УДК 004

SSL-сертификаты. Получение, генерация и подключение

Ленкин Алексей Викторович
Приамурский государственный университет имени Шолом-Алейхема
Студент

Голубь Илья Сергеевич
Приамурский государственный университет имени Шолом-Алейхема
Студент

Глаголев Владимир Александрович
Приамурский государственный университет имени Шолом-Алейхема
к.г.н., доцент кафедры информационных систем, математики и правовой информатики

Аннотация
В данной статье рассмотрена технология SSL и SSL-сертификатов. Показан пример генерации самоподписанного сертификата и использование SSL-сертификатов.
Ключевые слова: SSL, SSL-сертификат, OpenSSL

SSL certificate. Receive, generate, and connect

Lenkin Aleksei Viktorovich
Sholom-Aleichem Priamursky State University
Student

Golub Ilya Sergeevich
Sholom-Aleichem Priamursky State University
Student

Glagolev Vladimir Alexandrovich
Sholom-Aleichem Priamursky State University candidate of geographical Sciences, associate professor of the Department of information systems, mathematics and legal informatics

Abstract
This article discusses the technology SSL and SSL-certificates. Examples of generating a self-signed certificate and using SSL certificates are shown..
Keywords: SSL, SSL-certificate, OpenSSL

Обеспечение защиты данных в сети интернет на данный момент является одним из самых приоритетных задач для специалистов

кибербезопасности. Для защиты информации на сайте используются различные методы шифрования, одним из способов защиты информации на сайтах является использование технологии SSL.

SSL (SecureSocketsLayer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений[1]. Наличие SSLзащищает данныепользователя, которыми он обменивается с сайтом, такую информацию становится невозможно перехватить, так как она зашифрована.

Исследованиями по данной теме занимались следующие авторы. А.В. Майоров и А.И Иванов описали «Надежную биометрическую аутентификацию клиента в защищенных интернет-соединениях на базе протоколов SSL, TLS6» [2]. «Безопасность сертификатов SSL» была описана А.Сугано [3]. Рассказал о «SSL-сертификаты сайтов. Назначение и использование» Р. Ачилов [4].

SSL-сертификат - это индивидуальная цифровая подпись, которая является подтверждением того, что этот сайт действительно принадлежит компании, которую представляет, а также, что на сайте присутствует защита данных.

SSL-сертификат может быть получен следующими способами:

1. Сгенерирован самостоятельно. В специальных программахсоздан и подписан, например, OpenSSL. Такой способ является самым простым и бесплатен, но отображается пользователям как «Самоподписанный» о чем их предупреждает сам браузер. Это значит, что вы сами выдали его себе и сами подписали, что исключает доверие такому сайту.
2. Подписан недоверенным центром сертификации. Такие сертификаты выдаются компаниями, которые не имеют значительного влияния в сфере информационной безопасности и малоизвестны. Сертификаты, подписанные таким способом, обычно стоят очень мало либо бесплатны, наличие такого означает, что сертификат сайта проверен, но сам «проверяющий» доверия не удостоен.
3. Подписан доверенным центром сертификации. Такие сертификаты выдаются известными компаниями имеющими долгую историю в сетевой безопасности. Покупать такие сертификаты напрямую очень тяжело, так как их стоимость иногда превышает стоимость самого сайта, поэтому их покупают у посредников.

Опишем генерацию сертификата самостоятельно, через программное обеспечение OpenSSL [5]:

1. После установки OpeSSL в командную строке cmd переходим в родительский каталог программы (по умолчанию `c:\OpenSSL-Win32\bin`).

2. Указываем путь к конфигурации openssl: `set OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg`.
3. Генерируем приватный ключ и указываем пароль (пароль указывается в слепую, поле будет пустое при вводе): `openssl genrsa -des3 -out c:\private.key 2048`.
4. Генерируем запрос на сертификат: `openssl req -new -key c:\private.key -out c:\csr.csr`.
5. После выполнения данной команды, необходимо ввести данные о компании в латинской раскладке. Следует указать обязательно, остальное опционально: Country Name (2 letter code) [AU] - страна регистрации организации (для России - RU); State or Province Name (full name) [Some-State] - область, регион регистрации организации (EAO - JAO); Locality Name (eg, city) [] - город регистрации организации (Биробиджан - Birobidzhan); Organization Name (eg, company) [Internet Widgits Pty Ltd] - наименование организации; Common Name (e.g. server FQDN or YOUR name) [] - доменное имя сайта организации (localhost, test.com).
6. Генерируем сам сертификат сроком на 365 дней : `openssl x509 -req -days 365 -in c:\csr.csr -signkey c:\private.key -out c:\certificate.pem`.
7. В результате в каталоге `c:\` будет создан приватный ключ (`private.key`) и сертификат (`certificate.pem`) (результат выполнения на рисунке 1).

Подключение SSL-сертификата происходит в личном кабинете сайта, выдавшего домен для компании.

Технология SSL-сертификатов используется также для создания VPN (Virtual Private Network — виртуальная частная сеть). Также возможно использования в базах данных, например при использовании MySQL можно подключить сгенерированный SSL-сертификат и использовать базу удаленно, она становится доступна не только локально, но и в сети интернет, открывая доступ только пользователям, подключившимся через сертификат.

Таким образом, для подтверждения пользователям о защите их данных на сайте представителю компании необходимо купить SSL-сертификат и в обязательном порядке установить его на домен компании.

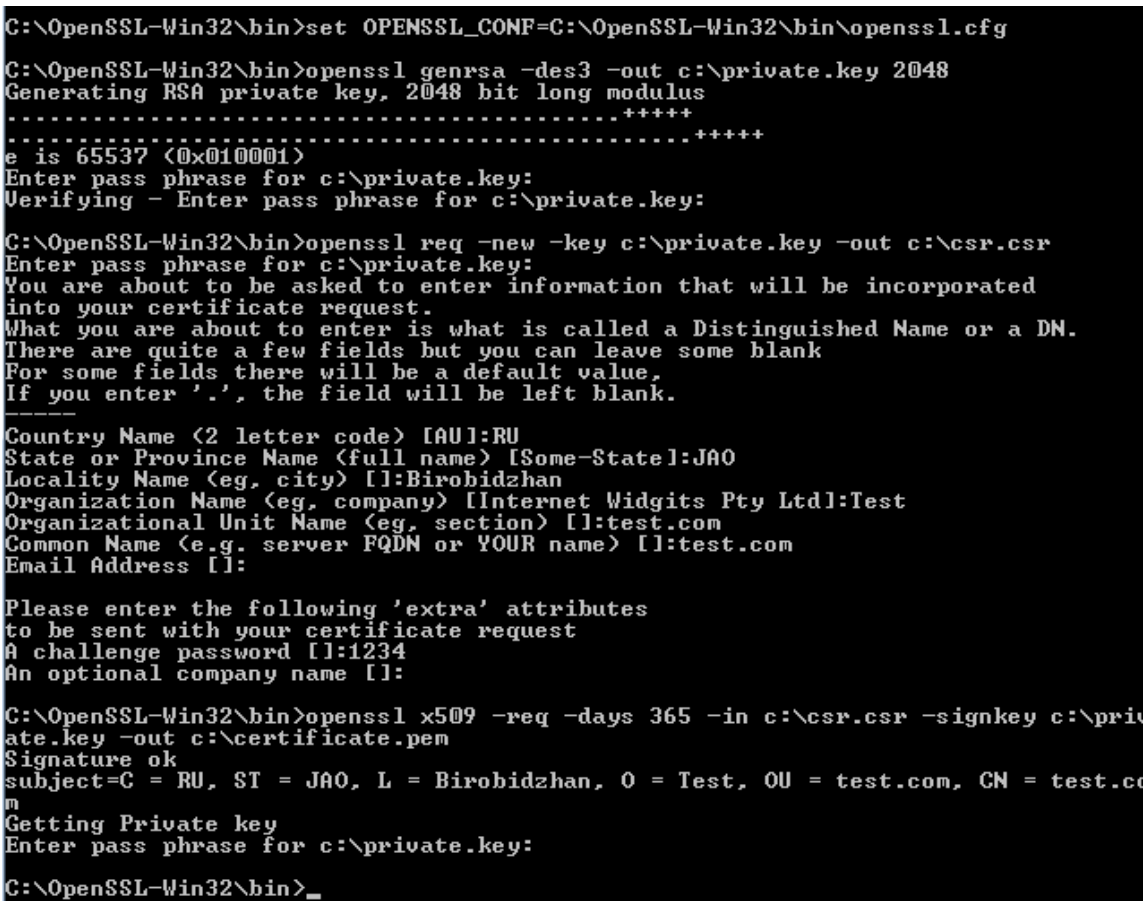

Рисунок 1. Генерация SSL-сертификата в программе OpenSSL

Библиографический список

1. SSL-сертификат [Электронный ресурс] URL: https://hostiq.ua/wiki/ssl-certificate/ (дата обращения 02.09.2018)
2. Майоров А.В., Иванов А.И.Надежная биометрическая аутентификация клиента в защищенных интернет-соединениях на базе протоколов SSL, TLS6.// Вопросы защиты информации. 2008. № 3 (82). С. 38-41.
3. Сугано А. Безопасность сертификатов SSL // WindowsITPro/ RE. 2010. № 11. С. 50-52.
4. Ачилов Р. SSL-сертификаты сайтов. Назначение и использование // Системный администратор. 2010. № 3 (88). С. 64-68.
5. Официальный сайт OpenSSL [Электронный ресурс] URL: https://www.openssl.org/ (дата обращения 02.09.2018)