Основы PKI

Введение

Инфраструктура Открытых Ключей (PKI: Public Key Infrastructure) довольно общее понятие. В него включается весь набор программно-аппараных средств для использования технологии открытых ключей, а также связанные с этим процедуры, политики, мероприятия и т.п. PKI является неотъемлемой частью информационной безопасности в Internet. Основной частью PKI является собственно система распределения ключей и управления сертификатами.
Само по себе непосредственное использование открытых ключей не предоставляет необходимого уровня защиты информации и идентификации пользователя, так как любой злоумышленник может представиться кем угодно. Например, злоумышленник, заменяя значение открытого ключа, может стать нелегальным получателем зашифрованных данных. В данном случае ни отправитель, ни получатель не знают открытые ключи друг друга и не могут их передать по незащищенному каналу с уверенностью, что между ними нет злоумышленника, изменяющего эти ключи. Здесь то мы и сталкиваемся с необходимостью участия третьей доверенной стороны (помимо легальных отправителя и получателя) - Удостоверяющего Центра.
Таким образом, мы хотим построить новую систему, где 2 стороны, участвующие в транзакции, не обязаны заранее знать всю информацию друг о друге (как открытые ключи из примера выше). Систему, которая базируется на технологии асимметричного шифрования и обеспечивает следующие свойства:

1. конфиденциальность (защита информации от просмотра при передаче и хранении)
2. аутентификацию (идентификация отправителя) и как следствие контроль доступа к ресурсу системы
3. обеспечение целостности данных (защита информации от изменения при передаче и хранении)
4. неотрекаемость (невозможность отправителя отказаться от своих действий).

Для обеспечения всех этих свойств и организации Инфраструктуры Открытых Ключей используются X.509 сертификаты и Центры Сертификации как средство формирования сертификатов и управления ими.

X.509 конечно же не единственный способ организовать Инфраструктуру Открытых Ключей. Рассмотрим некоторые из таких способов.
Инфраструктура Открытых Ключей SPKI [Simple Public Key Infrastructure] на основе сертификатов SDSI может использоваться с целью распространения сертификатов для авторизации. Главным отличием механизма сертификатов SDSI от X.509 является то, что для идентификации субъекта используются не имена, а ключи. Структура сертификатов привязывает имена либо информацию по авторизации к ключам. Эта привязка может происходить явно либо неявно с использованием хэш-функции от ключа или имени. Главной целью SDSI сертификатов является авторизация, т.е. выдача разрешения на совершение тех или иных действий. Более подробно требования к SPKI и описание SPKI/SDSI сертификатов рассмотрены в RFC 2692 и RFC 2693. Вообще говоря, стандарт SPKI/SDSI имеет пока испытательный характер и на данный момент не приходится говорить о его существенном распространении.
Другой альтернативой распространения ключей, не используя сертификаты X.509, мог бы послужить защищенный DNS. В RFC 2535 описано дополнение к стандартной службе DNS. Запись в защищенном DNS кроме информации о доменном имени и IP-адресе может содержать информацию для аутентификации с использованием цифровой подписи, а также ключ. Стандартом предусмотрено использование этих ключей с другими

протоколами Internet, время валидности подписи и т.д. Таким образом, существует возможность привязать ключ к IP адресу. Вполне понятно, что построенная таким образом Инфраструктура Открытых Ключей не может покрыть весь спектр задач и предоставить той гибкости, как и при использовании механизма X.509.

Далее пойдет описание структуры сертификатов X.509v3, широко используемых в данный момент, структуры Удостоверяющего Центра с описанием функциональности основных его компонент. Также приведена структурная схема Удостоверяющего Центра одного из российских производителей. В заключении рассказывается о списке отозванных сертификатов, его использовании, формировании и проверке цепочки сертификатов.

Структура сертификата X.509v3

В состав сертификата стандарта X.509 версии 3 входят следующие поля:

- *Версия (Version)*

Поле версия содержит номер версии данного сертификата.

- *Серийный номер (Serial Number)*

Поле серийный номер содержит целое число – идентификатор сертификата. Сертификаты, выпущенные данным Удостоверяющим Центром, имеют уникальный серийный номер. Вместе с именем издателя это поле является уникальным идентификатором сертификата.

- *Идентификатор алгоритма подписи*

Содержит идентификатор криптоалгоритма, на основе которого удостоверяющий центр подписал сертификат.

- *Имя издателя (Issuer Name)*

Поле имя издателя указывает на объект, который издал сертификат. Значение этого поля должно быть ненулевым и состоит из списка атрибутов и соответствующих им значений. Атрибуты могут быть следующими: C(Country Name), S(State Or Province Name), L(Locality Name), O(Organization Name), OU(Organizational Unit Name), CN(Common Name).

- *Срок действия (Validity Period)*

Поле срок действия содержит дату начала и дату окончания действия сертификата.

- *Имя владельца (Subject Name)*

Поле имя владельца указывает на владельца ключа подписи. Его структура полностью аналогична структуре поля Имя издателя.

- *Открытый ключ (Public Key)*

Поле открытый ключ содержит публичный ключ владельца, а также идентификатор используемого криптоалгоритма.

- *Идентификатор издателя*
- *Идентификатор владельца*
- *Дополнения (Extentions)*

ASN синтаксис дополнений выглядит следующим образом.

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING  }
```

Поле *extnID* определяет тип дополнения. Поле *critical* определяет, является ли данное дополнение критичным. Поле *extnValue* содержит всю информацию о дополнении.

Дополнения могут ограничивать область применения ключа и сам сертификат (ограничивающие дополнения). Также дополнения могут использоваться пользователем в

прикладном программном обеспечении (информационные дополнения). Далее приведены некоторые стандартные дополнения, взятые из RFC 2459.

1. Authority Key Identifier. Здесь содержится информация, с помощью идентифицируется публичный ключ, соответствующий приватному ключу, которым подписан сертификат. Это дополнение используется, когда издатель имеет несколько ключей, которыми он подписывает издаваемые сертификаты.
2. Subject Key Identifier. Здесь содержится информация, с помощью идентифицируются сертификаты, которые содержат данный публичный ключ.
3. Key Usage. Это дополнение определяет цель (шифрование, подпись, подписание сертификатов), с которой будет использоваться ключ сертификата. Другими словами здесь устанавливаются ограничения на использование ключа сертификата. Вот некоторые ограничения: digitalSignature (публичный ключ используется для простановки подписи), keyEncipherment (публичный ключ используется для транспорта ключей), dataEncipherment (публичный ключ используется для шифрования данных пользователя), keyAgreement (публичный ключ используется для выбора алгоритма установления общего ключа) и т.д.
4. Private Key Usage Period. Это дополнение позволяет издателю сертификата определить период использования приватного ключа, отличный от периода валидности сертификата.
5. Subject Alternative Name. Альтернативное имя владельца сертификата. Это дополнение позволяет более гибко идентифицировать владельца сертификата. Здесь представлены разнообразные поля, такие как DNS имя, e-мэйл, IP адрес, URI (Uniform Resource Identifier). Также здесь присутствует множественное представление имени.
6. Issuer Alternative Name. Альтернативное имя издателя сертификата. Аналогично дополнению Subject Alternative Name.
7. Basic Constraints. Основные ограничения. Здесь идентифицируется, является ли владелец сертификата Центром Сертификации и какова максимальная длина цепочки сертификатов для данного Центра Сертификации. Поле, определяющее максимальную длину цепочки, имеет значение только тогда, поле, идентифицирующее владельца как Центр Сертификации, установлено в TRUE.
8. Name Constraints. Ограничения имени. Это дополнение должно использоваться только в сертификатах Центра Сертификации. Оно идентифицирует пространство имен, которому должно соответствовать имя владельца сертификата в последующих сертификатах цепочки. Эти ограничения могут применяться к полям Subject DN и Subject Alternative Name.
9. CRL Distribution Points. Точки распространения Списков Отозванных Сертификатов (CRL: Certificate Revocation List). Здесь определяется, как может быть получен CRL. Точки распространения содержат информацию типа URI, указывающую на текущие CRL, которые изданы указанным издателем CRL.

Компоненты Удостоверяющего Центра и их функции

Основными компонентами Удостоверяющего Центра являются: Центр Сертификации, Центр Регистрации.

Центр Сертификации (CA: Certification Authority).

В основные функции Центра Сертификации входят:

1. Регистрация подчиненных Центров Сертификации.
2. Регистрация сертификатов подчиненных Центров Регистрации.
3. Обработка запросов на создание сертификатов и ключевых пар от Центра Регистрации.

4. Изменение статуса сертификата, включая создание, введение в действие, приостановление действия, возобновление действия, аннулирование.
5. Ведение базы данных с историями сертификатов в течение установленного срока хранения.
6. Подготовка Списков Отозванных Сертификатов к опубликованию.

Центр Регистрации (RA: Registration Authority).

В основные функции Центра Регистрации входят:

1. Начальная обработка запросов на создание сертификатов и ключевых пар от пользователя с последующей передачей запроса в Центр Сертификации.
2. Обработка запросов от пользователя на изменение статуса сертификата.
3. Ведение базы данных с запросами абонентов в течение установленного срока хранения.

На рисунке изображена структурная схема Удостоверяющего Центра сертификатов ключей подписи "Инега^{tm}-УЦ", разработанного ООО «Новый Адам». Схема и другая информация доступны с сайта компании [3].

Здесь одним из основных компонентов УЦ, помимо Центра Сертификации и Центра Регистрации являются Служба Реестра и Центр Арбитража.

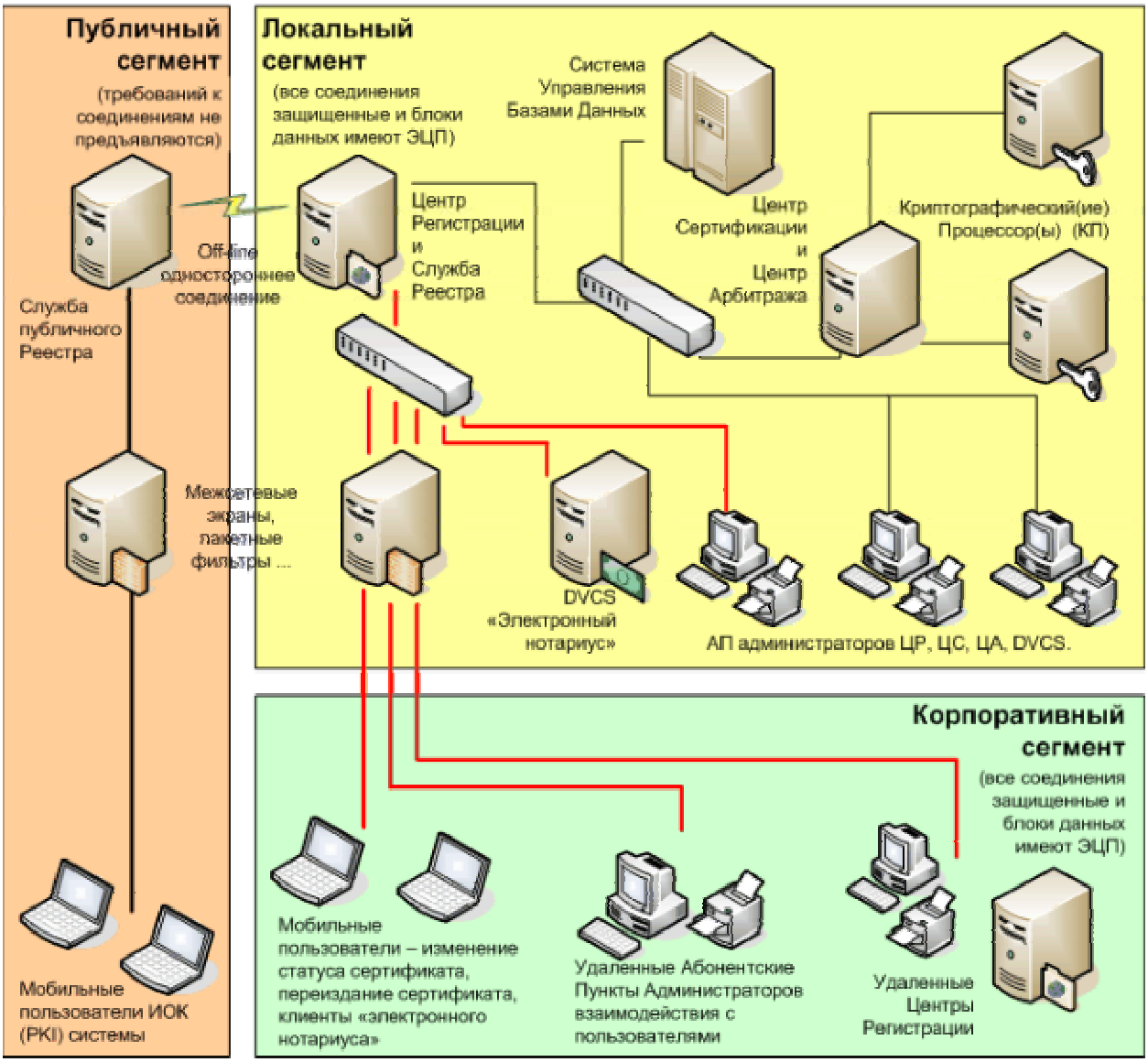
В обязанности **Службы Реестра** входят:

1. Ведение актуальной базы сертификатов/CRL, посредством взаимодействия с Центром Сертификации и Центром Регистрации.
2. Поддержка публикации CRL.
3. Организация свободного доступа.

В основные функции **Центра Арбитража** входят:

1. Регистрация конфликтных ситуаций, возникающих в процессе работы с сертификатами.
2. Осуществление официального подтверждения подлинности ЭЦП на электронном документе.

Все транзакции осуществляются с использованием защищенных протоколов (выше транспортного уровня OSI модели), и все данные, передаваемые по сети или хранящиеся на жестком диске, подписываются. Также на всех компонентах Удостоверяющего Центра предусмотрено резервное копирование.



Отзыв сертификатов и CRL

Когда издается сертификат, ожидается, что он будет использоваться в течение всего своего срока действия. Однако, по различным обстоятельствам, сертификат может стать недействительным еще до истечения своего срока действия. Такими обстоятельствами могут быть изменение имени, изменение связи владельца с Центром Сертификации (например, расторжение служащим контракта с организацией), компрометация либо предполагаемая компрометация приватного ключа. В таких случаях Центр Сертификации может отозвать сертификат.

Структура X.509 определяет способ отзыва сертификатов. Этот метод состоит в следующем: каждый Центр Сертификации периодически издает определенную подписанную структуру данных, называемую Списком Отозванных Сертификатов (CRL: Certificate Revocation List). CRL – это список с временной меткой, содержащий сертификаты, подписанные Центром Сертификации, и свободно доступный через публичный реестр. Каждый отозванный сертификат идентифицируется своим Серийным номером.

Преимущество этого метода состоит в том, что Списки Отозванных Сертификатов могут распространяться теми же самыми средствами, что и сами сертификаты. Однако существует один недостаток описанного выше метода – время отзыва сертификатов ограничивается периодом издания CRL. Например, если мы хотим узнать о статусе отзыва сертификата сейчас, мы не можем утверждать это, используя CRL, доступный на публичном сервере сейчас. Для этого мы должны дождаться следующего, периодически издаваемого CRL – а это время может составлять час, день, неделю – в зависимости от того, как часто Центр Сертификации издает CRL.
Существует критическое дополнение структуры CRL, которое называется delta-CRL. Использование delta-CRL значительно улучшает время обработки информации об отзыве сертификатов приложениями. Delta-CRL делает возможными добавление изменений в локальную базу данных игнорируя информацию, которая не изменяется и уже есть в локальной базе данных. Здесь нужно отметить, что каждый изданный Центром Сертификации delta-CRL соответствует изданному этим же Центром Сертификации CRL.

Цепочки сертификатов

Решение, доверять или нет конкретному владельцу сертификата, определяется на основании цепочки сертификатов, где конечным элементом цепочки является непосредственно сертификат владельца, а начальным – сертификат доверенного Центра Сертификации. Все промежуточные сертификаты цепочки подписаны предшествующим сертификатом, и сами подписывают последующий. Сертификат доверенного Центра Сертификации является самоподписанным и находится в персональном хранилище пользователя. Для каждого сертификата в цепочке нужно проверить:

- Основную информацию в сертификате:
  1. Что, сертификат был подписан предыдущим сертификатом цепочки или он является самоподписанным (используется публичный ключ).
  2. Что время валидности сертификата не истекло.
  3. Что сертификат не отозван в данный момент и что его действие не приостановлено.
  4. Имена владельца и издателя правильные, т.е. что издатель данного сертификата является владельцем предыдущего.
- Поля Subject Name и Subject Alternative Name дополнения.
- Регламенты (policy).
- Другие дополнения.

При успешной проверке всех этих свойств сертификат считают действительным. Для принятия утвердительного решения о доверии данному владельцу сертификата, должны быть действительными все сертификаты цепочки.

Заключение

В заключении хотелось бы отметить некоторые неудобства, с которыми сталкивается пользователь при использовании Инфраструктуры Открытых Ключей с использованием механизма X.509.

- Логичнее было бы использовать механизм, в котором за основу взят идентификатор владельца (либо ключ), а не DN (даже с использованием дополнений). Причин по крайней мере две. Во-первых, владелец может изменять место работы, e-mail, даже имя. Во-вторых, владелец мог бы иметь несколько сертификатов с одним и тем же идентификатором.

- Возникает неудобство в использовании иерархической структуры, когда Центр Сертификации прекращает свое действие. В этом случае становятся недействительными все сертификаты, им подписанные.
- Сертификаты не предоставляют право на совершение каких-либо действий, а служат лишь для аутентификации пользователя (Центр Сертификации только издает сертификат, но не предоставляет при этом каких либо прав).
- Возникают некоторые ограничения при использовании сертификатов с различным прикладным программным обеспечением.
- Иерархическая модель сертификатов – это нетипичная модель для бизнеса. Когда в сделке участвуют 2 стороны, то вовлечение третьей стороны является дополнительным усложнением.

Источники

1. RFC 2459. Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
2. Инфраструктура Открытых Ключей от Валидата (http://www.x509.ru).
3. Веб-сайт компании «Новый Адам» http://adam.ru.
4. Encryption and Security Tutorial (http://www.cs.auckland.ac.nz/~pgut001/tutorial).

Сухих Алексей, 015гр.