

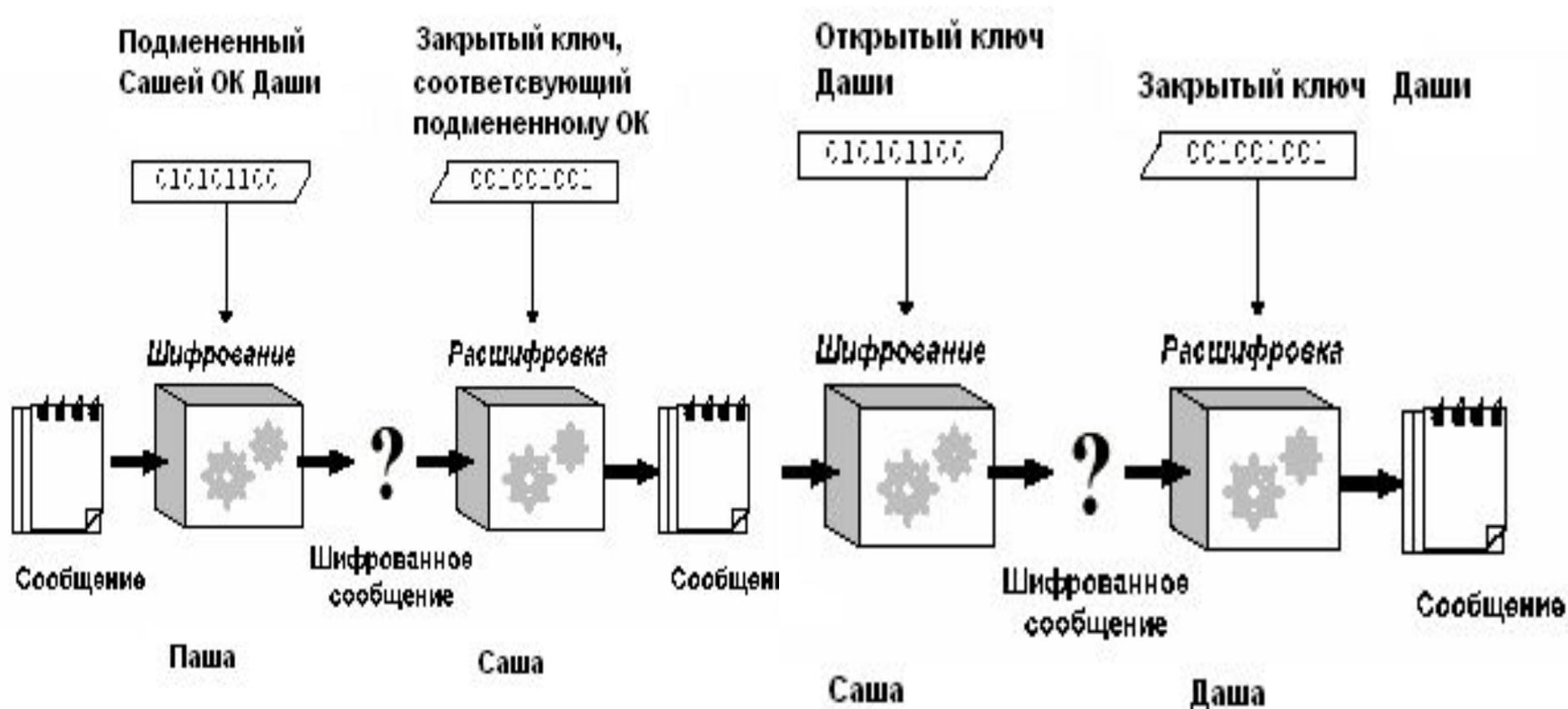
Сертификация открытых ключей.
Сертификационные агентства

Третий недостаток асимметричной криптографии



Возможность подмены
ОК
Проблема заключается
в проверке
принадлежности ОК
данному
конкретному человеку

Атака «Man in the middle»



Паша посылает сообщение Даши
Саша подменил ОК Даши и может незаметно читать все сообщения для Даши

Решение проблемы



```
graph TD; A[Решение проблемы] --> B[личной встречей с получателем]; A --> C[использованием сертификатов ОК, которые обеспечивают соответствие между человеком и ОК.]
```

личной встречей
с получателем

использованием
сертификатов ОК,
которые обеспечивают
соответствие между
человеком и ОК.

Решение проблемы

Используются сертификаты открытых ключей (ОК). ОК абонентов подписываются личным (закрытым) ключом удостоверяющего центра (УЦ), проверяющего и подтверждающего принадлежность ОК определенному лицу.

Сертификация открытого ключа (ОК) с помощью сертификационного агентства (СА).

СА генерирует собственную пару ключей для ЭЦП



СА подписывает свой ОК на своем ЛК



Пользователь создает свою собственную пару ключей



Данный ОК подписывается ЛК агентства и возвращается пользователю



Также пользователь получает ОК СА и сертифицированные ОК других абонентов данного СА

Обязанности сертификационного агентства

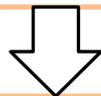


Работа без сертификационного агентства

2 абонента подписывают свои открытые ключи на личных ключах



2 пользователя обмениваются открытыми ключами, соблюдая юридические формальности



Пользователь удаляет подпись партнера и подписывает его сертифицированным личным ключом.

Цепочки доверия

```
graph TD; A[Цепочки доверия] --> B[Надежность (trust)]; A --> C[Достоверность (validity)]; B --> D[определяет уровень доверия к лицу, которое подписывает ключи третьих лиц]; C --> E[отображает степень уверенности в том, что ключ принадлежит номинальному владельцу];
```

Надежность
(trust)

определяет уровень доверия к лицу, которое подписывает ключи третьих лиц

Достоверность
(validity)

отображает степень уверенности в том, что ключ принадлежит номинальному владельцу

Структура сертификата по стандарту X.509

Certificate format version	version 3
Certificate serial number	12345678
Signature algorithm identifier for CA	RSA with MD5
Issuer X.500 name	c=US, o=ACME
Validity period	start=01/08/96, expiry=01/08/98
Subject X.500 name	c=US, o=ACME, cn=John Smith +
Subject public key information	 RSA with MD5
Issuer unique identifier	version 2
Subject unique identifier	version 2

CA Signature 

Сертификат

Общие Состав Путь сертификации

Показать: <Все>

Поле	Значение
Версия	V3
Серийный номер	67E7 3C1B 2F25 FC70 7F56 F...
Алгоритм подписи	md5RSA
Поставщик	VeriSign Class 1 CA Individual ...
Действителен с	23 апреля 2000 г. 6:00:00
Действителен по	23 июня 2000 г. 5:59:59
Субъект	vik@ugatu.rb.ru, Kladov Vitaliy...
Открытый ключ	RSA (512 Bits)

E = vik@ugatu.rb.ru
CN = Kladov Vitaliy
OU = Digital ID Class 1 - Microsoft
OU = Persona Not Validated
OU = www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98
OU = VeriSign Trust Network
O = VeriSign, Inc.

Свойства... Копировать в файл...

номер версии

уникальный порядковый номер

алгоритм ЭЦП и хэш-функция, используемые СА для подписи сертификата;

Срок действия

Имя субъекта и его организации по формату X.500(включая иерархию организационных подразделений

имя СА по формату X.500

информация об ОК субъекта

подпись сертификата

Дополнения к структуре сертификата по стандарту X.509

Версия 2 содержит:

уникальный
идентификатор издателя

уникальный
идентификатор субъекта

Версия 3 содержит:

уникальный
идентификатор издателя

уникальный
идентификатор субъекта

Дополнения.
Каждое
дополнение
состоит из
трех полей:

type

critical

value

Сертификационное
агентство Verisign

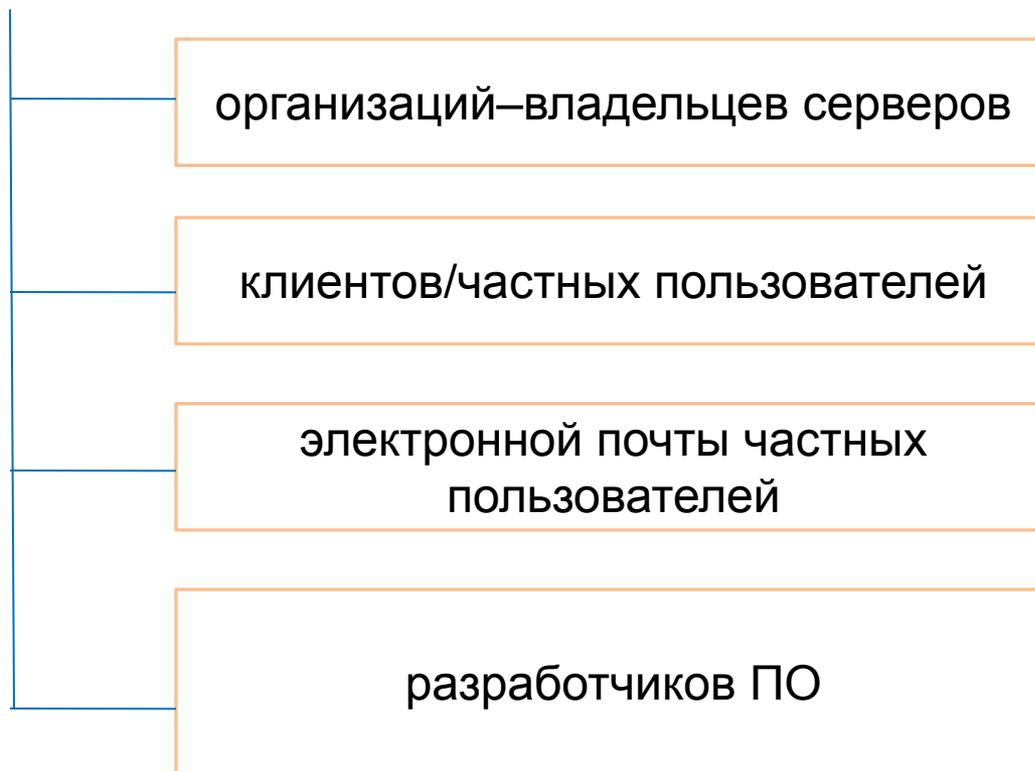
```
graph TD; A[Сертификационное агентство Verisign] --> B[наиболее крупное мировое сертификационное агентство]; A --> C[сертификаты низшего класса удостоверяют возможность доступа пользователя к электронной почте]; A --> D[сертификаты высшего класса выдаются в присутствии представителей компании];
```

наиболее крупное
мировое
сертификационное
агентство

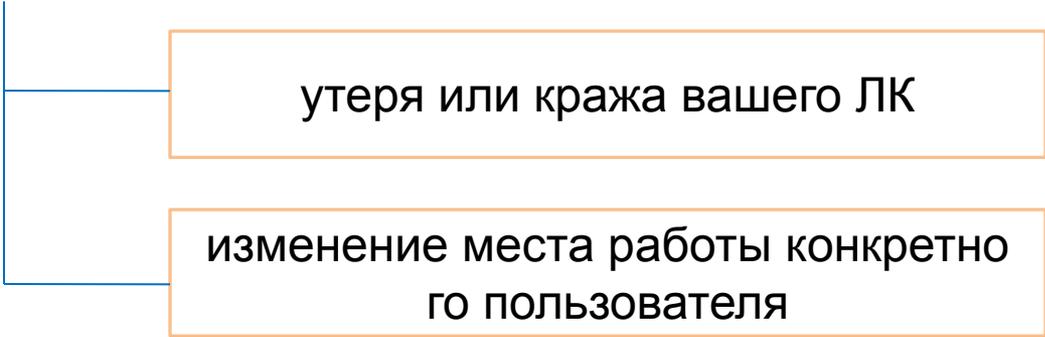
сертификаты низшего
класса удостоверяют
возможность доступа
пользователя к
электронной почте

сертификаты
высшего
класса выдаются
в присутствии
представителей
компании

СА оказывает услуги по сертификации ОК



Причины отзыва сертификатов



утеря или кража вашего ЛК

изменение места работы конкретно
го пользователя

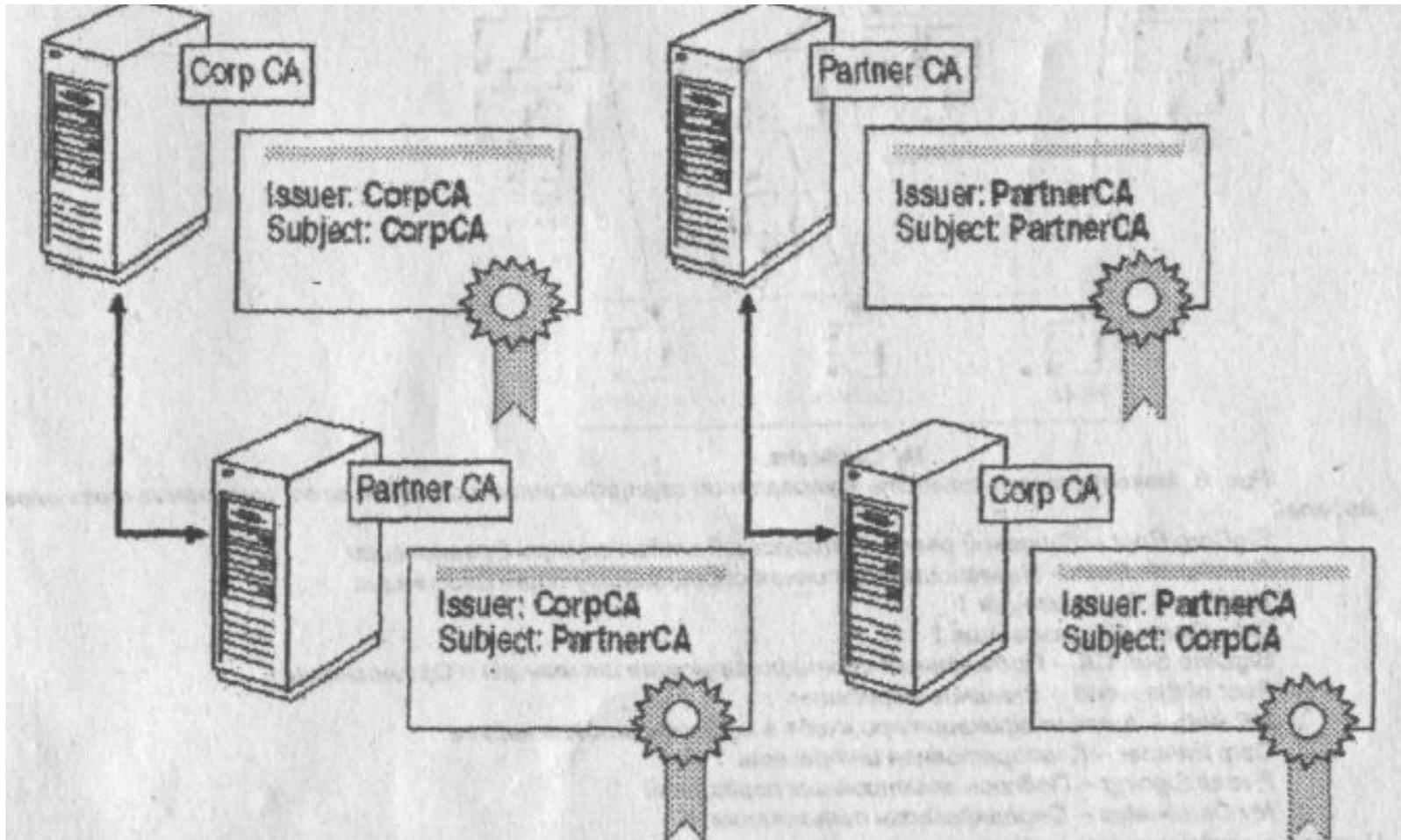
Целесообразность использование внешнего коммерческого СА

правомочность должна быть подтверждена
доверенной третьей стороной

не хватает ресурсов и времени для
формирования внутренней инфраструктуры
открытых ключей PKI

необходима совместимость сертификатов
организаций

Кросс-сертификация



каждая организация имеет сертификат,
выданный СА самой себе, а также
сертификат подчиненного СА, выданный
главным СА партнера

недостаток - чрезмерное
доверие между организациями

Реализация собственного СА

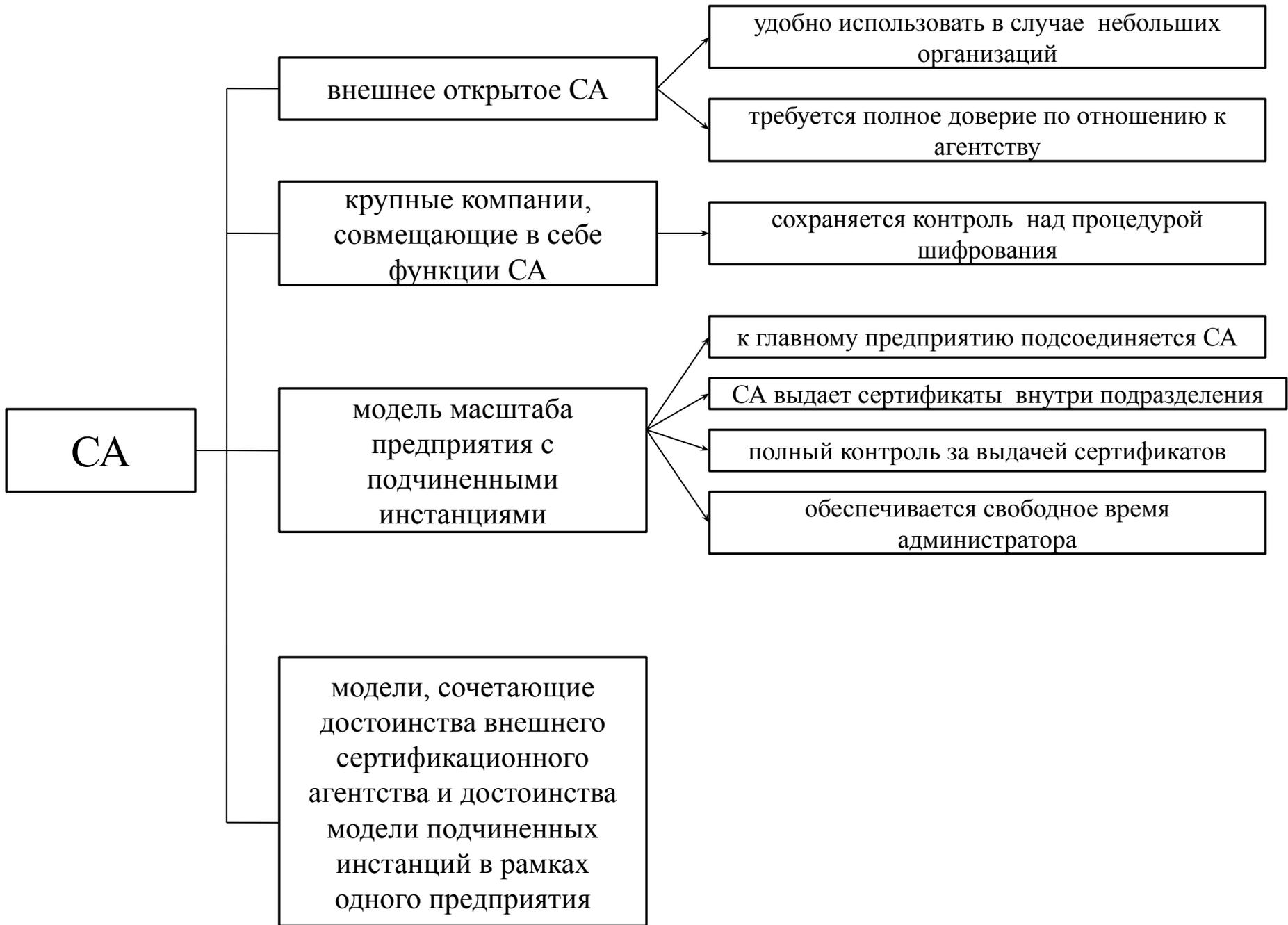
Достоинство

Достоинство-полный контроль за собственной инфраструктурой шифрования

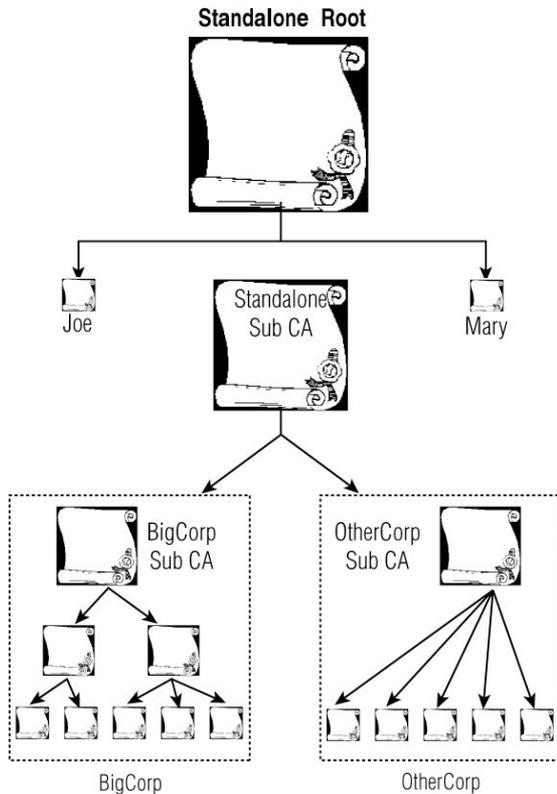
Недостатки

мелкие компании могут не иметь ни квалифицированного персонала, ни ресурсов

цифровой сертификат, выданной одной компанией, признается сотрудниками и партнерами только этой компании



Подчиненные СА



модель масштаба
предприятия с
подчиненными
инстанциями

к главному СА предприятия
подсоединяется подчиненные
СА, выдающие сертификаты
отдельным подразделениям

полный контроль за выдачей
сертификатов

дает возможность СА
подразделений выдавать
сертификаты своим
сотрудникам.

Сложная модель

Сочетает

модель независимой
инстанции

Коммерческое главное
СА

модель с
подчиненными
инстанциями

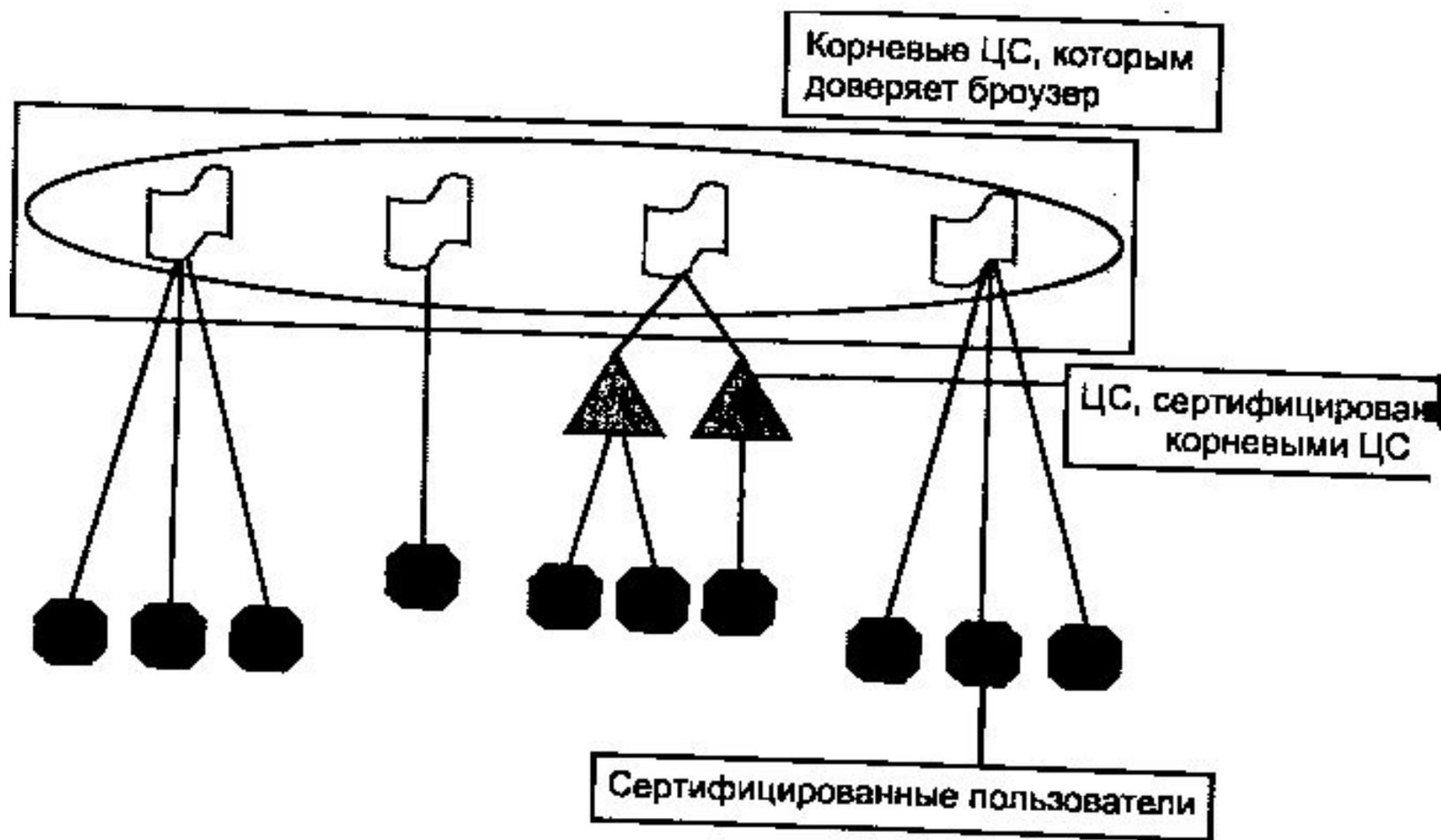
Иерархия СА в рамках
предприятия

Достоинство

Достоинство-полный контроль за собственной
инфраструктурой шифрования

Признание сертификатов за рамками
предприятия

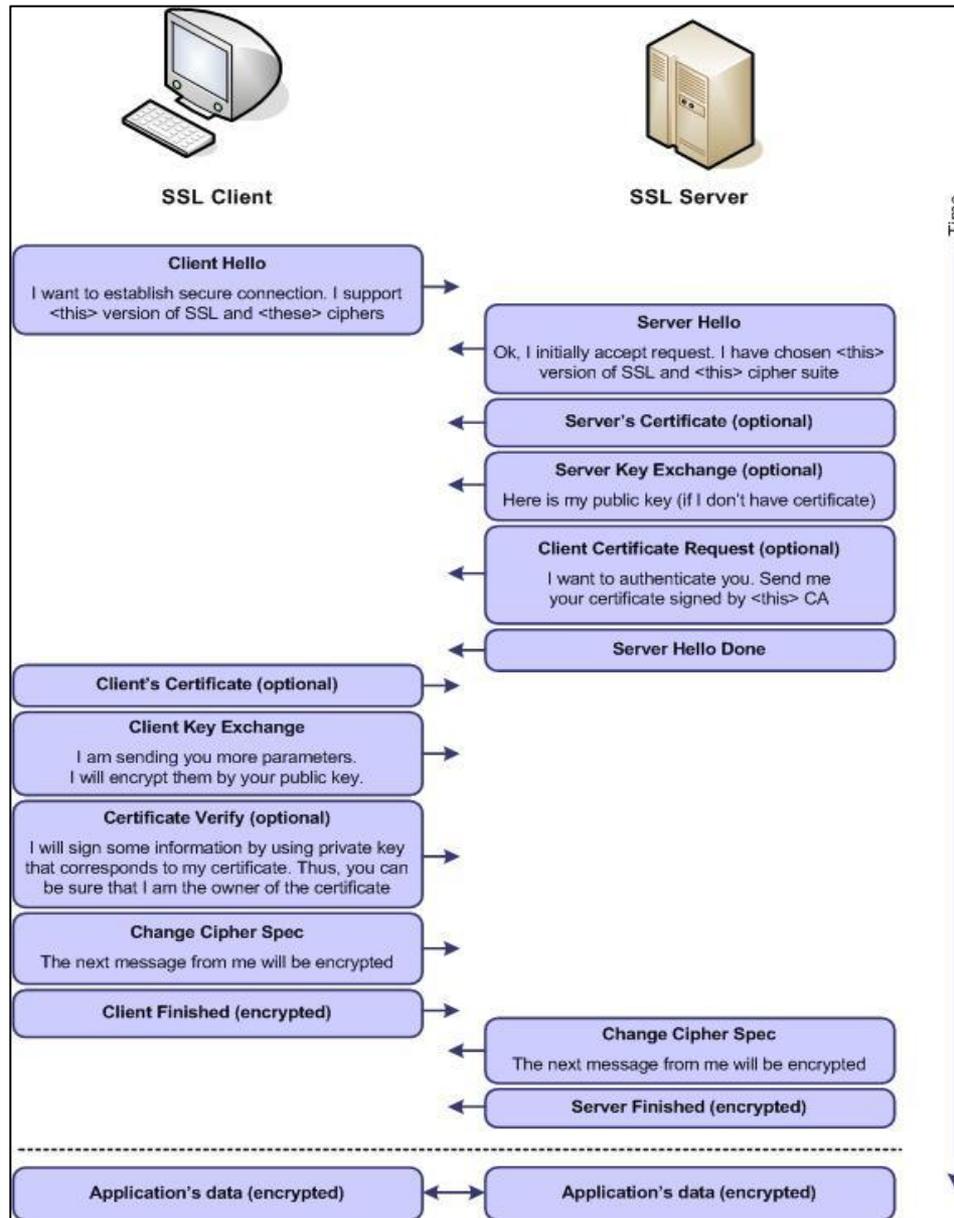
Модель доверительных отношений на веб-технологиях



Протокол SSL



Схема работы протокола SSL



Упрощенная схема работы протокола SSL



Работа протокола SSL



Порты, используемые SSL

```
graph TD; A[Порты, используемые SSL] --> B[https: 443]; A --> C[ssl - ldap: 836]; A --> D[snews: 563]; A --> E[ssmtp: 465]; A --> F[spop3: 995]; A --> G[ftps: 990];
```

https: 443

ssl – ldap: 836

snews: 563

ssmtp: 465

spop3: 995

ftps: 990

Механизм аутентификации на основе сертификата

пользователь передает серверу свой подписанный им же сертификат

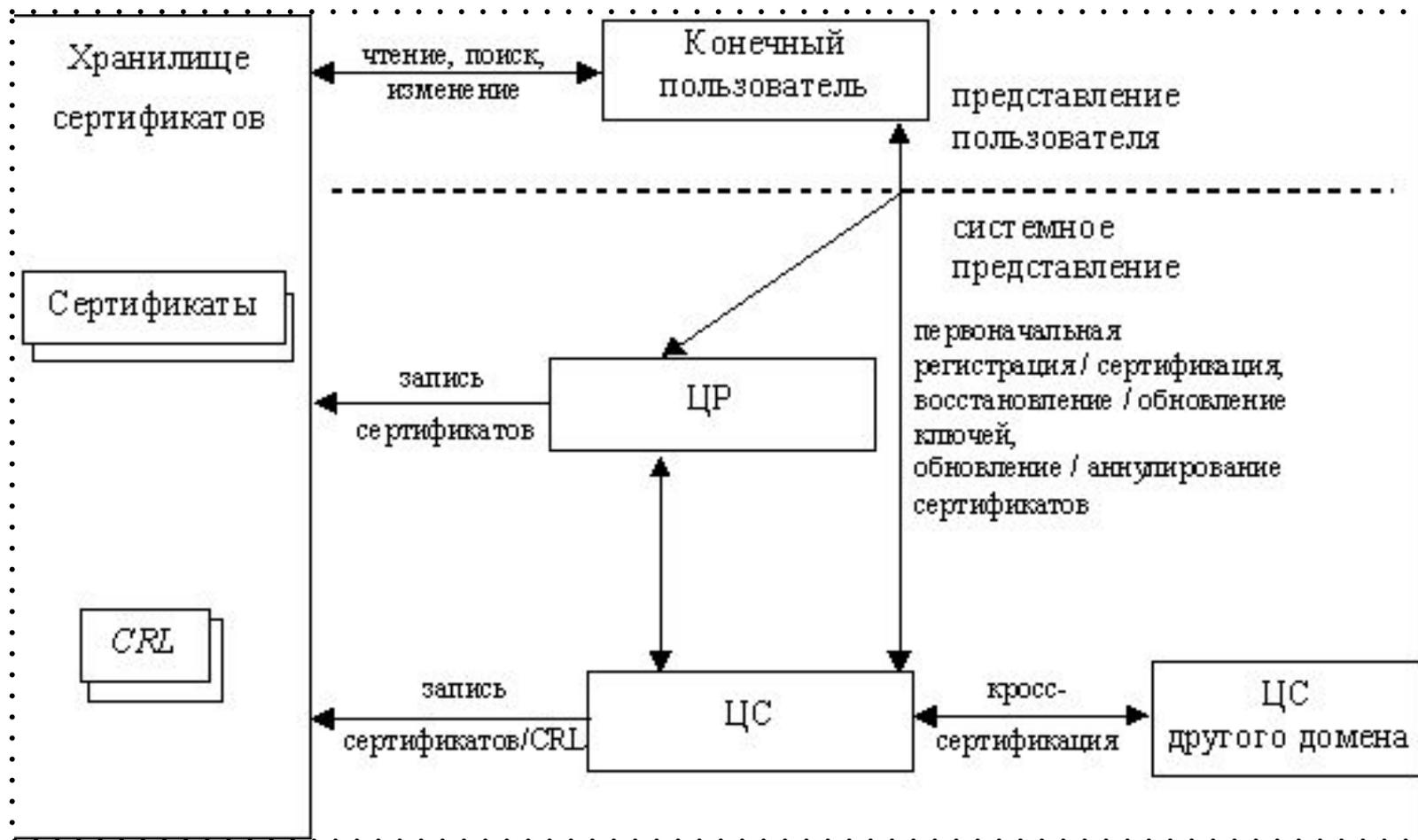
сервер извлекает из сертификата ОК пользователя и проверяет подпись пользователя

положительный результат свидетельствует, что пользователь является владельцем ЛК, парного с указанным ОК

с помощью ОК, указанного в сертификате агентства, проверяется подпись СА

положительный результат проверки свидетельствует о том, что пользователь действительно прошел регистрацию в СА и является тем, за кого себя выдает, а содержащиеся в его сертификате ОК и другие сведения принадлежат данному пользователю

Структура PKI, основанная на сертификатах формата X.509



Структура PKI, основанная на сертификатах формата X.509

Конечный пользователь - пользователь сертификата PKI и/или владелец сертификата (человек, организация или иная сущность) или объектом, запрашивающим сертификат или CRL (список отозванных сертификатов)

Центр сертификации – объект, который авторизован создавать, подписывать и публиковать сертификаты

Хранилище сертификатов – специальный объект PKI, где хранятся выпущенные сертификаты и списки отозванных сертификатов

Список аннулированных сертификатов(CRL) - список сертификатов, признанных недействительными в период их действия в случае компрометации секретного ключа или изменения атрибутов сертификата в момент его выпуска

Центр регистрации является дополнительным компонентом системы PKI, который авторизован Центром сертификации аутентифицировать пользователей и проверять информацию, которая заносится в сертификат