GLOBAL 2007

Обучение Java

Тема **Безопасность в JAVA**

Часть **Сертификаты**

Автор **ASKIL (omendba@gmail.com)**

26.02.2007

Когда имеется публичный и частный ключ, необходимо обеспечить других людей этим публичным ключом.

Главная проблема с ключом состоит в том, что он не предусматривает информацию о владельце, которому принадлежит этот ключ. Ключ – всего лишь последовательность цифр. Если отправитель посылает документ, подписанный цифровой подписью, он должен отправить также публичный ключ. Но нет никакой гарантии, что полученный вами публичный ключ прибыл от предполагаемого отправителя.

Сертификаты решают эту проблему при наличии известного юридического лица, которому принадлежит сертификат. Ю.Л. проверяет публичный ключ, который рассылается всем. Сертификат может гарантировать, что публичный ключ в сертификате действительно принадлежит тому, кто эти ключи рассылает. Однако сертификат только утверждает, что публичный ключ принадлежит лицу XXX, но нет никаких доводов тому, что вы должны доверять лицу XXX. Т.о. мы не знаем, что за личность XXX. Задача определения личности отправителя называется *задачей аутентификации*.

Практически, ключ не может принадлежать лицу XXX вообще. Специальные компании, отвечающие за освидетельствование, имеют различные уровни, на которых они оценивают идентичность юридического лица, прописанного в свидетельстве. Некоторые их этих уровней очень строгие и проводят обширную проверку, что XXX – тот, кого он за себя выдает. Другие уровни – вообще не строгие.

Сертификат содержит три части информации:

1. Название юридического лица, для которого был выписан сертификат.
2. Публичный ключ.
3. Цифровая подпись.

Формат сертификата X.509

Одним из самых популярных форматов для подписанных сертификатов является формат X.509. Сертификаты такого типа широко используются многими компаниями (в том числе Verisign, Microsoft, Netscape) для подписания электронных писем, аутентификации программного кода и сертификации многих других видов данных. Стандарт X.509 является частью набора рекомендаций X.500, разработанных Консультативным комитетом по международной телефонной и телеграфной связи США (Consultative Committee for International Telephone and Telegraphy— CCITT). Простейший вариант сертификата X.509 содержит перечисленные ниже данные.

- Версия формата сертификата.
- Номер сертификата.
- Идентификатор алгоритма подписи, а также параметры, которые используются для подписания сертификата.
- Имя лица, подписавшего сертификат.
- Период действия (начальная и конечная даты).

• Имя сертифицированного объекта.

• Открытый ключ сертифицированного объекта (идентификатор алгоритма + параметры алгоритма + значение открытого ключа).

• Подпись (хэш-код всех предыдущих полей, который закодирован с помощью закрытого ключа лица, подписавшего сертификат).

Таким образом, подписавшее сертификат лицо гарантирует, что у указанного объекта есть свой открытый ключ.

Специальные расширения базового формата X.509 позволяют включать в сертификаты дополнительные данные.

Точное описание структуры сертификата X.509 содержится в официальном документе ASN.1 (abstract syntax notation #1). Чтобы пользоваться данным форматом, не обязательно использовать точный синтаксис формата X.509. Основные правила шифрования (bask encoding rules – BER) достаточно полно и четко описывают правила записи этой структуры в двоичном файле. Иначе говоря, BER-правила описывают способ шифрования целых чисел, символьных строк, битовых строк и конструкций SEQUENCE, CHOICE и OPTIONAL.