УДК 004.056.55

РОЛЬ SSL СЕРТИФИКАТОВ В БЕЗОПАСНОЙ ПЕРЕДАЧЕ ДАННЫХ

С. А. Зубишин
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Дается общее описание цифровых сертификатов и центров сертификации. Представлены этапы подтверждения подлинности SSL сертификата и анализируется значимость этого процесса в безопасной передаче данных. Производится сравнение различных типов SSL сертификатов и выделяется их роль в безопасной передаче данных. Предлагается один из возможных способов самостоятельной проверки достоверности сертификата в браузере.

Ключевые слова: цифровые сертификаты, центры сертификации, подтверждение подлинности сертификатов, типы SSL-сертификатов, проверка, безопасность данных.

ROLE OF SSL CERTIFICATES IN SECURE DATA TRANSFER

S. A. Zubishin
Don State Technical University (Rostov-on-Don Russian Federation)

This paper provides a general description of digital certificates and certification authorities. The stages of validating the authenticity of an SSL certificate are presented and the significance of this process in secure data transfer is analyzed. The comparison of different types of SSL certificates is made and their role in secure data transfer is highlighted. One of the possible ways to independently check the validity of a certificate in a browser is suggested.

Keywords: digital certificates, certification authorities, certificate validation, types of SSL certificates, verification, data security.

Введение. На сегодняшний день сохранение целостности и конфиденциальности информации при электронном обмене данными требует наличия различных методов защиты. Одним из таких методов является цифровой сертификат безопасности, который, благодаря встроенным механизмам, позволяет достичь необходимого уровня защищенности информации. Цель данной статьи — сравнить типы SSL сертификатов, определить их роль в безопасной передаче данных

Цифровые сертификаты. Цифровой сертификат — это электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов. Также он используется для связывания пар криптографических ключей с различными объектами, такими как веб-сайты, организации или частые лица. Выпускается такой сертификат специальными удостоверяющими центрами, их также называют центрами сертификации.

Центром сертификации является организация или компания, которая выполняет проверку подлинности сущностей, также эти центры отвечают за управление криптографическими ключами пользователей посредством выпуска цифровых сертификатов.

Данные сертификаты обеспечивают:

- шифрование;
- аутентификацию.

В шифровании применяется ассиметричный алгоритм, который используется в подтверждении на подлинность сертификата. В процессе подтверждения пользователю

предоставляется открытый криптографический ключ, необходимый для инициирования безопасных соединений [1].

Этапы подтверждения подлинности сертификата:

1. Отправитель вычисляет хеш-сообщения, далее шифрует его закрытым ключом отправителя, создавая цифровую подпись (ЦП).

2. Отправитель посылает сообщение, в котором передаёт зашифрованную ЦП.

3. Получатель расшифровывает ЦП с помощью открытого ключа отправителя, восстанавливая хеш-сообщения отправителя.

4. Получатель вычисляет хеш-сообщения из полученных данных и проводит проверку, что эти два значения идентичны (рис. 1).

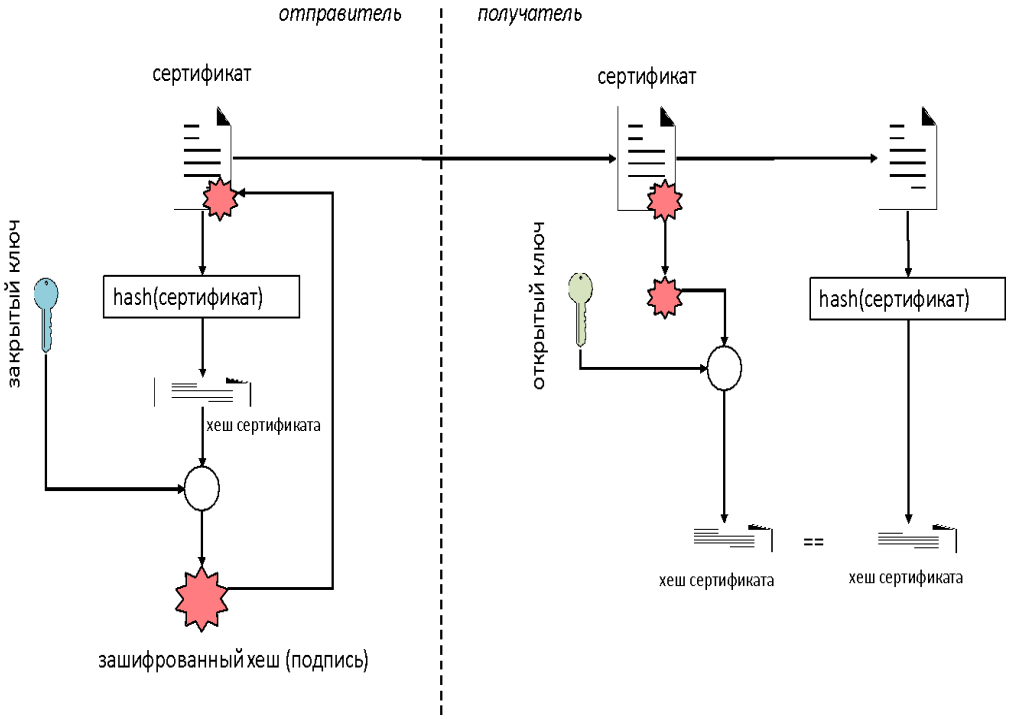

Рис. 1. Этапы подтверждения подлинности сертификата

Если подлинность подтверждена, то получателю известно, что:

— сообщение не подвергалось изменению во время передачи;

— сообщение было отправлено сущностью, которая заявляет, что отправила его.

Алгоритм цифровой подписи, применяемый в проверке сертификата, является частью служб обеспечения целостности и аутентификации [2]. Он также служит доказательством происхождения, так как только отправителю известен секретный ключ, а это — достаточное подтверждение того, что отправитель является автором сообщения.

Пользователи могут и самостоятельно удостовериться в подлинности сертификата путем сверки некоторых его полей. Для этого необходимо в браузере нажать на значок замка (слева от URL-адреса). Например, дата действия сертификата должна быть больше текущей даты, название обязано совпадать с именем веб-страницы или документа. Эти и некоторые другие параметры подтверждают, что сертификат на самом деле связан с организацией или частым лицом, с которыми клиент хочет соединиться (рис. 2).

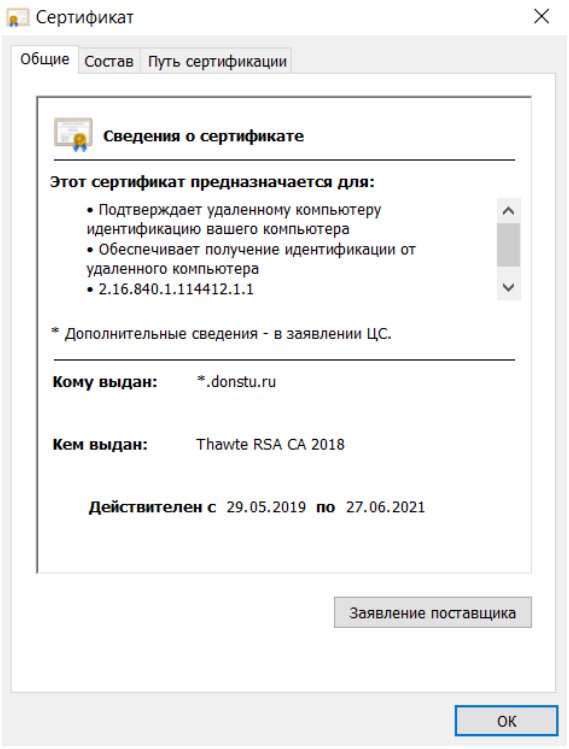

Рис. 2. Пример цифрового сертификата

Чтобы гарантировать защиту от злоумышленников, удостоверяющие центры проверяют организацию или частное лицо, которому они выдают сертификат.

Типы SSL сертификатов. В зависимости от уровня проверки выделяют следующие типы сертификатов [3]:

- Domain Validation (проверка домена).
- Organization Validation (проверка организации).
- Extended Validation (расширенная проверка).
- Self-signed (самоподписанный).

Сертификаты, выданные с проверкой домена (DV), являются наиболее популярными и самыми простыми в управлении. Их задача — зашифровать передаваемые данные от браузера клиента к серверу. Преимуществом таких сертификатов выступает их низкая стоимость. Недостатком же является то, что данный сертификат не обеспечивает аутентификацию компании, организации или частного лица, приобретающего его, так как такие сертификаты зачастую используются для подтверждения владения доменом, без проверки организации. Пользователи скорее доверятся веб-сайту, если знают компанию, которая использует данный домен. Такие сертификаты целесообразно использовать для защиты коммуникации по внутренней сети.

Более высоким уровнем доверия обладают сертификаты с проверкой организации (OV). При их выдаче производится не только проверка домена компании, но и проверка подлинности организации, заказывающей данный сертификат. Положительные стороны такого сертификата: шифрование передаваемых данных и гарантия, что данные об организации проверены по международным стандартам. Организация, использующая такой сертификат на своих сайтах, заслуживает повышенного доверия со стороны пользователей, даже если они не слышали о ней ранее.

Сертификаты с расширенной проверкой (EV) являются безоговорочным подтверждением безопасности сайта, так как при их выдаче организация, получающая сертификат, не только

проходит проверку уровня сертификатов DV и OV, производится еще и дополнительная тщательная проверка для защиты клиентов. Достоинствами EV сертификатов являются шифрование данных и углубленная проверка организации, а визуальным преимуществом является появление зеленой адресной строки, что воспринимается пользователем как гарантия защищенности сайта. Наличие такого сертификата — необходимое условие для сайтов крупных компаний, так как пользователи могут вносить свои пароли и личные данные, не боясь за их сохранность.

Существует особый тип цифрового сертификата, называемый самоподписанным. Обычно такого типа сертификаты выпускаются крупными компаниями, авторитетными в области информационной безопасности, однако техническая возможность создать подобный сертификат есть и у любого владельца веб-сайта. Этот тип цифрового сертификата не имеет отличий от сертификата, заверенного подписью удостоверяющего центра (УЦ), только вместо отправки на подпись в УЦ пользователь формирует свою персональную сигнатуру. Если говорить проще, то создатель сертификата сам служит в данном случае удостоверяющим центром. Все корневые сертификаты доверенных удостоверяющих центров являются самоподписанными. Преимуществом таких сертификатов выступает то, что их можно создавать неограниченное количество, не обращаясь к поставщикам услуг по их оформлению, стоимость этих сертификатов равна нулю. Недостатком является то, что самоподписанные SSL сертификаты можно применять между пользователями, которым известно о самоподписанном сертификате и которые подтвердили его надежность в браузере. Иначе, пользователь, подключающийся к каналу, в котором действует данный сертификат, получает уведомление: «Сертификат безопасности не является доверенным!» (рис. 3). В этом случае большинство посетителей откажется от использования данного сайта.

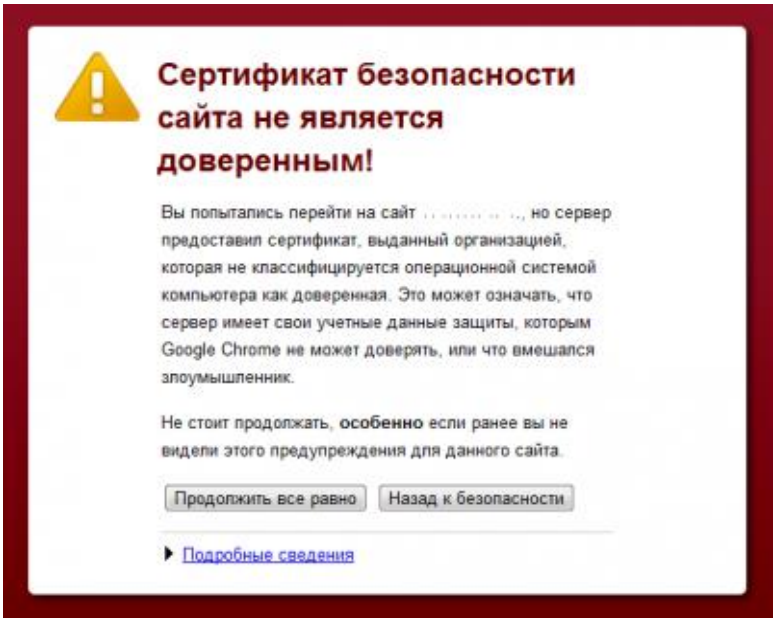

Рис. 3. Ошибка при проверке сертификата в браузере

В связи с этим самоподписанные сертификаты целесообразно использовать только на внутренних сайтах компании, и зачастую они применяются частными лицами или в небольших фирмах, работники которых знают о его наличии и необходимости добавлять его в список доверенных сертификатов браузера.

Заключение. Цифровые сертификаты позволяют в должной степени обеспечить целостность и конфиденциальность данных благодаря встроенным протоколам ассиметричного шифрования. Для повышения уровня защищенности данных при передаче по глобальной сети Интернет является целесообразным самостоятельная проверка сертификата на наличие необходимых признаков действующего сертификата.

Библиографический список

1. Цифровые сертификаты безопасности // Безопасность пользователей в сети Интернет : [сайт]. — URL:https://safe-surf.ru/users-of/article/546552/ (дата обращения: 10.03.2021).

2. Циммерманн, Ф. Цифровые сертификаты / Ф. Циммерманн // ВикиЧтение : [сайт]. — URL: https://it.wikireading.ru/42980 (дата обращения: 10.03.2021).

3. Какие бывают типы проверки сертификатов, и чем они отличаются // FirstSSL : [сайт]. — URL: https://firstssl.ru/faq/general-questions/tipy-proverki (дата обращения: 10.03.2021).

Об авторе:

Зубишин Степан Алексеевич, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), zubishin009@mail.ru

Author:

Zubishin, Stepan A., Student, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), zubishin009@mail.ru