тем, кому мы хотим предоставить доступ. Цифровой сертификат — это способ обеспечить такое доверие. Мы можем создать цифровой сертификат и получить цифровую подпись этого сертификата от центра сертификации, чтобы знать, что если центр сертификации доверяет этому человеку, то и мы должны доверять этому человеку.

Если вы находитесь в веб-браузере и у вас есть безопасное подключение к веб-сайту, вы заметите значок замка в адресной строке. Нажав на этот значок, вы сможете увидеть сведения о сертификате, связанном с этим веб-сервером. Вы заметите, что ваш браузер может отображать информацию о сертификате для этого веб-сервера независимо от того, к каким веб-сайтам вы подключены. Это связано с тем, что все эти веб-сайты используют единый формат сертификата, понятный всем.

Стандарт для этого формата называется X.509. Иногда можно услышать, как люди говорят о сертификате X.509. Они имеют в виду стандартизированный формат цифрового сертификата.

В этих цифровых сертификатах хранится огромное количество информации. У вас есть серийный номер, версия и алгоритм подписи. Вы можете увидеть, кто выдал цифровой сертификат, имя владельца цифрового сертификата, открытый ключ и другую информацию.

Например, когда мы впервые заходим на сайт через браузер, как браузер понимает, что мы подключаемся к нужному сайту, и как он устанавливает доверительные отношения между вами и этим ресурсом? Один из способов установить доверительные отношения — поручиться за сайт, к которому вы подключаетесь, чтобы, если третья сторона доверяет сайту, я тоже мог ему доверять.

Метод проверки подлинности, встроенный во все наши браузеры, позволяет нам понять, подключаемся ли мы к веб-сайту, которому можно доверять, или нет. При первом подключении к веб-сайту было бы здорово получать обратную связь о том, можно ли доверять этому сайту или нет. Поэтому мы будем использовать доверенную третью сторону, своего рода орган, называемый центром сертификации.

Центр сертификации — это организация, которая подписывает цифровой подписью сертификаты, хранящиеся на этом веб-сайте. Ваш браузер доверяет центру сертификации. Поэтому, когда вы впервые заходите на этот веб-сайт, вы можете

просмотреть его сертификат и убедиться, что он подписан цифровой подписью центра сертификации, которому уже доверяет ваш браузер. Следовательно, вы также будете доверять этому стороннему веб-сайту.

Это позволяет в режиме реального времени убедиться в том, что данному веб-сайту можно доверять. И этот процесс происходит на каждом веб-сайте, который мы посещаем в течение рабочего дня. Этот процесс, с помощью которого браузер определяет надёжность веб-сайта, встроен во внутреннюю структуру используемого вами браузера.

Если вы посмотрите на список центров сертификации, которым доверяет ваш браузер, то увидите, что в нём перечислены сотни центров сертификации. Это значит, что веб-сайт может приобрести сертификат у любого из этих сотен центров сертификации и разместить этот сертификат с цифровой подписью на своём веб-сервере. И пока они находятся в списке вашего браузера, им можно доверять.

Центр сертификации должен провести ряд проверок, чтобы убедиться, что человек, получающий цифровую подпись, действительно является владельцем этого конкретного веб-сайта. Это часть системы доверия, встроенной в центр сертификации. Именно так мы можем доверять любым веб-сайтам, которые посещаем в течение дня.

Допустим, мы хотим создать сертификат для нашего веб-сервера. Мы хотим отправить этот сертификат в центр сертификации для проверки, чтобы он был подписан цифровой подписью и возвращён нам. Процесс относительно прост.

Сначала мы создаём цифровой сертификат с помощью нашего открытого ключа, добавляем идентифицирующую информацию о том, к какому серверу он может быть подключен, а также информацию о нашей организации и объединяем их, чтобы создать запрос на подписание сертификата, или CSR. Этот CSR отправляется в центр сертификации. Центр сертификации выполняет проверку. Он подтверждает, что запрашиваемый вами сертификат действительно предназначен для веб-сервера, которым вы владеете и управляете. И если они согласятся с тем, что это действительный сертификат, они воспользуются своим закрытым ключом для цифровой подписи сертификата и отправят его вам обратно.

До сих пор мы говорили об использовании общедоступного центра сертификации, встроенного в браузеры по всему миру, для обеспечения доверия. Но если у вас есть собственные внутренние приложения и внутренние веб-серверы, к которым могут подключаться только сотрудники вашей организации, то вы можете стать собственным центром сертификации. Чтобы это работало, мы должны установить собственное программное обеспечение для центра сертификации в нашей организации.

Затем мы возьмём общедоступный сертификат этого центра сертификации и установим его на все компьютеры в нашей организации. Таким образом, все

компьютеры будут доверять внутреннему центру сертификации так же, как они доверяли бы внешнему центру сертификации. И вы увидите, что это довольно распространённая практика для организаций среднего и крупного размера, у которых есть собственные внутренние службы. Они могут создавать собственные сертификаты с помощью внутреннего центра сертификации.

Процесс создания цифрового сертификата, получения цифровой подписи этого сертификата от центра сертификации и его последующей передачи конечному пользователю точно такой же, как и при использовании внешнего центра сертификации. Единственное отличие заключается в том, что мы используем наш внутренний центр сертификации для обеспечения доверия и предоставления цифровых подписей для всех наших сертификатов. Если вы добавили сертификат внутреннего центра сертификации в цепочку доверенных сертификатов на всех своих устройствах, он будет работать точно так же, как внешний или общедоступный центр сертификации. Все эти устройства будут автоматически доверять всему, к чему подключаются, поскольку вы подписали их цифровой подписью с помощью внутреннего центра сертификации.

Если вы заходите на сайт в браузере и нажимаете на значок замка в адресной строке, вы можете увидеть все сведения об этом сертификате. Пролистав сертификат веб-сервера, вы можете увидеть раздел под названием «Альтернативное имя субъекта». Иногда мы называем его сертификатом с подстановочным знаком, потому что он позволяет указывать имя домена со звездочкой, связанной с именем устройства. Это означает, что созданный нами сертификат можно использовать на любом устройстве, которое использует полное доменное имя, указанное в поле Subject Alternative Name.

Бывают случаи, когда мы выводим из эксплуатации веб-сервер и хотим, чтобы этот сертификат перестал быть действительным. Или, возможно, мы обеспокоены тем, что злоумышленник получил доступ к нашим сертификатам. Поэтому мы хотим отозвать все эти сертификаты и создать новые.

Один из способов отзыва сертификата — использование CRL, или списка отзыва сертификатов. Это список всех отозванных сертификатов. Мы храним этот список в самом центре сертификации. Этот административный процесс создания и последующего отзыва сертификатов встроен в любой центр сертификации. Но могут быть и другие причины для отзыва сертификата.

Мы узнали об этом в апреле 2014 года, когда обнаружили атаку, в результате которой веб-сервер мог предоставить третьей стороне закрытый ключ веб-сервера. Мы называем эту атаку Heartbleed. Она была вызвана уязвимостью в библиотеке приложений OpenSSL. После обновления кода OpenSSL нам пришлось отозвать все наши сертификаты и создать новые.

Все наши старые сертификаты были перемещены в список отзыва сертификатов. Затем наши новые сертификаты были установлены на всех наших веб-

серверах. Вы видите, насколько важно иметь возможность отозвать доверие, которое ранее было установлено для конкретного сервиса.

После этого ваш браузер просмотрит этот список и убедится, что сертификат не был отозван. Если его нет в списке, вы можете продолжить работу в браузере. Но если сертификат этого стороннего веб-сайта указан в этом списке отзыва сертификатов, ваш браузер поймёт, что этому сайту нельзя доверять. Этот сертификат недействителен. И он не позволит вам получить доступ к этому веб-серверу.

Как вы понимаете, хранить все сведения об отзыве сертификатов в одном файле не очень эффективно. Было бы здорово, если бы мы могли использовать более эффективный процесс, который не требовал бы от нас посещения стороннего сайта и загрузки большого списка отзывов. К счастью, мы создали протокол, который позволяет это сделать.

Это **OCSP**, или протокол проверки статуса онлайн-сертификата. Полагаться на то, что центр сертификации предоставит список всех отозванных сертификатов всем, кто может зайти на наш сайт, по своей сути неэффективно. Чтобы сделать этот процесс более эффективным, мы можем размещать информацию о статусе наших сертификатов на самих веб-серверах.

Это достигается за счёт отправки сообщений о статусе вашего сертификата во время SSL-рукопожатия, которое происходит при первом подключении к веб-серверу. Это называется сшивкой OCSP, поскольку мы встраиваем статус этого сертификата в процесс рукопожатия с этим сервером. Очевидно, что мы не можем доверять стороннему веб-серверу в том, что он правдиво сообщит нам о статусе сертификата. Поэтому в протоколе OCSP для проверки статуса используется цифровая подпись центра сертификации.

Большинство браузеров сегодня поддерживают OCSP для протокола состояния онлайн-сертификата, что означает, что браузер сам может обрабатывать все проверки на отзыв при посещении веб-сайта сторонних производителей. Если вы не добавляете статус в сообщение о подтверждении связи, вы можете использовать сервер сторонних производителей для предоставления информации о состоянии OCSP. Это легко добавляется в сертификат. И это гораздо эффективнее, чем загружать весь список отзыва сертификатов из вашего центра сертификации.

Если в вашей организации используются очень устаревшие браузеры, вы можете столкнуться с тем, что OCSP не поддерживается. И даже в некоторых новых браузерах указано, что они поддерживают OCSP, но, к сожалению, не выполняют должным образом проверку, чтобы можно было подтвердить статус сертификата. Большинство современных браузеров поддерживают OCSP. Но вам стоит проверить свой браузер и убедиться, что он действительно выполняет проверку при подключении к веб-сайту, чтобы вы могли узнать статус этих сертификатов.