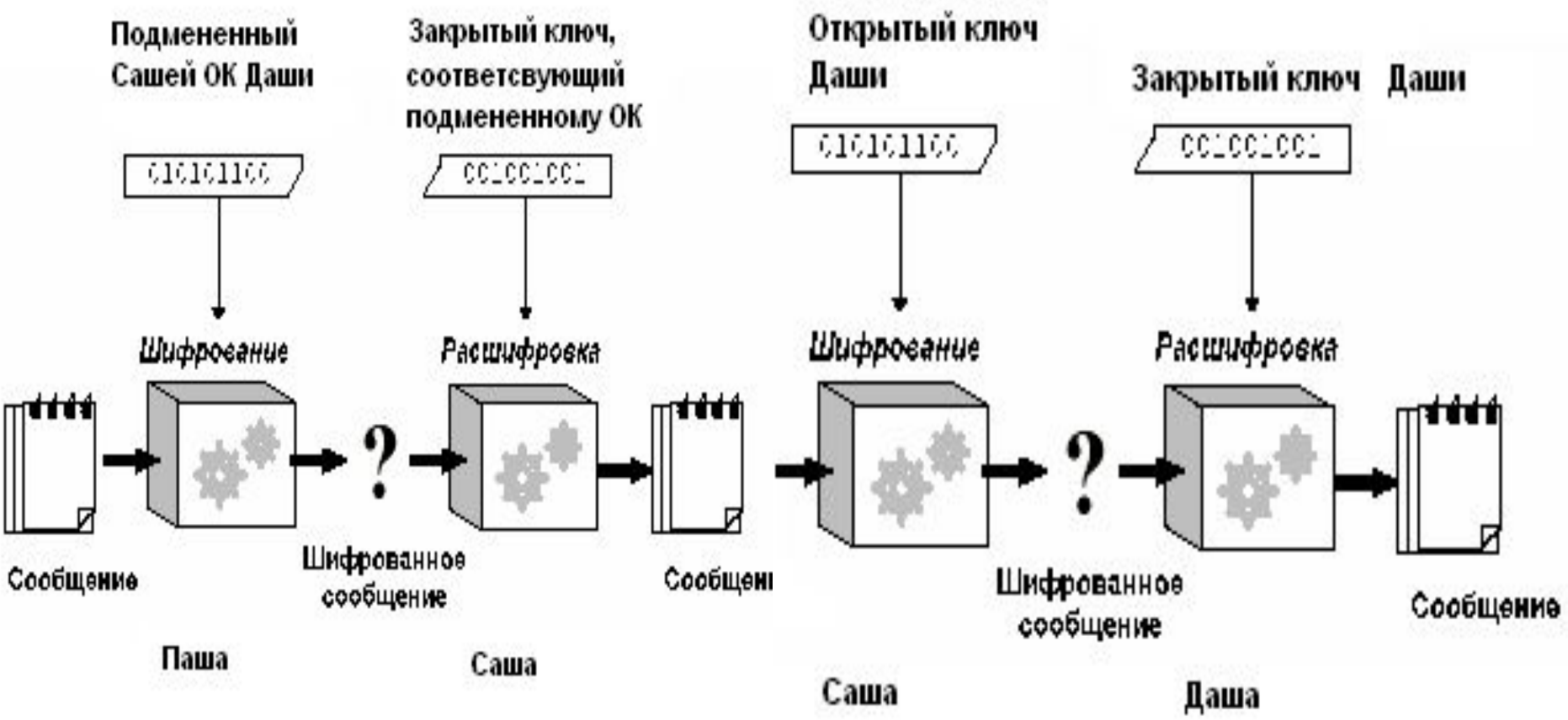
Сертификация открытых ключей. Сертификационные агентства

Третий недостаток ассиметричной криптографии

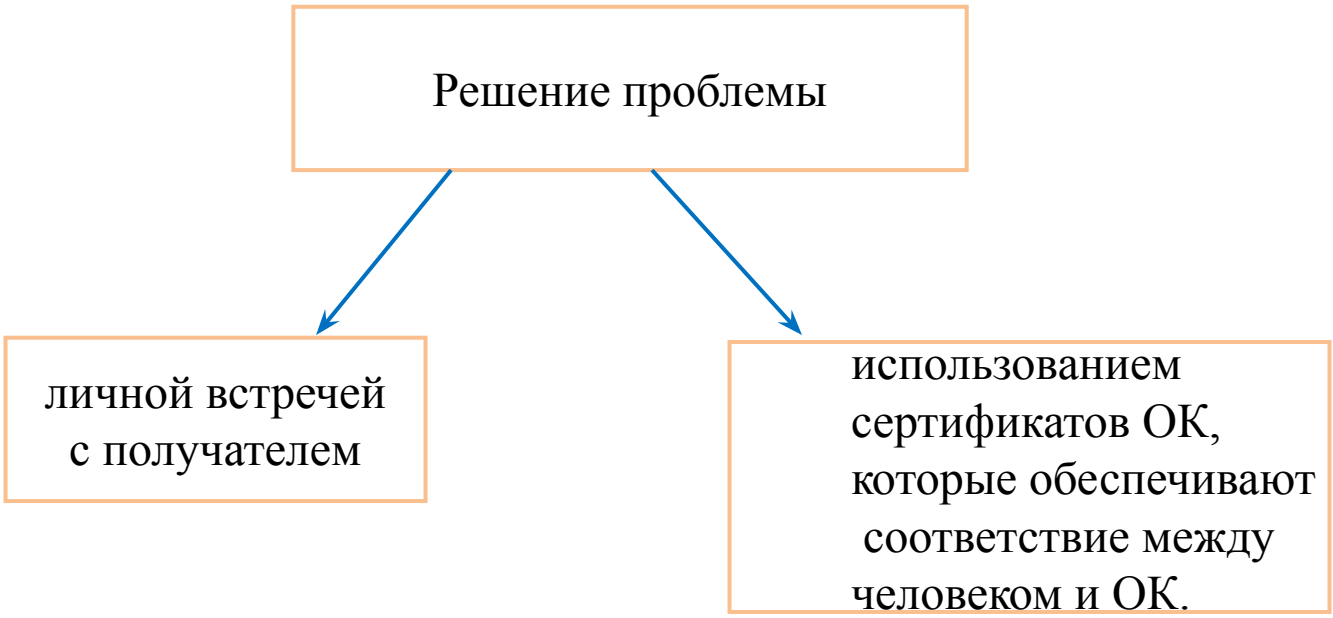
Возможность подмены ОК
Проблема заключается в проверке принадлежности ОК данному конкретному человеку

Атака «Man in the middle»



Паша посылает сообщение Даше

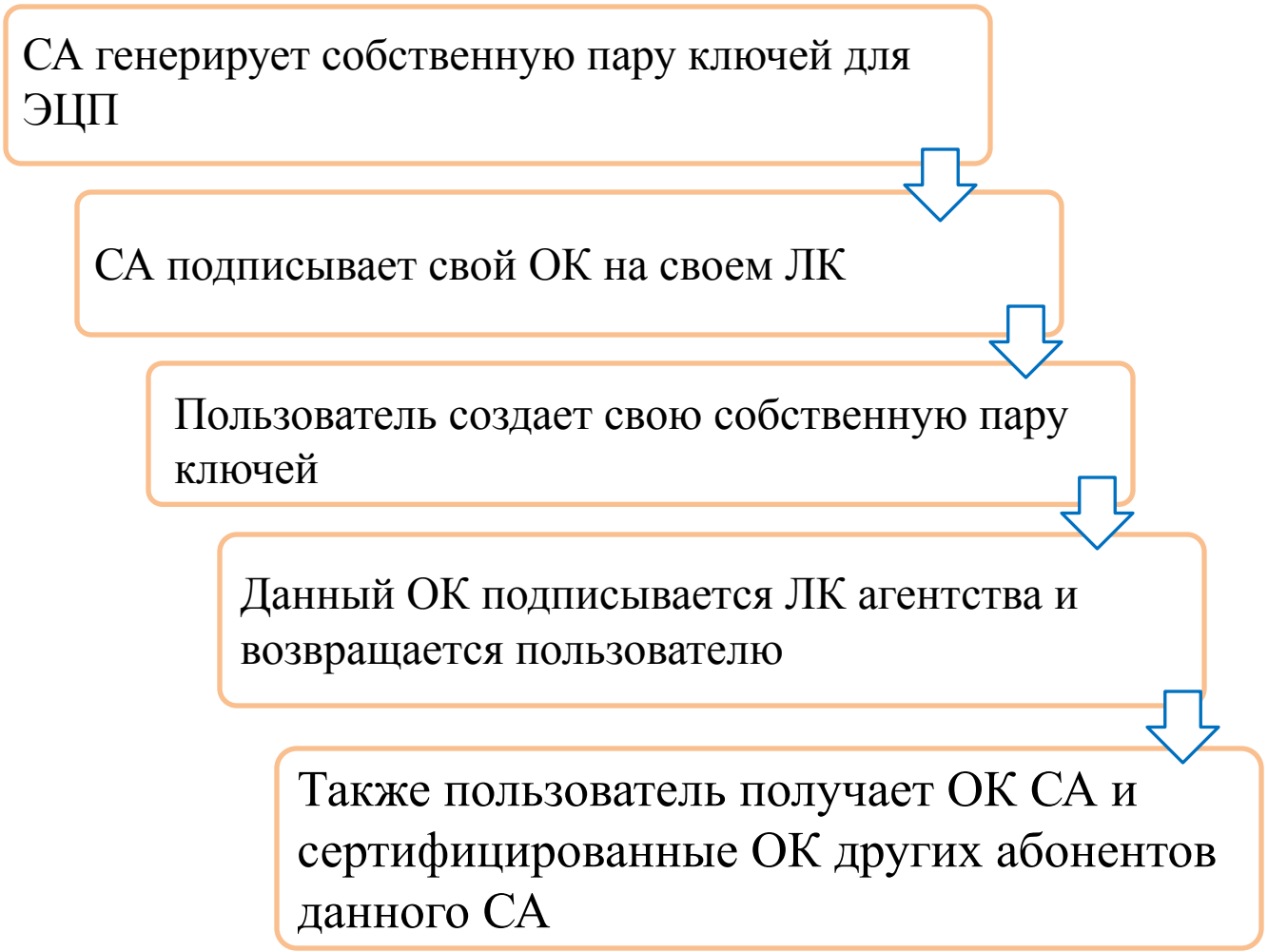
Саша подменил ОК Даши и может незаметно читать все сообщения для Даши


Решение проблемы
личной встречей
с получателем
использованием
сертификатов ОК,
которые обеспечивают
соответствие между
человеком и ОК.

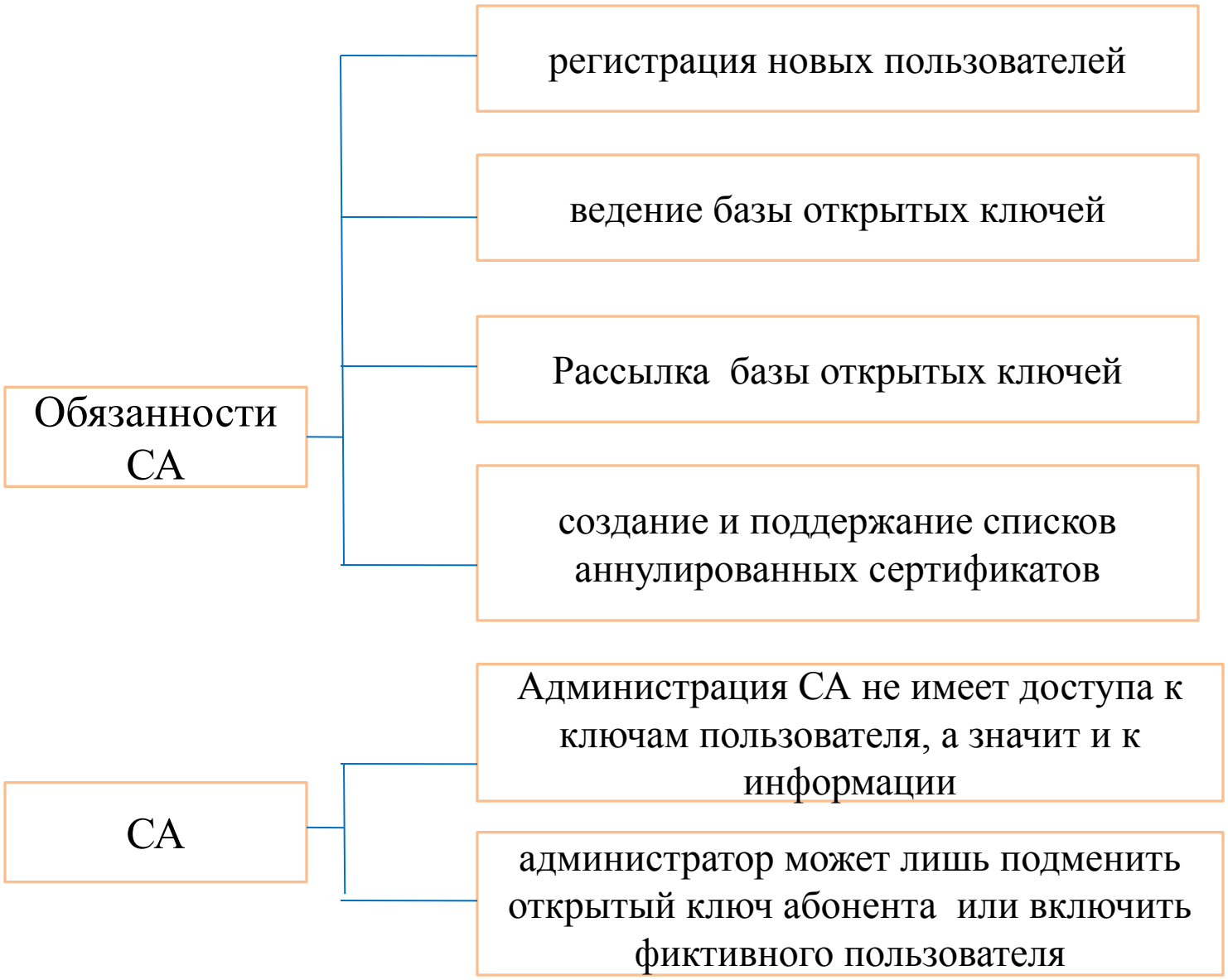
Решение проблемы

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).



Обязанности сертификационного агентства

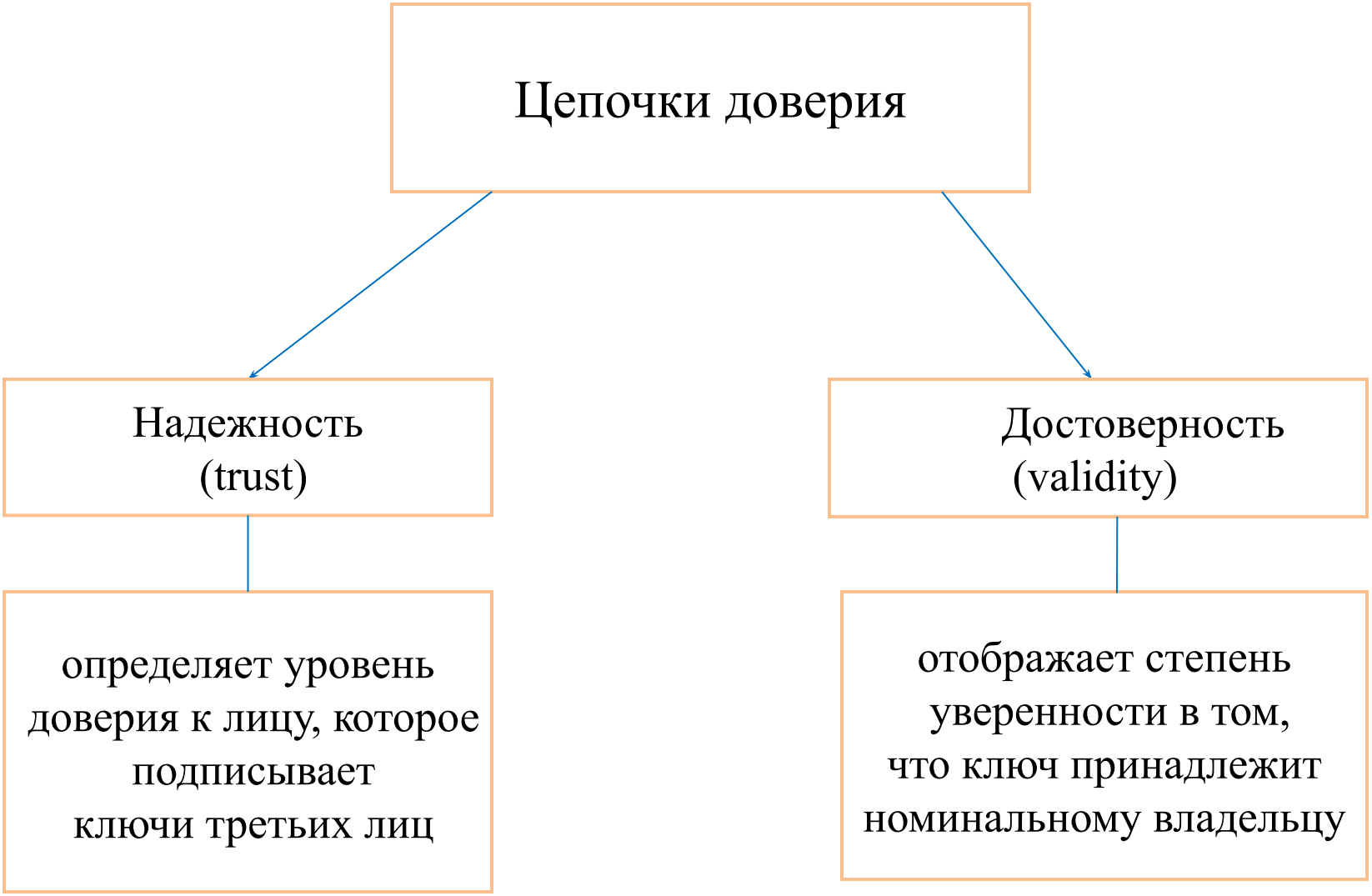


Работа без сертификационного агентства

2 абонента подписывают свои открытые ключи на личных ключах

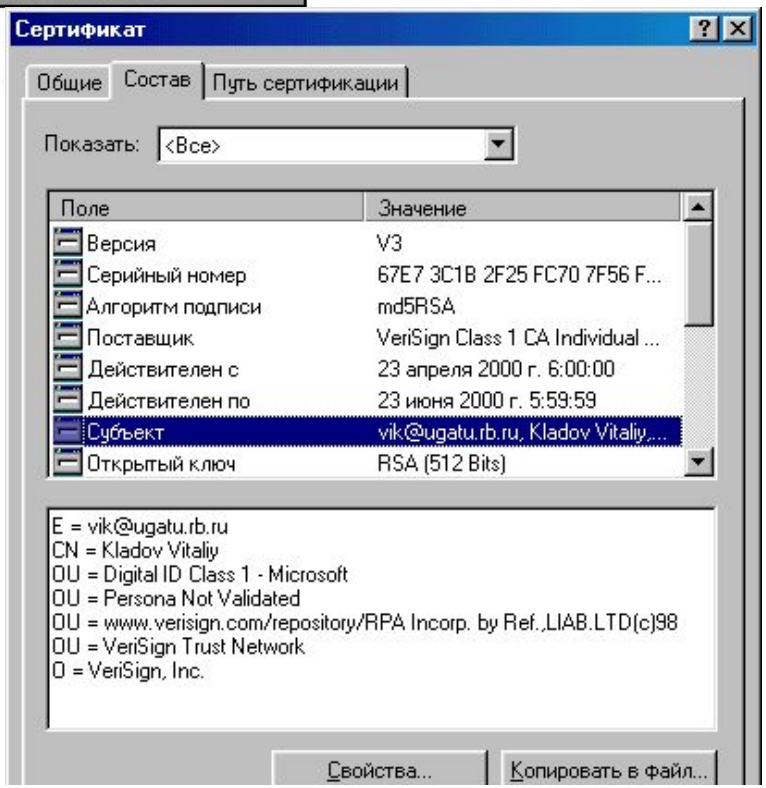
2 пользователя обмениваются открытыми ключами, соблюдая юридические формальности

Пользователь удаляет подпись партнера и подписывает его сертифицированным личным ключом.


Цепочки доверия
Надежность
(trust)
Достоверность
(validity)
определяет уровень
доверия к лицу, которое
подписывает
ключи третьих лиц
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
version 2 Issuer unique identifier	
version 2 Subject unique identifier	
CA Signature	



- номер версии
- уникальный порядковый номер
- алгоритм ЭЦП и хэш-функция, используемые CA для подписи сертификата;
- Срок действия
- Имя субъекта и его организации по формату X.500(включая иерархию организационных подразделений
- имя CA по формату X.500
- информация об ОК субъекта
- подпись сертификата

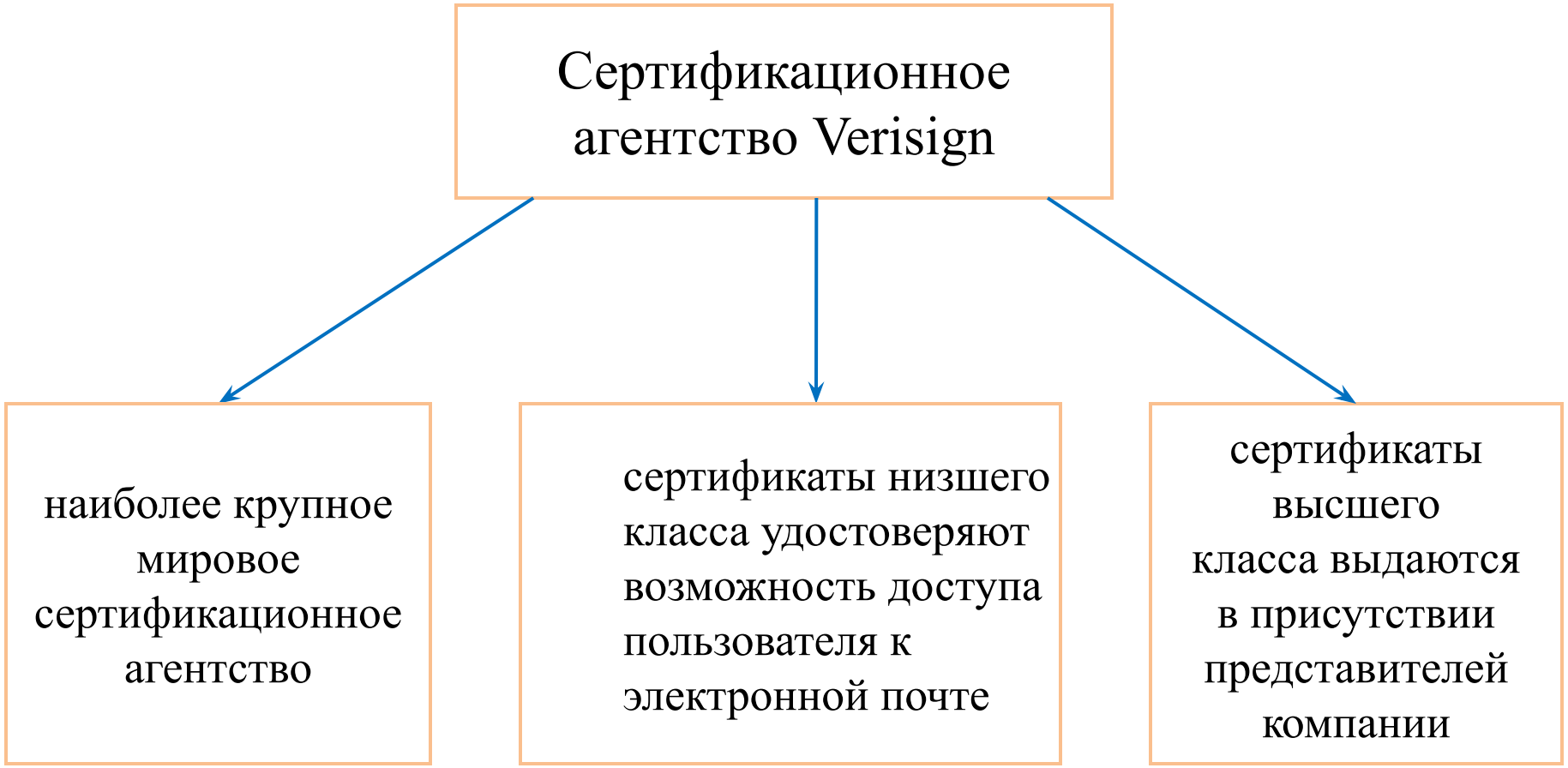
Дополнения к структуре сертификата по стандарту X.509

Версия 2 содержит:

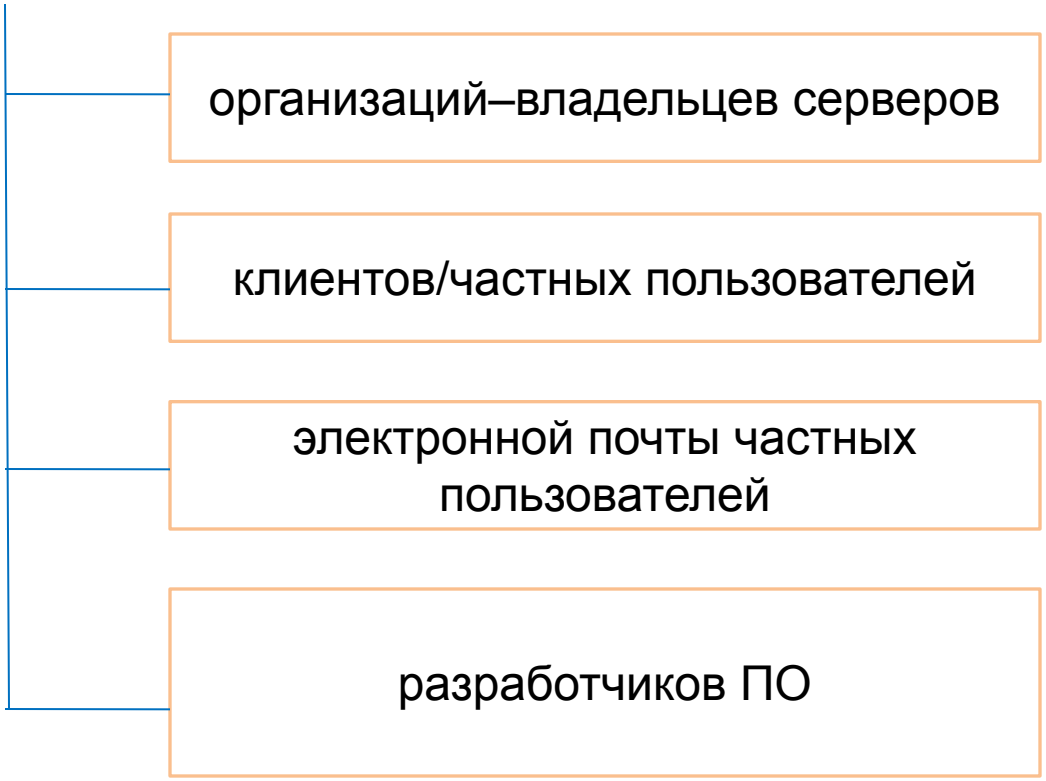
- уникальный идентификатор издателя
- уникальный идентификатор субъекта

Версия 3 содержит:

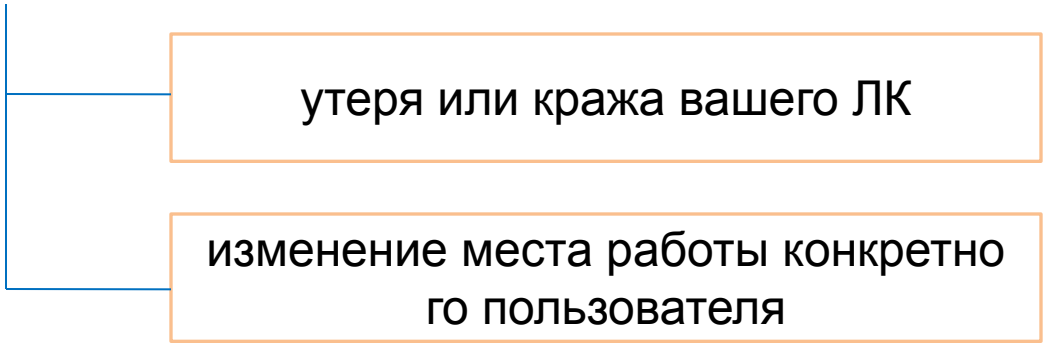
- уникальный идентификатор издателя
- уникальный идентификатор субъекта
- Дополнения. Каждое дополнение состоит из трех полей:
  - type
  - critical
  - value


Сертификационное агентство Verisign
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



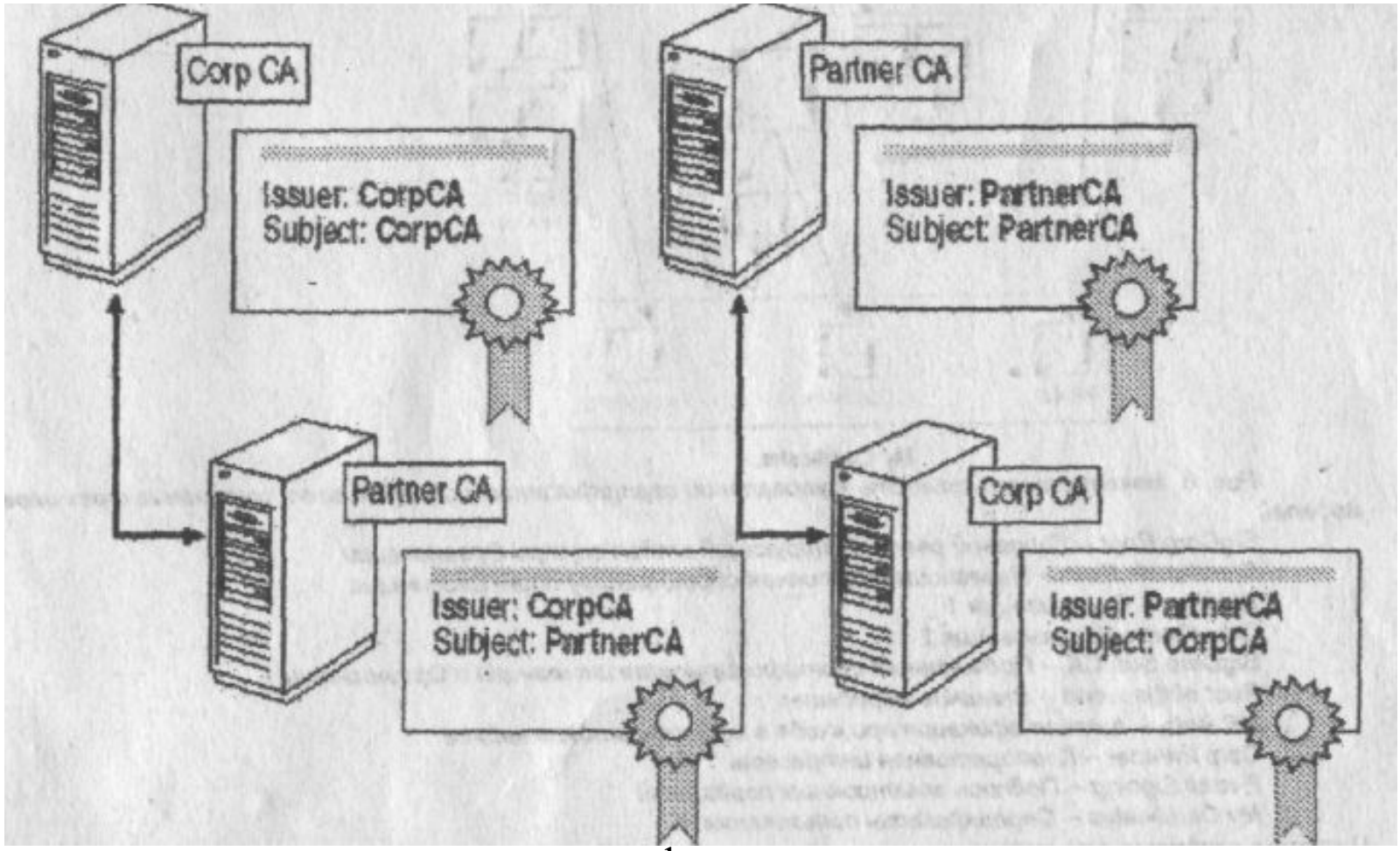
Причины отзыва сертификатов



Целесообразность использование внешнего коммерческого CA

- 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 CA самой себе, а также сертификат подчиненного CA, выданный главным CA партнера

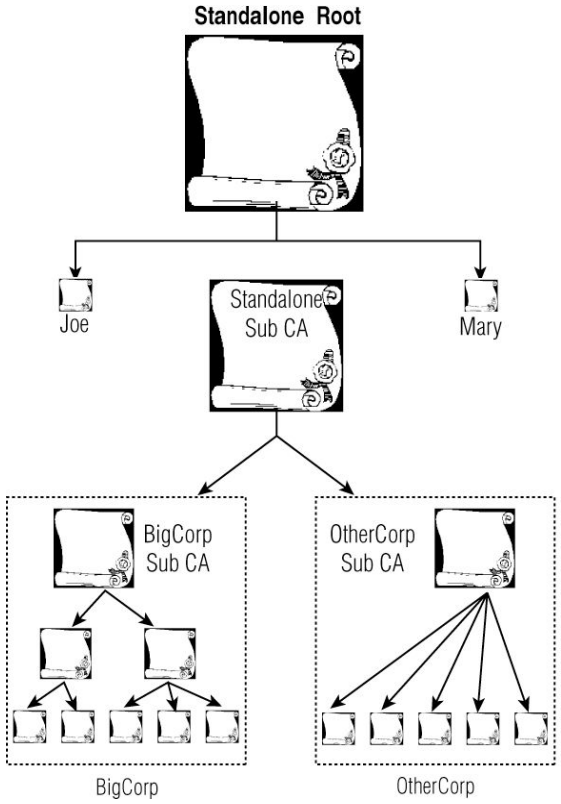
недостаток - чрезмерное доверие между организациями

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


CA
внешнее открытое CA
удобно использовать в случае небольших организаций
требуется полное доверие по отношению к агентству
крупные компании, совмещающие в себе функции CA
сохраняется контроль над процедурой шифрования
модель масштаба предприятия с подчиненными инстанциями
к главному предприятию подсоединяется CA
CA выдает сертификаты внутри подразделения
полный контроль за выдачей сертификатов
обеспечивается свободное время администратора
модели, сочетающие достоинства внешнего сертификационного агентства и достоинства модели подчиненных инстанций в рамках одного предприятия

Подчиненные CA

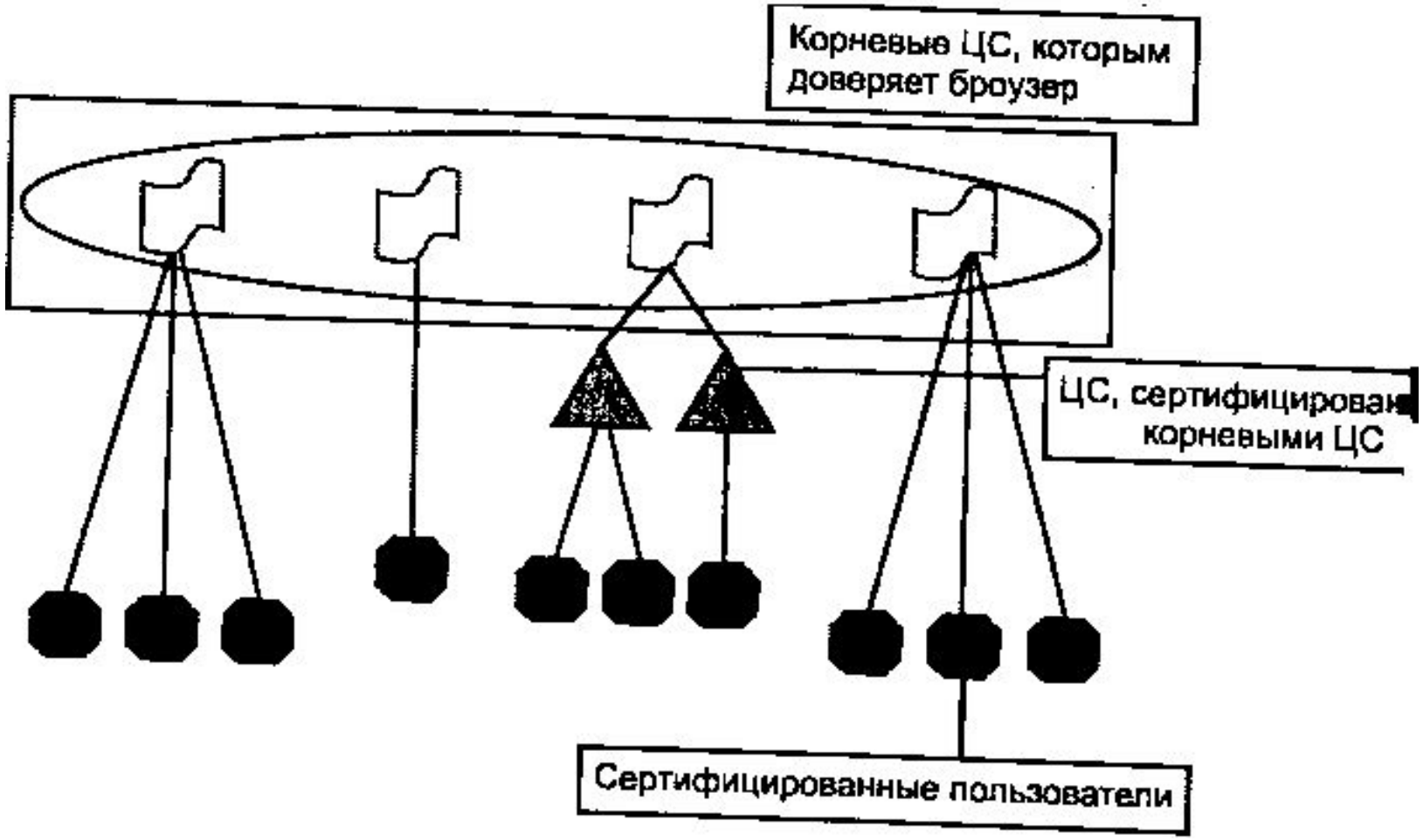


модель масштаба предприятия с подчиненными инстанциями

- к главному CA предприятия подсоединяется подчиненные CA, выдающие сертификаты отдельным подразделениям
- полный контроль за выдачей сертификатов
- дает возможность CA подразделений выдавать сертификаты своим сотрудникам.

Сложная модель

Модель доверительных отношений на веб-технологиях



Протокол SSL

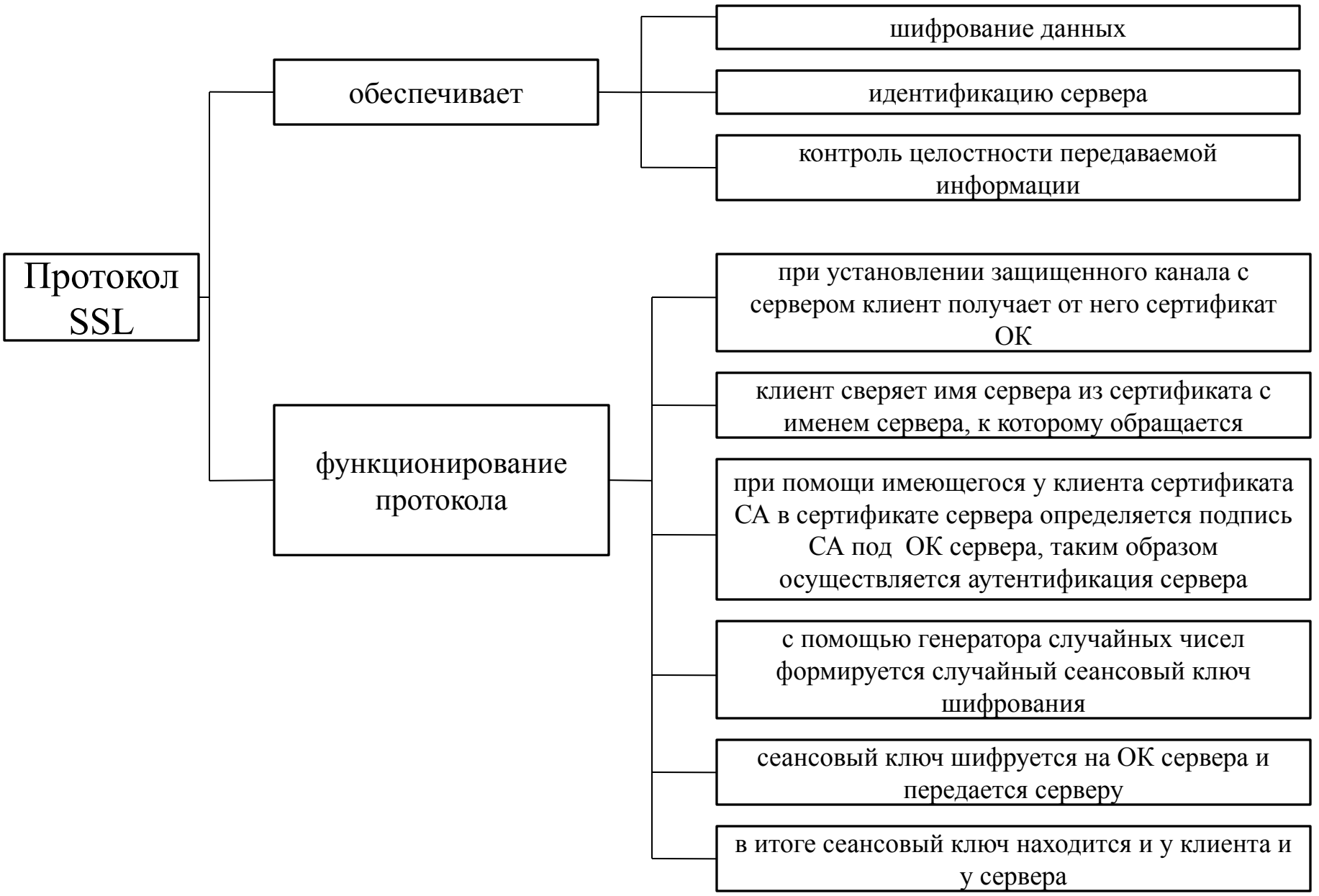
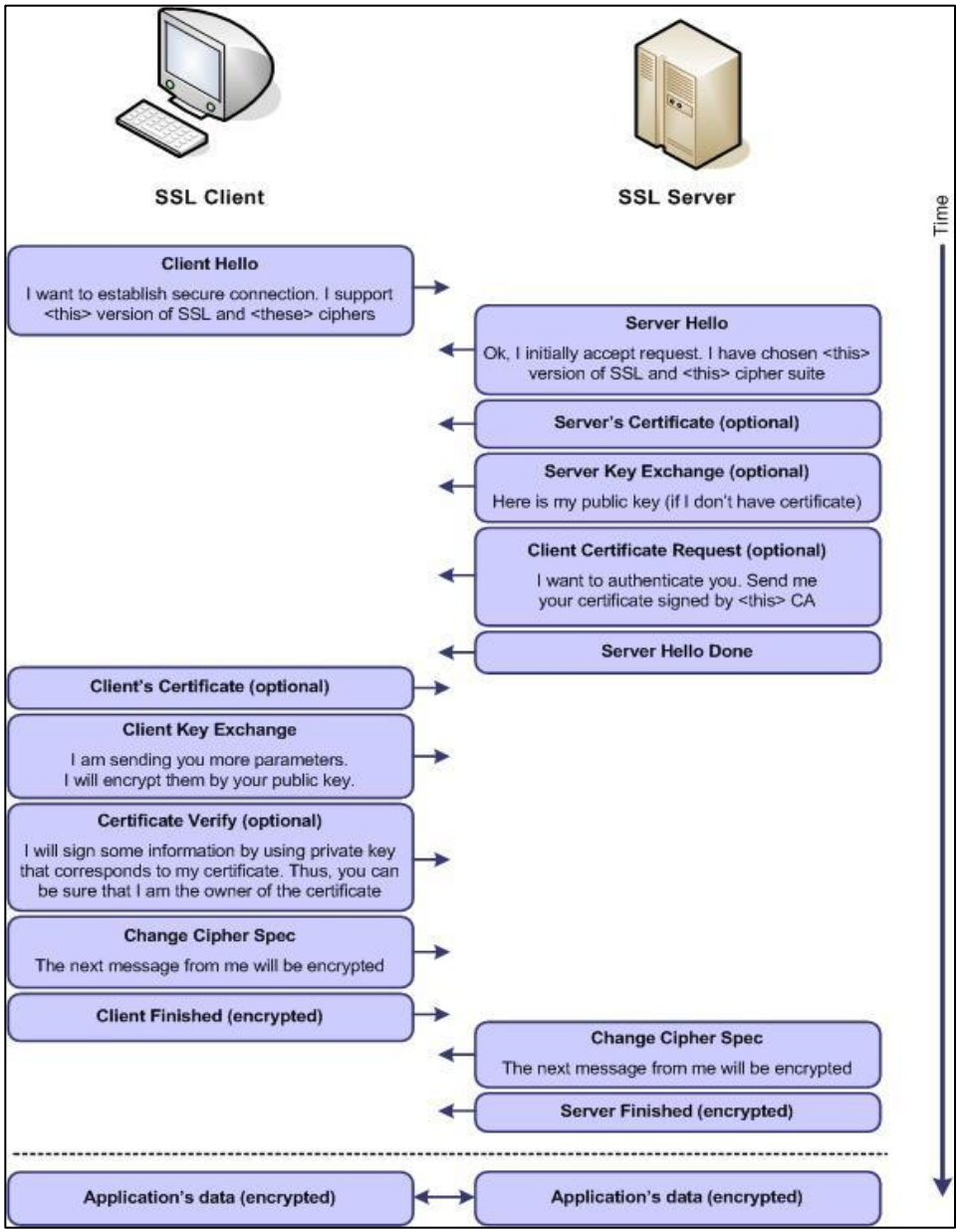
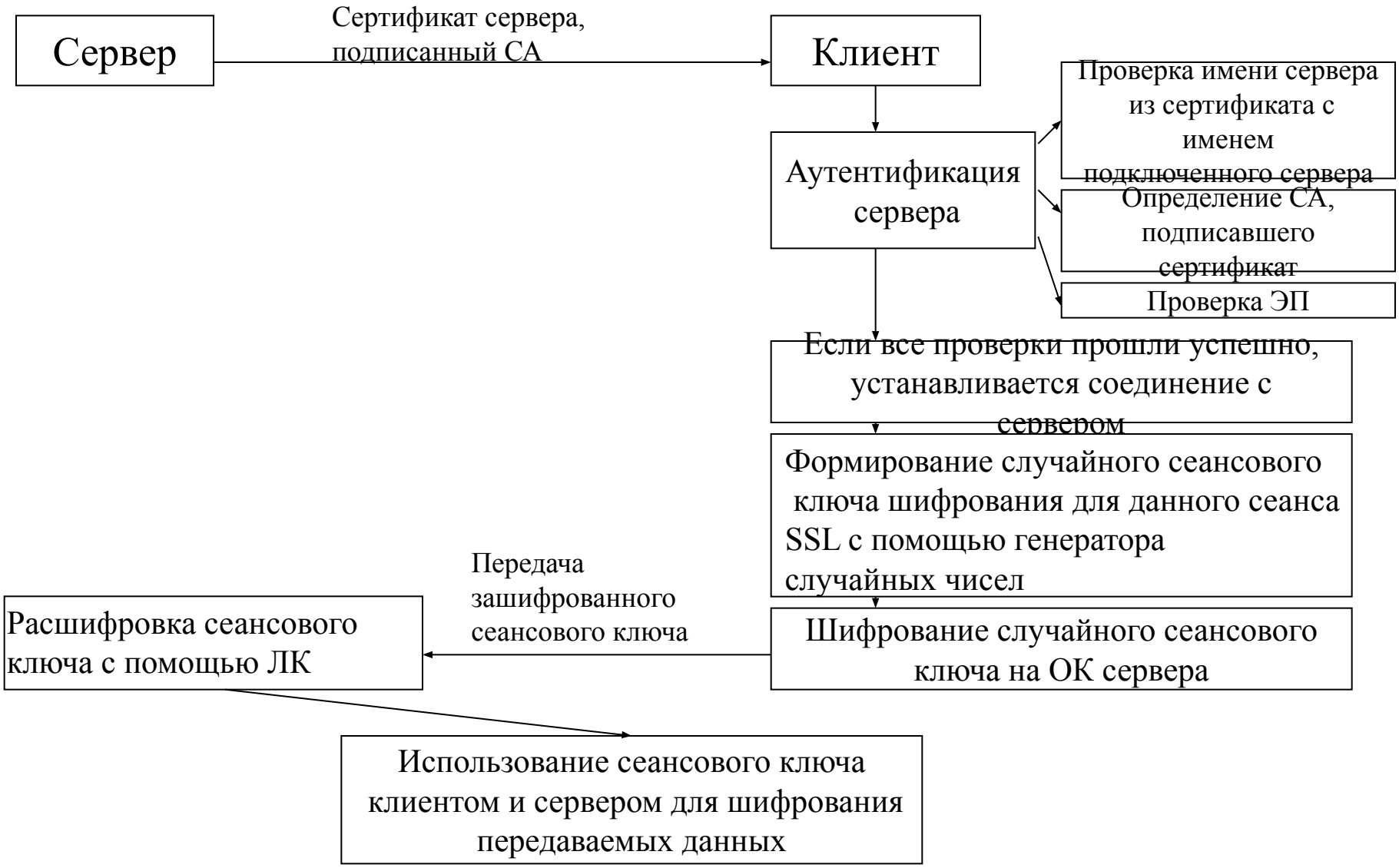


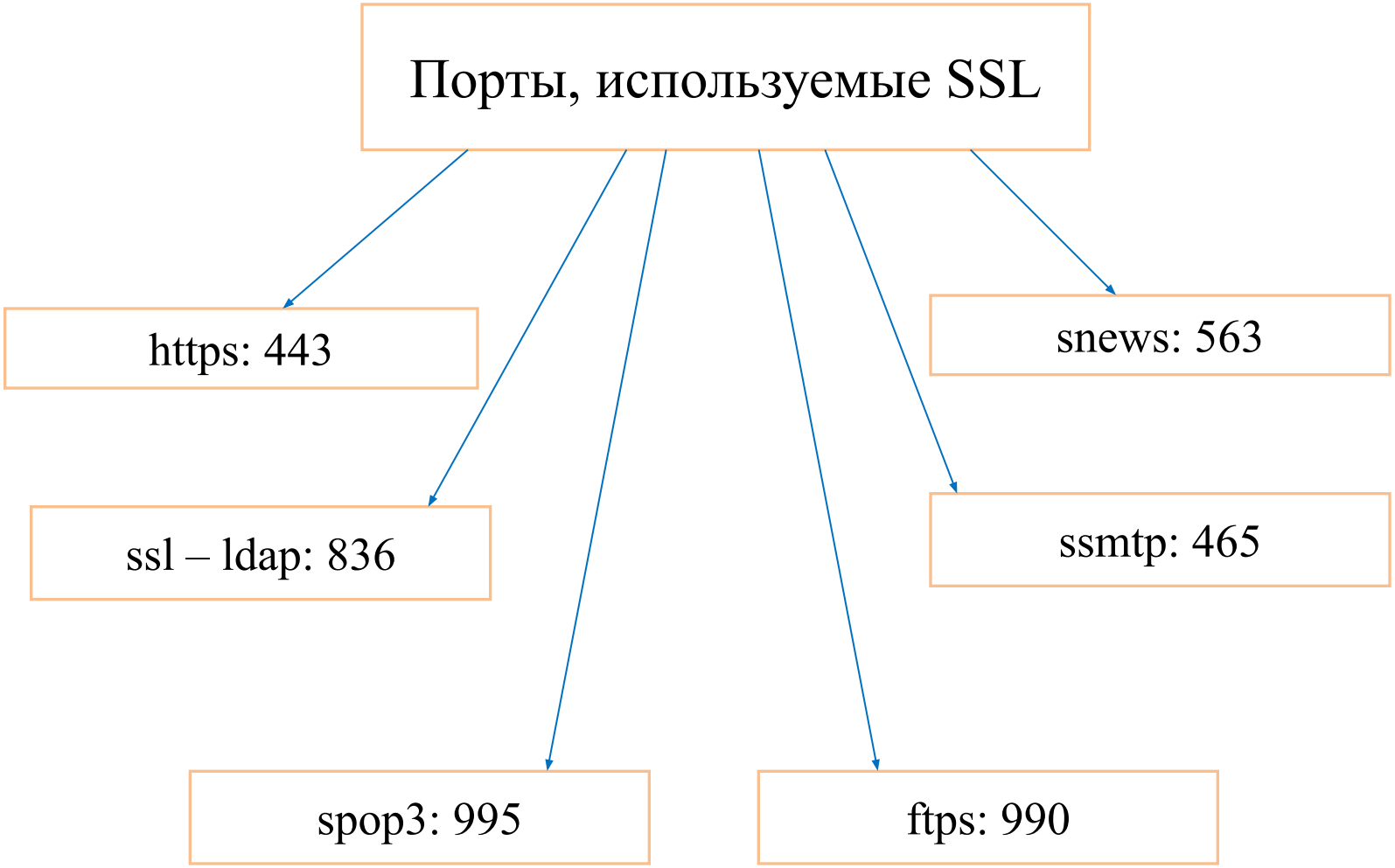
Схема работы протокола SSL



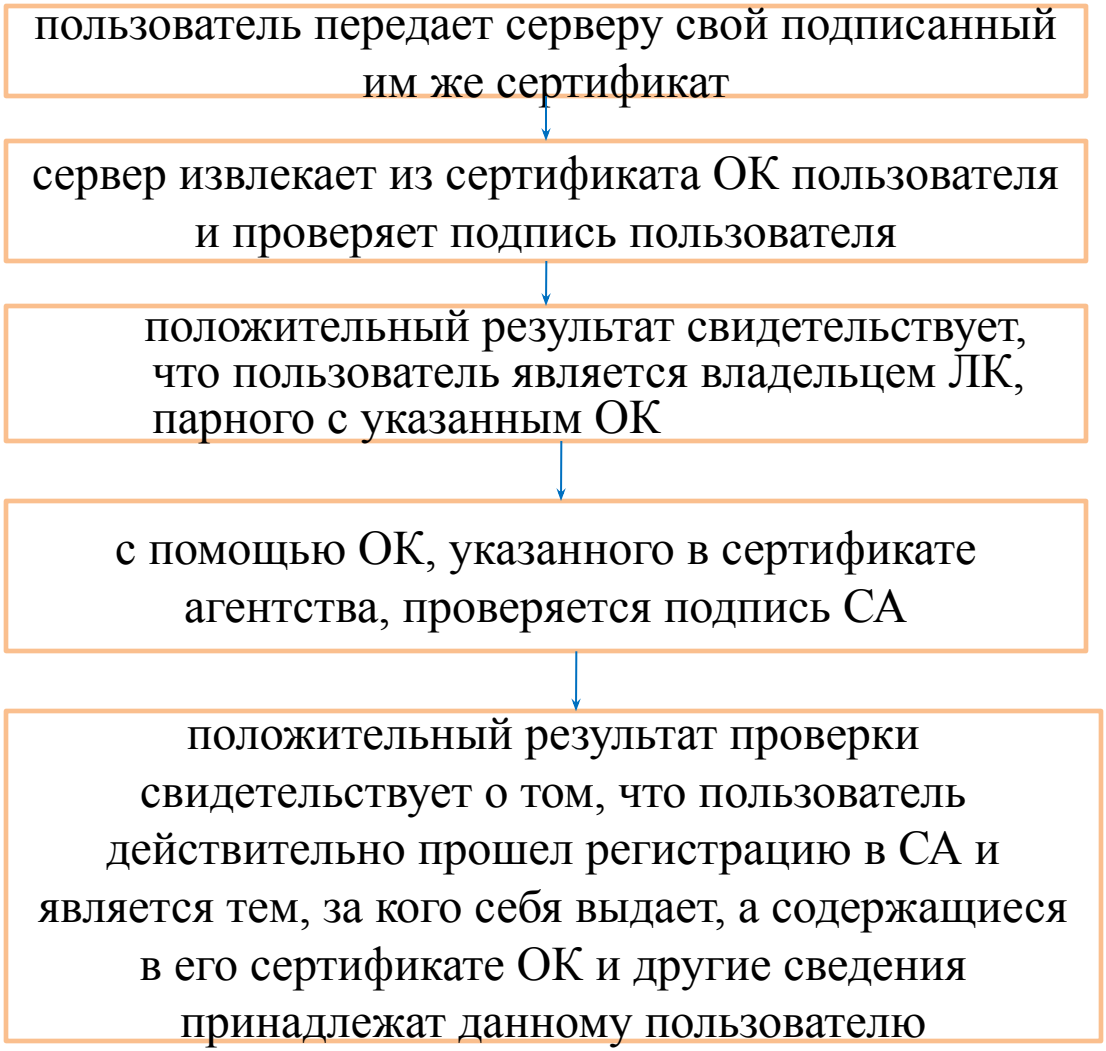
Упрощенная схема работы протокола SSL



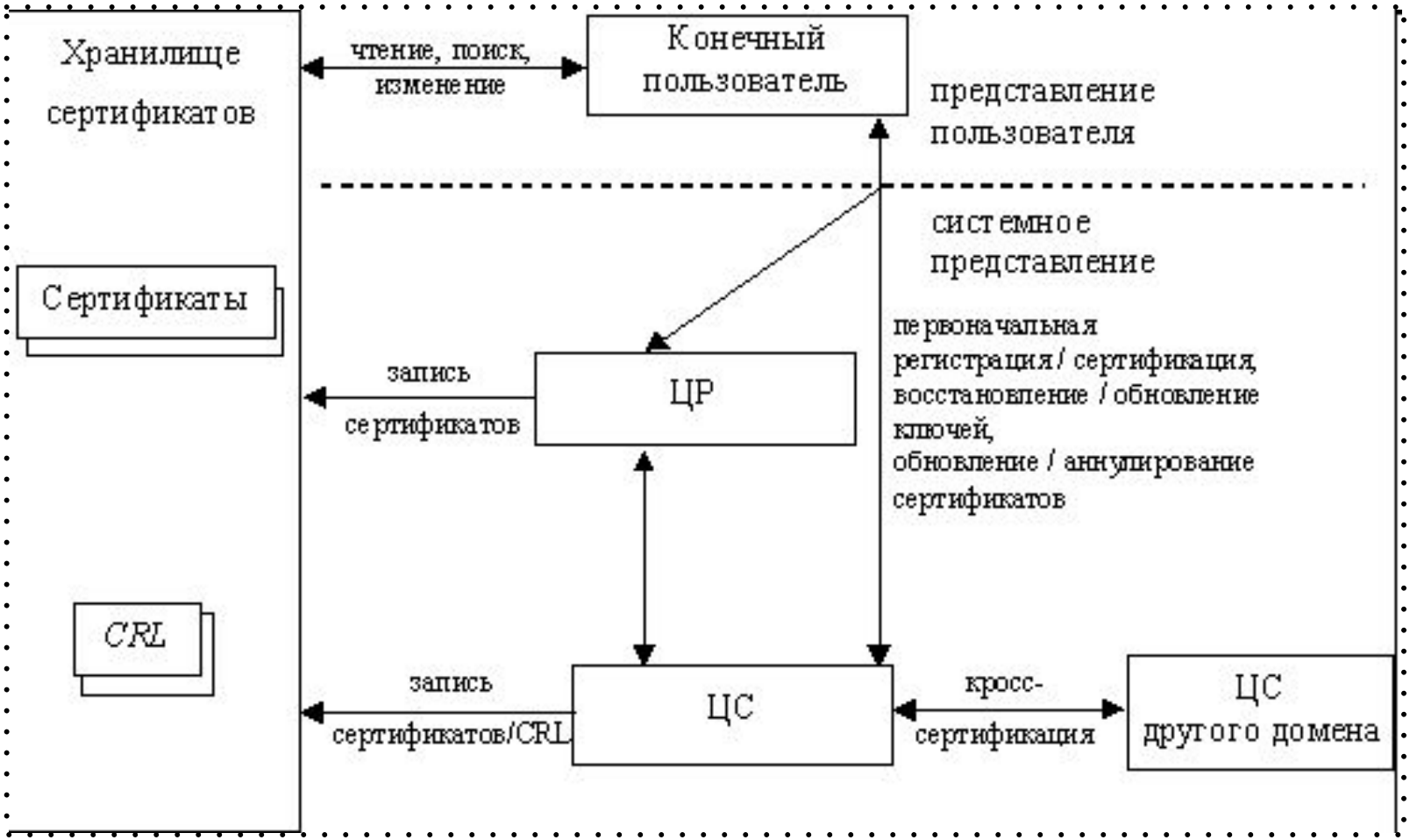
Работа протокола SSL


Порты, используемые SSL
https: 443
ssl – ldap: 836
spop3: 995
ftps: 990
ssmtp: 465
snews: 563

Механизм аутентификации на основе сертификата



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