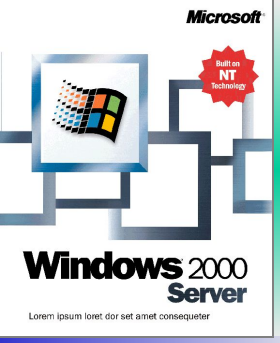
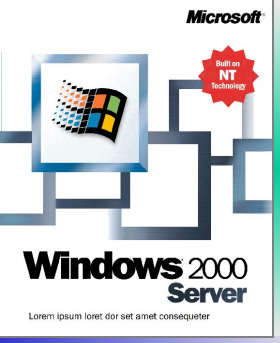


Защита информации средствами Windows 2000

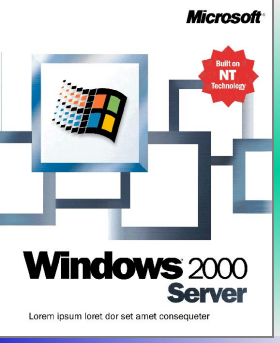
Лепихин В. Б.

УЦ «Информзащита»



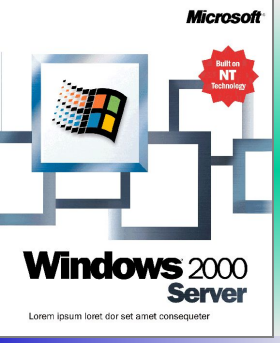
Система безопасности

- ✔ **Аутентификация пользователей**
- ✔ **Разграничение доступа к ресурсам**
  - Права и привилегии пользователей
  - Делегирование административных полномочий
  - Аудит событий, происходящих в системе
- ✔ **Защита информации**
  - Шифрование данных
  - Цифровые подписи
- ✔ **Защита от атак**



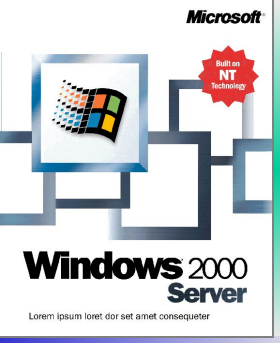
Аутентификация

- **Прежде чем допустить пользователя к ресурсам система должна его идентифицировать**
  - Учетная запись
    - Имя пользователя
    - Пароль пользователя
- **Локальная регистрация на рабочей станции**
  - Протокол NTLM
- **Регистрация в домене Active Directory**
  - Протокол Kerberos v5 rev6



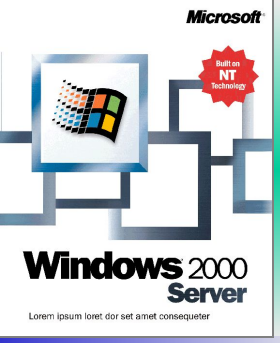
Службы Kerberos

- **Key Distribution Center (KDC)**
  - Authentication Service (AS)
    - Интерактивная регистрация пользователя в домене
    - Билет Ticket-Grant Ticket (TGT)
      - Персональное “удостоверение” пользователя
  - Ticket Granting Service (TGS)
    - Неинтерактивная регистрация пользователя при обращении к ресурсам домена
    - Билет Service Ticket
      - Персональный “пропуск” пользователя на сервер, управляющий ресурсами

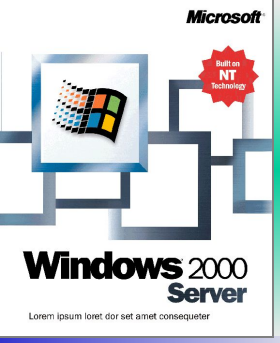


Возможности Kerberos

- ✔ **Транзитивные доверительные отношения между доменами**
  - Inter-Realm Key для каждой пары доверяющих доменов
  - Пошаговое движение клиента по дереву до KDC искомого домена
- ✔ **Делегирование**
  - Ограниченная имперсонация
  - Полная имперсонация
- ✔ **Аутентификация в домене с помощью Smart-Card**
  - Расширение Kerberos PKINIT

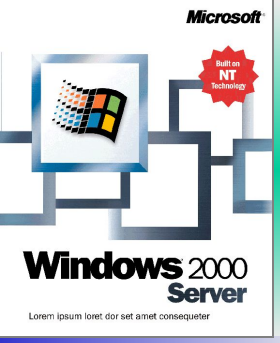


Контроль доступа к объектам



Субъект

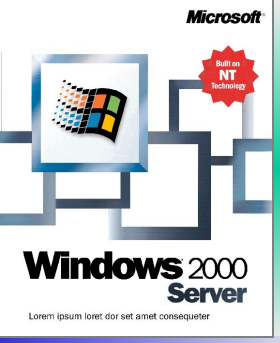
- **Привилегии**
  - Возможность выполнять ту или иную операцию на данном компьютере
    - Ассоциированы с пользователем
- **Права**
  - Запреты и разрешения на выполнение тех или иных действий с объектом
    - Ассоциированы с объектом
- **Пользователь**
  - Однозначно определяется своей учетной записью в каталоге
  - Security Identifier (SID) пользователя



Маркер доступа

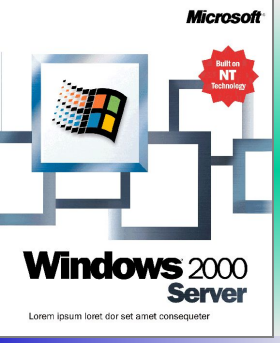
✔ Маркер доступа субъекта

- Формируется для каждого субъекта
  - Ассоциируется с каждым потоком, исполняемым от имени пользователя
- Важнейшие компоненты
  - SID пользователя
  - SID-ы всех групп, в которые пользователь входит
  - Установленные на данном компьютере привилегии пользователю и группам, в которые он входит



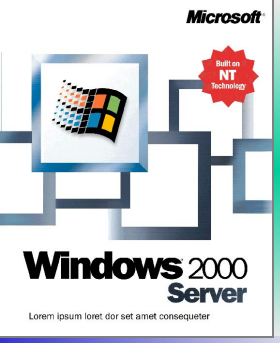
Объект

- **Объекты файловой системы**
  - Файлы
  - Папки
- **Объекты каталога Active Directory**
  - Пользователи
  - Компьютеры
  - Принтеры
  - Контейнеры
- **Свойства объекта определяются набором атрибутов**



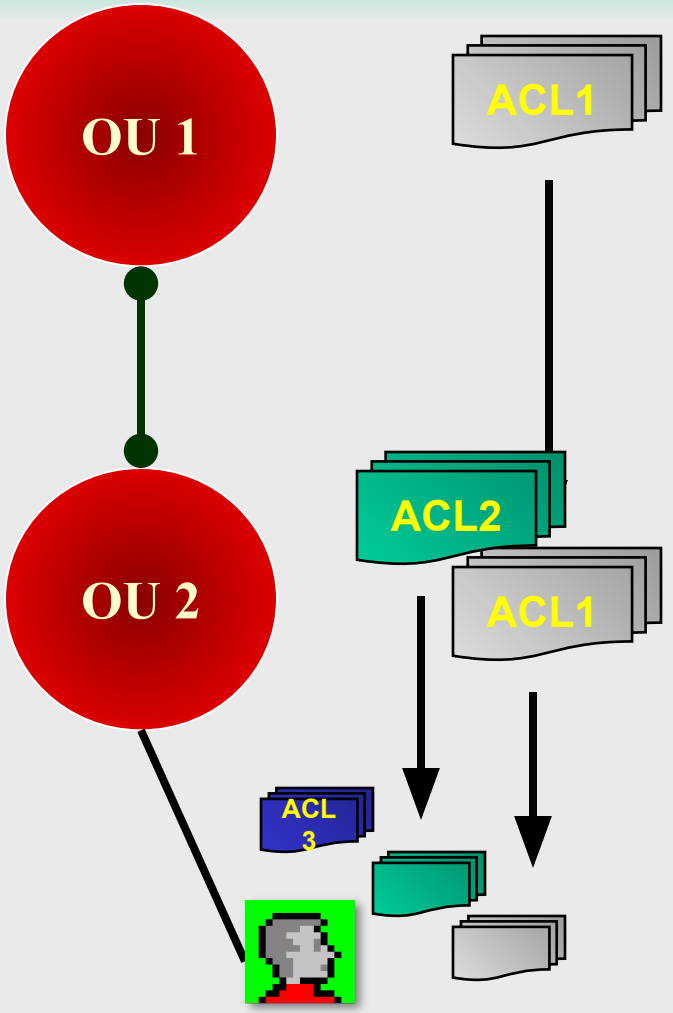
Дескриптор безопасности объекта

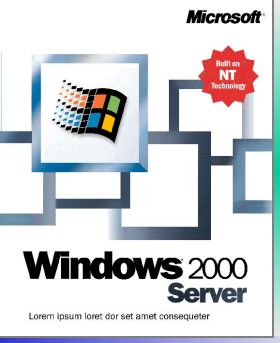
- **Discretionary Access Control List, DACL**
  - Список запретов и разрешений, установленных для данного объекта
- **System Access Control List, SACL**
  - Список назначений аудита
- **Access Control Entry, ACE**
  - Каждая ACE содержит назначение прав для конкретного SID
  - ACL объекта Active Directory может содержать строки ACE, назначенные отдельным атрибутам



Наследование

- **Формирование ACL объекта в иерархии**
  - Явные назначения
  - Наследование с верхних уровней
- **Статический механизм наследования**
- **Делегирование полномочий**

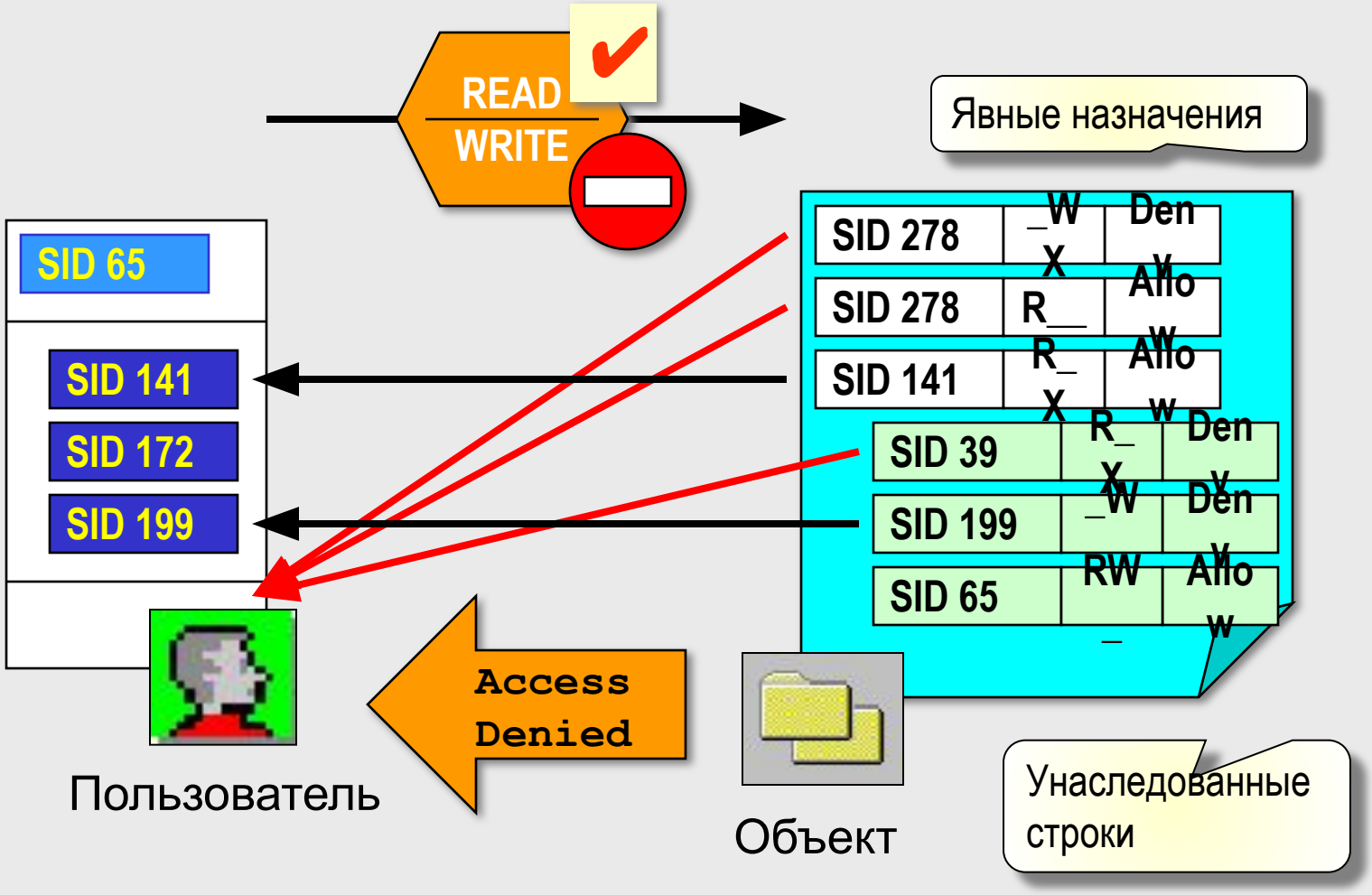


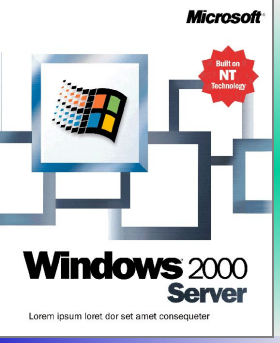


Эффективные права

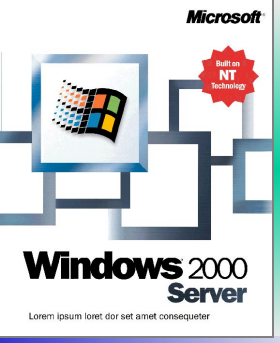
- **Порядок следования строк ACE в финальном списке**
  - Явные запреты
  - Явные разрешения
  - Унаследованные запреты
  - Унаследованные разрешения
- **Проверка прав выполняется в порядке следования строк ACE**
  - До первого появления запрета на какую-либо операцию
  - До явного разрешения всех запрошенных операций

Проверка прав



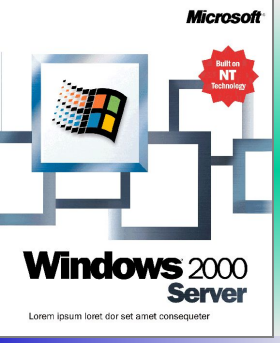


Инфраструктура открытого ключа



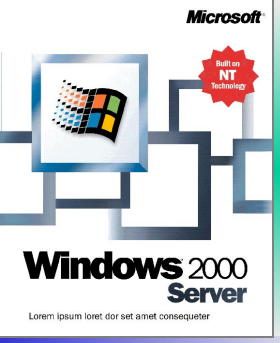
Концепции PKI

- **Методы шифрования**
  - Симметричное шифрование
    - Шифрование потоков данных с помощью сеансового ключа, известного обоим участникам
  - Шифрование с открытым ключом
    - Обмен сеансовым ключом при установлении защищенного канала
    - Цифровая подпись
- **Инфраструктура открытого ключа**
  - Цифровые сертификаты открытых ключей
  - Службы управления сертификатами



CSP и CryptoAPI

- **CryptoAPI**
  - Программные интерфейсы к криптографическим службам Windows 2000
- **Cryptographic Service Provider**
  - Криптографические операции
  - Генерация и хранение ключей
- **Microsoft CSPs**
  - Базовый набор
  - High Encryption Pack

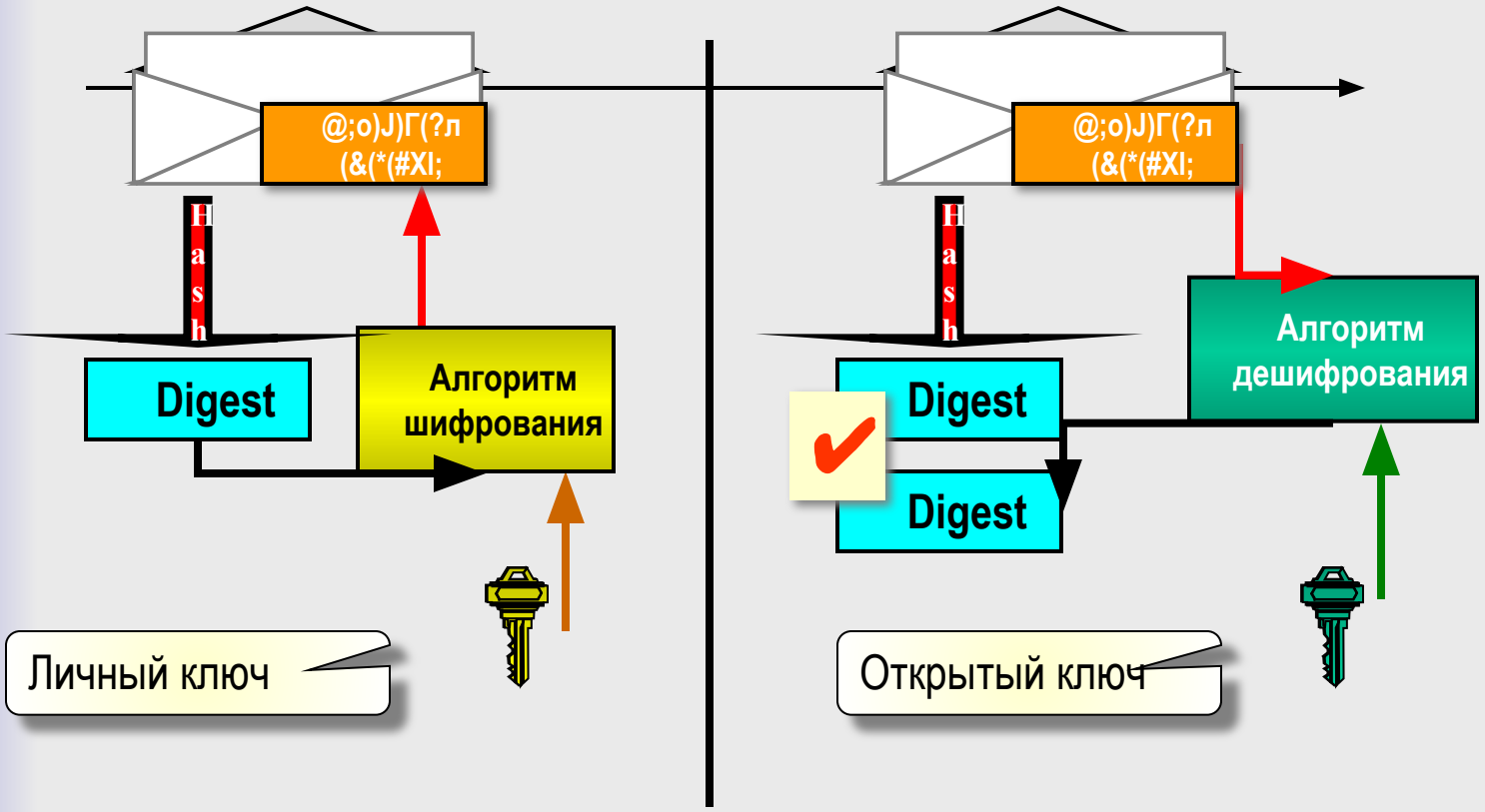


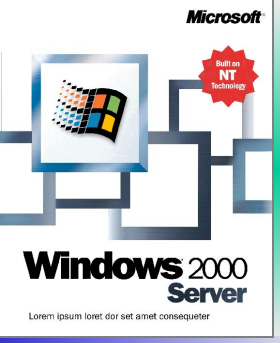
Алгоритмы

- **Симметричное шифрование**
  - Data Encryption Standard (DES)
    - DES-CBC, Triple DES, DESX
  - Rivest's Cipher (RC)
    - RC2, RC4
- **Обмен ключами**
  - Diffie-Hellman Key Agreement
  - RSA Key Exchange
- **Хеширование**
  - Message Digest (MD)
    - MD2, MD4, MD5
  - Secure Hash Algorithm (SHA)
  - Hashed Message Authentication Code (HMAC)

Цифровая подпись

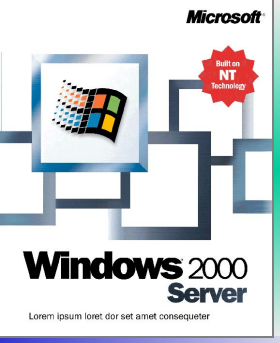
- ✔ Digital Signature Algorithm (DSA)
- ✔ RSA Digital Signature





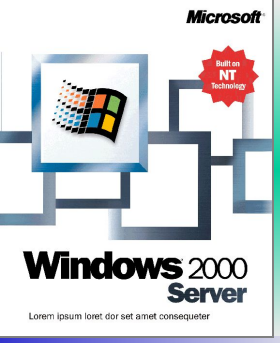
Сертификат

- **Цифровое удостоверение**
  - Стандарт X.509 версия 3
- **Информация, однозначно идентифицирующая субъекта**
  - Его открытый ключ
    - Допустимые режимы использования
- **Информация, необходимая для проверки сертификата**
  - Срок действия сертификата
  - Информация о службе, выдавшей сертификат
- **Цифровая подпись CA**



Microsoft Certificate Services

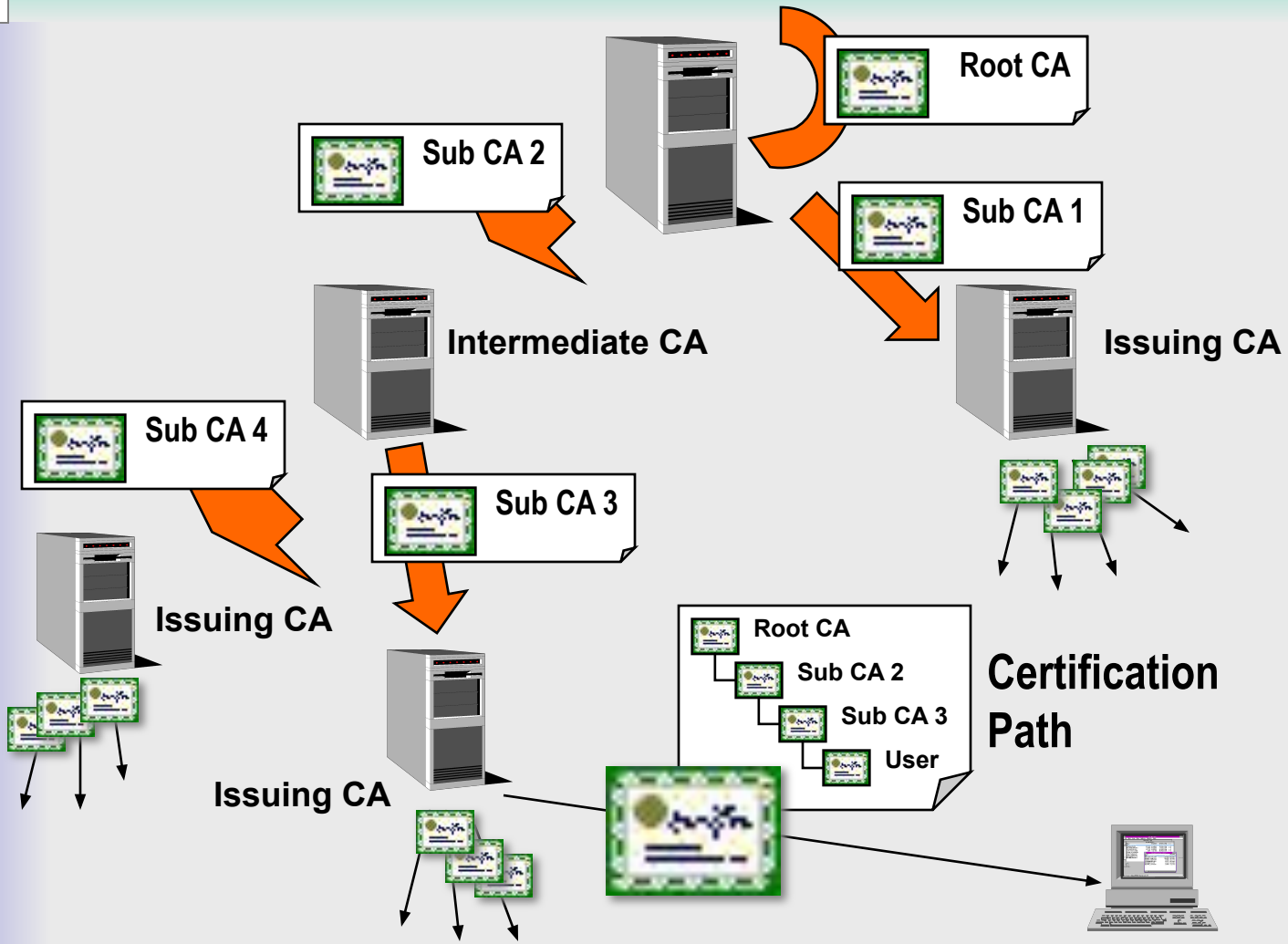
- **Certification Authority**
  - Выдача сертификатов клиентам
    - Генерация ключей, если нужно
  - Отзыв сертификатов
    - Публикация Certificate Revocation List
  - Хранение истории всех выданных сертификатов
- **Web Enrollment Support**
  - Запрос и получение сертификата через Web-интерфейс

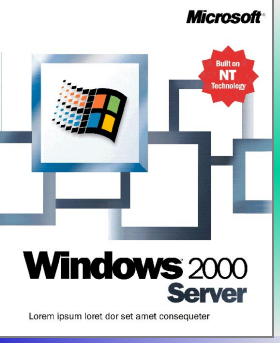


Microsoft CA

- **Enterprise CA**
  - Интегрирован с Active Directory
  - Выдает сертификаты только объектам, имеющим учетные записи в каталоге
  - Использует шаблоны сертификатов
- **Stand-Alone CA**
  - Не зависит от Active Directory
  - Может использоваться в качестве независимого центра сертификации для любых объектов

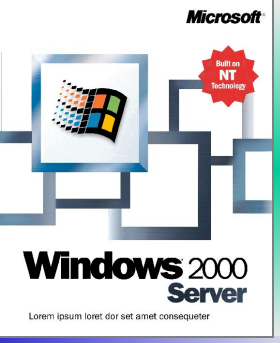
Иерархия CA


Root CA
Sub CA 2
Sub CA 1
Intermediate CA
Issuing CA
Sub CA 4
Sub CA 3
Issuing CA
Issuing CA
Root CA
Sub CA 2
Sub CA 3
User
Certification Path



CRL

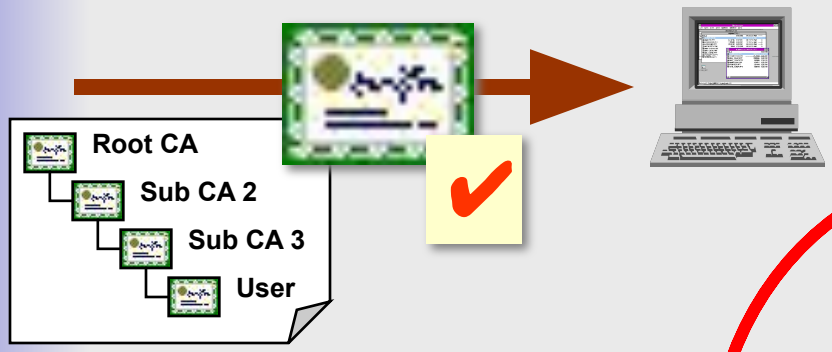
- **Certificate Revocation List**
  - Список отозванных сертификатов
  - Должен публиковаться и регулярно обновляться каждым CA
    - Active Directory
    - Web
    - Файловая система
- **Сертификат содержит список узлов публикации CRL**



Хранилища сертификатов

- **Физические хранилища**
  - Active Directory
  - Реестр операционной системы клиента
  - Файловая система
- **Логические хранилища**
  - Personal
  - Trusted Root Certification Authorities
  - Enterprise Trust
    - Certificate Trust List (CTL)
  - Intermediate Certification Authorities
  - Active Directory User Object
  - Software Publisher’s Certificate

Проверка сертификата



Тип сертификата

Сертификат разрешено использовать в данном режиме.

Срок действия

Сертификат действителен в данный момент.

Целостность

Цифровая подпись CA, выдавшего сертификат, верна.

Легитимность

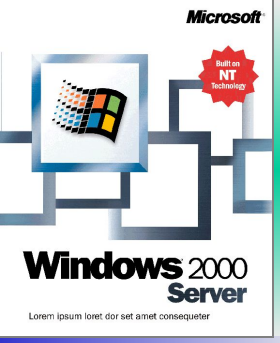
Сертификат не был отозван.

Запреты

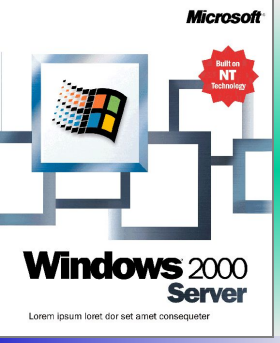
Списки CTL не запрещают использование сертификата для данной задачи.

Доверие

Сертификат корневого CA присутствует в хранилище Trusted Root Certification Authorities.



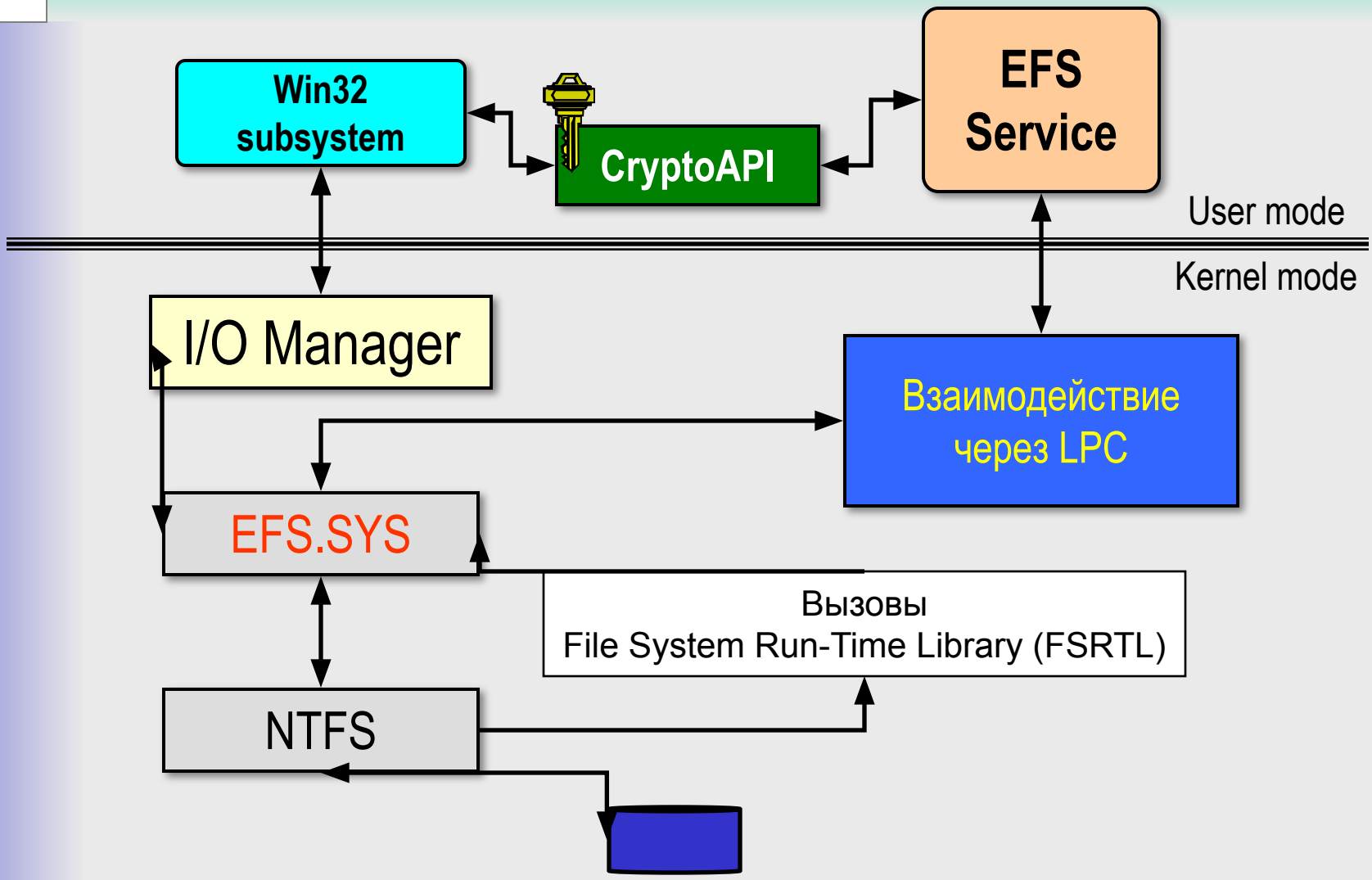
Шифрующая файловая система (EFS)



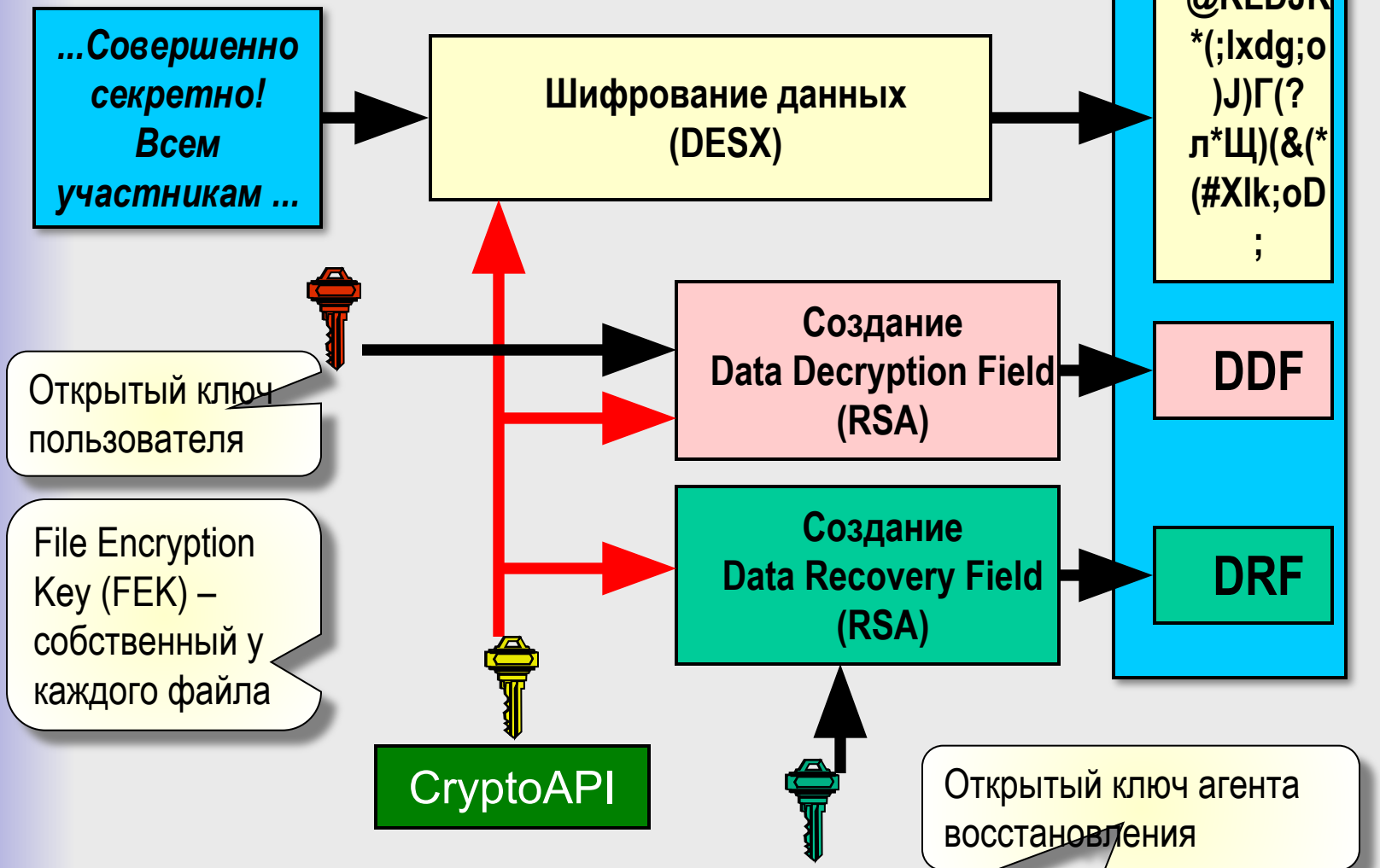
Концепции EFS

- ✔ **Шифрование данных, на уровне файловых операций NTFS**
- ✔ **Прозрачный доступ к зашифрованным данным из приложений**
- ✔ **Возможность восстановления зашифрованных данных**
  - Emergency Data Recovery Policy

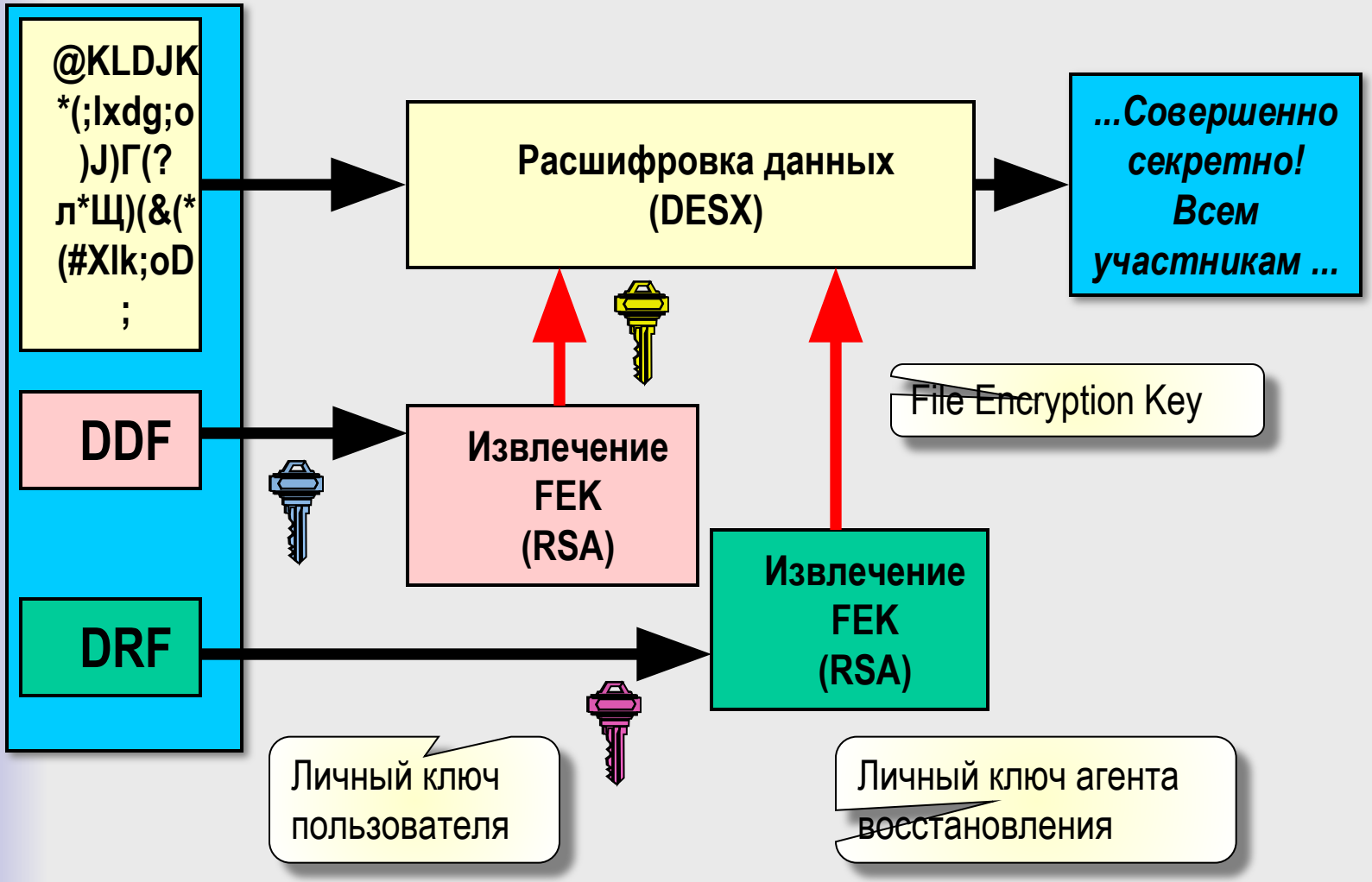
Архитектура EFS

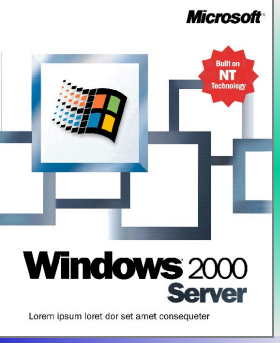


Шифрование файла



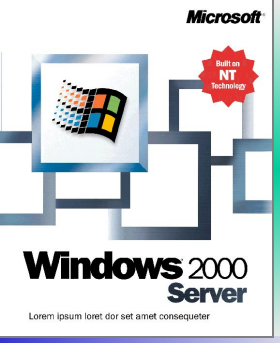
Расшифровка файла



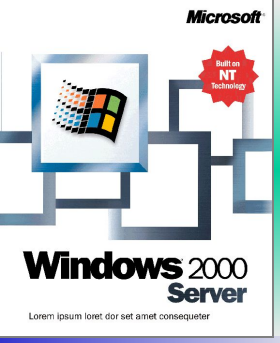


Особенности EFS

- ✔ **Работает только при наличии хотя бы одного агента восстановления**
- ✔ **Нельзя зашифровать**
  - Системные файлы
  - Сжатые файлы
- ✔ **За пределы области влияния EFS файл передается в открытом виде**
  - Локальная сеть
  - Другие носители и файловые системы
    - Исключение: Windows 2000 Backup

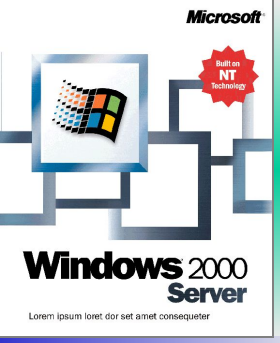


Защита коммуникаций



Secure Channel

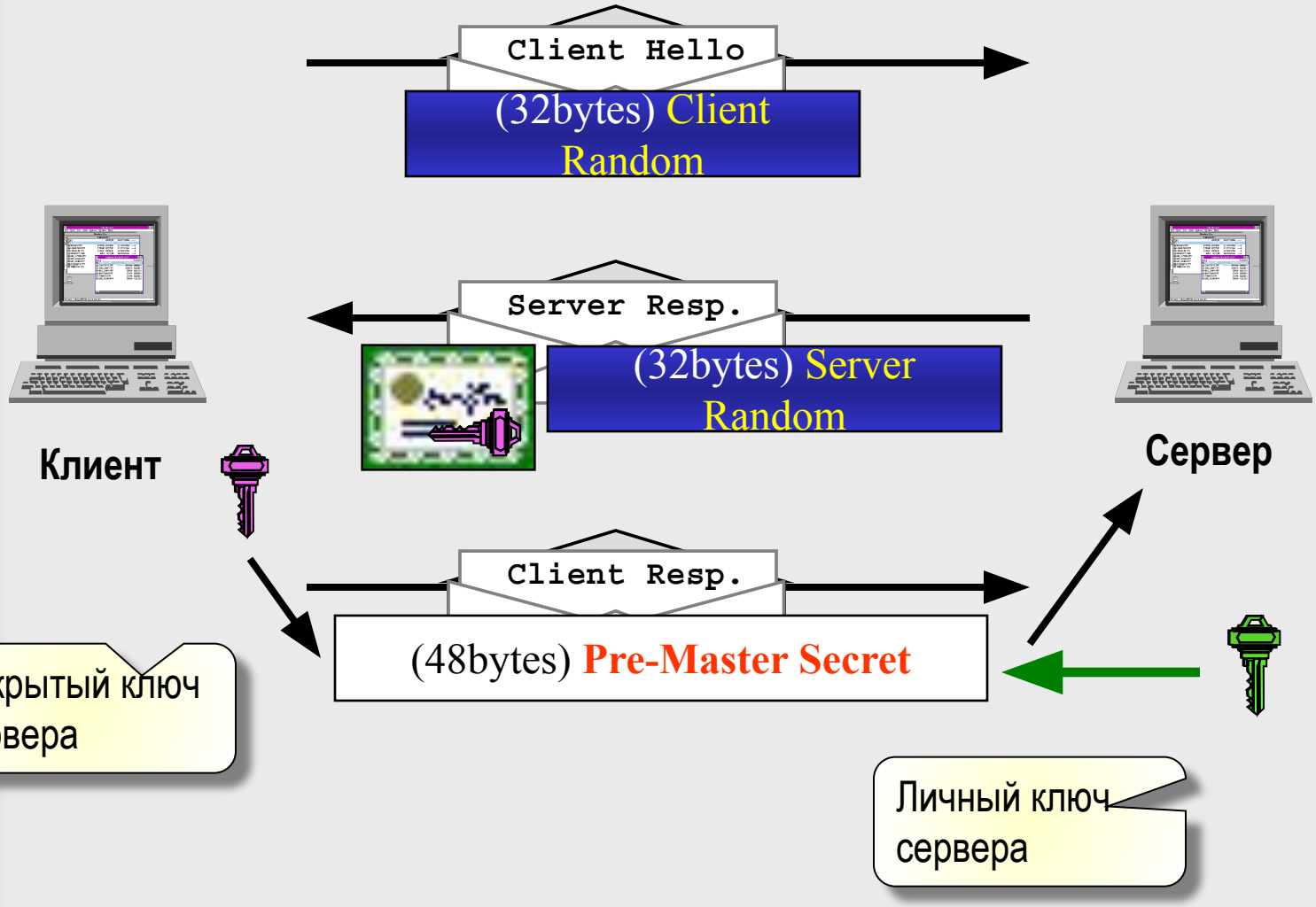
- **“Microsoft Unified Security Support Provider”**
  - Secure Sockets Layer (SSL) 3.0
  - SSL 2.0
  - Transport Layer Security (TLS) 1.0
  - Private Communication Technology (PCT) 1.0
- **Аутентификация и защита данных при связи через публичные сети**
- **TLS - основной (рекомендуемый) протокол**
  - Модернизация протокола SSL

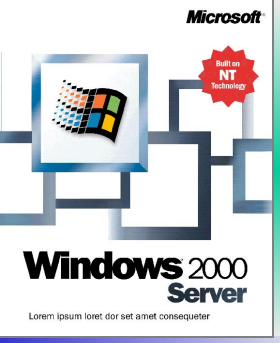


Концепции SSL/TLS

- **При установлении защищенного сеанса участники**
  - Договариваются, какие криптографические алгоритмы будут использоваться в рамках сеанса
    - RSA – при обмене ключами
    - RC4 – для шифрования данных
    - SHA и MD5 – для хеширования
  - Взаимно аутентифицируют друг друга с помощью сертификатов
  - Генерируют ключи для шифрования и хеширования

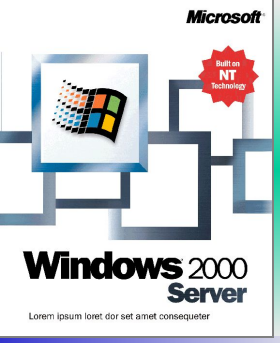
Алгоритм SSL/TLS





Применение SSL/TLS

- **Протоколы Secure Channel работают на уровне “Application” (OSI)**
  - Приложение должно явно поддерживать протоколы SSL/TLS
    - Internet Information Services
    - Internet Explorer
- **Windows 2000 обеспечивает полную функциональность**
  - Schannel SSP
  - Крипто-провайдеры
    - Microsoft RSA/Schannel CSP
    - Microsoft DSS and Diffie-Hellman/Schannel CSP

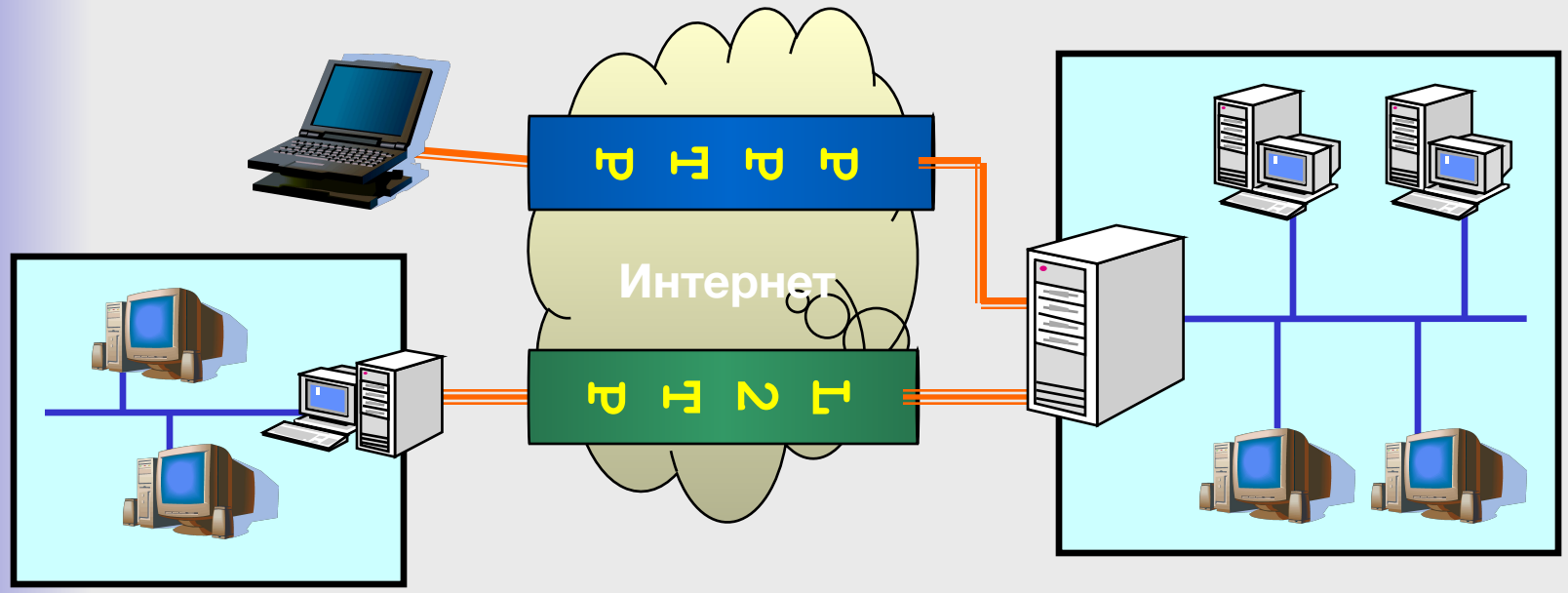


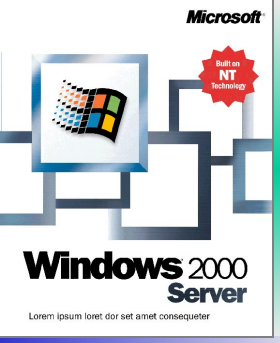
Remote Access Service

- **Защищенное подключение удаленного клиента по PPP**
- **Два уровня аутентификации**
  - Аутентификация PPP
    - PAP, SPAP
    - CHAP, MS-CHAP v1, MS-CHAP v2
    - EAP-TLS, EAP-MD5
  - Аутентификация в домене
- **Internet Authentication Service**
  - RADIUS
- **Шифрование**
  - Microsoft Point-to-Point Encryption (MPPE)

Виртуальные сети

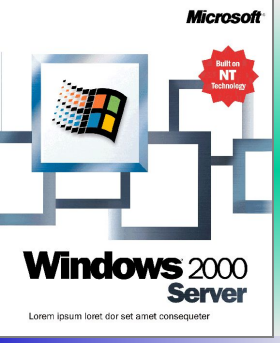
- **Защищенное подключение клиента к серверу удаленного доступа через виртуальный туннель, созданный в открытой сети**
  - Инкапсуляция и шифрование сетевых пакетов



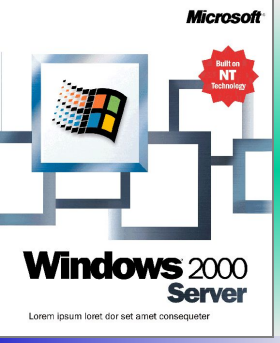


Туннельные протоколы

- **Point-to-Point Tunneling Protocol (PPTP)**
  - Generic Routing Encapsulation (GRE)
  - Шифрование
    - Модификация протокола MPPE
- **Layer 2 Tunneling Protocol (L2TP)**
  - Комбинация PPTP и L2F (CISCO)
  - IP Security
    - Аутентификация
    - Шифрование



IP Security (IPSec)

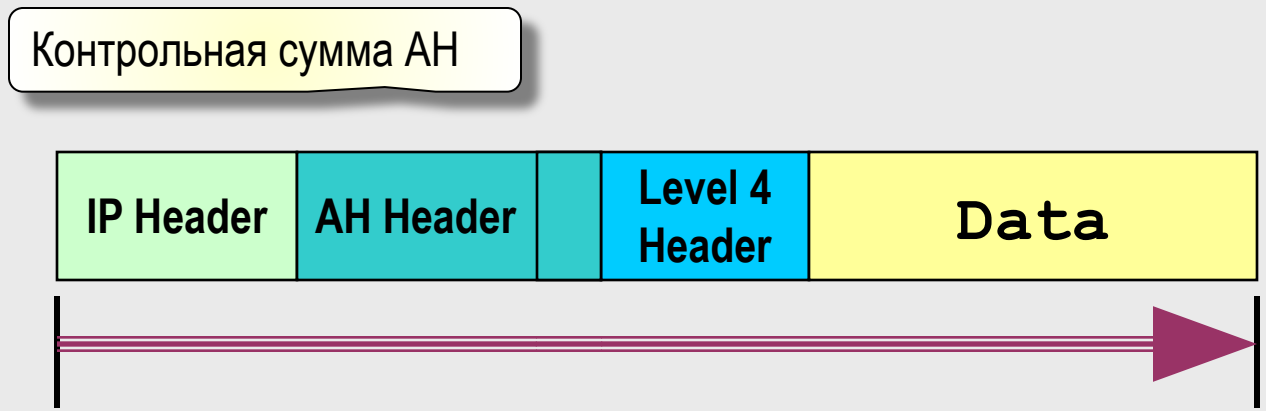


Концепции IPSec

- **Защита данных на уровне сетевых пакетов**
  - Прозрачно для приложений
- **Два уровня защиты**
  - Обеспечение целостности пакета
  - Шифрование данных, передаваемых в пакете
- **Возможность туннелирования**
  - Защищенный канал между маршрутизаторами удаленных подсетей

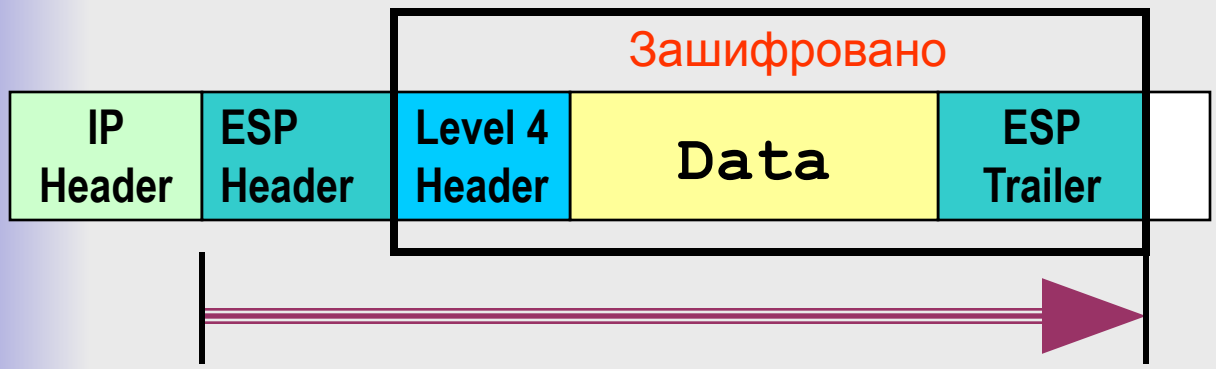
Протоколы IPSec

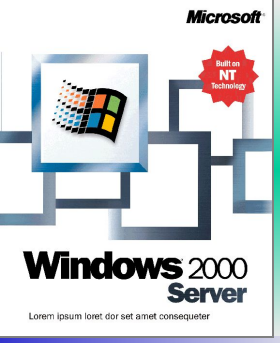
- **Authentication Header (AH)**
  - Подписывает неизменяемую часть заголовка и данные IP-пакета
    - HMAC MD5
    - HMAC SHA
  - Не производит шифрования данных



Протоколы IPSec

- **Encapsulating Security Payload (ESP)**
  - Зашифровывает весь пакет, за исключением заголовков IP и ESP
    - DES-CBC
    - Triple-DES
  - Подписывает зашифрованные данные вместе со своим заголовком

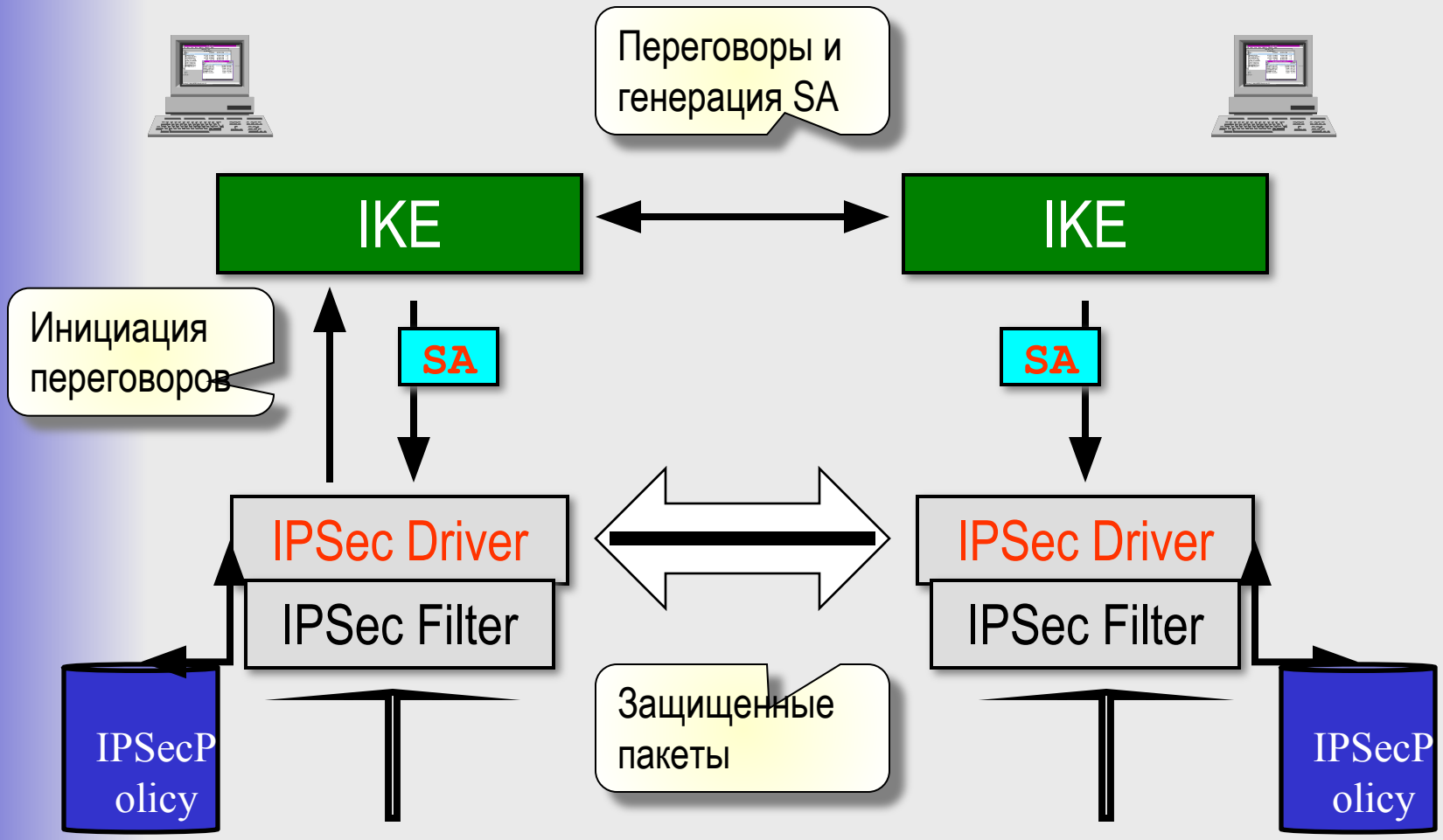


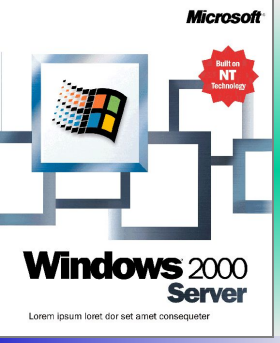


Компоненты IPSec

- **IPSec Driver**
  - Обрабатывает пакеты
- **IPSec Filter**
  - Указывает, какие пакеты и как нужно обрабатывать
- **IPSec Policy**
  - Определяет параметры IP Security для компьютеров
- **Internet Key Exchange (IKE)**
  - Организует переговоры между хостами
    - ISAKMP/Oakley

Процессы IPSec





Переговоры IKE

- **Фаза 1**
  - Предварительные переговоры
  - Взаимная аутентификация машин
    - Kerberos (в рамках домена/леса)
    - Сертификаты
    - Заданный ключ (для тестовых задач)
- **Фаза 2**
  - Создание Security Associations
    - SA = {алгоритм, ключ}
    - Для каждого протокола -собственная пара SA
      - SA1 – для исходящих пакетов
      - SA2 – для входящих пакетов


Microsoft
Built on NT Technology
Windows 2000 Server
Lorem ipsum loret dor set amet consequeter
Ответы
Вопросы?