



Михаил Масленников

Инфраструктура открытых ключей. Часть 1.

18+

Михаил Масленников

Инфраструктура

открытых ключей. Часть 1.

<https://litres.ru/74604004>

SelfPub; 2026

Аннотация

Что читатель знает об инфраструктуре открытых ключей, или PKI – Public Key Infrastructure? Для большинства людей все хитросплетения криптографии остаются до сих пор во многом загадкой, полной сложных терминов и понятий. Однако криптография все чаще используется в повседневной жизни и ее применение часто осуществляется «вслепую», когда человек полностью доверяется наукообразным терминам, даже не пытаясь вникнуть в их суть.

Изложение наиболее важных криптографических понятий простым и доступным для обычного пользователя языком – это очень важная задача. В этой книге мне хотелось бы поговорить о таком криптографическом понятии, как PKI – инфраструктура открытых ключей. Я позволю себе предположить, что читатель уже имеет некоторое представление о том, что такое симметричная и асимметричная криптография, секретный и открытый ключ, как и для чего они применяются.

Кое-что об этом, не вдаваясь в подробности, я постараюсь вкратце рассказать, но основное внимание буду уделять РКІ.

Содержание

Введение.	5
Американская революция в криптографии.	7
Единый и нерушимый блок криптографов и бюрократов.	11
Генералы УЦ.	14
Криптографическое древоведение.	18
Централизованная PKI.	19
Криптодерево формата ASN.1.	21
Пример ASN.1 дерева, выращенного Microsoft.	22
ЭЦП сертификата.	24
OID различных свойств сертификата.	25
Конец ознакомительного фрагмента.	26

Михаил Масленников

Инфраструктура открытых ключей. Часть 1.

Введение.

Что читатель знает об инфраструктуре открытых ключей, или PKI – Public Key Infrastructure? Если этот термин ему хорошо знаком и не вызывает вопросов, то такой читатель, на мой взгляд, хорошо знаком и с современной криптографией. Но, боюсь, продвинутых читателей не очень много. Для большинства людей все хитросплетения криптографии остаются до сих пор во многом загадкой, полной сложных терминов и понятий. Однако криптография все чаще используется в повседневной жизни и ее применение часто осуществляется «вслепую», когда человек полностью доверяется наукообразным терминам, даже не пытаясь вникнуть в их суть.

Изложение наиболее важных криптографических понятий простым и доступным для обычного пользователя языком – это очень важная задача. Первоначальная осведомленность в криптографии и ее роли в современном цифровом мире являются жизненно необходимыми практически любо-

му пользователю, даже не имеющему специальной технической или математической подготовки.

В этой книге мне хотелось бы поговорить о таком криптографическом понятии, как РКІ – инфраструктура открытых ключей. Я позволю себе предположить, что читатель уже имеет некоторое представление о том, что такое симметричная и асимметричная криптография, секретный и открытый ключ, как и для чего они применяются. Кое-что об этом, не вдаваясь в подробности, я постараюсь вкратце рассказать, но основное внимание буду уделять РКІ.

Американская революция в криптографии.

В середине 70-х годов прошлого века произошло то, что впоследствии назвали «американской революцией в криптографии». До нее традиционная или симметричная криптография использовалась только для шифрования, ключи для шифрования должны были быть одинаковыми у отправителей и получателей шифрованных сообщений. Американцы в 1976 году предложили сначала асимметричный алгоритм Диффи-Хеллмана (DH), а затем, в 1977 году, trio замечательных криптографов Рон Ривест, Ади Шамир и Леонард Адлеман, в ночь после бурной вечеринки по случаю праздника Песах, предложили то, что на мой взгляд является жемчужиной современной криптографии – асимметричный алгоритм RSA.

Как в DH, так и в RSA, вводится понятие асимметричного ключа – пары, состоящей из секретного (private) и открытого (public) ключа. Открытый ключ далее частенько для краткости будем обозначать как ОК. Из самого названия нетрудно понять, что секретный ключ держится пользователем в секрете от посторонних, а открытый – нет, т.е. может быть известен всем. Математической изюминкой асимметрично-

го ключа является то, что определить секретный ключ по известному открытому практически невозможно, это требует таких трудозатрат, которые недостижимы в условиях современного уровня развития вычислительной техники.

Первоначально асимметричная ключевая система предполагалась только для шифрования. В ДН отправитель и получатель обмениваются своими открытыми ключами, после чего, используя пару «свой секретный ключ – открытый ключ адресата» вычисляют общий ключ для шифрования, который могут вычислить только они двое. В RSA все проще: для зашифрования нужен только открытый ключ получателя, а тот расшифровывает полученное сообщение, используя только свой секретный ключ.

Но одним асимметричным шифрованием американская революция в криптографии не ограничилась. Вскоре появилась ЭЦП – электронно-цифровая подпись.

Задача шифрования – скрыть от посторонних глаз содержание конфиденциального сообщения, передаваемого по открытым каналам связи. Задача ЭЦП – защитить любое сообщение или хранящийся массив информации, в том числе и несекретный, от подделки, т.е. от несанкционированного изменения. Методы для такой защиты используются криптографические, хотя само слово «криптография» означает «тайнопись». При ЭЦП тайнописи нет, но методы получения ЭЦП тесно связаны с асимметричной криптографией.

Итак, что же такое ЭЦП? Это цифровая проверочная ком-

бинация для некоторого произвольного массива информации, которая обладает такими свойствами.

Это случайная последовательность, достаточно длинная для того, чтобы практически исключить возможность построения другого массива с такой же ЭЦП;

Для построения ЭЦП необходим секретный ключ владельца этой информации;

Для проверки подлинности ЭЦП достаточно открытого ключа владельца информации.

При асимметричном шифровании можно особо не беспокоиться о подлинности используемого при этом (как в DH, так и в RSA) открытого ключа. Подмена открытого ключа приведет к тому, что получатель шифрованного сообщения просто не сможет его расшифровать. А для ЭЦП подмена открытого ключа владельца информации весьма критична: она дает возможность потенциальному злоумышленнику подменять и саму подписанную информацию. Поэтому всеми правдами и неправдами перед проверкой ЭЦП необходимо убедиться в подлинности открытого ключа, предназначенного для проверки.

К примеру, если неоднократно упоминавшиеся в криптографических примерах Алиса и Боб ведут переписку и Алиса получает от Боба письмо с предложением выйти за него замуж, то перед радостным возгласом «я согласна!» ей стоит внимательно изучить это письмо, и если там есть ЭЦП, то тщательно ее проверить. Причем проверить не только мате-

матическое соотношение, определяющее подлинность ЭЦП, но и подлинность открытого ключа Боба. Различных свадебных аферистов очень много!

А как проверить подлинность открытого ключа?

Единый и нерушимый блок криптографов и бюрократов.

Это я про сертификат открытого ключа.

Сразу же, как только появилось понятие ЭЦП, многим бюрократам стала ясна ее коммерческая ценность. Банки, платежи, операции с ценными бумагами и прочая, прочая, прочая – везде очень востребована ЭЦП. Как следствие – востребована проверка подлинности ЭЦП и, в частности, проверка подлинности открытого ключа. Очень часто ЭЦП – это любимая многими бюрократами близость к деньгам. Следовательно, проверка подлинности ЭЦП – это тоже близость к деньгам. Пора делать бюрократический бизнес!

Думали бюрократы, думали и решили: на проверке математического соотношения, определяющего подлинность ЭЦП, бизнес построить сложно, а на проверке подлинности открытого ключа – сам бог велел!

Давайте представим себе такую картину: криптографы и бюрократы собрались на совещание. Стали обсуждать, как проверять подлинность открытого ключа.



- Нужно министерство по делам открытых ключей.
- Мысль хорошая. Но что такое открытый ключ – это пока мало известно большинству народа. Пугать простых людей такое название будет.
- А давайте назовем это министерство просто «Удостоверяющий Центр», сокращенно «УЦ».
- А по-английски?
- «Certificate Authority» - сокращенно СА.
- И что этот УЦ будет делать?
- Издавать сертификаты открытых ключей, с помощью которых будет проверяться их подлинность.

Вот она, основная бизнес-составляющая РКІ! Открытый ключ вырабатывают криптографы, чаще всего – бесплатно, а сертификат открытого ключа – бюрократы, чаще всего за

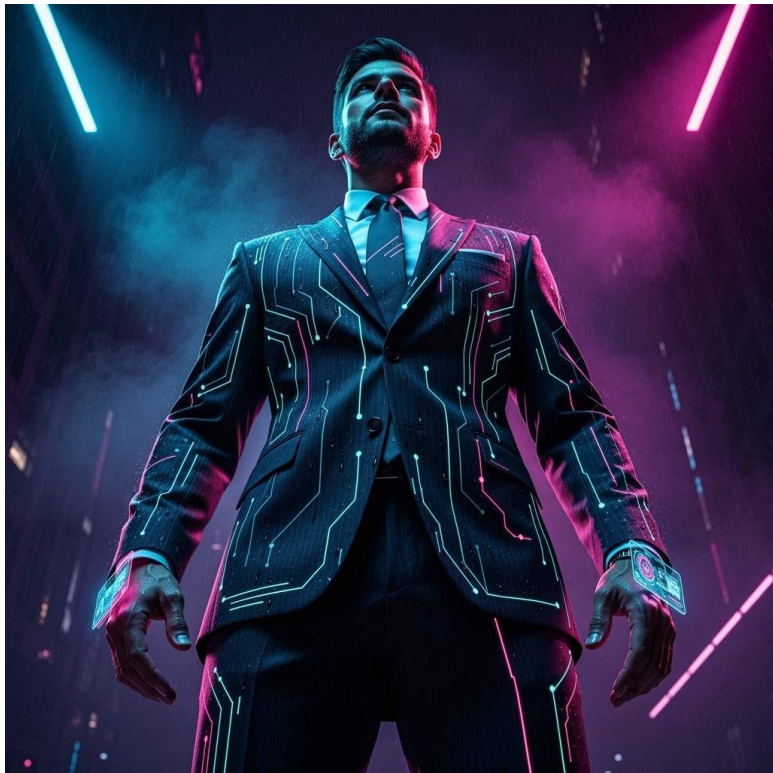
деньги.

Генералы УЦ.

Совещание продолжается. Идея с УЦ всем понравилась. Теперь необходимо согласовать все детали проверки подлинности открытых ключей.

- В УЦ нужны генералы УЦ!

сразу же заявили бюрократы, уже предчувствуя запах денег.



- А это кто или что такое?
спросили их криптографы.

- Это кристально честные асимметричные ключи. Подлинность их открытых ключей ни у кого не должна вызывать ни малейших сомнений просто по определению!

Криптографы их моментально поняли.

- С помощью ключа-генерала будем подписывать поступивший на сертификацию открытый ключ рядового пользователя

Бюрократы не унимались.

- И не только сам открытый ключ, но и всякую другую связанную с ним информацию: кому принадлежит, для чего предназначен, срок действия, алгоритм построения, и т.д. и т.п. Открытый ключ рядового пользователя, объединенный с этой дополнительной информацией о нем, подписывается генералом УЦ, и все это назовем сертификатом открытого ключа.

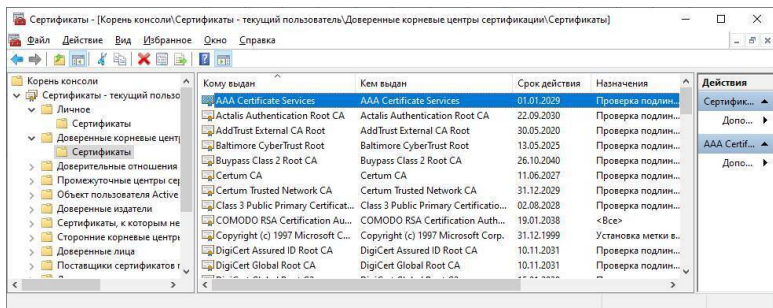
Криптографы тут же оценили все эти фантазии бюрократов. Сертификат открытого ключа можно сделать древовидной неограниченной по размерам структурой, деревом, веточками и листочками которого являются различные свойства, так или иначе связанные с открытым ключом. Все это дерево подписывается генералом УЦ и не может быть никем искажено! Каких только свойств ОК можно повесить на это дерево! Например, фамилию, имя и отчество владельца ОК, его адрес проживания, место работы и даже кличку любимой им собаки.

Но как сделать так, чтобы подлинность генералов УЦ ни у кого не вызвала сомнений?

- А давайте обратимся за помощью к мировым гигантам цифровой индустрии, например, к Microsoft.

Обратились. Те предложили сменить название с пугаю-

щего «генералы УЦ» на нейтральное «Доверенные корневые центры сертификации». Каждый такой корневой центр имеет свой уникальный асимметричный ключ, предназначенный для подписи поступивших к нему сертификатов открытых ключей рядовых пользователей. Из открытой части этого асимметричного ключа строится сертификат корневого центра сертификации и подписывается с помощью его же секретной части. Получается самоподписанный сертификат, который включается в наиболее популярную и широко распространенную операционную систему Windows. А Windows стоит у многих мировых пользователей и негласно принято, что незаметно подменить в нем чей-то самоподписанный сертификат корневого центра сертификации очень трудно. Слишком много неожиданных проблем может возникнуть!



Криптографическое древоведение.

Итак, криптографы предложили сделать сертификат открытого ключа древовидной и неограниченной по размерам структурой. Давайте с ней знакомиться.

Централизованная PKI.

Читаем в Википедии.

«Инфраструктура открытых ключей — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач, на основе закрытого и открытого ключей. В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

закрытый ключ (private key) известен только его владельцу;

удостоверяющий центр (УЦ или СА — certificate authority) создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается;

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.»

Эта цитата из Википедии подтверждает серьезным язы-

ком все сказанное в предыдущем разделе. Единственное, что мне хотелось бы добавить – это *централизованная* PKI. И главным в большинстве современных централизованных PKI является понятие формата ASN.1

Криптодерево формата ASN.1.

Выше уже упоминалось, что каждый сертификат открытого ключа – это древовидная структура, в веточках и листиках которой находятся те или иные свойства ОК. Давайте поглядим на это криптографическое дерево повнимательнее.

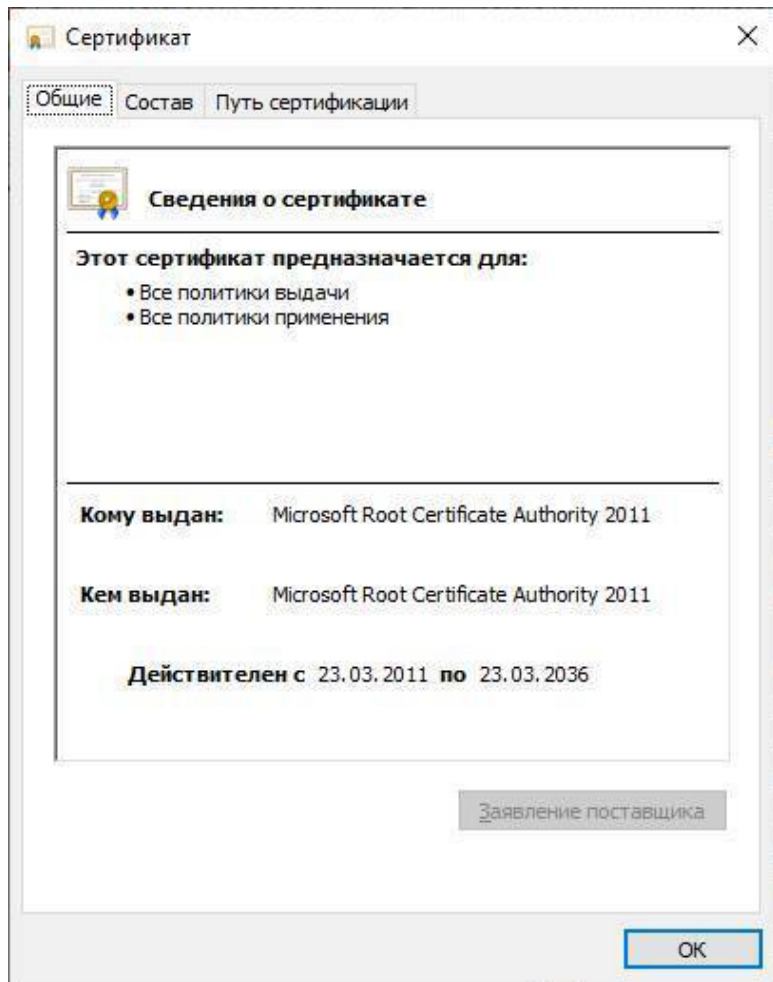
Обычные деревья бывают хвойные и лиственные, а криптографические – только «лиственные», листочки на веточках содержат различные крипто-бюрократические свойства. Мы же с вами знаем, кто их создавал! В природе типов лиственных деревьев – вагон и маленькая тележка, а в криптографии очень часто используется всего один-единственный тип – ASN.1. Опять смотрим Википедию.

«ASN.1 (англ. Abstract Syntax Notation One) — в области телекоммуникаций и компьютерных сетей язык для описания абстрактного синтаксиса данных... Он обеспечивает набор формальных правил для описания структуры объектов, которые не зависят от конкретной машины.»

Сочувствую обычному читателю, который отважится залезть в Википедию и прочитать все, что там написано в статье про ASN.1. У меня в этой книжке много всяких картинок, не исключая и картинки сертификата в формате ASN.1.

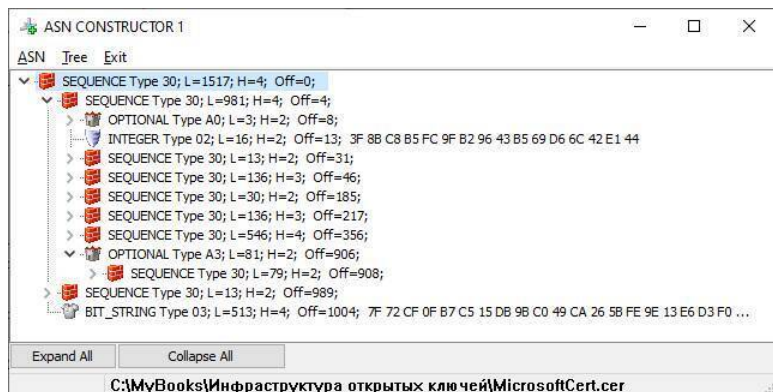
Пример ASN.1 дерева, выращенного Microsoft.

Microsoft встроил в Windows удобный интерфейс для просмотра сертификатов. Давайте посмотрим с помощью этого интерфейса сертификат УЦ самого Microsoft.



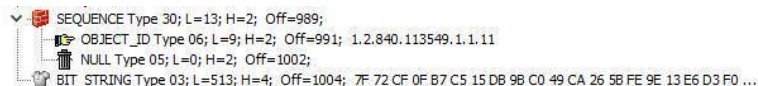
А где же дерево типа ASN.1? Вот оно, только почти все

свернутое, чтобы сразу не пугать неопытного читателя.



ЭЦП сертификата.

Дерево как дерево, с веточками и листочками. Поглядим повнимательнее на последние две строчки – веточку и листик.



Это – ЭЦП сертификата. Точнее, сама ЭЦП – это последняя строчка. Интерес представляет значение OBJECT_ID,

или сокращенно – OID. Мы хорошо запомнили, что сертификат – это крипто-бюрократический продукт, который никак не мог обойтись без различных идентификаторов.

OID различных свойств сертификата.

Давайте разбираться с идентификатором 1.2.840.113549.1.1.11. Заглянем в т.н. репозиторий OID - <https://oid-base.com/>. В нем есть «выставка деревьев». На этой «выставке» находим:

- 1 - Международная организация по стандартизации (ISO)

- 1.2 – Члены ISO

- 1.2.840 – Соединенные Штаты Америки

- 1.2.840.113549 - RSA Security Limited Liability Company (LLC)

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.