ТЕСТИРОВАНИЕ СРЕДСТВ ПРОВЕРКИ МАРШРУТОВ СЕРТИФИКАЦИИ

Н. Н. Шенец

НИИ прикладных проблем математики и информатики БГУ
Минск, Беларусь
E-mail: Shenec@bsu.by

Описывается разработанное в НИИ ППМИ руководство по тестированию средств проверки маршрутов сертификации. Приводится сравнительный анализ данного руководства с зарубежным аналогом.

Ключевые слова: инфраструктура открытых ключей, сертификат открытого ключа, маршрут сертификации.

Введение

В современных информационных системах, требующих проведения аутентификации пользователей, контроля целостности, обеспечения конфиденциальности и/или невозможности отказа от авторства, широко используются *инфраструктуры открытых ключей* (ИОК). Каждый пользователь системы владеет личным ключом, которому соответствует открытый ключ. Открытые ключи в системе распространяются в виде *сертификатов открытых ключей* (СОК) – структур, содержащих данные о владельце (*субъекте*) сертификата, информацию об *эмитенте* (стороне, которая выпустила сертификат), уникальный серийный номер сертификата, идентификатор и параметры алгоритма электронной цифровой подписи (ЭЦП), непосредственно открытый ключ пользователя, срок действия открытого ключа, полномочия пользователя и, возможно, другую дополнительную информацию. Все эти данные эмитент подписывает с помощью ЭЦП. Эмитенты сертификатов иначе называются *удостоверяющими центрами* (УЦ). Есть один главный УЦ, которому доверяют все пользователи и который называется *корневым*. Корневой УЦ может выпускать сертификаты как для отдельных пользователей, так и для подчиненных ему УЦ. Например, в государстве власть на местах делится по областям, и в каждой области действует свой УЦ, который подчиняется лишь корневому. В пределах государства можно выделить два основных уровня сложности приложений, использующих ИОК:

- *корпоративные* (*enterprise*) ИОК: приложение используется пользователями, зарегистрированными в одной ИОК;
- *распределенные* (*bridge-enabled*) ИОК: приложение используется пользователями из различных ИОК, в том числе и иностранцами.

Некоторые сертификаты могут быть признаны недействительными раньше истечения их срока действия. Для этих целей УЦ выпускают списки отозванных сертификатов (СОС). В Республике Беларусь СОК и СОС должны соответствовать СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» [1]. Там же в разделе 8 определена процедура проверки цепочки СОК и СОС (*маршрута сертификации*). Приложения, основанные на ИОК, должны реализовывать эту процедуру для проверки действительности сертификатов открытых ключей.

Маршрут сертификации представляет собой упорядоченную цепочку сертификатов, начинающуюся с сертификата, выданного корневым УЦ, и заканчивающуюся *сертификатом конечного участника* (проверяемым сертификатом). Процедура проверки маршрута сертификации позволяет гарантировать, что проверяемый сертификат действителен в текущий момент времени и выдавался законному владельцу, т. е. владелец имеет предъявляемый открытый ключ и полномочия, указанные в сертификате. Маршрут сертификации может быть ограничен путем определения стандартных расширений в одном или нескольких сертификатах маршрута, а также входными данными проверяющей стороны.

Алгоритм проверки маршрута сертификации использует информацию, содержащуюся в СОК и СОС для определения того, может ли приложение доверять предоставленному для проверки сертификату и авторизовать владельца сертификата. Информация, используемая модулем проверки маршрута сертификации (МПМС), может содержаться как в основной части СОК и СОС, так и в стандартных расширениях. Входными данными алгоритма является имя (адрес) корневого УЦ. Это не означает, что все маршруты сертификации будут начинаться с данного корневого УЦ: для каждого маршрута сертификации может быть определен свой корневой УЦ. Обычно сертификаты корневых УЦ являются *самоподписанными сертификатами*. Алгоритм проверяет, что маршрут сертификации удовлетворяет, по меньшей мере, следующим требованиям:

- для всех сертификатов x в цепочке $\{1, \ldots, n-1\}$ субъект сертификата x является эмитентом сертификата $x+1$;
- сертификат с номером 1 выпущен корневым УЦ;
- сертификат с номером n является проверяемым сертификатом конечного участника;
- все сертификаты x в цепочке $\{1, \ldots, n\}$ являются действительными в текущий момент времени.

Для тестирования реализации МПМС в НИИ ППМИ разработано Руководство по тестированию, основой которого являются «Public Key Interoperability Test Suite (PKITS) Certification Path Validation» (PKITS) [2] и «NIST Recommendation for X.509 Path Validation» [3]. Кроме того, были разработаны тестовые данные (маршруты сертификации) с использованием алгоритмов электронной цифровой подписи СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» [4] и СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» [5]. В качестве функции хэширования в сертификатах, представленных в тестах, используется функция хэширования СТБ 34.101.31-2011 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности» [6].

Руководство по тестированию

Первая версия PKITS вышла в 2004 году. Она содержит наборы тестов, покрывающие проверку корректности реализации алгоритма проверки маршрутов сертификации в МПМС, используемых как в корпоративных, так и в распределенных ИОК. В 2011 году появилась обновленная версия v.1.0.1, которая по своей структуре и набору тестов не отличается от первой версии. Отличие заключается в сроке дейст-

вия тестовых СОК и СОС (с января 2010 года по декабрь 2030 года) и в адресе сервера, на котором они расположены (он изменился по сравнению с 2004 годом).

Вместе с PKITS в том же 2004 году вышел документ «NIST Recommendation for X.509 Path Validation», в котором объясняется, как следует использовать тесты из PKITS. В частности, в нем указано, какие тесты необходимо выполнять для МПМС, используемой в корпоративной ИОК, а какие – в распределенной ИОК. Кроме того, в документе отражены требования к реализации МПМС как в корпоративной ИОК, так и в распределенной ИОК. Приложение А данного документа содержит таблицу, где для каждого теста указаны условия, при которых необходимо его выполнять. В том числе в PKITS есть и необязательные тесты, которые вообще можно не выполнять.

В разработанном в НИИ ППМИ Руководстве по тестированию были учтены все рекомендации из «NIST Recommendation for X.509 Path Validation». Структура Руководства соответствует структуре PKITS, за исключением добавленных разделов, содержащих требования по реализации МПМС в различных ИОК. С учетом ввода в Республике Беларусь государственной ИОК с единым корневым удостоверяющим центром, в Руководство были включены лишь те тесты из PKITS, которые необходимо выполнять для МПМС в корпоративной ИОК, а также обязательные тесты для любых МПМС. Необязательные тесты были исключены.

Тестовые данные

Тестовые данные можно разделить на три группы: СОК корневого УЦ (самоподписанный сертификат) и его СОС, СОК и СОС промежуточных УЦ и СОК конечных участников. Промежуточные УЦ имеют право выпускать сертификаты открытых ключей и СОС, поэтому назначение их личного ключа – подписывать СОК и СОС. Личный же ключ конечного пользователя может использоваться для подписи дынных, авторизации в системе (невозможности отказа от авторства), транспорта ключа и/или шифрования данных.

В тестовых данных PKITS СОК содержат открытые ключи алгоритма RSA [7], который может использоваться для всех перечисленных выше целей. В некоторых тестах используется алгоритм DSA [8]. В качестве функции хэширования применяется (SHA-256) [9]. В Руководстве алгоритм RSA заменен алгоритмом СТБ 34.101.45-2013 (как основным алгоритмом ЭЦП в Республике Беларусь в ближайшем будущем), алгоритм DSA – алгоритмом СТБ 1176.2-99, а алгоритм SHA-1 – алгоритмом СТБ 34.101.31-2011 (как основным алгоритмом хэширования в Республике Беларусь в ближайшем будущем). В связи с тем, что белорусские алгоритмы ЭЦП по умолчанию не используются для шифрования данных, то в тестовых сертификатах флаг **dataEncipherment** расширения **KeyUsage** везде установлен в FALSE.

Кроме того, атрибут страны «US» в тестовых данных заменен атрибутом «BY». Другие атрибуты имен не менялись, кроме нескольких специальных тестов, где, например, в названии фигурирует DSA. Идентификаторы политик NIST оставлены без изменений. Таким образом, сформированные тестовые данные удовлетворяют требованиям PKITS с учетом использования белорусских алгоритмов.

Для формирования тестовых данных была написана специальная программа на языке С, которая:

- генерирует пару ключей для сертификата;

- устанавливает идентификаторы требуемых алгоритмов и их параметры, меняет атрибут страны «US» на «BY» везде, где он может встретиться в СОК и СОС;
- устанавливает значение компонента **publicSubjectKeyInfo** СОК, расширения **AuthorityKeyIdentifier** СОК и СОС, расширений **KeyUsage** и **SubjectKeyIdentifier** СОК;
- вычисляет хэш-значение по СТБ 34.101.31-2011 от содержимого СОК (СОС) и подписывает СОК (СОС) на личном ключе эмитента.

Для самоконтроля дополнительно в программе введен режим проверки ЭЦП: программа использует открытый ключ эмитента и проверяет подпись СОК (СОС).

Библиографические ссылки

1. СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей». Госстандарт, 2012.
2. Public Key Interoperability Test Suite (PKITS): Certification Path Validation. Version 1.0.1. April 14. 2011. URL: http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html.
3. NIST Recommendation for X.509 Path Validation. Version 0.5. May 3. 2004.
4. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых». Госстандарт, 2013 (вводится в действие).
5. СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи». Госстандарт, 1999.
6. СТБ 34.101.31-2011 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности». Госстандарт, 2011.
7. PKCS#1 v.2.2 : RSA Cryptography Standard, RSA Laboratories, 2012.
8. FIPS PUB 186-3: Digital Signature Standard (DSS), 2009.
9. FIPS PUB 180-3: Secure Hash Standard (SHS), 2008.