# ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ (PKI) С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ OPENSSL

*Nichita SVECICHIN*

*Universitatea Tehnică a Moldovei*

***Аннотация:*** *Доклад содержит представления об инфраструктуре открытых ключей (Public Key Infrastructure - PKI), а именно ее использовании в информационных технологиях в области создания электронной подписи. Рассмотрена самая популярная архитектура PKI. Представлены основные компоненты, структура данных, сервисы и актуальность PKI. Рассмотрено создание сертификатов открытых ключей пользователей на основе библиотеки OpenSSL.*

***Ключевые слова:*** *инфраструктура открытых ключей, секретный и публичный ключ, сертификат, уполномоченный центр, список отозванных сертификатов.*

## Введение

Информационные технологии являются неотъемлемой частью современного мира, поэтому для безопасного взаимодействия субъектов в распределенных сетях связи необходимо обеспечить безопасность передаваемой информации. Одним из методов обеспечения безопасного взаимодействия в сети *Internet* является использование цифровых сертификатов. Цифровые сертификаты являются необходимым элементом в области безопасного обмена информацией, обеспечивая такие информационные сервисы, как: достоверность, конфиденциальность, целостность, неотрекаемость и своевременность. Однако, одного наличия сертификата недостаточно. Действительно, защищенный обмен сообщениями, надежная идентификация и электронная коммерция невозможны без инфраструктуры открытых ключей - *Public Key Infrastucture (PKI)*.

PKI является комплексом аппаратных и программных средств, стандартов, политик и процедур. Инфраструктура открытых ключей необходима организациям и компаниям для безопасного обмена электронными документами и ведения бизнеса, требующего гарантированной защиты электронных транзакций и доступа к данным через *Internet* [1].

## 1. Основные принципы PKI

Проблемы "*доверия*" и "*идентичности*" являются основой для построения PKI. Необходима некая договоренность между использующими ключи субъектами о том, как именно доказать связь ключа и пользователя. Решение этого вопроса и составляет основу PKI.

Задача заключается в том, чтобы существовала доверенная третья сторона (*trusted third party*), которой бы все доверяли, и которая бы сертифицировала публичные ключи субъектов. Реализация PKI основана на создании *уполномоченного центра сертификации* (англ. - *Certificate Authority - CA*) публичных ключей субъектов. Корпоративные уполномоченные центры (УЦ) сертификации должны соответствовать всем критериям безопасности в области электронного документооборота, а также строго следовать международным стандартам и политике PKI.

Такой УЦ может быть представлен различной архитектурой и содержать определенные компоненты, но он обязательно должен следовать политике и международным стандартам PKI [2].

PKI строится на математической основе процесса однонаправленной функции с лазейкой. Шифрование текста выполняется в прямом направлении, причем все указания по шифрованию открыты, любой может зашифровать сообщение. Дешифрование, выполняемое в обратном направлении, настолько сложно и трудоёмко, что, не зная секрета, даже на самых передовых компьютерах процесс дешифрования занял бы сотни, а то и тысячи лет. Лазейкой, в этом случае, служит приватный (секретный) ключ пользователя, который делает дешифрование таким же простым, как и шифрование. Основными требованиями к ключам являются следующие: приватный ключ - должен быть тайным и никому никогда не передаваться, публичный ключ - известен всем и находится в свободном доступе. Когда число участников (субъектов) сети одинаковой криптосистемы достигает большого количества, то их публичные ключи помещаются в общедоступную "базу данных" - репозиторий.

Важным условием процесса является обмен открытыми ключами между сторонами, участвующими в передачи информации. Возникает вопрос: как *субъект X* сможет проверить, что полученный публичный ключ — это ключ *субъекта Y*, а не *злоумышленника Z*? Такая проблема решается созданием ***сертификата публичного ключа*** (или просто ***сертификатом - certificate***) [3].

## 2. Архитектура PKI

Сертификаты открытых ключей выдаются субъектам специально созданными системами удостоверяющих центров. Инфраструктура открытых ключей строиться на базе взаимодействия основных компонентов PKI, без которых невозможна работа эффективной системы. К ним относятся:

- удостоверяющий центр (***Certificate Authority - CA***);
- регистрационный центр (***Registration Authority -RA***);
- реестр сертификатов (***Repository***);
- архив сертификатов (***Database***);
- конечные субъекты / пользователи (***EE - End Entity / Users***).

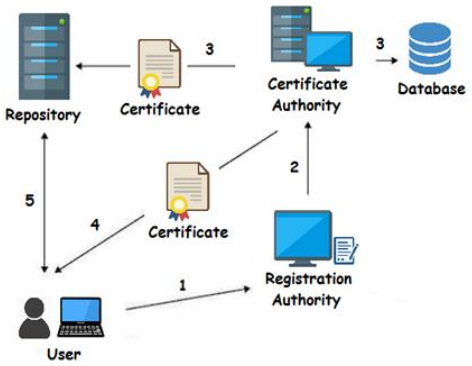



Рисунок 1. Структурная схема ***Single CA***

На рис.1 представлена структурная схема простой модели PKI (***Single CA***). В системе PKI обязательно должны функционировать подсистемы, отвечающие за: списки аннулированных сертификатов (***Certificate Revocation List - CRL***), прямой доступ к реестру сертификатов - (***Online Certificate Status Protocol - OCSP***), создание резервных копий и восстановление ключей, управление "историей" ключей и поддержку взаимной сертификации [2].

Удостоверяющие центры организуются иерархически под управлением, так называемого, *корневого УЦ (**Root CA**)*, который выпускает ***само подписанный сертификат*** и сертификаты для подчиненных УЦ. Подчиненные УЦ могут выпускать сертификаты для УЦ, находящихся ниже них по уровню иерархии, или для конечных субъектов. В иерархической PKI каждая доверяющая сторона знает открытый ключ подписи корневого УЦ. Ниже, на рис.2, представлена структурная схема иерархической PKI (3 уровня).

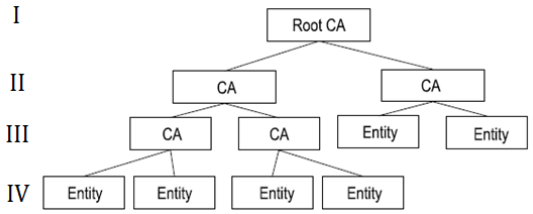



Рисунок 2. Структурная схема иерархической трехуровневой PKI

## 3. Сертификат публичного ключа

Структура данных PKI представлена в виде сертификата открытого ключа, определенного в рекомендациях ***ITU (X.509)*** и документе ***PKIX - RFC 3280 Certificate & CRL Profile*** [4]. В настоящее время основным принятым форматом является ***X.509v3***. Формат сертификата открытого ключа предоставляет гибкий и мощный механизм передачи разнообразной информации и может применяться в корпоративной практике. Сертификат открытого ключа подписи или шифрования представляет собой структурированную двоичную запись в формате ***ASN.1***. Сертификат содержит элементы данных, сопровождаемые цифровой подписью издателя сертификата (рис. 3).

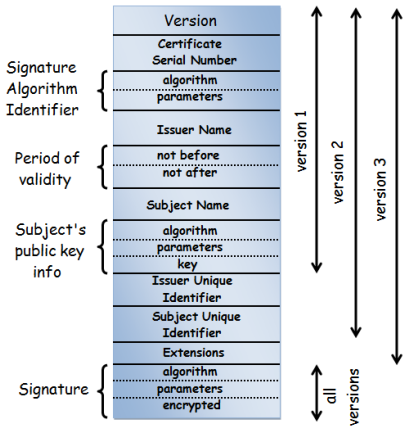



Рисунок 3. Структура сертификата открытого ключа стандарта X.509

Сертификат открытого ключа со всеми вкладками представлен на рис.4.

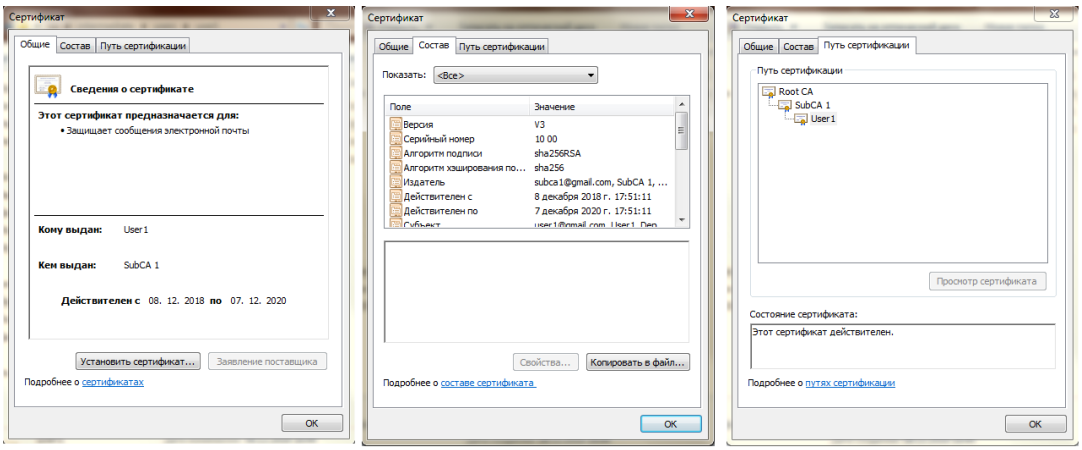



Рисунок 4. Структура полей сертификата открытого ключа субъекта

**5. Разработка PKI на базе библиотеки OpenSSL**

Одна из платформ для создания сертификатов открытых ключей основана на базе библиотеки ***OpenSSL***.

Для создания самоподписанного сертификата для ***корневого УЦ*** необходимо выполнить следующие команды в OpenSSL:

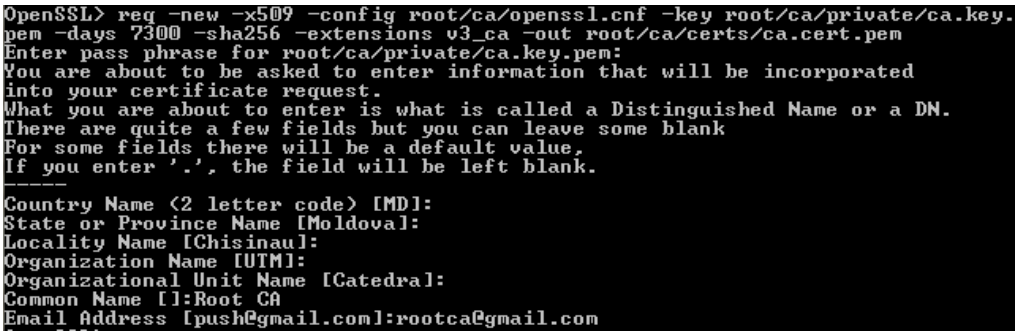
1) **OpenSSL> genrsa -aes256 -out root/ca/private/ca.key.pem 4096**
2) **OpenSSL> req -new -x509 -config root/ca/openssl.cnf -key root/private/ca.key.pem -days 7300 -sha256 -extensions v3_ca -out root/ca/certs/ca.cert.pem**

Таким образом, при помощи первой команды был сгенерирован секретный ключ для корневого центра сертификации ***Root CA*** - ca.key.pem, с учетом определенных требований: длина ключа - ***4096 бит***; ключ шифруется для конфиденциальности - алгоритм ***aes256***; формат ключа - ***pem (base64)*** [5].

Вторая команда создает само подписанный (*self-signed*) сертификат корневого центра сертификации со сроком действия 20 лет, т.е. 7300 дней:

Скриншоты представлены ниже:

```
OpenSSL> genrsa -aes256 -out root/ca/private/ca.key.pem 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................
.....................................................................++
.....................................................................
...++
e is 65537 (0x010001)
Enter pass phrase for root/ca/private/ca.key.pem:
Verifying - Enter pass phrase for root/ca/private/ca.key.pem:
```




Проверка сертификата осуществляется следующим образом:

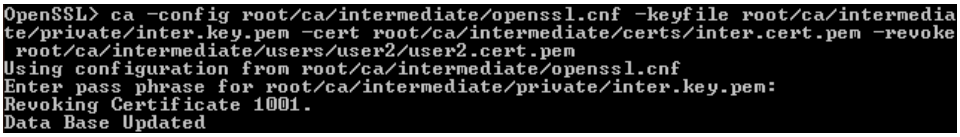
**OpenSSL> x509 -noout -text -in root/ca/certs/ca.cert.pem**

Выдача сертификата для промежуточного УЦ и выдача сертификата для субъектов осуществляется аналогичным способом только необходимо еще создать запрос (***CSR***) на создание (подписание) сертификата открытого ключа вышестоящему УЦ, командой [6]:

**OpenSSL> req -config root/ca/intermediate/openssl.cnf -new -sha256 -key root/ca/intermediate/private/inter.key.pem -out root/ca/intermediate/csr/inter.csr.pem**

В случае отзыва (***revocation***) сертификата открытого ключа, к примеру, по причине компрометации секретного ключа субъекта User2, выполняется команда:

**OpenSSL> ca -config root/ca/intermediate/openssl.cnf -keyfile root/ca/intermediate/private/inter.key.pem -cert root/ca/intermediate/certs/inter.cert.pem -revoke root/ca/intermediate/users/user2/user2.cert.pem**




База данных обновляется после отзыва сертификата. В нее добавляется запись:

```
R   201207160423Z   181208163115Z   1001    unknown /C=MD/ST=Moldova/L=Chisinau/O=UTM/OU=Catedra/CN=User2/emailAddress=user2@gmail.com
```

**Библиография:**


1. http://www.bwg.ru/pki.php.
2. *Горбатов В. С., Полянская О. Ю.* Г67 Основы технологии PKI. - М.: Горячая линия -Телеком, 2004. - 248 с.
3. *Трутнев Д.Р*. Инфраструктура доверия в государственных информационных системах: Учебное пособие. - СПб.:НИУ ИТМО, 2012. - 95 с.
4. https://www.ietf.org/rfc/rfc3280.txt
5. *Брюс Шнайер*. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. - 610 с.
6. https://jamielinux.com/docs/openssl-certificate-authority/