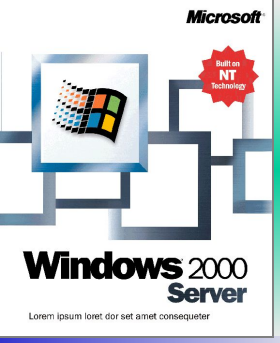
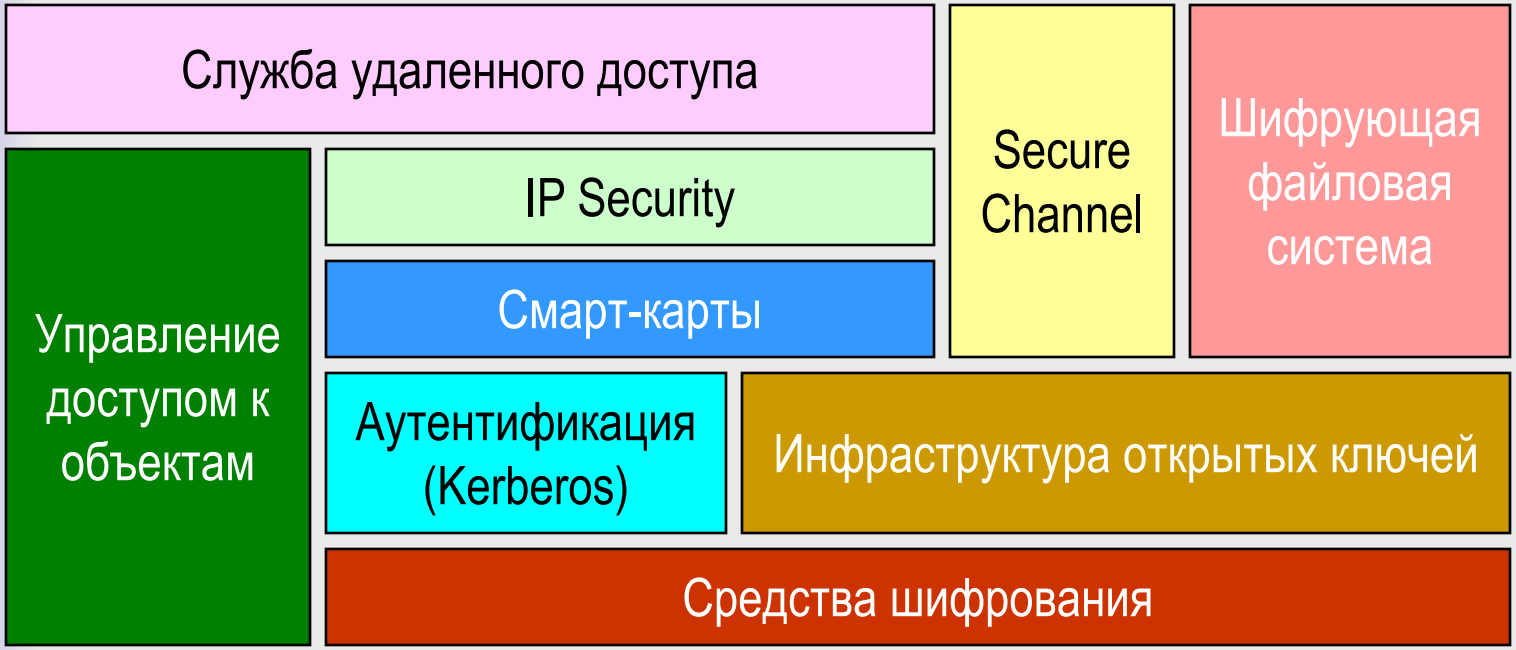
Концепции обеспечения безопасности в Microsoft Windows 2000

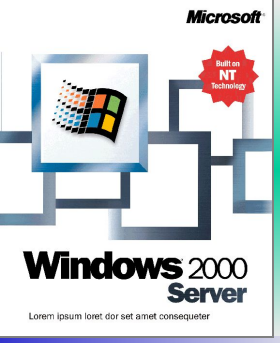
Главные задачи

- Аутентификация пользователей
- Авторизация доступа к ресурсам
- Конфиденциальность информации
- Целостность информации
- Невозможность отказа от совершенных действий

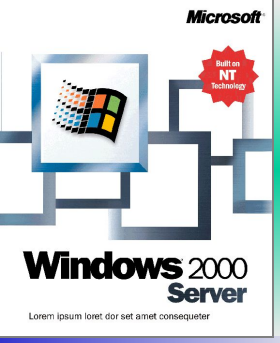


Компоненты системы безопасности Windows 2000



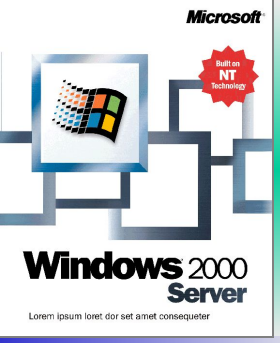


Службы аутентификации



Общие принципы

- 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



Архитектура

Приложение

Winlogon

GINA

LSA

SSPI

Negotiate

NTLM SSP

Schannel SSP

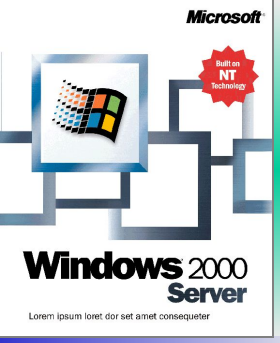
Kerberos SSP

Third-party SSP

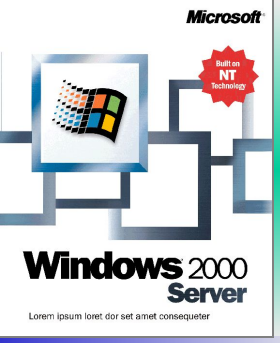
MSV1_0 SSP

Kerberos package

Third-party package

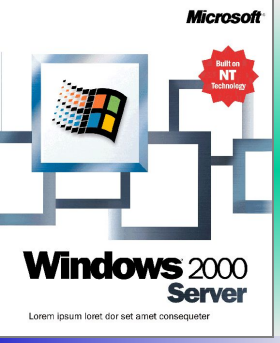


Контроль доступа



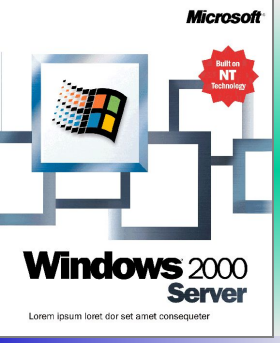
Субъект

- 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



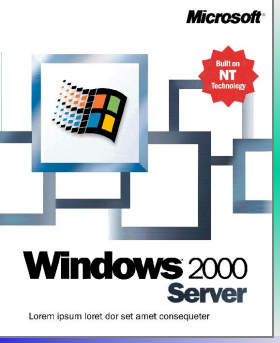
Маркер доступа

- 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



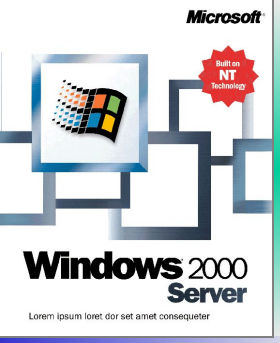
Объект

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



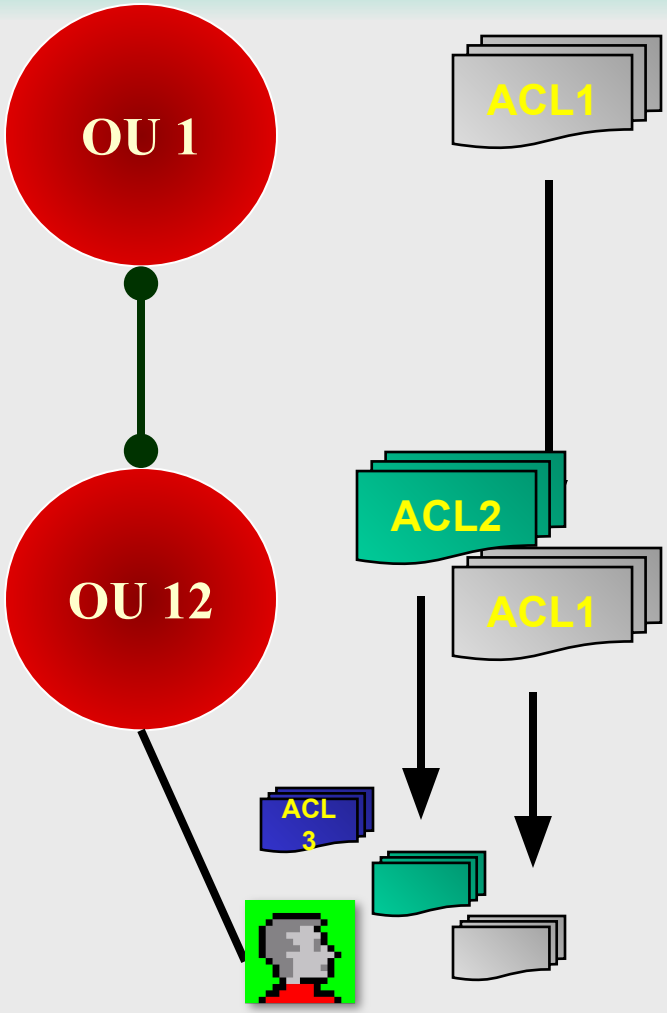
Дескриптор безопасности объекта

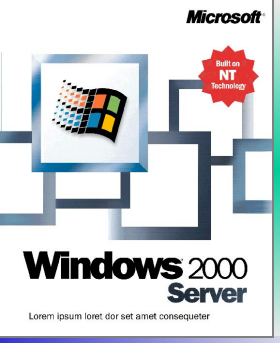
- Discretionary Access Control List, DACL
  - Список запретов и разрешений, установленных для данного объекта
- System Access Control List, SACL
  - Список назначений аудита
- Access Control Entry, ACE
  - Каждая ACE содержит назначение прав для конкретного SID
  - ACL объекта Active Directory может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



Наследование

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





Проверка прав

READ
WRITE

Явные назначения

SID 278	_WX	Deny
SID 278	R__	Allow
SID 141	R_X	Allow
SID 39	R_X	Deny
SID 199	_W_	Deny
SID 65	RW_	Allow

SID 65

SID 141

SID 172

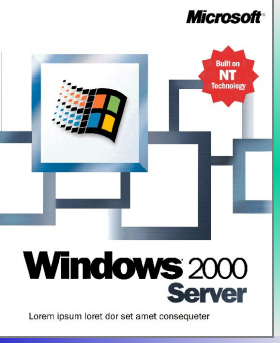
SID 199

Access Denied

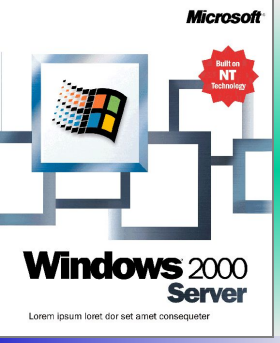
Пользователь

Объект

Унаследованные строки

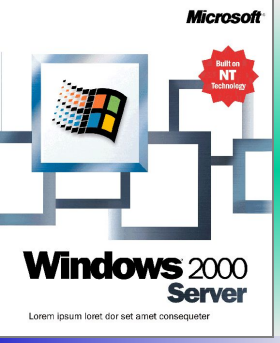


Средства шифрования

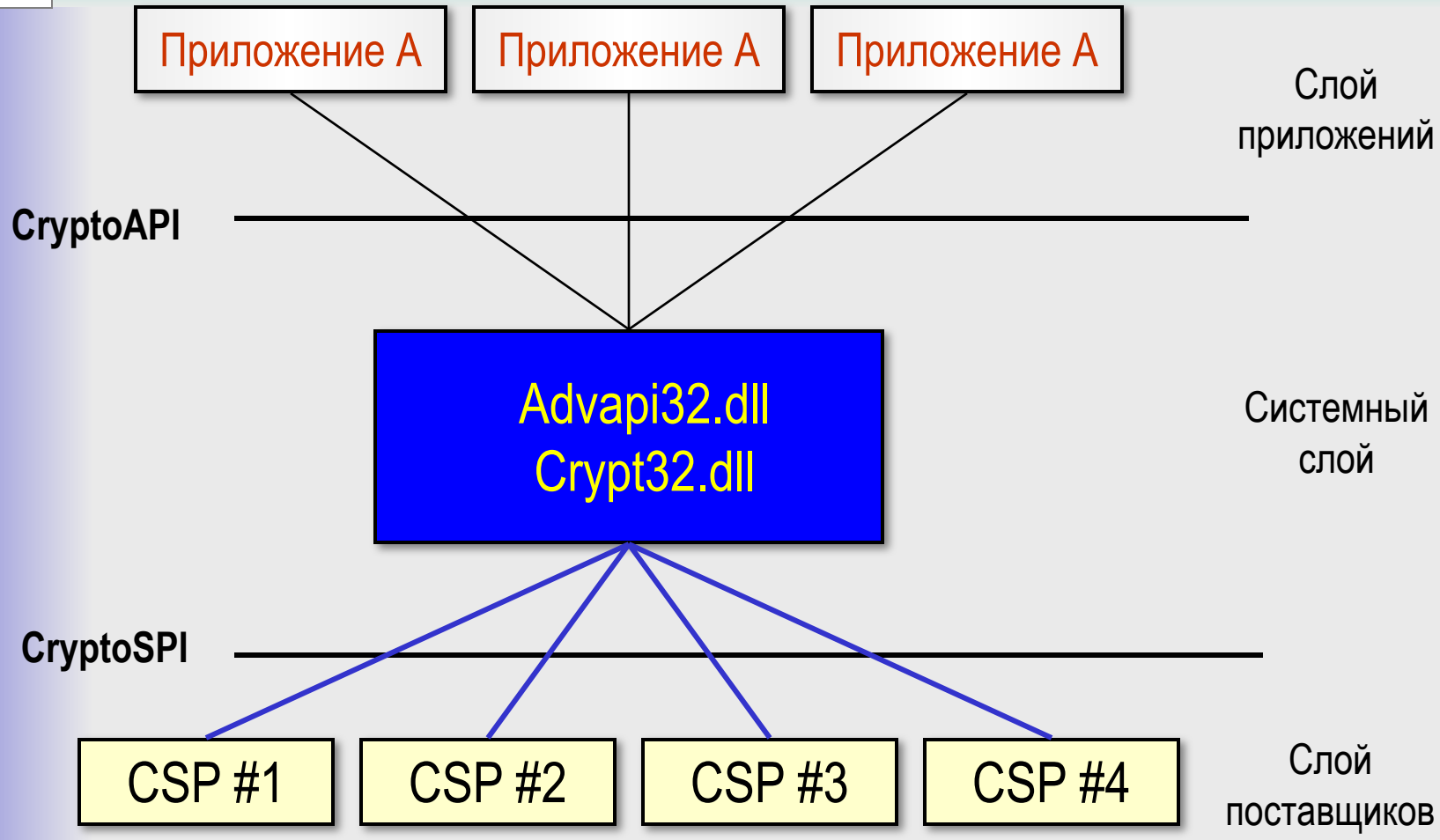


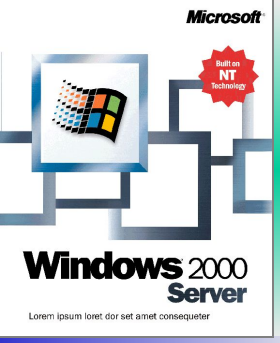
CSP и CryptoAPI

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



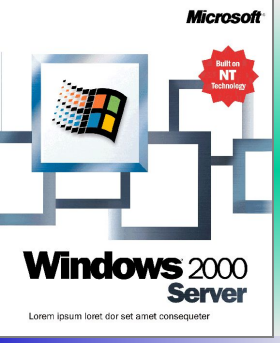
CSP и CryptoAPI





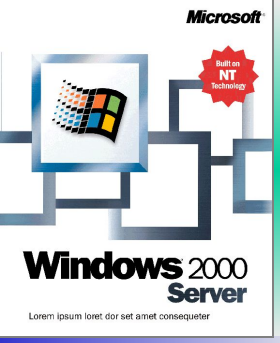
Встроенные CSP

- Стандартные криптопровайдеры
  - Microsoft Base CSP
  - Microsoft DSS CSP
  - Microsoft DSS and Diffie-Hellman CSP
  - Microsoft DSS and Diffie-Hellman/Schannel CSP
  - Microsoft RSA/Schannel CSP
  - Schlumberger CSP
  - GemPlus CSP
- High Encryption Pack
  - Microsoft Strong CSP
  - Microsoft Enhanced CSP



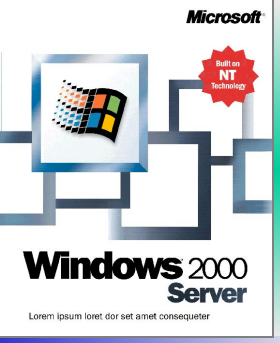
Алгоритмы

- Симметричное шифрование
  - Data Encryption Standard (DES)
    - DES: 56 бит
    - DESX: 128 бит
    - Triple DES: 112 бит, 168 бит
  - Rivest’s Cipher (RC)
    - RC2, RC4: 40 бит, 56 бит, 128 бит
- Обмен ключами
  - Diffie-Hellman Key Agreement
  - RSA Key Exchange



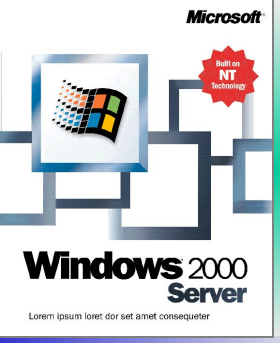
Алгоритмы

- Хеширование
  - Message Digest (MD)
    - MD2, MD4, MD5
  - Secure Hash Algorithm (SHA-1)
  - Hashed Message Authentication Code (HMAC)
- Цифровая подпись
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature

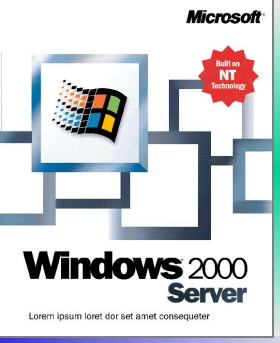


Разработка CSP

- Создание и тестирование модуля CSP с помощью *Microsoft Cryptographic Service Provider Developer's Kit (CryptoSDK)*
  - http://msdn.microsoft.com/downloads/
    - Раздел "Security"
- Цифровая подпись Microsoft
  - Модуль с описанием нужно передать Microsoft
  - Процесс подписи занимает 1 – 2 рабочих дня

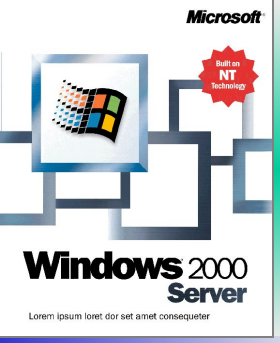


Инфраструктура открытых ключей



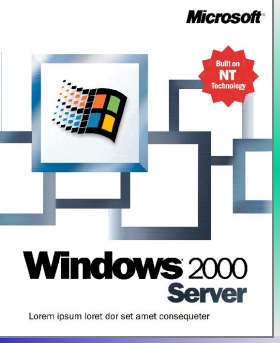
Сертификат

- 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



Архитектура CA

Protected Store

Личные ключи

Открытые ключи

CSP

Запросы PKCS10

Entry Module

Certificate Services

Exit Module

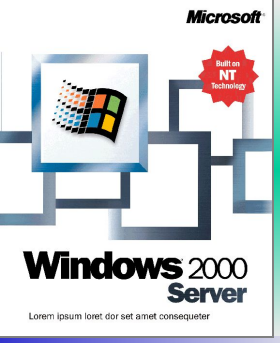
Сертификаты

CRL

Certificate Templates

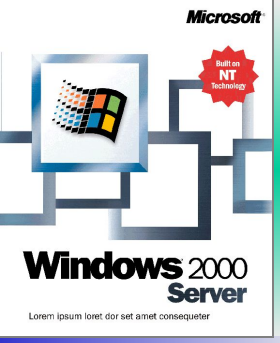
Policy Module

Certificate Database



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

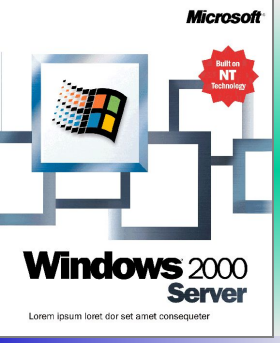
Sub CA 3

Issuing CA

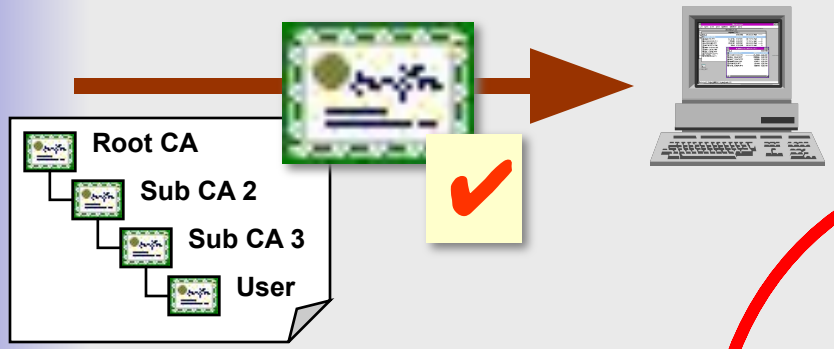
Issuing CA

Root CA
Sub CA 2
Sub CA 3
User

Certification Path



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

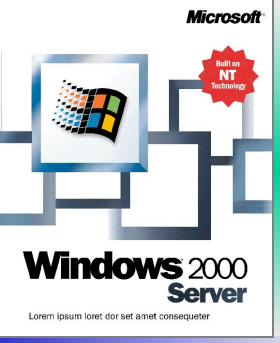
Сертификат не был отозван.

Запреты

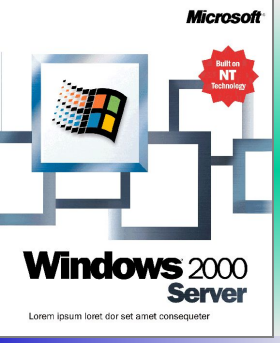
Списки CTL не запрещают использование сертификата для данной задачи.

Доверие

Сертификат корневого CA присутствует в хранилище Trusted Root Certification Authorities.

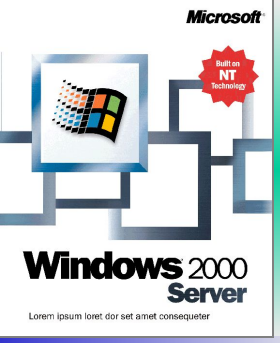


Службы, базирующиеся на Windows 2000 PKI



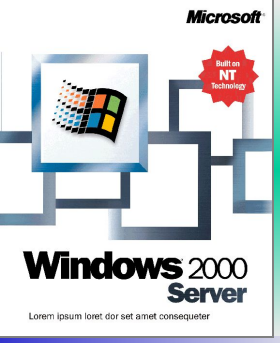
Secure Channel

- “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



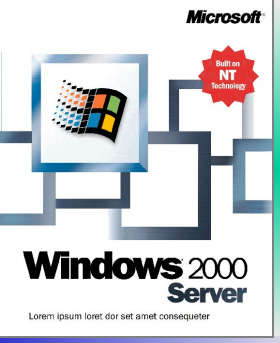
Концепции SSL/TLS

- 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
  - Вырабатывают ключи для шифрования и хеширования



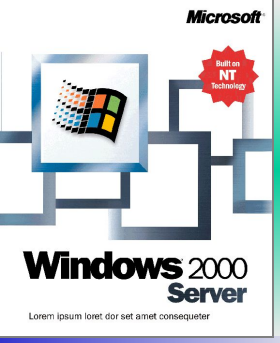
Смарт-карты

- Микрочип, интегрированный в пластиковую карточку
  - Сертификат пользователя
  - Личный ключ пользователя
- Идентификация владельца
  - Персональный идентификационный номер (PIN)
- Поддержка Smart Cards в Windows 2000
  - Gemplus
  - Schlumberger



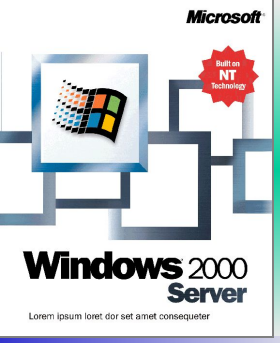
Аутентификация

- Сертификат вместо пароля
  - Надежность аутентификации Kerberos зависит от качества паролей
- PKINIT
  - Расширение Kerberos для интерактивной аутентификации с помощью Smart Card
- Соответствие сертификата учетной записи домена
  - SSL/TLS, EAP-TLS
  - Возможна аутентификация пользователей, не имеющих учетных записей в домене

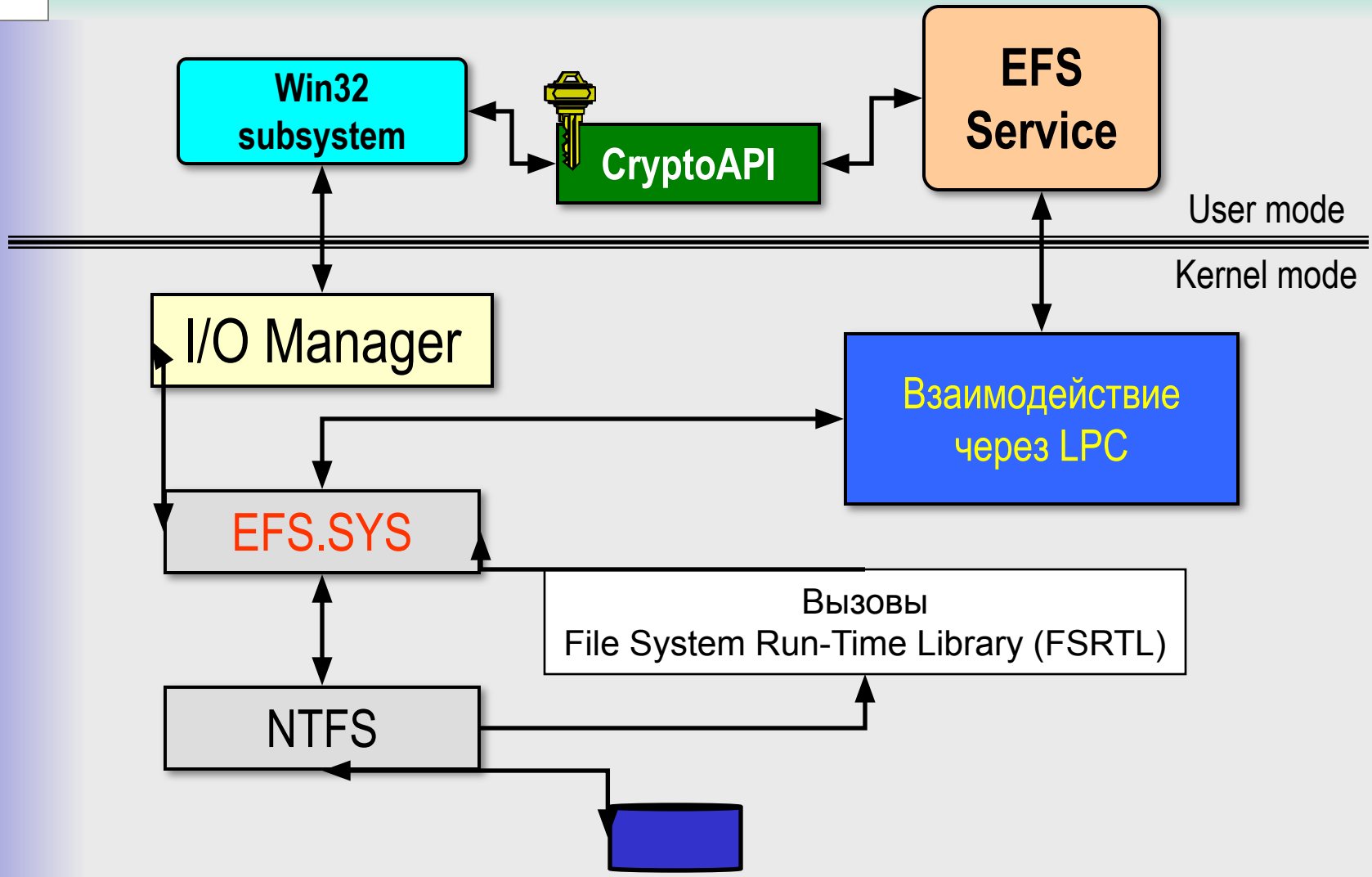


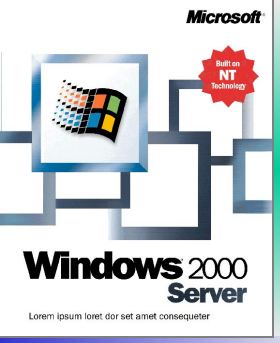
Шифрующая файловая система (EFS)

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



Архитектура EFS

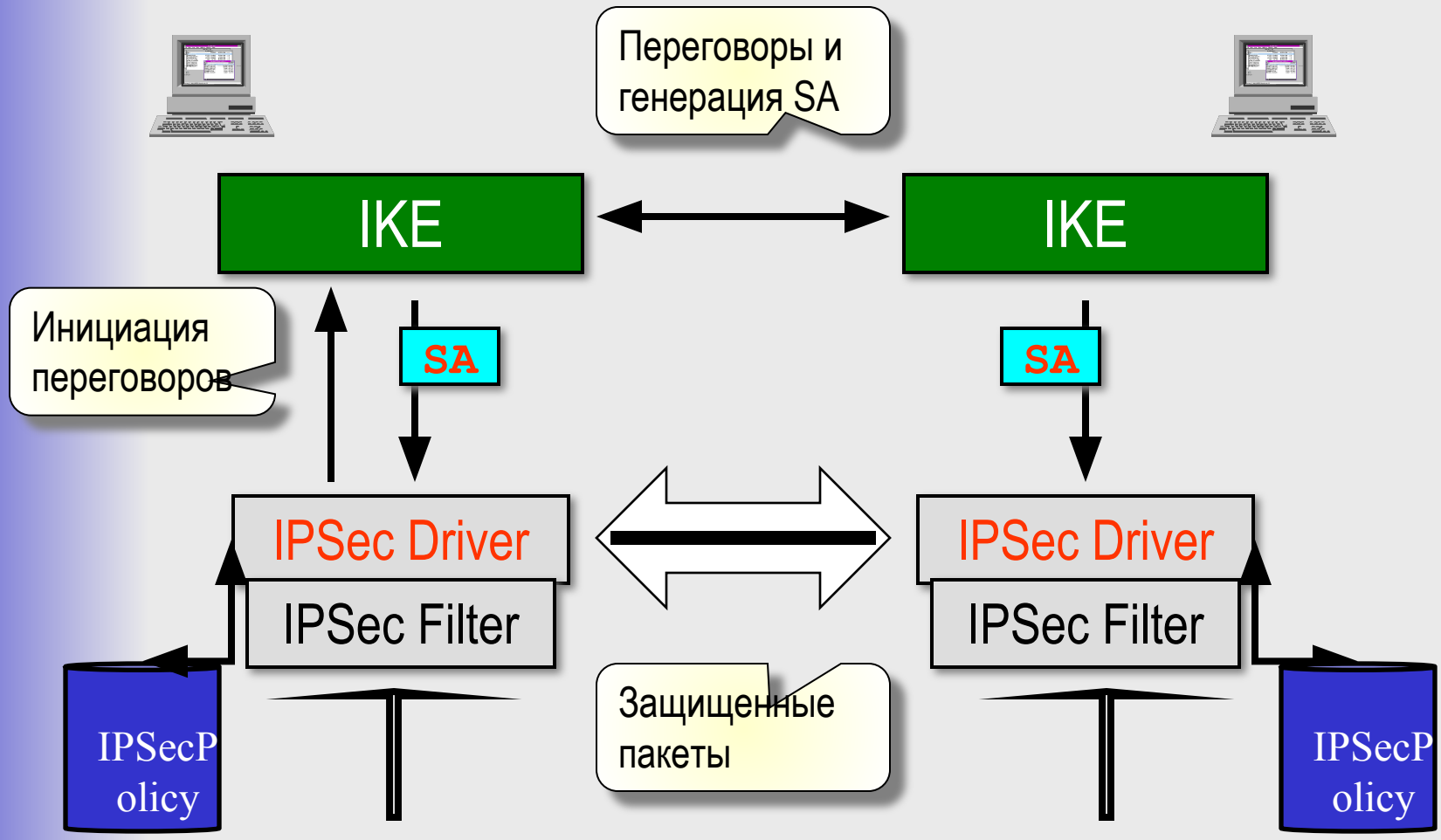




Безопасность IP (IPSec)

- Защита данных на уровне сетевых пакетов
  - Прозрачно для приложений
- Два уровня защиты
  - Обеспечение целостности пакета
    - Authentication Header (AH)
  - Шифрование данных, передаваемых в пакете
    - Encapsulating Security Payload (ESP)
- Возможность туннелирования
  - Защищенный канал между маршрутизаторами удаленных подсетей

Процессы IPSec



Система безопасности Windows 2000

- Защита на всех уровнях
  - Аутентификация
  - Контроль доступа к ресурсам
  - Конфиденциальность данных в хранилище
  - Конфиденциальность и целостность коммуникаций
- Модульность и возможность расширения
  - Подключение модулей шифрования CSP
  - Собственные механизмы аутентификации

Ответы

Вопросы?