РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ ВЫДАЧИ SSL-СЕРТИФИКАТОВ

Д.В. Плахин
Научный руководитель: С.Г. Цапко
Томский политехнический университет
pdv-mail@mail.ru

Введение

Современный мир трудно представить без сетевых технологий. Обмен данными между удалёнными машинами, синхронизация различных устройств, идентификация пользователей на различных сайтах и другие возможности сетей находят широкое применение в различных сферах деятельности человека. Важную роль в этом процессе играет безопасность соединения. Пользователь сети не может быть уверен в корректности полученных данных и в конфиденциальности передаваемой информации, если соединение не защищено.

Обеспечить безопасность обмена данными можно с помощью ssl-сертификатов. Они позволяют передавать зашифрованные данные по протоколу HTTPS, предотвращая их перехват и изменение с третьей стороны [1]. При этом проверяется цифровая подпись сертификатов.

Для создания таких сертификатов было разработано приложение, описываемое в данной статье.

Получение сертификатов

Существующим сертификатом можно подписать какой-либо другой сертификат. Корневые сертификаты производятся специальными центрами сертификации. Далее ими подписываются выдаваемые пользователям сертификаты. При выдаче проверяется существование компании, корректность доменного имени и его принадлежность к этой компании, а также некоторые другие параметры, в зависимости от стоимости услуги.

Как правило, выдача сертификата центром сертификации – дорогостоящий процесс. Более дешёвым решением может быть заказ сертификата у компаний-партнёров центра сертификации, поскольку они закупают их оптом по сниженным ценам. Бесплатным способом является создание самоподписного сертификата, который пользователь выдаёт сам себе. Однако доверять такому сертификату можно только в пределах сети, использующей его в качестве корневого.

Покупка множества сертификатов для одной компании была бы весьма затратным процессом. Одним же купленным сертификатом можно подписать несколько других, а последними – третьих. Таким образом, можно организовать дерево сертификатов, которым можно доверять, поскольку корневой сертификат выдан центром сертификации. При этом ответственность за неправомерное использование таких сертификатов будет лежать на компании, в которой они произведены.

Поскольку приватные ключи сертификатов находятся только в сети компании, постороннее лицо не может, обладая каким-либо сертификатом одного из узлов полученного дерева, подписать свой сертификат.

Удобным решением, содержащим инструментарий для создания и редактирования такого дерева, стало легковесное программное обеспечение, разработанное на языке C# специально для этих целей и описанное в данной статье.

Описание приложения

Приложение «Генератор сертификатов» предоставляет пользователю простой интуитивно понятный графический интерфейс для создания иерархии сертификатов. Отображение элементов осуществляется специальными невизуальными компонентами TreeViewManager и PropertyListViewManager, позволяющими отделить данные от их отображения в дереве TreeView и сетке свойств PropertyGrid. Другими словами, через описанные компоненты осуществляется вся работа по добавлению, удалению и изменению данных в таблицах и своевременному отображению этих изменений на форме. Более подробно эти компоненты описаны автором данной статьи в источнике [2].

Генератор сертификатов реализован для компании СибНефтеКарт, разрабатывающей программное обеспечение для сетей АЗС [3]. В связи с этим, в соответствии со структурой торговых сетей клиентов организации в реализованной версии приложения глубина вложенности объектов составляет 3 уровня. Тем не менее, при внесении небольших изменений в код приложения, это ограничение может быть снято. К таким изменениям относится динамическое создание компонентов для редактирования параметров выгрузок, о которых будет сказано позднее в данной статье, а также дополнительная настройка компонента отображения дерева сертификатов.

На каждом уровне дерева сертификаты дочерних уровней могут быть выданы и подписаны сертификатом текущего уровня. Если на текущем уровне сертификат отсутствует, выдача не производится. Сертификаты корневого уровня могут быть импортированы, либо сгенерированы. В первом случае следует указать файл с сертификатом и файл с приватным ключом. Во втором результатом операции является самоподписной сертификат.

Параметры выдаваемого сертификата настраиваются в соответствующем разделе сетки свойств

в правой половине главного окна приложения, представленного на рисунке 1. К таким параметрам относятся двухбуквенный код страны, срок действия, название организации и некоторые другие.

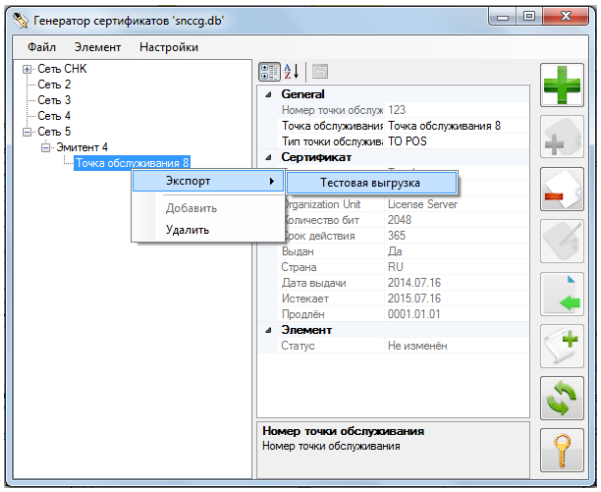

Рисунок 16. Главное окно приложения

После того как сертификат выдан, редактировать его параметры вручную нельзя. Можно лишь продлить срок действия сертификата нажатием специальной кнопки, расположенной в правой части окна.

Там же расположены другие кнопки, открывающие доступ к функционалу приложения. Весь функционал доступен также из контекстного меню и в главном меню приложения. К нему относится редактирование структуры дерева сертификатов, подразумевающее добавление и удаление уровней. Также в функционал входят возможность выдачи и импорта сертификатов и настройка паролей для каждого уровня.

Для каждого уровня предусмотрен свой пароль, который используется при создании цифровой подписи и может быть задан в специальной форме. Приватный и публичный ключи шифруются паролем соответствующего уровня для большей надёжности.

Отредактированная структура дерева сертификатов сохраняется в файле SQLite базы данных [4]. При этом сохраняются также сами сертификаты с их приватными и публичными ключами. Поскольку ключи генерируются в зашифрованном виде с использованием пароля, определённого для соответствующего уровня, пользователь, не зная пароля, после открытия файла базы данных в каком-либо SQLite-редакторе не сможет получить эти ключи.

Генерация ключей в данном приложении использует алгоритм RSA [5]. При этом публичный ключ хранится в самом сертификате, а приватный – в отдельной записи, в случае с базой данных, или в отдельном файле при экспорте файлов.

Экспорт файлов сертификатов и ключей осуществляется в специальные файлы-выгрузки. Выгрузка является архивом с паролем, в который включаются необходимые файлы сертификатов или ключей. Настройка выгрузки осуществляется в форме, представленной на рисунке 2.

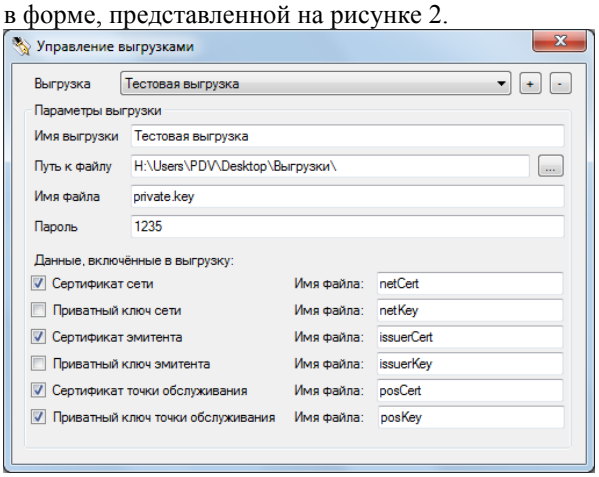

Рисунок 17. Окно настройки выгрузок

Выгрузка информации в файл может быть осуществлена при помощи контекстного меню, либо из главного меню. При этом в разделе «Экспорт» появляются только те элементы, которые могут быть применены к текущему узлу. Такими элементами для текущего узла являются узлы, выгрузки которых не содержат пунктов, соответствующих последующим уровням.

Заключение

Полученный программный продукт позволяет сэкономить время и деньги, тратящиеся на получение сертификатов. Приложение не требовательно к ресурсам, имеет максимально простой и интуитивно-понятный интерфейс для подобной задачи и не требует специальной подготовки и чтения документации перед использованием.

Список литературы

1. В. Мао - Современная криптография: Теория и практика - Москва: Вильямс, 2005. - 768 с.
2. Современные техника и технологии: сборник докладов XX Международной юбилейной научно-практической конференции студентов, аспирантов и молодых ученых. В 3 т. Т. 2 / Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2014. – 333 с.
3. Закрытое акционерное общество научно-производственная фирма Сибнефтекарт [Электронный ресурс]. Режим доступа: http://sncard.ru/, свободный.
4. Jay A. Kreibich Using SQLite - O'Reilly Media 2010. - 530 с.
5. Баричев С.В. Криптография без секретов. – Москва: Горячая Линия - Телеком, 1998. – 43 с.