93: Общие сведения об инфраструктуре открытых ключей

Информационное обеспечение:

Что такое PKI? Главное об инфраструктуре открытых ключей. – https://habr.com/ru/post/655135/

Инфраструктура открытых ключей. – http://security.demos.ru/crypto/pki/

Инфраструктура открытых ключей. – https://dic.academic.ru/dic.nsf/ruwiki/151605

Public Key Cryptography: осваиваем открытые ключи на практике. – https://xakep.ru/2016/03/11/pki/

Актуализация опорных знаний

Существующие криптосистемы можно разделить на два класса — **симметричные** и **асимметричные**.

В **симметричных** схемах шифрования (классическая криптография) секретный ключ шифрования совпадает с секретным ключом дешифрования.
В **асимметричных** схемах шифрования (криптография с открытым ключом) ключ шифрования не совпадает с ключом дешифрования.

Методы симметричного шифрования часто называют также «методы шифрования с закрытым (секретным) ключом». Соответственно методы асимметричного шифрования называют методами с открытым ключом.

Алгоритм Диффи-Хеллмана

Метод Диффи—Хеллмана используется для обмена секретными ключами без передачи их по открытому каналу связи. Он основан на использовании свойств односторонних функций.

Пусть абоненты Алиса и Боб решили обмениваться шифрованными сообщениями, но в их распоряжении имеется только незащищенный открытый канал связи, при этом никаких возможностей встретиться или передать секретный ключ через кого-нибудь другого у них нет.

В соответствии с алгоритмом Диффи—Хеллмана для успешного решения задачи Алиса и Боб должны выполнить следующие действия. Прежде всего они открыто договариваются о том, что будут использовать одностороннюю функцию $Y = D^x \bmod P$. Затем они договариваются о значениях параметров D и P. Пусть, например, они договорились, что D = 7 и P = 13, то есть функция имеет вид $Y = 7^x \bmod 13$. Еще раз подчеркнем, что в соответствии с алгоритмом Диффи—Хеллмана вся эта информация не является секретной.

Дальнейшие действия участников обмена описываются в табл.1.

Таблица 1. Действия Алисы и Боба в соответствии с алгоритмом Диффи—Хеллмана

	Действия Алисы		Действия Боба	
1	Алиса секретным образом выбирает произвольное число A (закрытый ключ Алисы)	Пусть, например, A = 2	Боб также секретно выбирает произвольное число B (закрытый ключ Боба)	Пусть, например, B = 4
2	Алиса вычисляет значение a односторонней функции Y, используя в качестве аргумента свое секретное число A: то есть $a = D^A \bmod P$	$a = D^A \bmod P = 7^2 \bmod 13 = 10$	Боб также вычисляет значение b односторонней функции У, используя в качестве аргумента свое секретное число B: $b = D^B \bmod P$	$b = D^B \bmod P = 7^4 \bmod 13 = 2401 \bmod 13 = 9$

	(открытый ключ Алисы)		(открытый ключ Боба)	
3	Алиса посылает Бобу свой открытый ключ a	10	Боб посылает Алисе свой открытый ключ b	9
4	Алиса, получив от Боба число b, вычисляет по формуле $K = b^A \bmod P$ (разделяемый секретный ключ)	$K = b^A \bmod P = 9^2 \bmod 13 = 81 \bmod 13 = 3$	Боб, получив от Алисы число a, вычисляет по формуле $K = a^B \bmod P$ (разделяемый секретный ключ)	$K = a^B \bmod P = 10^4 \bmod 13 = 10000 \bmod 13 = 3$

По правилам модульной арифметики

$$b^a \bmod P = (D^B \bmod P)^A \bmod P = D^{BA} \bmod P$$
$$a^b \bmod P = (D^A \bmod P)^B \bmod P = D^{BA} \bmod P$$

В результате описанной процедуры на шаге 4 Алиса и Боб получили одно и то же число 3. Это и есть общий секретный ключ.

Алгоритм RSA

Обмен сообщениями по протоколу RSA происходит следующим образом:
1. Абонент-получатель шифрованных сообщений Б генерирует открытый и закрытый ключи.
2. Открытый ключ получатель Б рассылает всем отправителям (в том числе А).
3. Отправитель (А) шифрует сообщение открытым ключом получателя Б и отправляет его получателю.
4. Получатель Б расшифровывает сообщение своим закрытым ключом.

Пусть пользователь Алиса хочет передать пользователю Бобу сообщение «8275».

1. В этом случае вначале пользователь Боб должен подготовить открытый и закрытый ключи. Пусть им выбраны, например, следующие параметры:

два случайных простых числа (для простоты расчетов примем очень маленькие числа) $P = 3$ и $Q = 11$, тогда

$N = P \cdot Q = 3 \cdot 11 = 33$ $\quad F = (P - 1)\cdot(Q - 1) = 2 \cdot 10 = 20$

2. Затем пользователь Боб выбирает любое число D, **не имеющее общих делителей с F**. Пусть $D = 13$. Это число будет одним из компонентов открытого ключа: (D, N) = (3, 33).

Далее необходимо найти число E, которое можно будет использовать в качестве закрытого ключа для расшифровки сообщения. **Значение E должно удовлетворять соотношению $ED \bmod F = 1$** . В нашем случае подходит E =17. (Проверяем: 13*17 mod 20 = 221 mod 20 = 1.) Это – закрытый ключ.

3. Теперь пользователь Боб должен запомнить свой закрытый ключ 17 (число *E*), отправить открытый ключ (13, 33) пользователю Алисе и уничтожить числа $P = 3$ и $Q = 11$.

4. Пользователь Алиса, получивший открытый ключ (13, 33), увидев, что N=33, разбивает исходное сообщение на три блока, причем значение каждого меньше N. В нашем случае получаем три блока m_1=8, m_2=27, m_3,=5. Затем пользователь А шифрует каждый блок: $c_i = m_i^D \bmod N$:

$c_1=8^{13} \bmod 33 = 17$ $c_2 = 27^{13} \bmod 33 = 15$ $c_3 = 5^{13} \bmod 33 = 26$

Вычисление модуля от степени числа упрощается при использовании следующего правила:

$$(Y^{a+b+c}) \bmod P = (Y^a \bmod P \times Y^b \bmod P \times Y^c \bmod P) \bmod P$$

Зашифрованное сообщение, состоящее из трех блоков (17, 15, 26), передается пользователю Бобу.

5. Далее Боб, используя свой закрытый ключ $E = 17$ и N=33, расшифровывает сообщение: $m_i = c_i^E \bmod N$:

$m_1 = 17^{17} \bmod 33 = 8$ $m_2 = 15^{17} \bmod 33 = 27$ $m_3 = 26^{17} \bmod 33 = 5$

Таким образом, абонент Б расшифровал сообщение от абонента А.

Общие сведения об инфраструктуре открытых ключей (PKI)

Определение

Инфраструктура открытых ключей (ИОК, англ. ***PKI*** — *Public Key Infrastructure*) — это термин, подразумевающий **набор мер и политик**, позволяющих развертывать и управлять одной из наиболее распространенных форм онлайн-шифрования — шифрованием с открытым ключом.

Помимо того, что PKI является хранителем ключей для вашего браузера, он также обеспечивает защиту различных инфраструктур, включая внутреннюю коммуникацию внутри организаций, Интернета вещей (IoT), одноранговых соединений (P2P) и так далее.

Другое определение:

Public Key Infrastructure (PKI) - совокупность сервисов для управления ключами и цифровыми сертификатами пользователей, программ и систем.

Упрощенно,

PKI представляет собой систему, основными компонентами которой являются удостоверяющий центр и пользователи, взаимодействующие между собой используя сертификаты, выданные этим удостоверяющим центром.

В PKI участвуют как минимум три стороны: минимум два пользователя (назовем их Алиса, Боб) и удостоверяющий центр (УЦ). У Алисы и Боба есть сертификаты с закрытым ключом, подписанные так называемым корневым сертификатом УЦ. У Алисы есть сертификат Боба с открытым ключом, а у Боба — сертификат Алисы с открытым ключом. Алиса и Боб доверяют УЦ и благодаря этому могут доверять друг другу.

Деятельность инфраструктуры управления открытыми ключами осуществляется на основе регламента системы. Инфраструктура открытых ключей основывается на использовании принципов криптографической системы с открытым ключом.

Инфраструктура управления открытыми ключами состоит из центра сертификации, конечных пользователей и опциональных компонентов: центра регистрации и сетевого справочника.

PKI использует технологию открытых ключей для:

- идентификации участников электронного обмена (пользователей, программ, систем),
- обеспечения конфиденциальности информации,
- контроля за целостностью информации,
- установления происхождения информации.

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- ❑ закрытый ключ известен только его владельцу;
- ❑ удостоверяющий центр создает сертификат открытого ключа, таким образом удостоверяя этот ключ;
- ❑ никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- ❑ удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Существует два основных типа PKI:

• **Веб-PKI**, также известный как «Internet PKI. По умолчанию он работает с браузерами и со всем остальным, что использует TLS
• **Внутренний (или локальный) PKI** — это PKI, который используется для собственных нужд

, а именно для зашифрованных локальных сетей, контейнеров данных, корпоративных ИТ-приложений или корпоративных конечных точек, таких как ноутбуки и телефоны.

Внутри PKI имеется открытый криптографический ключ, который используется не для шифрования данных, а, скорее, для аутентификации общающихся сторон.

Это как вышибала возле элитного клуба: ты не попадешь туда, если тебя нет в списке. Однако без этого «вышибалы» концепция *безопасного* онлайн-общения будет невозможна.

Основные задачи

Основные задачи системы информационной безопасности, которые решает инфраструктура управления открытыми ключами:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи;
- обеспечение возможности подтверждения совершенных пользователями действий с информацией (неотказуемость, или апеллируемость — англ. non-repudiation).

PKI напрямую не реализует авторизацию, доверие, именование субъектов криптографии, защиту информации или линий связи, но может использоваться как одна из составляющих при их реализации.

Основная идея

Задачей PKI является определение политики выпуска цифровых сертификатов, выдача их и аннулирование, хранение информации, необходимой для последующей проверки правильности сертификатов.

В число приложений, поддерживающих PKI, входят: защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной цифровой подписью (ЭЦП).

Деятельность инфраструктуры управления открытыми ключами осуществляется на основе регламента системы.

Инфраструктура открытых ключей основывается на использовании принципов криптографической системы с открытым ключом.

Инфраструктура управления открытыми ключами состоит из центра сертификации (удостоверяющего центра — УЦ), конечных пользователей, и опциональных компонентов: центра регистрации и сетевого справочника.

> **PKI оперирует в работе сертификатами**. Сертификат — это электронный документ, который содержит электронный ключ пользователя, — открытый или же ключевую пару (keypair), — информацию о пользователе, которому принадлежит сертификат, удостоверяющую подпись центра выдачи сертификатов (УЦ) и информацию о сроке действия сертификата.

Для того, чтобы клиент мог работать с удостоверяющим центром, необходимо включить центр в список доверенных. После включения в этот список, любой сертификат, выданный доверенным центром, считается достоверным, а его владелец — достойным доверия.

Удостоверяющий центр также публикует и списки отозванных сертификатов (Certificate Revocation List/CRL), которые могут использовать клиенты инфраструктуры открытого ключа, когда решают вопрос о доверии сертификату пользователя и/или компьютера.

> ***Ключевая пара*** — это набор, состоящий из двух ключей: закрытого ключа (private key) и открытого ключа (public key).

Эти ключи создаются вместе, являются комплементарными по отношению друг к другу (то, что зашифровано с помощью открытого ключа можно расшифровать, только имея закрытый ключ, а подпись сделанную с помощью закрытого ключа можно проверить используя открытый ключ).

Создаётся пара ключей либо центром выдачи сертификатов (удостоверяющим центром), по запросу пользователя, или же самим пользователем с помощью специального программного обеспечения. Пользователь делает запрос на сертификат, после чего, после процедуры идентификации пользователя, центр выдаёт ему сертификат со своей подписью. Эта подпись свидетельствует о том, что данный сертификат выдан именно этим центром выдачи сертификатов и никем другим.

> Закрытый ключ используется для подписи данных, открытый ключ в свою очередь используется для шифрования данных. Открытый ключ известен всем, а закрытый ключ хранится в тайне.

Владелец закрытого ключа всегда хранит его в защищённом хранилище и ни при каких обстоятельствах не должен допустить того, чтобы этот ключ стал известным злоумышленникам или другим пользователям. Если же закрытый ключ всё таки станет известен злоумышленникам, то он считается скомпрометированным и должен быть отозван и заменен. Только владелец закрытого ключа может подписать данные, а также расшифровать данные, которые были зашифрованы открытым ключом, соответствующим закрытому ключу владельца. Подпись на данных или письме гарантирует авторство

полученной информации и то, что информация в процессе передачи не подверглась изменениям. Подпись двоичного кода гарантирует, что данное программное обеспечение действительно произведено указанной компанией и не содержит вредоносного кода, если компания это декларирует.

Структура и принципы работы PKI

Основные компоненты PKI

PKI реализуется в модели клиент-сервер, то есть проверка какой-либо информации, предоставляемой инфраструктурой может происходить только по инициативе клиента.

Основные компоненты PKI:

- **Удостоверяющий центр** (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей. УЦ является главным управляющим компонентом PKI:
  1. он является доверенной третьей стороной (trusted third party)
  2. это сервер, который осуществляет управление сертификатами.
- **Сертификат открытого ключа** (чаще всего просто *сертификат*) — это данные пользователя и его открытый ключ, скрепленные подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет секретным ключом, который соответствует этому открытому ключу.
- **Регистрационный центр** (РЦ) — необязательный компонент системы, предназначенный для регистрации пользователей. Для этих целей РЦ обычно предоставляет web-интерфейс. Удостоверяющий центр доверяет регистрационному центру проверку информации о субъекте. Регистрационный центр, проверив правильность информации, подписывает её своим ключом и передаёт удостоверяющему центру, который, проверив ключ регистрационного центра, выписывает сертификат. Один регистрационный центр может работать с несколькими удостоверяющими центрами (то есть состоять в нескольких PKI), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.
- **Репозиторий** — хранилище, содержащее сертификаты и списки отозванных сертификатов (COC) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется *реестр сертификатов ключей подписей*.
- **Архив сертификатов** — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком дей-

ствия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.

- **Центр запросов** — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат.
- **Конечные пользователи** — пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

Принцип работы

> PKI выстраивается вокруг двух основных концепций – **ключи** и **сертификаты**.

Как и в случае с машиной «Энигма», где настройки используются для шифрования сообщения (или установления безопасного протокола), ключом внутри PKI является длинная строка битов, используемая для шифрования или дешифрования закодированных данных. Основное различие между машиной Enigma и PKI заключается в том, что с последней вы должны каким-то образом сообщить получателю настройки, используемые для кодирования зашифрованного сообщения.

> Инфраструктура открытых ключей называется именно так, потому что каждая сторона в защищенном соединении имеет два ключа: открытый и закрытый.

Открытый ключ известен всем и используется во всей сети для кодирования данных, но доступ к данным невозможен без закрытого ключа, который используется для декодирования. Эти два ключа связаны сложными математическими функциями, которые трудно перепроектировать или взломать грубой силой. Кстати, этот принцип является воплощением *ассиметричной криптографии.*

Так шифруются данные в инфраструктуре открытых ключей. Но давайте не будем забывать, что проверка личности не менее важна при работе с PKI, и именно здесь в игру вступают сертификаты.

> Сертификаты PKI чаще всего рассматриваются как цифровые паспорта, содержащие множество присвоенных данных.

Одна из наиболее важных частей информации в таком сертификате связана с открытым ключом: сертификат – это механизм, с помощью которого этот ключ передается. Точно так же, как, например, когда вы предоставляете кому-то своё удостоверение личности.

Но на самом деле это удостоверение недействительно, если оно не выдано каким-то легитимным органом. В нашем случае такой орган — это **центр сертификации (ЦС).** Здесь есть подтверждение надежного источника, что субъект является тем, за кого себя выдает.

Некоторые основные моменты

Разберём подробнее следующие моменты:

- В чём заключается работа УЦ
- Как происходит выдача сертификата, обмен открытыми ключами и как понять, что открытый ключ, который мы имеем, не фальшивый
- Какие бывают PKI.

УЦ и его работа

Основная работа удостоверяющего центра заключается в идентификации пользователей и их запросов на сертификаты, в выдаче пользователям сертификатов, в проверке подлинностей сертификатов

и в проверке по сертификату, не выдаёт ли пользователь сертификата себя за другого, в аннулировании или отзыве сертификатов, в ведении списка отозванных сертификатов.

Процесс работы с сертификатами

Для того чтобы получить сертификат, нужно найти какой-либо УЦ в интернете (альтернативным решением является использование ПО PGP или ему подобных), после чего выписать сертификат и установить его себе в систему.

Обычно этот процесс происходит автоматически. После установки сертификата его можно будет увидеть у себя в хранилище личных сертификатов. Для того чтобы просмотреть его свойства, достаточно просто открыть его. (Для операционных систем семейства Windows: Пуск -> Выполнить -> certmgr.msc -> OK). В свойствах можно увидеть время действия сертификата, кем он был выдан, кому был выдан, его уникальный номер и прочие свойства. После получения сертификатов двумя или более пользователями от одного УЦ, происходит организация простейшей по архитектуре PKI. PKI — с одиночным УЦ. Пользователи, сохранив сертификаты в файл обмениваются ими (таким образом происходит обмен открытыми ключами) и начинают защищённую переписку. Проверка подлинности полученного открытого ключа проводится по электронному отпечатку этого ключа. В простейшем случае достаточно позвонить коллеге выславшему открытый ключ и сверить с ним электронный отпечаток ключа. Если он совпал — можно смело начинать защищённую переписку, если нет — обменяться ключами ещё раз.

Архитектуры PKI

В основном выделяют 5 видов архитектур PKI, это:

- ❑ простая PKI (одиночный УЦ)
- ❑ иерархическая PKI
- ❑ сетевая PKI
- ❑ кросс-сертифицированные корпоративные PKI
- ❑ архитектура мостового УЦ

В основном PKI делятся на разные архитектуры по следующим признакам:

- количество УЦ (а также количество УЦ, которые доверяют друг-другу)
- сложность проверки пути сертификации
- последствия выдачи злоумышленника себя за УЦ

Рассмотрим более подробно каждую из архитектур PKI в отдельности.

1. Простая PKI

Как уже говорилось выше, самая простая из архитектур, это архитектура одиночного УЦ. В данном случае все пользователи доверяют одному УЦ и переписываются между собой. В данной архитектуре, если злоумышленник выдаст себя за УЦ, необходимо просто перевыпустить все выписанные сертификаты и продолжить нормальную работу.

2. Иерархическая PKI

Иерархическая структура — это наиболее часто встречающаяся архитектура PKI. В данном случае во главе всей структуры стоит один Головной УЦ, которому все доверяют и ему подчиняются нижестоящие УЦ. Кроме этого головного УЦ в структуре присутствуют ещё не один УЦ, который подчиняется вышестоящему, которому в свою очередь приписаны какие-либо пользователи или нижестоящие УЦ. Частный пример иерархической PKI — корпоративная PKI. Например если у нас есть одна большая фирма, у которой в подчинении множество филиалов по всей стране. В главном здании фирмы есть головной УЦ и в каждом филиале есть УЦ, который подчиняется головному. В иерархической PKI, даже если злоумышленник выдал себя за какой — либо УЦ, сеть продолжает работать без него, а когда он восстанавливает нормальную работоспособность — он просто снова включается в структуру.

3. Сетевая PKI

Сетевая архитектура PKI строится как сеть доверия, многочисленные удостоверяющие центры которой предоставляют PKI-сервисы и связаны одноранговыми, то есть равноправными, отношениями. Но в данном случае нет одного головного УЦ, которому все доверяют. В этой архитектуре все УЦ доверяют рядом стоящим УЦ, а каждый пользователь доверяет только тому УЦ, у которого выписал сертификат. Удостоверяющие центры выпускают сертификаты друг для друга; пара сертификатов описывает двусторонние отношения доверия. В данную архитектуру PKI легко добавляется новый УЦ, для этого ему нужно обменяться сертификатами, по крайней мере, с одним УЦ, который уже входит в сеть. В данной архитектуре наиболее сложное построение цепочки сертификации.

Сетевые PKI обладают большой гибкостью, так как имеют многочисленные пункты доверия. Компрометация одного УЦ не отражается на сетевой PKI в целом: удостоверяющие центры, которые выпустили сертификаты для скомпрометированного УЦ, просто аннулируют их, тем самым удаляя из инфраструктуры ненадежный УЦ. В результате не нарушается работа поль-

зователей, связанных с другими удостоверяющими центрами, — они по-прежнему могут полагаться на надежные пункты доверия и защищенно связываться с остальными пользователями своей PKI. Компрометация сетевой PKI приводит либо к тому, что сворачивается работа одного УЦ вместе с его сообществом пользователей, либо, если стали ненадежными несколько удостоверяющих центров, к тому, что PKI распадается на несколько меньших инфраструктур. Восстановление после компрометации сетевой PKI происходит проще, чем иерархической, прежде всего, потому что компрометация затрагивает меньше пользователей.

Построить путь сертификации в сети достаточно сложно, поскольку этот процесс не детерминирован и имеются многочисленные варианты формирования цепи сертификатов. Одни из них приводят к построению правильного пути, другие — заводят в тупик. По этой причине валидация пути сертификации часто выполняется одновременно с его построением, частью этого процесса является удаление неверных ветвей. Для построения правильного пути используется несколько дополнительных полей сертификатов.

4. Архитектура кросс-сертифицированной корпоративной PKI

Данный вид архитектуры можно рассматривать как смешанный вид иерархической и сетевой архитектур. Есть несколько фирм, у каждой из которых организована какая-то своя PKI, но они хотят общаться между собой, в результате чего возникает их общая межфирменная PKI.В архитектуре кросс-сертифицированной корпоративной PKI самая сложная система цепочки сертификации.

5. Архитектура мостового УЦ

Архитектура мостового УЦ разрабатывалась для того, чтобы убрать недостатки сложного процесса сертификации в кросс-сертифицированной корпоративной PKI. В данном случае все компании доверяют не какой-то одной или двум фирмам, а одному определённому мостовому УЦ, который является практически их головным УЦ, но он не является основным пунктом доверия, а выступает в роли посредника между другими УЦ.

Использование PKI

Примеры использования PKI

Электронно-цифровая подпись (ЭЦП)

Сторона А формирует ЭЦП документа и отправляет документ стороне Б. Сторона Б запрашивает сертификат открытого ключа стороны А у удостоверяющего центра, а также информацию о действительности сертификата. Если сертификат стороны А действителен и проверка ЭЦП прошла успешно, значит документ был подписан стороной А, а не кем-то другим.

Шифрование сообщений

Сторона Б зашифровывает документ открытым ключом стороны А. Чтобы убедиться, что открытый ключ действительно принадлежит стороне А, сторона Б запрашивает сертификат открытого ключа у удостоверяющего

центра. Если это так, то только сторона А может расшифровать сообщение, так как владеет соответствующим закрытым ключом.

Авторизация

Сертификаты могут использоваться для подтверждения личности пользователя и задания полномочий, которыми он наделен. В числе полномочий субъекта сертификата может быть, например, право просматривать информацию или разрешение вносить изменения в материал, представленный на web-сервере.

Область применения PKI

PKI отлично подходит для защиты веб-трафика: данные, проходящие через Интернет, могут быть легко перехвачены и прочитаны, если они не зашифрованы. Более того, может быть трудно доверять личности отправителя, если нет какой-то процедуры проверки.

Сертификаты SSL/TLS (защищающие действия в Интернете) демонстрируют наиболее распространенную реализацию PKI, но список на этом не заканчивается. PKI также может быть использован для:

• Цифровых подписей в программном обеспечении;

• Ограниченного доступа к корпоративным интранетам и VPN;

• Бесплатного доступа к Wi-Fi без пароля в зависимости от владельца устройства;

• Процедуры шифрования электронной почты и данных.

Использование PKI растет в геометрической прогрессии, в наши дни даже микроволновая печь может подключиться к Instagram. Этот развивающийся мир устройств Интернета вещей ставит перед нами новые задачи, и даже устройства, которые, казалось бы, существуют в закрытых средах, теперь требуют безопасности. Многие из наиболее убедительных примеров использования PKI сегодня сосредоточены вокруг Интернета вещей. Производители автомобилей и производители медицинских изделий — вот ещё два ярких примера отраслей, которые в настоящее время внедряют PKI для устройств Интернета вещей. Электронная система медицинского освидетельствования Эдисона также является прекрасным примером.

Функции PKI

- **Регистрация (Registration)** - процесс сбора информации о пользователе и проверки ее подлинности, которая затем используется при регистрации пользователя, в соответствии с правилами безопасности.
- **Выдача сертификата (Certificate Issuance)**. Как только CA подписал сертификат он выдается просителю и/или отправляется в хранилище сертификатов. CA проставляет на сертификатах срок действия, требуя таким образом периодического возобновления сертификата.
- **Аннулирование сертификата (Certificate Revocation)**. Сертификат может стать недействительным до окончания срока действия в силу различных причин: пользователь уволился из компании, сменил имя или если его

частный ключ был скомпрометирован. При этих обстоятельствах CA аннулирует сертификат, занося его серийный номер в CRL.

- **Восстановление ключа (Key Recovery)**. Дополнительная функция PKI позволяет восстанавливать данные или сообщения в случае утери ключа.
- **Управление работой (Lifecycle Management)** - постоянная поддержка сертификатов в PKI, включающая обновление, восстановление и архивирование ключей. Эти функции выполняются периодически, а не в ответ на специальные запросы. Автоматизированное управление ключами наиболее важная функция для больших PKI. Ручное управление ключами может ограничить масштабируемость PKI.

Стандарты и протоколы

Протоколы PKI

Информация, необходимая для работы PKI, содержится в стандарте **X.509**

- **IPSec (IP Security)**. Набор протоколов разрабатываемых Internet Engineering Task Force (IETF) для встраивания улучшенных средств безопасности в IP уровень. Используется для осуществления безопасной связи. IPSec один из наиболее популярных протоколов, использующихся для построения частных виртуальных сетей (VPN). IPSec требует использования ключей для шифрования и идентификации, и PKI масштабируемый способ управления IPSec ключами.
- **LDAP (Lightweight Directory Access Protocol)**. Упрощенная реализация стандартов X.500, которая совместима с TCP/IP сетями. LDAP - протокол, чаще всего использующийся для доступа к сертификатам и списку аннулированных сертификатов.
- **PKIX (PKI for X.509 certificates)**. Рабочая группа IETF совершенствует стандарты открытых ключей для использования в Интернете. PKIX - это передовое средство совместимости PKI стандартов.
- **S/MIME (Secure Multipurpose Internet Mail Extensions)**. Разработка EITF для безопасного обмена сообщениями всех типов. S/MIME определяет тип шифрования и/или цифровой подписи электронного сообщения, используя шифрование с открытым ключом.
- **SSL (Secure Sockets Layer)**. SSL и развивающийся IETF стандарт, TLS (Transport Layer Security), который основан на SSL, самые важные протоколы для обеспечения безопасного доступа к web-серверам. SSL и TLS так же используются для обеспечения общей безопасности при обращении пользователя к серверу во множестве не-web-приложений. Оба используют PKI при получении сертификатов для пользователей и серверов.
- **VPN (Virtual Private Network)**. Туннель зашифрованной информации проложенный поверх общей сети, для обеспечения конфиденциальности, такой же как и в частной сети, как при соединении серверов (или роутеров)

друг с другом так и при обращении пользователя к серверу (client-to-server). Перспективный стандарт для создания туннелей при общении серверов друг с другом - протокол IPSec.

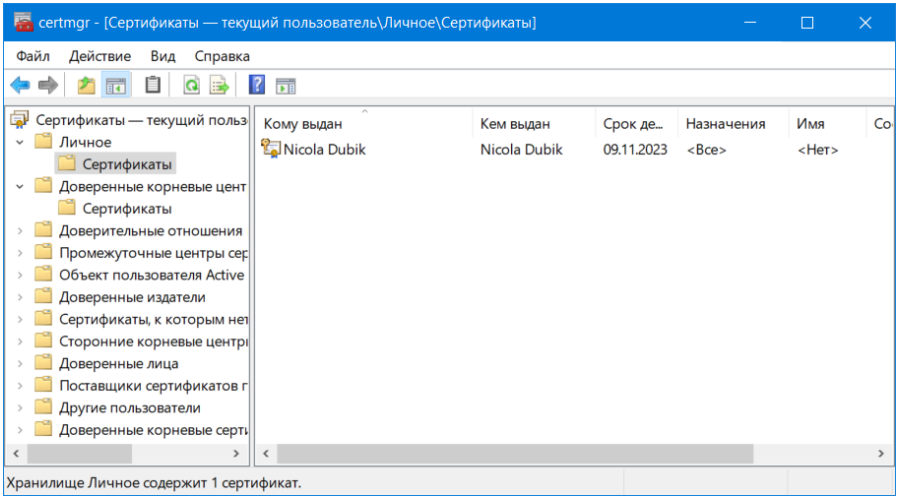
Сертификаты X.509

Так повелось, что

> основным «активом» в PKI является сертификат **X.509**.

Сертификат — это что-то вроде паспорта, он содержит информацию, позволяющую идентифицировать субъект, которому выдан сертификат (поле Subject), указывает, кем он был выпущен (поле Issuer), серийный номер сертификата и многое другое.

> В Windows управлять сертификатами можно с помощью оснастки «Сертификаты» (**run->certmgr.msc**).

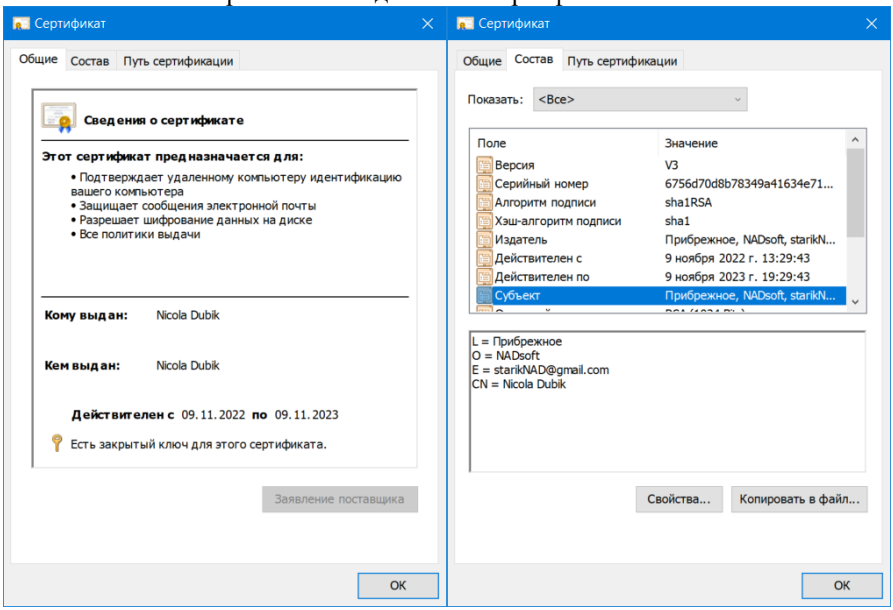


Менеджер сертификатов

Сертификаты хранятся в хранилищах («Личное», «Доверенные центры сертификации», «Доверенные лица»...).

При получении сертификата важно установить его в правильное хранилище. Так, сертификаты, которые вы хотите использовать для электронной подписи, должны быть установлены в хранилище «Личное», а сертификаты получателей, которым нужно будет отправлять зашифрованные сообщения, — в хранилище «Доверенные лица». Сертификаты удостоверяющих центров (УЦ) должны быть установлены в хранилище «Доверенные корневые центры сертификации». При установке сертификата система предлагает два варианта: выбрать хранилище автоматически либо указать вручную. Рекомендую использовать второй вариант, так как автоматика иногда устанавливает сертификат не в то хранилище. Сертификат, которым мы хотим подписывать

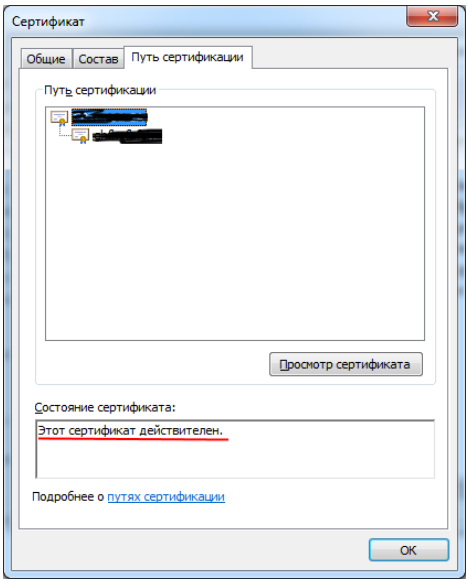
сообщения, должен иметь закрытый ключ. О наличии закрытого ключа можно узнать, посмотрев на свойства сертификата, где русским по белому будет написано: «есть закрытый ключ для этого сертификата».



Закрытый ключ для сертификата. Состав сертификата

Самое интересное о сертификате мы можем узнать на вкладке «Состав».

Обратите внимание на поля «Алгоритм подписи», «Алгоритм хеширования подписи» и «Открытый ключ». Если хотите использовать сертификат для осуществления транзакций в России, во всех этих полях вы должны видеть слово «ГОСТ». Также следует обратить внимание на значение поля «Использование ключа» и поля «Действителен с» и «Действителен по»: первое позволит понять, возможно ли использование сертификата для выполнения нужной нам операции (шифрование, подпись), а второе и третье — возможно ли использовать данный сертификат в указанный момент времени. В дополнение к этому следует убедиться, что сертификат действителен. В этом нам поможет вкладка «Путь сертификации». Если с сертификатом все хорошо, мы увидим надпись: «Этот сертификат действителен».



Состояние сертификата

Развертывание PKI

Процесс развертывания PKI состоит из нескольких этапов, каждый из которых должен сопровождаться соответствующим документированием и проверками:

- ❑ Предварительный этап
- ❑ Проектирование.
- ❑ Создание прототипа.
- ❑ Пилотный проект.
- ❑ Внедрение.

Каждый из этапов создания PKI дает результат в виде явно оформленного "продукта", позволяющего убедиться в законченности и общем продвижении процесса.

Предварительный этап

Предварительный этап включает:

- ❑ подготовительную работу для принятия решения о необходимости развертывания инфраструктуры,
- ❑ оценку материальных ресурсов и финансовых возможностей организации,
- ❑ определение цели развертывания и сферы применения PKI,
- ❑ выбор приоритетных сервисов безопасности,

- ❑ анализ данных и приложений PKI.

Дополнительные материалы

из чего состоит PKI:

• **Центр сертификации**, который выдает цифровые сертификаты, подписывает их своим открытым ключом и хранит в репозитории для справки;

• **Регистрирующий орган**, который проверяет личность тех, кто запрашивает цифровые сертификаты. Центр сертификации может выступать в качестве своего регистрационного органа или использовать для этого третью сторону;

• **База данных сертификатов,** в ней хранятся как сами сертификаты, так и их метаданные и, самое главное, даты истечения срока действия;

• **Политика сертификатов —** описание процедур PKI (в основном это набор инструкций, который позволяет оценить, насколько надежен PKI).

****

Внедрение инфраструктуры управления открытыми ключами с учетом снижения затрат и сроков внедрения осуществляется в течение семи этапов.

- Этап 1. Анализ требований к системе.
- Этап 2. Определение архитектуры.
- Этап 3. Определение регламента.
- Этап 4. Обзор системы безопасности. Анализ и минимизация рисков.
- Этап 5. Интеграция.
- Этап 6. Развертывание.
- Этап 7. Эксплуатация.

****

Компоненты PKI

- **Сертификационный центр (Certificate Authority (CA))** - часть системы открытых ключей, которая выпускает сертификат для подтверждения прав пользователей или систем обратившихся с запросом. Она создает сертификат и подписывает его, используя частный ключ. Благодаря своей функции по созданию сертификатов, сертификационный центр является центральной частью PKI.
- **Хранилище сертификатов (Certificate Repository)**. Хранилище действующих сертификатов и списка аннулированных (Certificate Revocation Lists (CRLs)). Приложения проверяют пригодность сертификата и уровень доступа предоставляемый им, сверяя с образцом содержащимся в хранилище.
- **Сервер восстановления ключей (Key Recovery Server)** - сервер, осуществляющий автоматическое восстановление ключей, если данный сервис установлен.
- **PKI-готовые приложения (PKI-Enabled Application)** - приложения, которые могут использовать средства PKI для обеспечения безопасности. PKI управляет цифровыми сертификатами и ключами, используемыми для шиф-

рования информации, содержащейся на web-серверах, при использовании электронной почты, при обмене сообщениями, при просмотре Интернет-страниц и пересылке данных. Некоторые приложения изначально могут использовать PKI, а другие требуют внесения изменений программистами.

- **Регистрационный центр (Registration Authority)** - модуль отвечающий за регистрацию пользователей и принятие запросов на сертификат.
- **Сервер безопасности (Security Server)** - сервер, который обеспечивает управление доступом пользователей, цифровыми сертификатами и надежными взаимосвязями в среде PKI. Сервер безопасности централизованно управляет всеми пользователями, сертификатами, связями с сертификационным центром, отчетами и проверяет список аннулированных сертификатов.

Терминология PKI

Из всего выше сказанного можно выделить некоторые пункты, а также добавить новые, для того чтобы определить основные термины, используемые в PKI. Итак, в PKI используются термины:

сертификат – электронный документ, который содержит электронный ключ пользователя, информацию о пользователе, удостоверяющую подпись центра выдачи сертификатов и информацию о сроке действия сертификата.

закрытый ключ – ключ, хранящийся в безопасном хранилище, созданный с использованием алгоритмов шифрования, имеющий свой уникальный электронный отпечаток и использующийся для получения зашифрованных данных и подписи данных

открытый ключ – ключ, созданный в паре с закрытым ключом, имеющем такой же электронный отпечаток, как и закрытый ключ, которому он соответствует, используется для шифрования данных и проверки подписи

электронный отпечаток (fingerprint) – это информация при помощи которой можно проверить, является ли полученный открытый ключ именно тем, который был отослан отправителем. Электронные отпечатки открытого и закрытого ключа одной пары идентичны, поэтому сверив отпечаток полученного ключа (например, по телефону) с отпечатком закрытого ключа отправителя, можно установить соответствие открытого ключа закрытому.

подписанные данные – данные, подписанные при помощи закрытого ключа пользователя

зашифрованные данные – данные, зашифрованные при помощи открытого ключа пользователя

Термины, которые необходимы для общего понимания:

путь доверия – цепочка документов, которая позволяет удостовериться, что предъявленный сертификат был выдан доверенным центром; последним звеном в этой цепочке является предъявленный сертификат, начальным — сертификат корневого доверенного центра сертификации, а промежуточными — сертификаты, выданные промежуточным центрам сертификации. Особенностью пути доверия является то, что при потере доверия к начально-

му звену цепочки (корневому центру сертификации) теряется доверие ко всей цепочке, то есть ко всем выданным данным центром сертификатам и к предъявленному в том числе.

личные сертификаты – сертификаты которые хранятся у пользователя в личном хранилище сертификатов.

корневые центры сертификации – центры сертификации, которым доверяют изначально все, либо руководствуясь политикой предприятия, либо из-за предустановленных настроек хранилища сертификатов, и которые могут находиться в начале пути доверия.

доверенные центры сертификации – список центров сертификации, которым доверяют владельцы сертификатов. Чтобы сделать какой либо центр доверенным, достаточно получить от него сертификат и внести его в список доверенных центров.

Библиография

- *Полянская О. Ю., Горбатов В. С.* Инфраструктура открытых ключей. Учебное пособие., Москва, 2007. ISBN 978-5-94774-602-0

Основные определения

- **Certificate Revocation Lists (CRLs)** - список аннулированных сертификатов. Аннулирование может быть вызвано сменой места работы, кражей частного ключа или другими причинами. Приложения, работающие с PKI, могут сверять сертификаты пользователей со списком CRL, прежде чем предоставить доступ в соответствии с этим сертификатом.
- **Цифровой сертификат (Digital Certificate/X.509 Certificate)**. Структура данных, применяющаяся для связывания определенного модуля с определенным открытым ключом. Цифровые сертификаты используются для подтверждения подлинности пользователей, приложений и сервисов, и для контроля доступа (авторизации). Цифровые сертификаты издаются и распределяются CA.
- **Цифровой конверт (Digital Envelope)**. Метод использования шифрования с открытым ключом для безопасного распространения секретных ключей использующихся при симметричном шифровании и для посылки зашифрованных сообщений. Значительно сокращается проблема распространения ключей связанная с симметричным шифрованием.
- **Цифровая подпись (Digital Signature)**. Метод использования шифрования с открытым ключом для обеспечения целостности данных и невозможности отказа от посылки. Зашифрованный блок информации после расшифровки получателем, идентифицирует отправителя и подтверждает сохранность данных. Например: документ "сжат", HASH зашифрован с помощью частного ключа отправителя и приложен к документу (по сути, это означает приложить "отпечаток пальца" этого документа). Получатель использует открытый ключ для расшифровки полученного сообщения до состояния "выжимки", которая затем сравнивается с "выжимкой" полученной

после "сжатия" присланного документа. Если обе "выжимки" не совпали, то это означает, что документ был изменен или поврежден в процессе пересылки.

- **Шифрование с открытым ключом (Public Key Cryptography)**. Есть два основных типа шифрования: с открытым ключом и с секретным (симметричным) ключом. При шифровании с открытым ключом используется пара ключей: открытый, т.е. свободно доступный, и соответствующий ему частный ключ, известный только конкретному пользователю, приложению или сервису, которые владеют этим ключом. Эта пара ключей связана таким образом, что зашифрованное частным ключом, может быть расшифровано только открытым ключом и наоборот.
- **Симметричное шифрование (Shared Secret Cryptography)**. Есть два основных типа шифрования: с открытым ключом и с секретным (симметричным) ключом. При симметричном шифровании получатель и отправитель используют один и тот же ключ для шифрования и расшифровки. Это означает, что множество пользователей должны иметь одинаковые ключи. Очевидно, что до получения ключа пользователем шифрование невозможно, при этом распространение ключа по сети не является безопасным. Другие же способы распространения, такие как специальный курьер, дорогие и медленные.
- **Алгоритм RSA** - первая шифровальная система с открытым ключом, названная в честь ее изобретателей: Ronald Rivest, Adi Shamir и Leonard Adleman.
- **Смарт-карта.** Устройство похожее на кредитную карточку со встроенной памятью и процессором, используемое для защищенного хранения ключей и сертификатов пользователя а также другой информации (как правило, социального и медицинского назначения).
- **Digital Credentials.** В рамках технологии PKI, стандарт ISO/TS 17090-1 определяет этот термин как криптографически защищенный объект, который может содержать индивидуальные ключи пользователя, сертификаты индивидуальных ключей, сертификаты Центров Сертификации PKI-структуры пользователя, список доверенных ЦС, а также другие параметры, относящиеся к домену пользователя - идентификатор пользователя, наименования применяемых криптографических алгоритмов, значения стартовых величин и т.д.. Credentials могут размещаться на аппаратных или программных носителях.