

# ОСНОВЫ РКІ

© Учебный Центр безопасности информационных технологий Microsoft  
Московского инженерно-физического института (государственного университета), 2014 (обновлено)

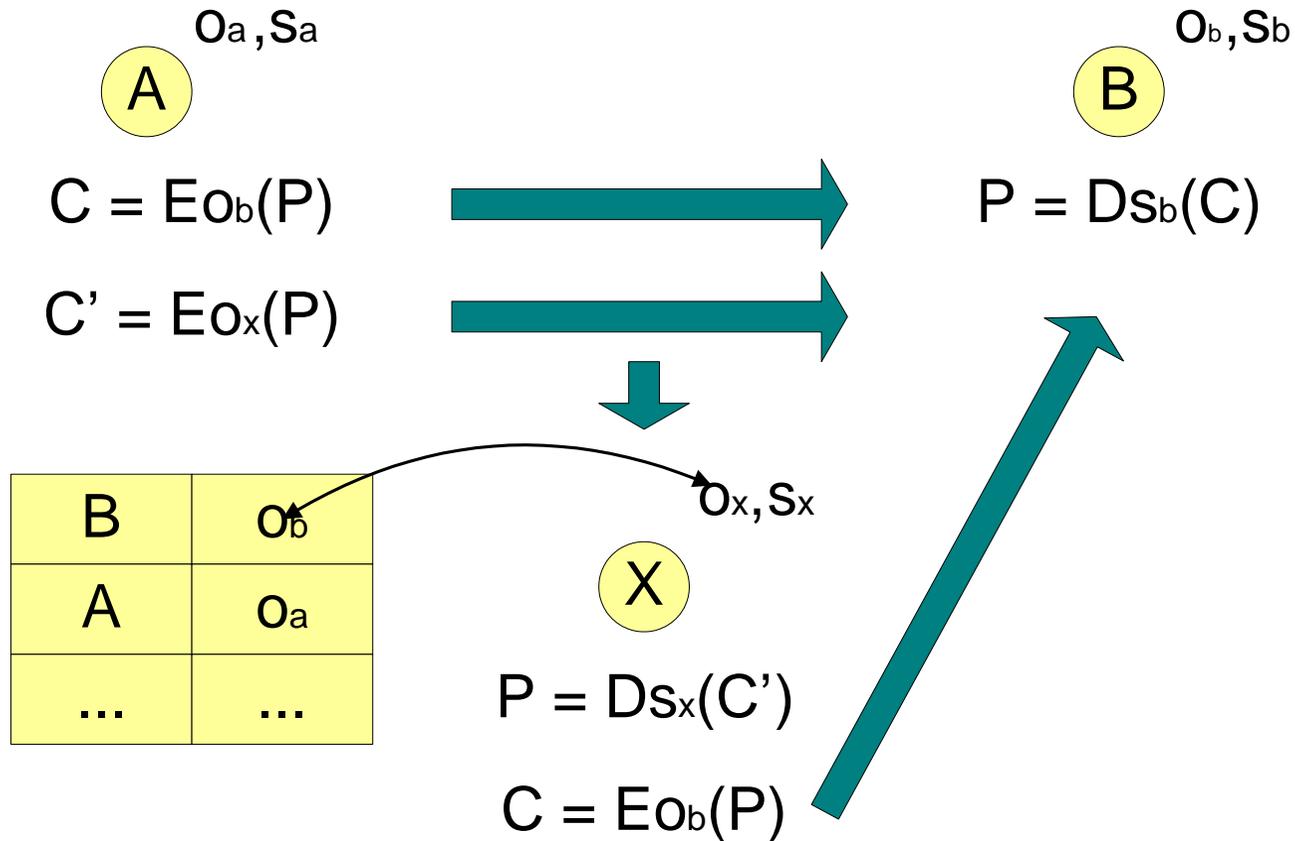
## Содержание лекции

1. Предпосылки возникновения технологии PKI
2. Понятие сертификата
3. Роль PKI в современной информационной системе
4. Структура PKI
5. Удостоверяющий центр
6. PKI: субъекты, объекты, сервисы, модули
7. Библиография

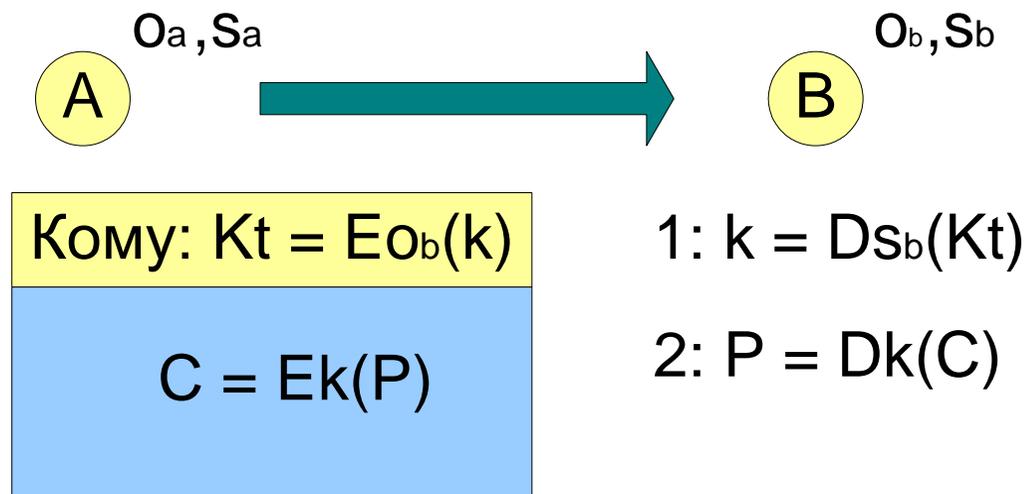
# Предпосылки возникновения PKI

1. Особенности атак на несимметричные криптосистемы
2. Появление технологии “цифрового конверта”

## Атака “посредника”



# Технология “цифрового конверта”



## Понятие сертификата

**Сертификат** – электронный документ, подтверждающий взаимосвязь между открытым ключом и идентификационными данными его владельца

*Понятие сертификата впервые было введено Конфельдером в 1976 году для решения задачи снижения нагрузки на сервер распределения открытых ключей*

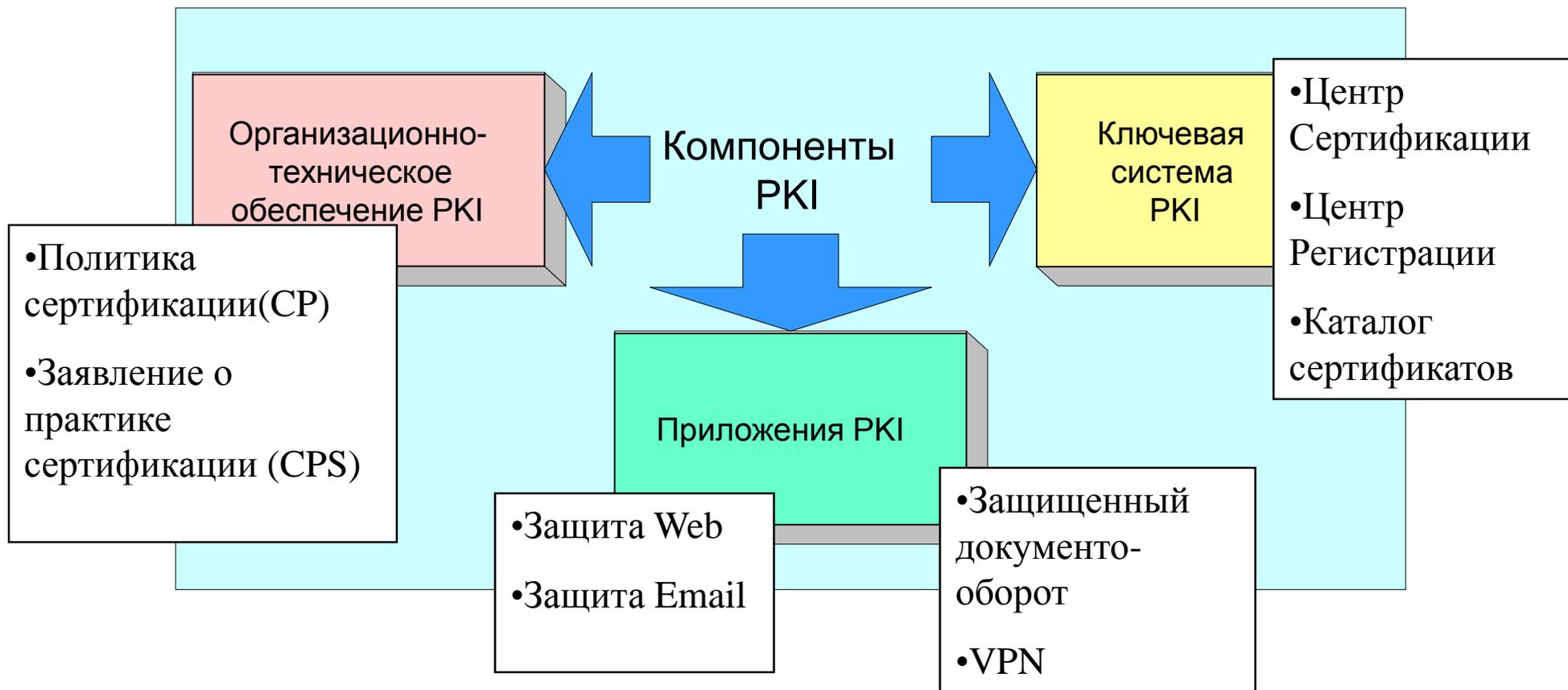
# PKI в фокусе современных систем безопасности



## Преимущества PKI

1. Дифференцирование открытых ключей по назначению и уровню безопасности
2. Гибкое управление отношениями доверия
3. Снабжение ключа идентифицирующей информацией
4. Мощный механизм контроля статуса открытого ключа

## Компоненты PKI



# Организационно-технический компонент

## Обеспечивает:

- реализацию политики безопасности

## Включает:

- политику сертификации (Certificate Policy – CP)
- заявление о практике сертификации (Certification Practice Statement – CPS)

# Регламент сертификации

1. Введение
2. Общие положения
3. Идентификация и аутентификация
4. Эксплуатационные требования
5. Физический, процедурный и персональный контроль безопасности
6. Технический контроль безопасности
7. Структуры сертификатов и СОС
8. Технические требования к администрированию

# Компонент управления ключевой системой

## Обеспечивает:

- сертификацию открытых ключей пользователей и управление жизненным циклом сертификатов открытых ключей

## Включает (в соответствии с РКIX ):

- Центр Сертификации
- Центр Регистрации
- Хранилище сертификатов

## Прикладной компонент

### Обеспечивает:

- использование сертификатов открытых ключей в прикладных системах

### Включает технологии:

- защищенной электронной почты
- защищенного доступа к Web
- защищенного документооборота
- виртуальных частных сетей (VPN)

## Удостоверяющий центр (УЦ)

**Удостоверяющий центр** – организация, осуществляющая деятельность по сертификации открытых ключей и сопровождению жизненного сертификатов открытых ключей.

*Удостоверяющий центр должен обладать необходимыми возможностями, позволяющими ему нести ответственность перед пользователями сертификатов открытых ключей за убытки, понесенные ими вследствие недостоверности информации представленной в сертификатах открытых ключей.*

## Функции УЦ

- Изготовление сертификатов открытых ключей
- Приостановка действия, возобновление и аннулирование сертификатов
- Ведение реестра сертификатов и обеспечения его актуальности
- Проверка уникальности открытых ключей в реестре сертификатов
- Разбор конфликтных ситуаций, связанных с использованием сертификатов открытых ключей в информационных системах

# Корпоративный и коммерческий УЦ

## Корпоративный УЦ:

- пространство сертификатов отражает требования политики безопасности,
- деятельность регламентируется внутренними нормативными документами

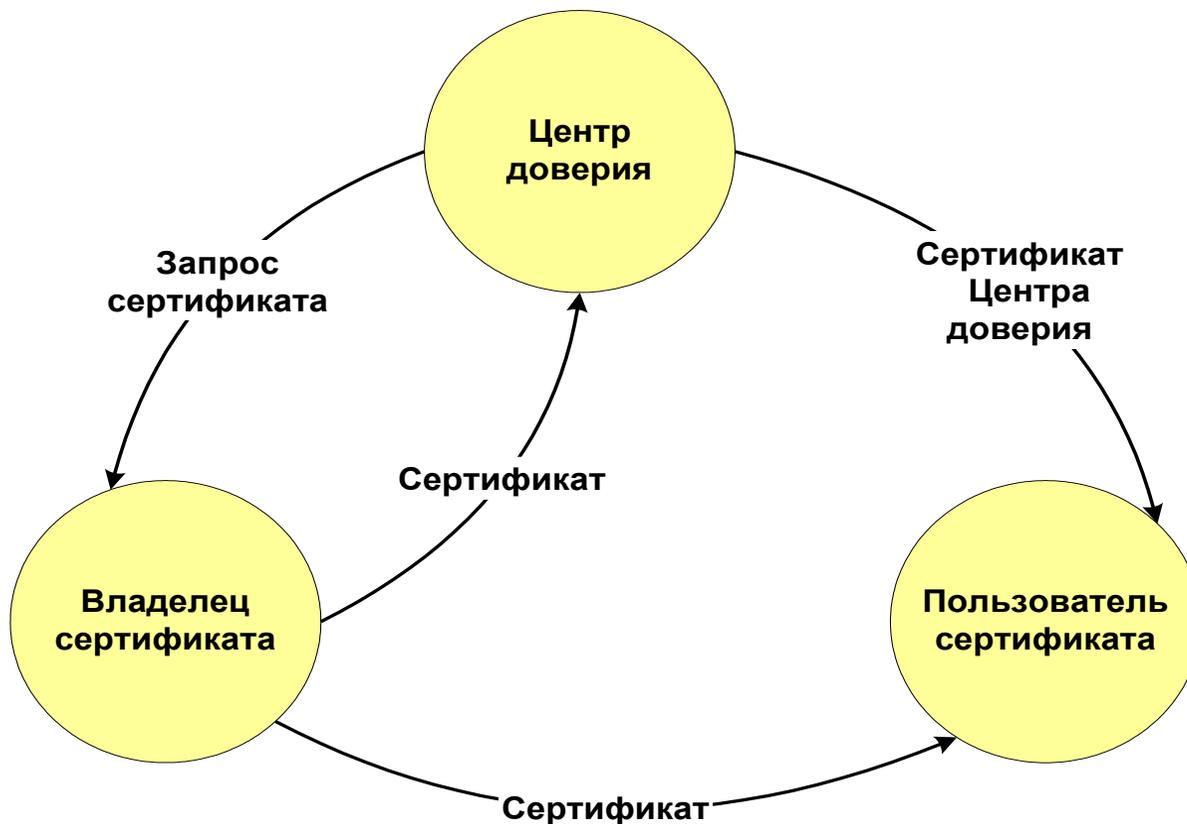
## Коммерческий УЦ:

- Пространство сертификатов представляет собой некоторое универсальное множество
- Деятельность регламентируется CPS, определяющим права и обязанности УЦ и его клиентов

## **РКІ: основные понятия и определения**

- **Субъекты РКІ** – участники информационного взаимодействия
- **Объекты РКІ** – элементы данных, участвующие в процессе информационного обмена
- **Сервисы РКІ** – сервисы, предоставляемые РКІ конечным пользователям
- **Модули РКІ** – структурные элементы РКІ-технологии

## Субъекты PKI



## Объекты PKI

- Сертификат
- Список отозванных сертификатов
- Запрос на выпуск сертификата
  - Первичный выпуск сертификата
  - Обновление сертификата
- Запрос на изменение статуса сертификата
  - Приостановка действия
  - Возобновление действия
  - Аннулирование

# Сервисы PKI

1. Сервисы управления идентификационной информацией
2. Сервисы управления ключами
3. Сервисы управления сертификатами
4. Сервисы поддержки политики безопасности
5. Прикладные сервисы

## Модули PKI

Модули	Функции
Центр Сертификации	Выпуск сертификатов и списков отозванных сертификатов
Центр Регистрации	Регистрация пользователей
Каталог	Распространение сертификатов и списков отозванных сертификатов
Архив	Долговременное хранение сертификатов и списков отзыва по истечении срока действия
Сервер восстановления ключей	Архивирование и восстановление секретных ключей
Сервер валидации	Проверка сертификатов и цепочек сертификатов

## Библиография (1)

1. L.- M. Kohnfelder. Towards a practical public-key cryptosystem. B.S. Thesis, supervised by L. Adleman, May, 1978
2. A. Nash, B. Duane, D. Brink, C. Joseph. PKI: Implementing & Managing E-Security. McGraw-Hill, Osborne Media, March, 2001
3. R. Housley, T. Polk, Planning for PKI. Best Practices Guide for Deploying Public Key Infrastructure. John Wiley & Sons, Inc., 2002
4. C. Adams, S. Lloyd. Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations. Macmillan Technical Publishing, 1999

## Библиография (2)

5. S. A. Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, August, 2000
6. M. Branchaud. A Survey of Public-Key Infrastructures. Master's thesis, McGill University, Montreal, March, 1997
7. R. Kohlas and U. Maurer, “Reasoning About Public-Key Certification: On Bindings Between Entities and Public Keys,” in Proceedings of Financial Cryptography '99 (FC99), ser. Lecture Notes in Computer Science, vol. 1648, February, 1999, pp. 86–103