Криптографические средства защиты объектов информатизации

Часть 3: Инфраструктура открытых ключей (Public Key Infrastructure)

Обеспечение доверия к открытому ключу

- Криптография с открытыми ключами основывается на:
  - владении своим личным Секретным ключом и
  - владении Открытым ключом получателем
- Получатели используют Открытый ключ для подтверждения владения отправителем секретным ключом
- Проблема:
  Как получатель может быть уверен, что открытый ключ действительно принадлежит отправителю?
- Решение:
  Использование доверенного третьего лица для заверения Открытого ключа. Третье лицо является Центром Сертификации или Доверенным Центром. Заверенный этим центром открытый ключ является сертификатом

Инфраструктура открытых ключей (Public Key Infrastructure - PKI)

- Понятие
  - PKI - интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.
- Основные задачи:
  - управление ключами и их сертификатами при организации юридически значимого электронного документооборота
  - обеспечение доверия к сертификатам открытых ключей

Системы перераспределения доверия

- PGP (Pretty Good Privacy) – программа шифрования электронной почты (использует: небольшой объем инф. -RSA, большой объем инф. - IDEA, хеш - MD5, SHA-1)
- SSL (Secure Socket Layer) – протокол защищенных сокетов, используется для обеспечения безопасности Интернет – магазинов и продаж по сети. (DES, RC)

Сертификат открытого ключа

Сертификат представляет собой документ, подтверждающий принадлежность открытого ключа и дополнительных атрибутов владельцу сертификата, выданный и заверенный Центром сертификации.

Сертификат открытого ключа

Федеральный закон РФ от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи»

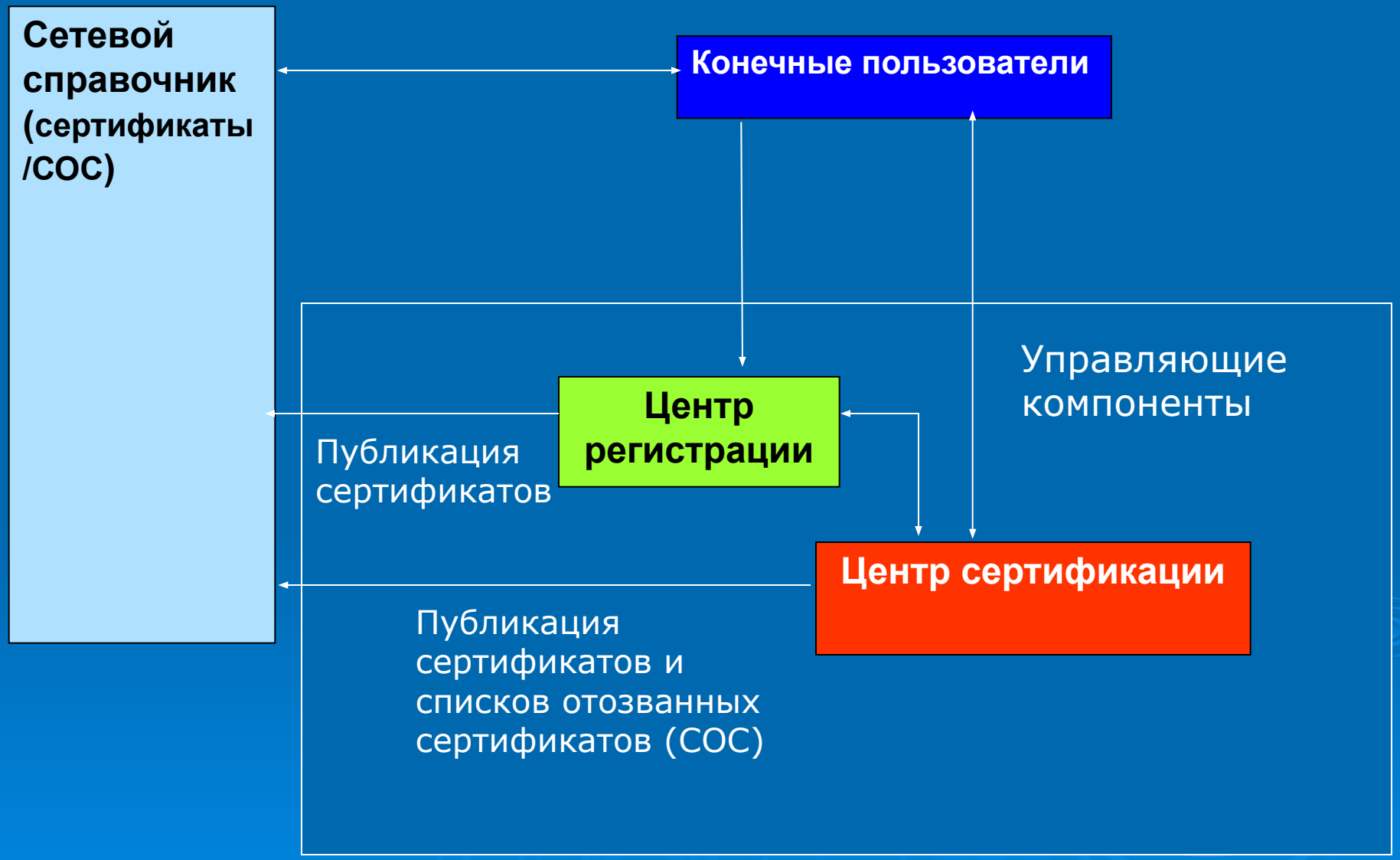
- **Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи.

Применение PKI

Инфраструктура открытых ключей позволяет обеспечить:

- организацию внутрикорпоративного защищенного документооборота, а также защищенного документооборота и обмена информацией с сторонними организациями;
- защищенный доступ пользователей к информационным ресурсам по сетям связи общего пользования;
- централизованное управление жизненным циклом криптографических ключей и цифровых сертификатов;
- проверку цифровой подписи, подтверждение целостности и авторства электронных документов, обеспечение юридической значимости электронных документов и гарантирование «неотрекаемости» действий в сфере электронного документооборота.

Компоненты PKI



Центр Сертификации

Основные функции:

- Ведение базы данных сертификатов
  - Создание сертификата
  - Отзыв сертификата
  - Хранение сертификатов
- Обеспечение уникальности информации в сертификатах
  - Открытый ключ сертификата
  - Серийный номер сертификата
- Формирование списка отозванных сертификатов
- Обеспечение взаимодействия с Центром Регистрации
- Протоколирование работы Центра Сертификации

Центр Регистрации

Основная задача

- регистрация пользователей и обеспечение их взаимодействия с центром сертификации.

Основные функции:

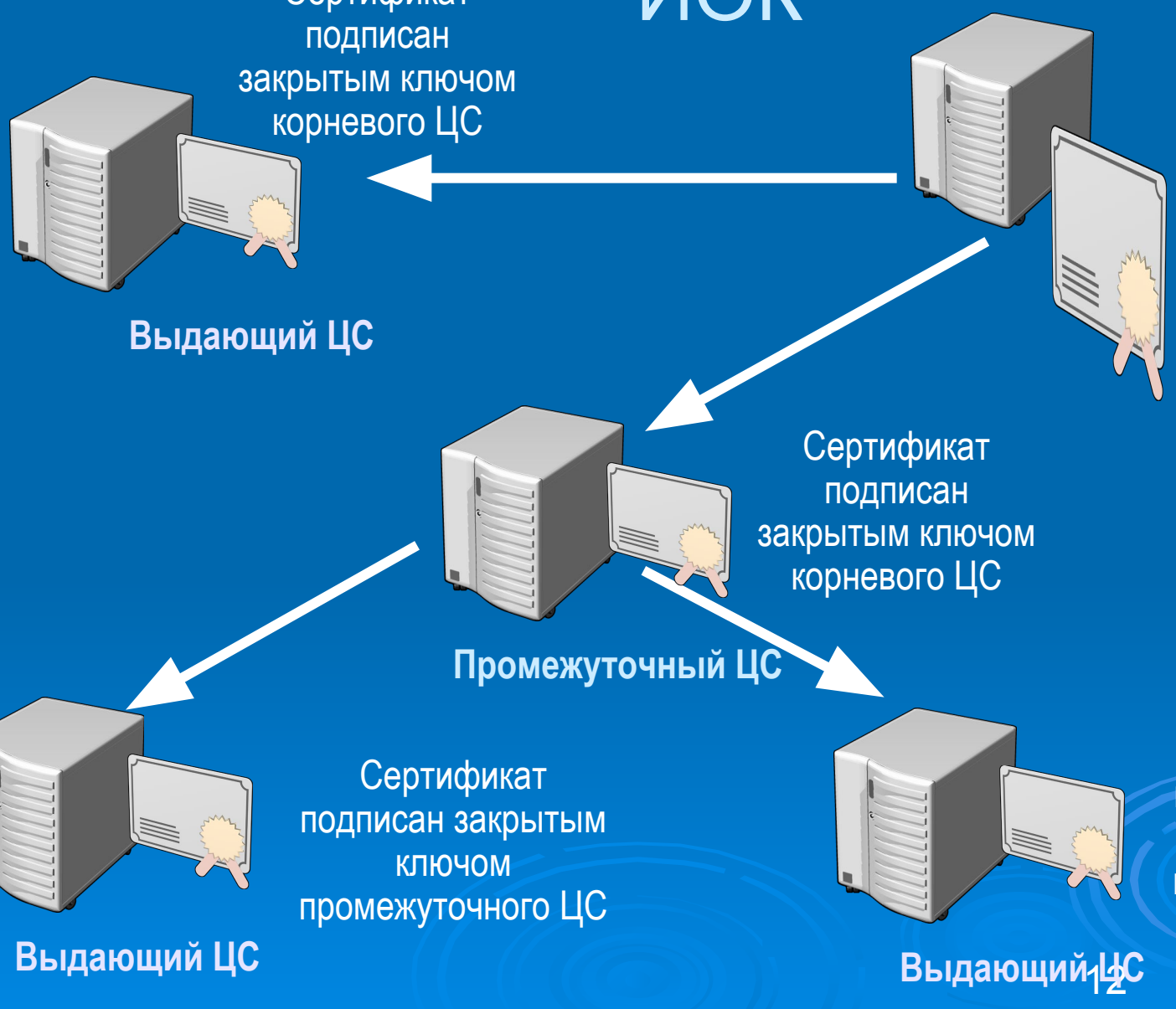
- Обеспечение аутентификации приложений
- Ведение Базы Данных пользователей
- Ведение Базы Данных о сертификатах и операций с ними
- Взаимодействие с Центром Сертификации и внешними приложениями
- Обеспечение выполнения задач по регламенту обращения сертификатов и ключевой информации
- Протоколирование работы Центра Регистрации

Удостоверяющий центр (Закон об ЭЦП)

Задачи УЦ:

- изготовление сертификатов ключей подписей и выдачу сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов;
- изготовление ключей подписи по обращению участников ИС;
- приостановление и возобновление действия сертификатов ключей подписей;
- аннулирование сертификатов ключей подписи;
- ведение реестра сертификатов ключей подписи;
- обеспечение актуальности реестра и свободного доступа к нему участников ИС;
- обеспечение уникальности открытых ключей подписи в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Иерархия Центров сертификации в ИОК



Преимущества и недостатки

Преимущества:

- иерархическая архитектура аналогична существующим федеральным и ведомственным организационно-управляющим структурам и может строиться с учетом этого;
- иерархическая архитектура определяет простой алгоритм поиска, построения и верификации цепочек сертификатов для всех взаимодействующих сторон;
- для обеспечения взаимодействия двух пользователей одному из них достаточно предоставить другому свою цепочку сертификатов, что уменьшает проблемы, связанные с их взаимодействием.

Недостатки:

- для обеспечения взаимодействия всех конечных пользователей должен быть только один корневой УЦ(удостоверяющий центр);
- взаимодействие сторонних организаций носят скорее прямой, а не иерархический характер;
- компрометация секретного ключа корневого УЦ приостанавливает работу всей системы и требует защищенной доставки нового сертификата до каждого конечного пользователя.

Основные стандарты PKI

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 3280)	**Инфраструктура открытых ключей Интернет X.509: сертификат и профиль списка отозванных сертификатов CRL**
Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)	**Инфраструктура открытых ключей Интернет X.509: протоколы управления сертификатами**
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560)	**Инфраструктура открытых ключей Интернет X.509: протокол онлайновой проверки статуса сертификата**
PKCS #7 Cryptographic Message Syntax Standard	**Стандарт на синтаксис криптографического сообщения**
PKCS #10 Certificate Request Syntax Standard	**Стандарт на синтаксис запроса сертификации**

Формат сертификата

Должен содержать (статья 6 закона об ЭЦП):

- уникальный регистрационный номер;
- даты начала и окончания срока действия;
- фамилия, имя и отчество владельца или псевдоним владельца;
- открытый ключ электронной цифровой подписи;
- наименование средства ЭЦП;
- наименование и место нахождения удостоверяющего центра;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Может содержать:

- должность;
- наименование организации;
- местонахождение организации;
- квалификация владельца;
- другие сведения по заявлению владельца

Формат сертификата

RFC 3280:

Имя Пользователя: C=RU, org=УФК, cn=UserName
Имя Издателя: C=RU, org= УФК
Номер Сертификата: #12345678
Открытый ключ пользователя
Алгоритм: GOST P 34.10-94
Значение ключа: 010011101001001010010101
Сертификат действует с: 01.10.2001 00:00:00
Сертификат действует до: 31.09.2006 23:59.59

Идентификационные данные

Дополнительная информация (X.509 v3 Extensions)
Регламент использования сертификата: Электронная почта, подпись файлов и т.д
Секретный ключ действует с: 01.09.2003 23:59.59
Секретный ключ действует до: 31.09.2004 23:59.59
Область применения ключа: Идентификатор 1
Область применения ключа: Идентификатор i
Область применения ключа: Идентификатор N
Права и полномочия: Администратор
Атрибуты пользователя: IP, URI, RFC822, Номер счета, Адрес,...
. . .

Подпись Центра Сертификации:
Алгоритм: GOST P 34.11-94/ P 34.10-94
Значение : 010011101001001010010101

Формат сертификата

Статья 17.3 закона об ЭЦП:

- Содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы.

Получение сертификата

Запрос на получение сертификата

Статья 9.2 закона об ЭЦП

- Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 (состав сертификта) настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

Запрос на получение сертификата в формате PKCS #10

```
CertificationRequest ::= SEQUENCE {
certificationRequestInfo  CertificationRequestInfo,        //информация запроса
signatureAlgorithm        AlgorithmIdentifier,        //алгоритм подписи
signature                 BIT STRING                  // подпись
}

Информация запроса

CertificationRequestInfo ::= SEQUENCE {
version                   INTEGER { v1(0) } (v1,...),          //версия
subject                   Name,                       //имя запросившего
subjectPKInfo    SubjectPublicKeyInfo                 //информация об ОК
attributes                [0] Attributes                    //атрибуты
}
Информация об ОК
SubjectPublicKeyInfo { ALGORITHM : IOSet} ::= SEQUENCE {
algorithm         AlgorithmIdentifier                  //идентификатор алгоритма
subjectPublicKey  BIT STRING                           //Открытый ключ
}
```

Отзыв сертификатов

Существует множество причин, по которым сертификаты становятся недействительными до истечения срока их действия. Например:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение правил хранения ключевых носителей.
- Получение сертификата незаконным путем.
- Изменение статуса субъекта.
- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Для распространения сведений о недействительных сертификатах между абонентами используются списки отозванных сертификатов или интерактивные протоколы проверки статуса сертификата.

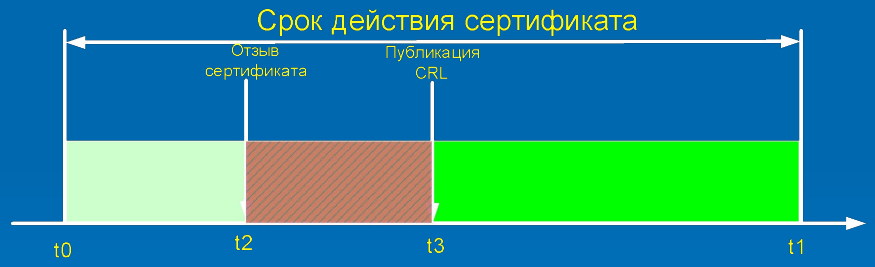
Списки отозванных сертификатов Certificate Revocation Lists (CRL)

CRL – список, содержащий серийные номера всех отозванных сертификатов выпущенных данным Центром сертификации, включающий время публикации и заверенный ЭЦП.

Недостатки CRL

- Увеличение размера с течением времени (и как следствие увеличение времени получения и рост нагрузки на сеть)
- Существование промежутка времени между обновлениями CRL
- Необходимость хранения CRL за несколько лет

Увеличение CRL с каждым отзывом - 45 байт



Разностные списки отозванных сертификатов

Публикация разностных CRL (Delta CRL), которые содержат только изменения по отношению к основному

Интерактивный протокол состояния сертификата OCSP — Online Certificate Status Protocol (RFC 2560)

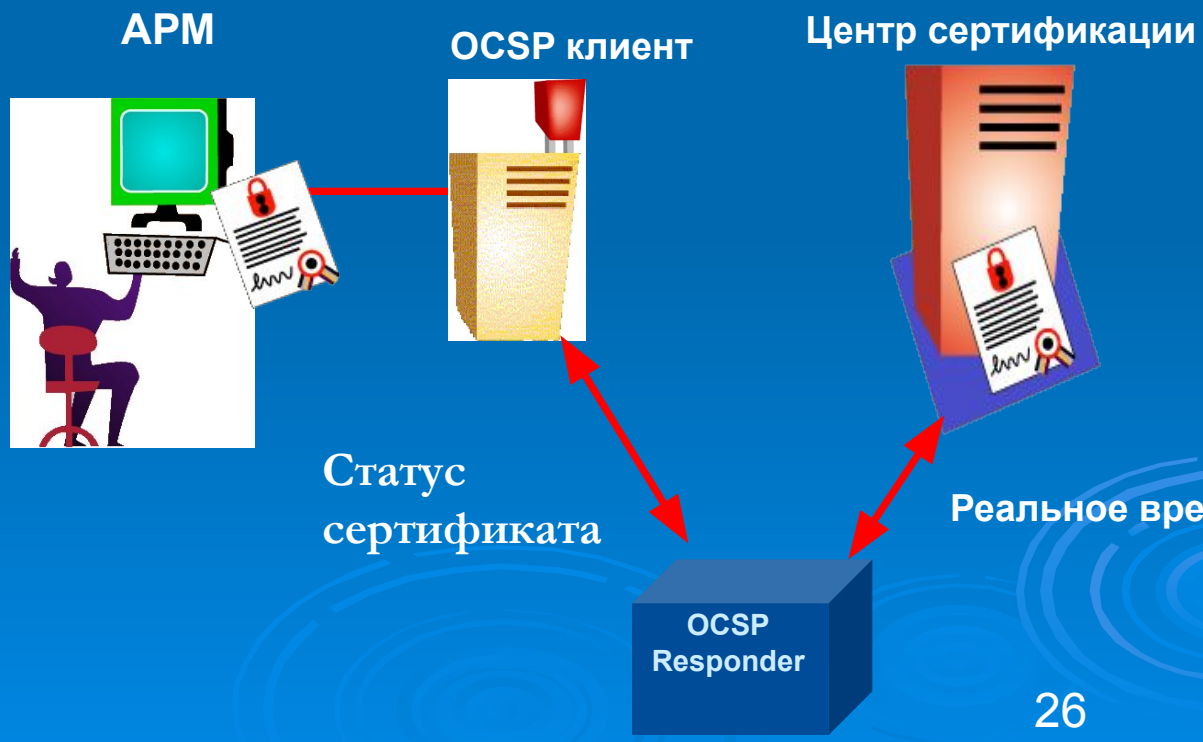
Подразумевает использование OCSP-сервера (респондера), взаимодействующего с конечными пользователями через механизм запрос/ответ.

Является протокольно независимым:

в качестве прикладных протоколов обмена запросами и ответами в соответствии с [RFC2560] могут использоваться HTTP/HTTPS, SMTP, LDAP и другие.

OCSP реального времени

При проверке статуса и полномочий, приложение получает информацию о рассматриваемых сертификатах от OCSP респондера, после проверки им ***данных хранящихся в репозитариии - в реальном времени.***



Обычая модель OCSP - проверка CRL

При проверке статуса и полномочий, приложение получает информацию о рассматриваемых сертификатах от OCSP респондера, после проверки им ***CRL, опубликованного заранее***.

Верификация сертификатов

Для того, чтобы доверять сертификату пользователь должен…

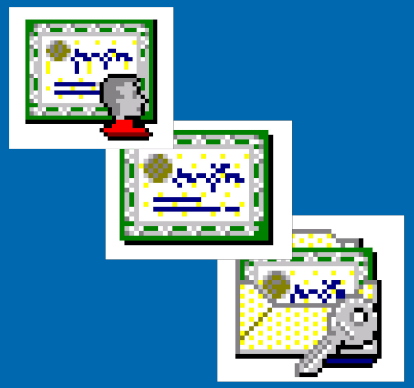
- Знать что сертификат не изменен (обеспечена его целостность)
- Проверить что он действителен по срокам
- Проверить что сертификат не отозван Центром Сертификации
- Проверить приемлемость сертификата в соответствующем приложении по типу ключа и определенной в нем политике безопасности (регламенте использования)
- Доверять сертификату открытого ключа ЭЦП своего Центра Сертификации

Доверие сертификату открытого ключа ЭЦП своего центра основано на заверении его сертификата ключом вышестоящего Центра и так далее.

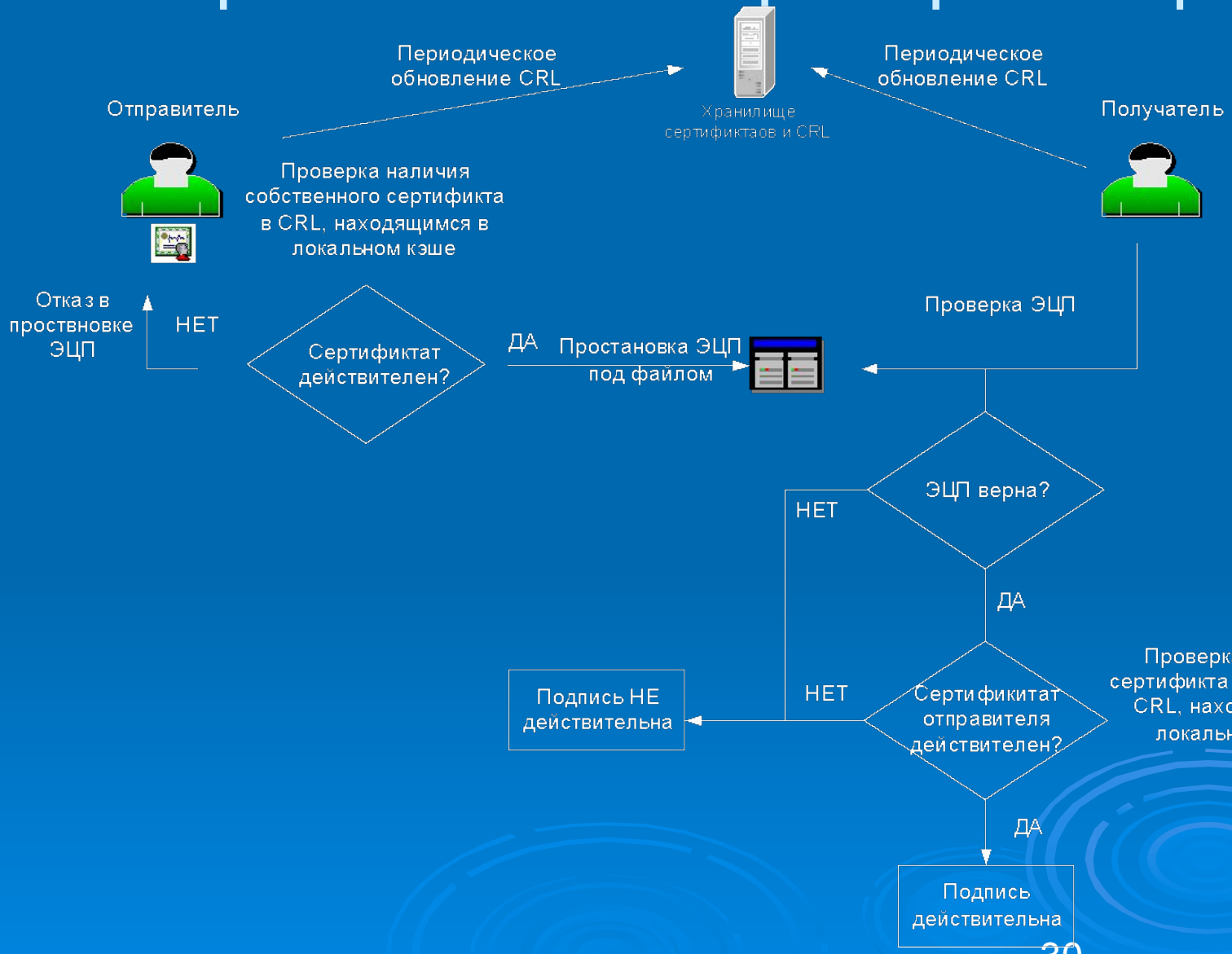
Таким образом выстраивается цепочка сертификатов.

Цепочка сертификатов

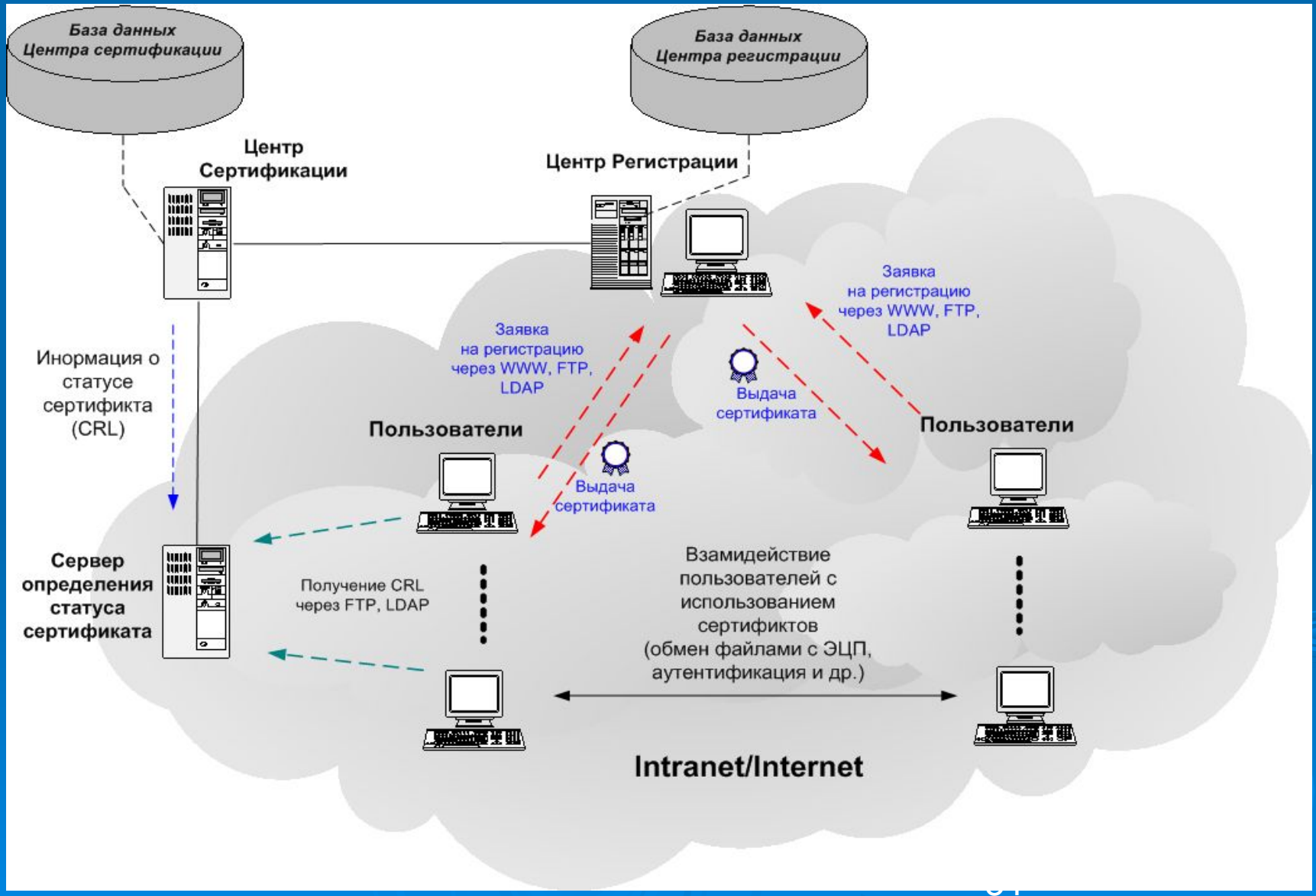
- Собственный сертификат подписан ” своим” ЦС
- Сертификат ”своего” ЦС подписан ”его” ЦС
- И так далее…
- Образуется “Цепочка Сертификатов”
- Последний сертификат - самоподписанный сертификат Главного ЦС
- Длина цепочки обычно ограничена 3 уровнями
- Сертификат Корневого ЦС обеспечивает схему доверия центров сертификаций



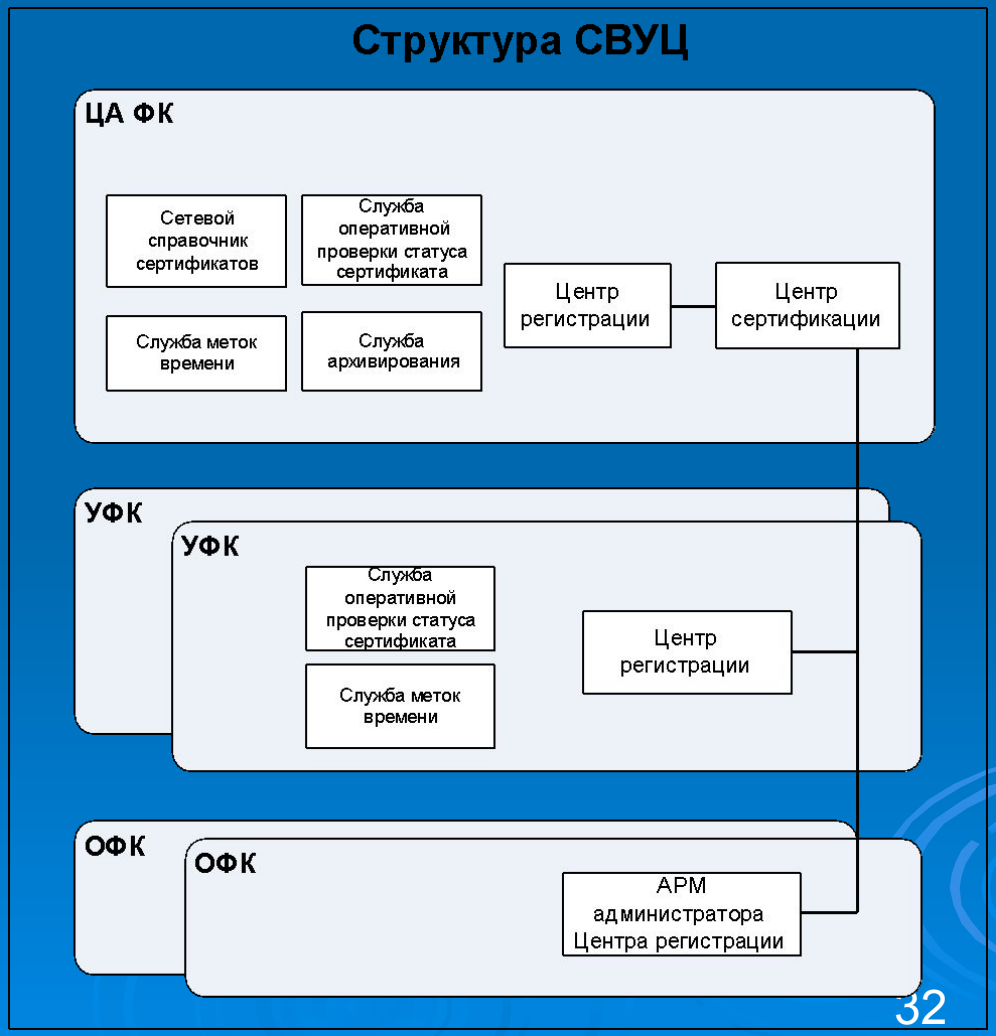
Простановка и проверка ЭЦП



Типовая архитектура ИОК



Типовая структура СВУЦ (**сеть ведомственных удостоверяющих центров**)



Структура СВУЦ