ЗИСОПД
Лекция

Стандарт X.509

X.509 — стандарт ITU-T для инфраструктуры открытого ключа (Public key infrastructure, PKI) и инфраструктуры управления привилегиями (Privilege Management Infrastructure).

Основная задача: избежать криптографической атаки «человек-посередине» методом сертификации участников информационного обмена.

Впервые опубликован ITU-T в 1988 году в качестве части рекомендаций X.500 (RFC 5280) — X.509 v1. В 1993 году — X.509 v2. Затем — X.509 v3.

X.509 определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями, которые предоставляются удостоверяющими центрами. Предполагается наличие иерархической системы удостоверяющих центров для выдачи сертификатов.

Вопросами реализации стандарта в сети Интернет занимается рабочая группа IETF, сформированная в 1995 году и более известная как Public-Key Infrastructure (X.509) working group (PKIX). Результатами её работы, в частности, стали рекомендации RFC 3280 и 5280.

X.509 стал основой для построения иерархической системы удостоверяющих центров, несмотря на появление в 1991 году технологии PGP. Стандарт поддерживается в таких протоколах и механизмах как TLS / SSL, HTTPS, IPsec, SSH и других.

Стандарт X.509 определяет понятие «сертификат с открытом ключом» и другие базовые определения PKIX. При этом сертификат с открытым ключом представляет собой определенную структуру данных, которая содержит имя пользователя, открытую составляющую ключа двухключевой криптосистемы этого пользователя и имя компании (далее — «издатель»), который подтверждает, что открытая составляющая привязана к имени пользователя. Эти данные через каждый временной интервал подписываются эмитентом. После подписания, сертификаты могут храниться на LDAP серверах. Передаются сертификаты через незащищенные обменные сообщения или через любое другое средство, которое делает сертификаты легко доступными при отправке сообщений пользователям.

Сертификат имеет ограниченный срок действия. Поскольку пользователь сертификата может самостоятельно проверить его подпись и срок действия, сертификаты могут распространяться через незащищённые каналы связи и серверные системы, а также храниться в кеш-памяти незащищённых пользовательских систем.

Структура сертификата X.509

- Сертификат
  - Версия
  - Серийный номер
  - Идентификатор алгоритма подписи
  - Имя издателя
  - Период действия:
    - Не ранее
    - Не позднее
  - Имя субъекта
  - Информация об открытом ключе субъекта:
    - Алгоритм открытого ключа
    - Открытый ключ субъекта
  - Уникальный идентификатор издателя (v2 и v3)
  - Уникальный идентификатор субъекта (v2 и v3)
  - Алгоритм подписи сертификата (v3)
- Подпись сертификата

Существуют ограничения стандарта X.509 при использовании его для шифрования сообщений электронной почты и совместной работы приложений. X.509 предлагает неполную совместимость работы приложениями.

Иерархичность

Согласно RFC 4387: в браузере хранятся не сертификаты сайтов, а сертификаты УЦ. Когда браузер получает сертификат сайта при установке соединения, он видит помимо адреса сайта ещё и «адрес» УЦ, а также цифровую подпись, которую сгенерировал УЦ с использованием своего секретного ключа. Дальше браузер берёт из локального хранилища цепь сертификатов УЦ, достаёт из него публичный ключ и с помощью него проверяет подпись в сертификате сайта. Если подпись правильная, соединение успешно устанавливается.

- Подпись каждого сертификата (за исключением последнего) является удостоверяющим центром-преемником.
- Все сертификаты, за исключением последнего, подписываются с помощью закрытого ключа следующего УЦ.
- Последний сертификат в цепи является сертификатом единственного пункта доверия, являющегося корневым УЦ.

Иерархические PKI способны быстро реагировать на компрометацию отдельного УЦ внутри инфраструктуры. Если УЦ скомпрометирован, вышестоящий УЦ аннулирует его сертификат. Как только работа УЦ восстанавливается, он выпускает новые сертификаты для всех своих пользователей. Вышестоящий УЦ выпускает для скомпрометированного УЦ новый сертификат с новым открытым ключом, что позволяет вернуть этот центр обратно в иерархию.

Список аннулированных сертификатов (CRL)

Согласно RFC 3280, CRL подписывается удостоверяющим центром и свободно распространяется через общедоступный репозиторий сертификатов. Репозиторий сертификатов обычно размещается на сервере каталогов в соответствии с международным стандартом X.500 и его подмножеством. В списке CRL каждый аннулированный сертификат опознается по своему серийному номеру. Когда у какой-то системы возникает необходимость в использовании сертификата, эта система не только проверяет подпись сертификата и срок его действия, но и просматривает последний из доступных списков CRL, проверяя, не аннулирован ли этот сертификат.

Причины:

- превышение срока действия,
- потеря или компрометация закрытого ключа, связанного с сертификатом,
- изменение хотя бы одного поля, входящего в имя владельца сертификата
- утрата или компрометация закрытого ключа УЦ, которым подписан сертификат.

Поэтому стандарт определяет формат списка с указанием сертификатов, которые стали недействительными для УЦ. Этот список подписывается УЦ для предотвращения изменений неуполномоченным лицом.

Он включает в себя дату выдачи, дату обновления (необязательно), и сам список в виде пар (серийный номер аннулированного сертификата; причина возможного аннулирования).

Большим недостатком является ограничение CRL, которое состоит в долгом поступлении информации об аннулировании сертификата. Чтобы ускорить, был разработан протокол OCSP для проверки сертификата. Описанный изначально в RFC 2560, а затем снова в RFC 6960, протокол OCSP дает почти ту же информацию, что и CRL. Сервер OCSP (Online Certificate Status Protocol) обслуживает пользователей в режиме онлайн и занимается проверкой статуса аннулирования цифрового сертификата.