

Администрирование локальных сетей

Лекция 9

Построение инфраструктуры открытых ключей (PKI)

Обзор лекции

- Описание элементов и функций инфраструктуры открытых ключей (PKI).
- Функции сертификаты и сертификации (ЦС).
- Структура иерархии СА.
- Список различий между центрами сертификации предприятия и автономным ЦС.
- Установка и настройка центра сертификации.
- Описание процесса выдачи сертификатов.
- Публикация списков отзыва сертификатов.

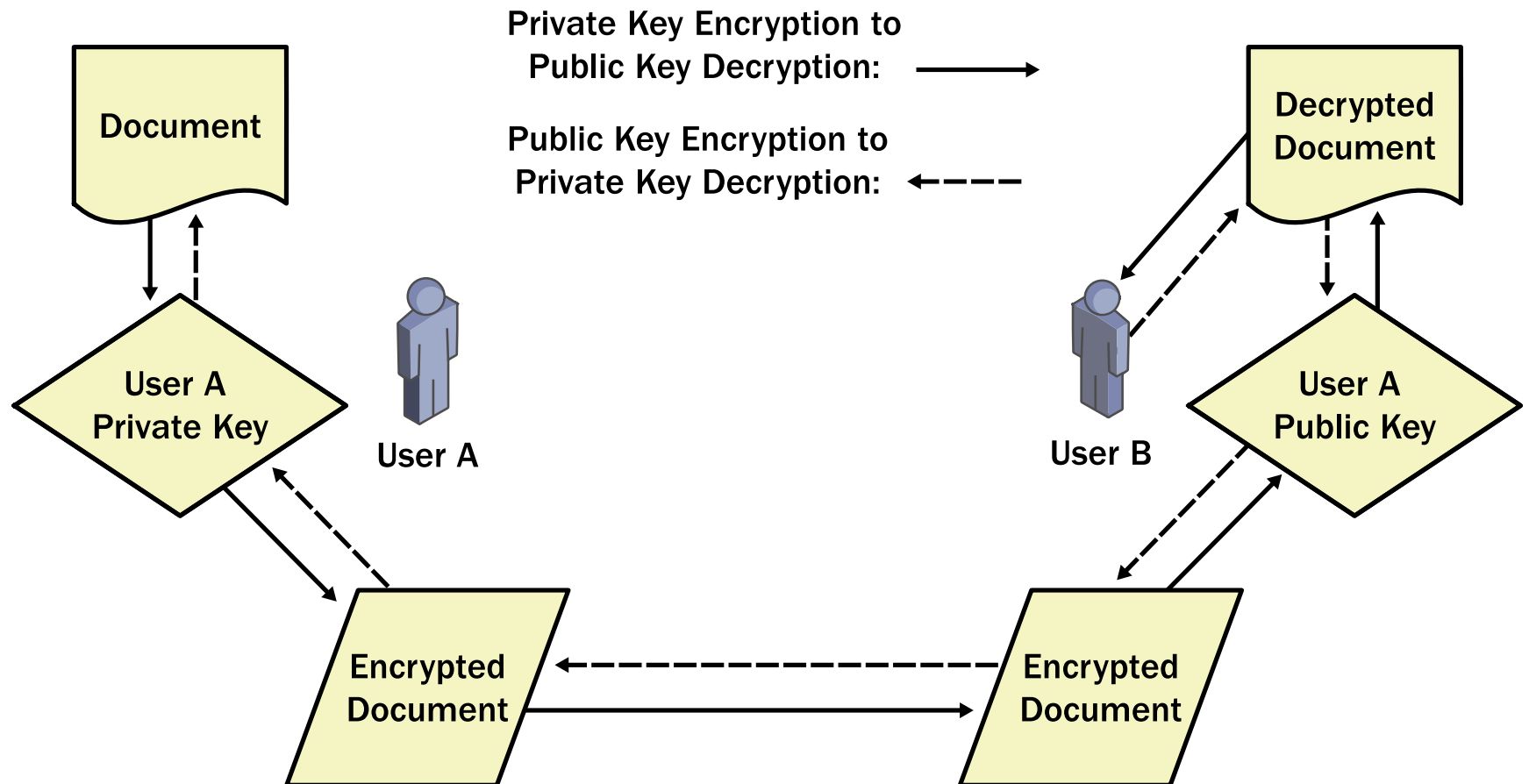
Введение в инфраструктуру открытых ключей

- **Инфраструктура открытых ключей (PKI)** представляет собой набор программных компонентов и политик в области распределения и использования государственных и частных ключей на основе использования цифровых сертификатов.

Шифрование на основе криптографических ключей

- Шифрование представляет собой систему, в которой один символ (набор символов) заменяется другим.
- Шифрование в сети передачи данных обычно используется метод шифрования с открытым ключом.
- В шифрование с открытым ключом, каждый пользователь имеет два ключа – **открытый** ключ и **закрытый** ключ.
- Данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы с помощью закрытого ключа, и наоборот.

Шифрование данных



Цифровая подпись

- Цифровая подпись относится к процессу шифрования с помощью закрытого ключа для всех или части данных.
- Цифровая подпись данных, зашифрованных с вашего секретного ключа, могут быть расшифрованы только с вашим открытым ключом.
- Цифровая подпись предотвращает другим пользователям выдавать себя за вас, посылая данные от вашего имени.

Проверка данных

- **Хэш-значения**, или контрольные суммы, используются, чтобы гарантировать, что данные не были изменены, с момента как контрольная сумма была создана.
- Принимающая система проверяет контрольную сумму, чтобы определить, действительно ли данные не были изменены.

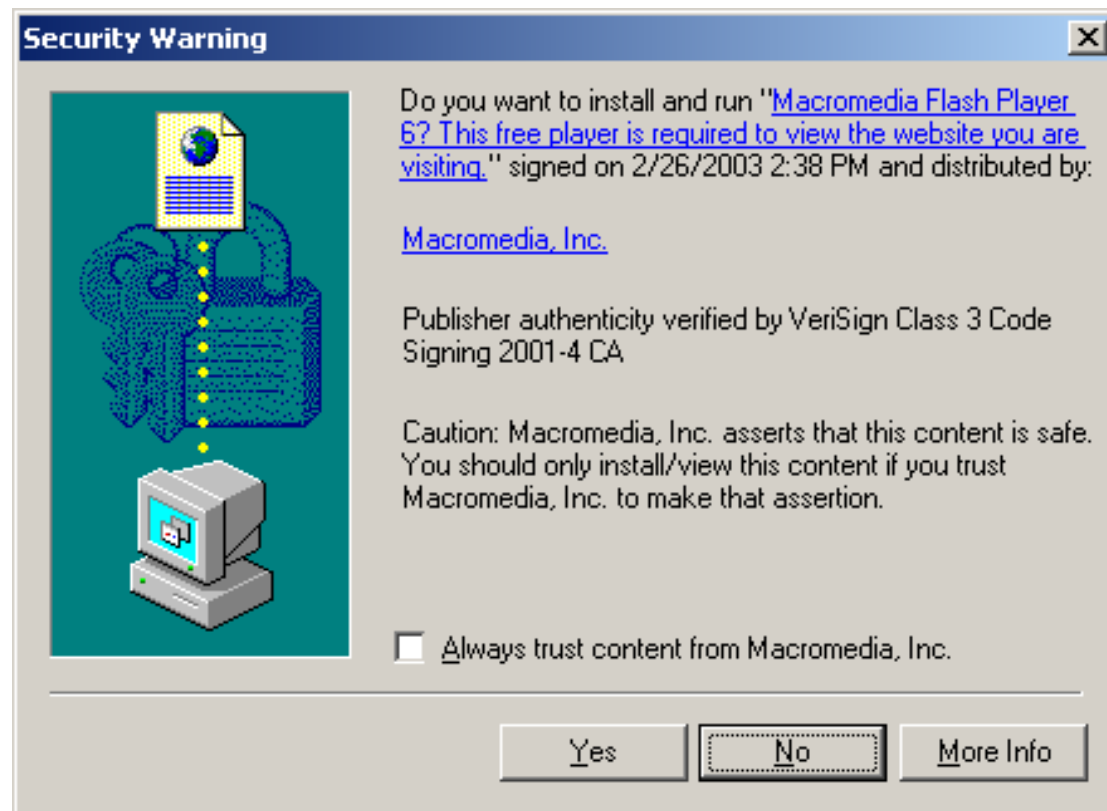
Применение цифровых сертификатов

- **Цифровые сертификаты** являются документами, которые позволяют проверить связь открытого ключа с определенным человеком или организацией.
- Сертификаты передаются из административных сущности, называемой **центром сертификации (ЦС)**.
- ЦС выпускает открытый ключ и закрытый ключ в качестве согласованной пары.
 - Секретный ключ хранится на компьютере пользователя, а открытый ключ выдается как часть сертификата.

Содержимое сертификатов

- Цифровые сертификаты содержат открытый ключ для конкретного лица, а также информации о сущности.
- Почти все сертификаты соответствуют ITU-T стандарту X.509: «The Directory: Public-Key and Attribute Certificate Frameworks».
- Стандартизация формата сертификата имеет существенное значение, в противном случае обмен сертификатов и ключей будет затруднен.

Загрузка сертификатов из Интернет



Использование внутренних и внешних ЦС

- Чтобы сертификат мог быть использован, он должен быть выдан полномочным центром, и обе стороны доверяли проверку идентичности друг друга.
- В организации можно использовать Windows Server Certificate Services – служба, которая позволяет компьютеру функционировать как ЦС.
- При общении с внешними организациями, может быть использован сертификат, выданный третьей доверенной стороной.

Назначение PKI

- Использование PKI обеспечивает дополнительную безопасность в сети Windows Server.
- Используя инструменты управления, администраторы могут публиковать, использовать, обновлять и отзываться сертификаты. Они также могут перечислить клиентов в PKI.
- Пользователи могут использовать сертификаты для обеспечения дополнительной безопасности.

Проектирование инфраструктуры открытых сетей

- Планирование PKI включает следующие основные этапы:
 - Определение назначения сертификатов
 - Создание инфраструктуры ЦС
 - Настройка сертификатов

Определение назначения сертификатов

При проектировании PKI необходимо определить потребности клиентов в безопасности обмена данных и как сертификаты могут помочь обеспечить безопасность.

Необходимо определить, какие пользователи, компьютеры, услуги и приложения будут использовать сертификаты, и какие сертификаты будут необходимы.

Практика подсказывает, что создается небольшой набор определений безопасности, а затем применяются к пользователям и компьютерам по мере необходимости.

Создание инфраструктуры ЦС

Планирование создания системы сертификации требует понимания иерархии ЦС.

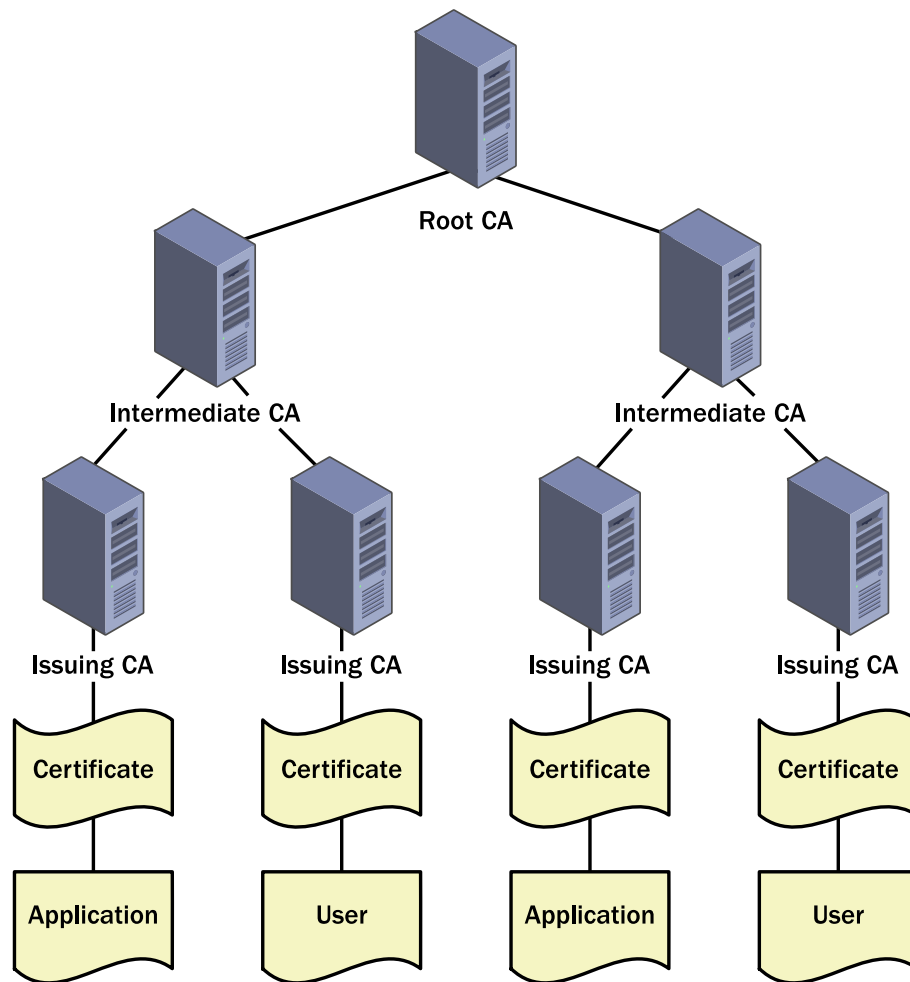
Иерархия СА относится к структуре, в которой каждый центр сертификации подтвержден ЦС на более высоком уровне.

Корневой ЦС считается главным уполномоченным центром для организации.

Количество ЦС

- Один ЦС на основе Windows Server 2003 поддерживает до 35 миллионов сертификатов и может издать два миллиона или более в день, в зависимости от спецификации системы.
- Производительность системы является фактором, определяющим количество ЦС в организации.
- Для процесса выдачи сертификатов ЦС определяющими являются диск и процессор.
- Несколько ЦС могут быть реализованы для обеспечения отказоустойчивости или распределения нагрузки.

Иерархия ЦС



Типы Центров сертификации в Windows Server

Центры сертификации предприятия:

- Интегрированы в Active Directory
- Могут использовать только клиенты каталога

Автономные центры сертификации:

- Не отвечают автоматически на запросы сертификатов
- Предназначен для пользователей за пределами предприятия, которые могут подавать заявки на сертификаты

Настройка сертификатов

Критерии при настройке сертификатов:

- Тип сертификата
- Длина ключа и алгоритм шифрования
- Время жизни сертификата
- Политики обновления

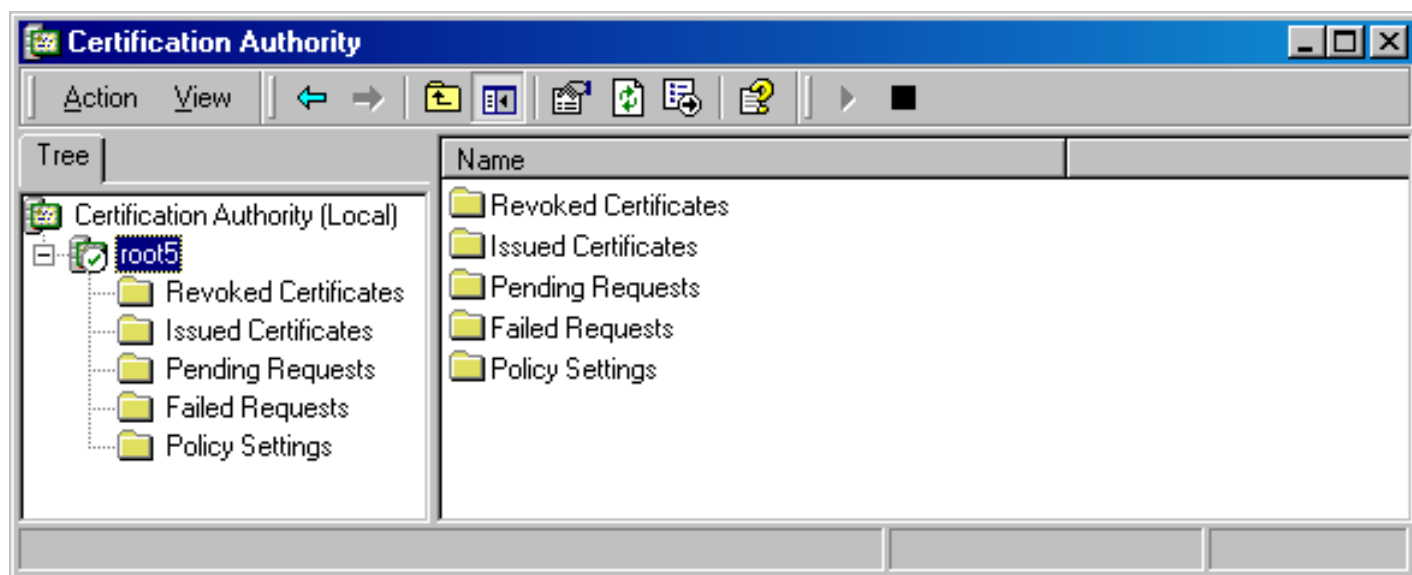
Использование шаблонов сертификатов

- Шаблоны сертификатов определяют, какие атрибуты доступны или необходимые для данного вида сертификатов.
- Windows Server включает в себя большое число Шаблонов сертификатов, предназначенных для большинства требований к сертификатам.

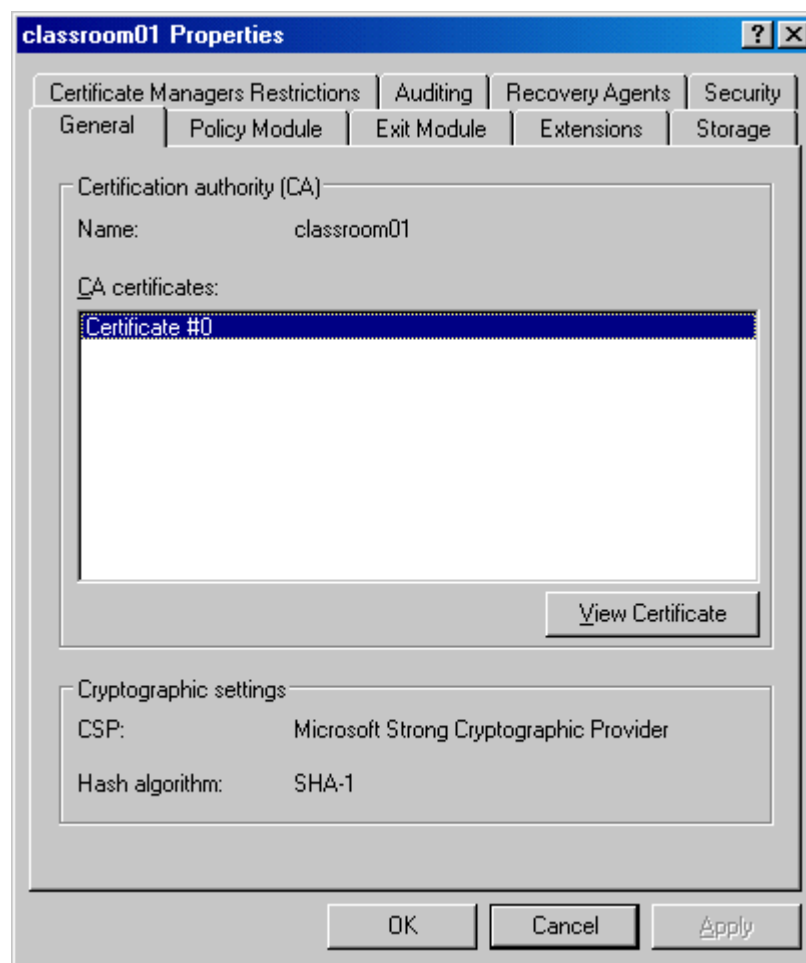
Защита ЦС

- ЦС является критически важным сетевым сервисом.
- Защитные меры и планы должны включать:
 - Физическую защиту
 - Управление ключами
 - План восстановления

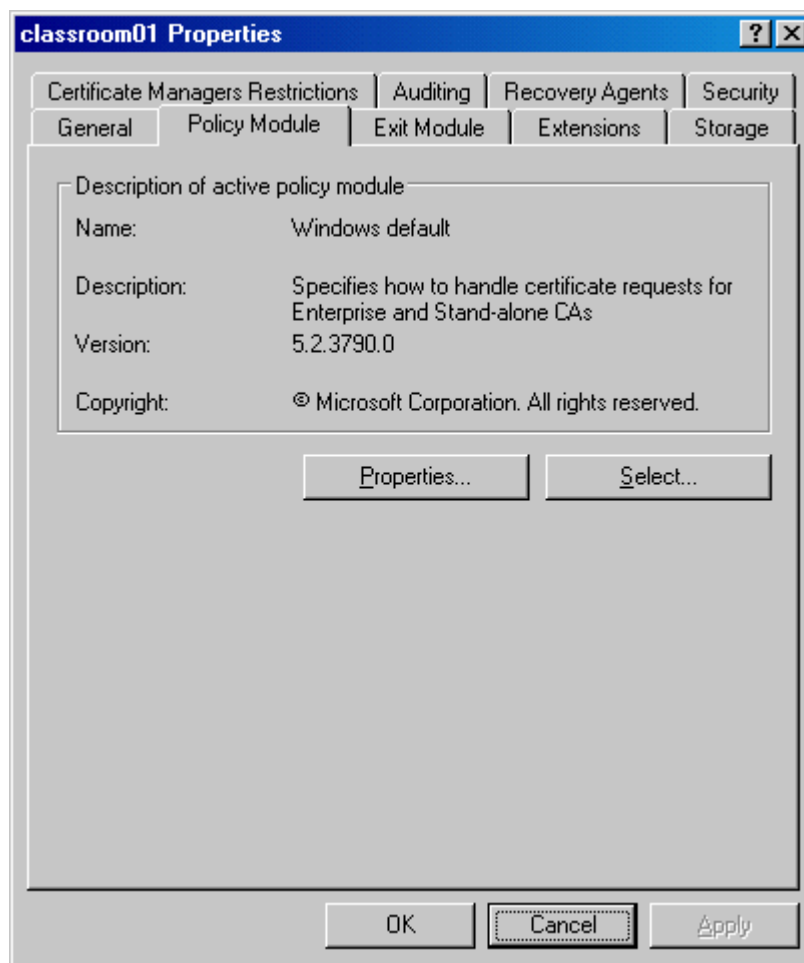
Конфигурирование ЦС



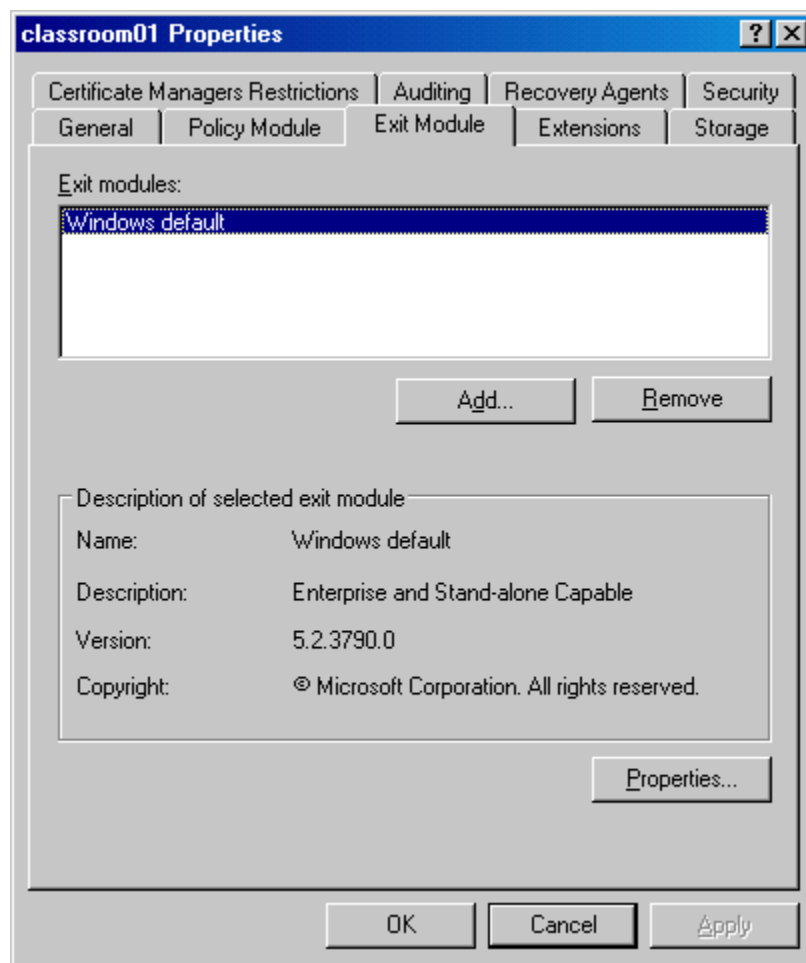
Вкладка Основное



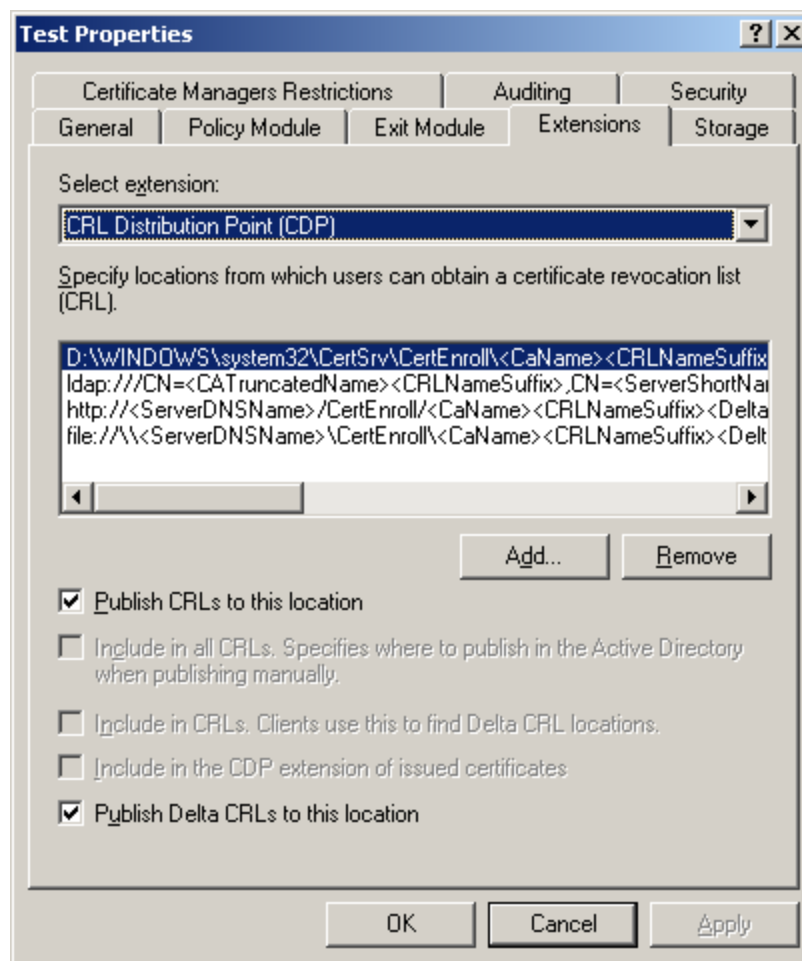
Вкладка Модуль политик



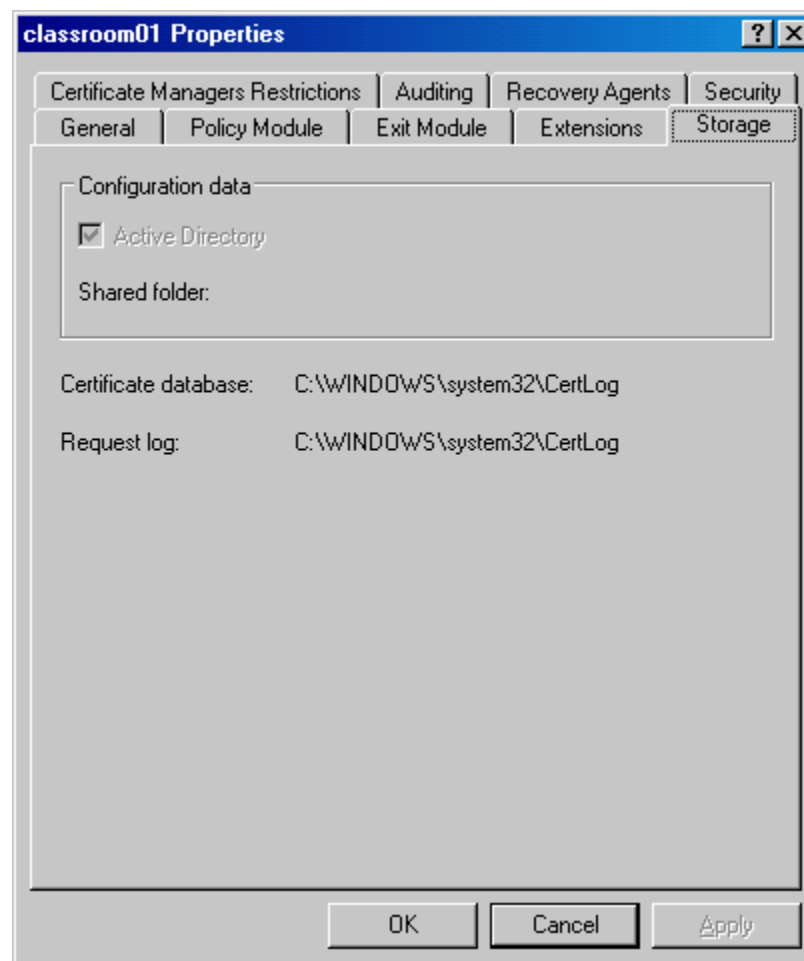
Вкладка Модуль выхода



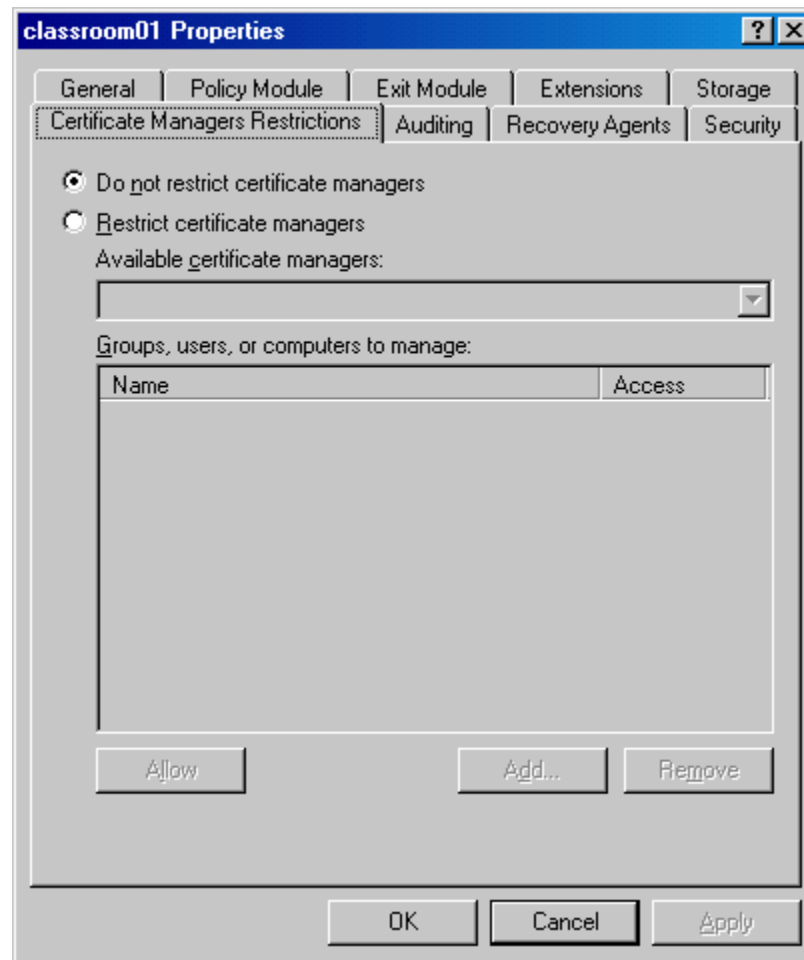
Расширения



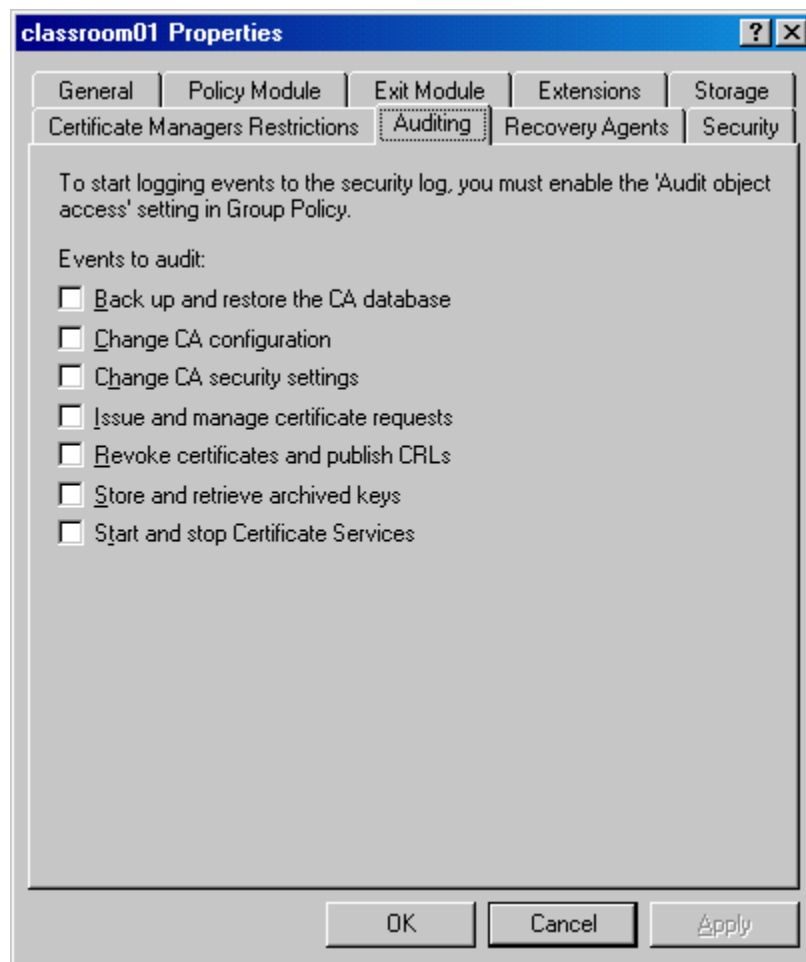
Вкладка Хранилище



Вкладка Ограничения Диспетчера сертификата



Вкладка Аудит



Вкладка Агент восстановления

The screenshot shows the 'classroom01 Properties' dialog box with the 'Recovery Agents' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are two rows of tabs: 'General', 'Policy Module', 'Exit Module', 'Extensions', 'Storage' in the first row, and 'Certificate Managers Restrictions', 'Auditing', 'Recovery Agents', 'Security' in the second row. The 'Recovery Agents' tab is active and contains the following content:

Do the following when a certificate request includes key archival:

- ☒ Do not archive the key
- ☐ Archive the key

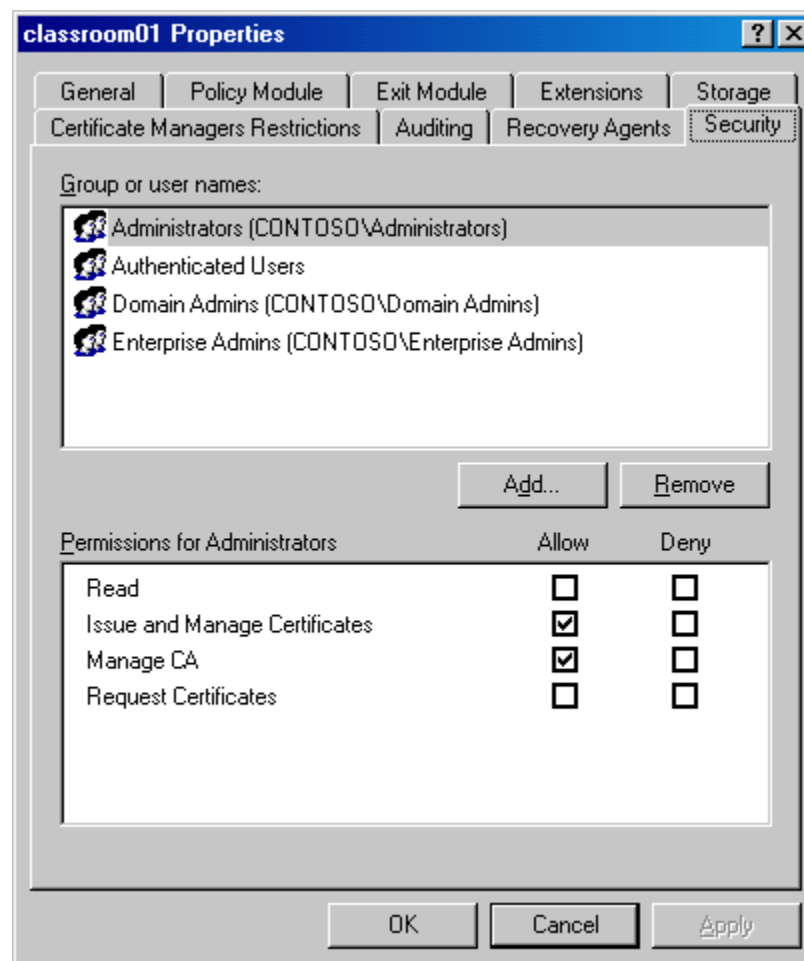
Number of recovery agents to use:

Key recovery agent certificates:

Subject	Issuer	Expiration Date	Status
---------	--------	-----------------	--------

At the bottom of the tab are three buttons: 'Add...', 'Remove', and 'View'. At the bottom of the entire dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Вкладка Безопасность



Резервное копирование и восстановление ЦС

- База данных службы сертификатов всегда открыта, что делает его трудным для резервного копирования.
- Специальное программное обеспечение может использоваться для резервного копирования файлов или консоль центра сертификации может обеспечить функцию резервного копирования.
- Функция резервного копирования ЦС из консоли центра сертификации вызывает мгновенное закрытие базы данных службы сертификации, и создание копию базы данных ЦС.

Выдача и обновление цифровых сертификатов

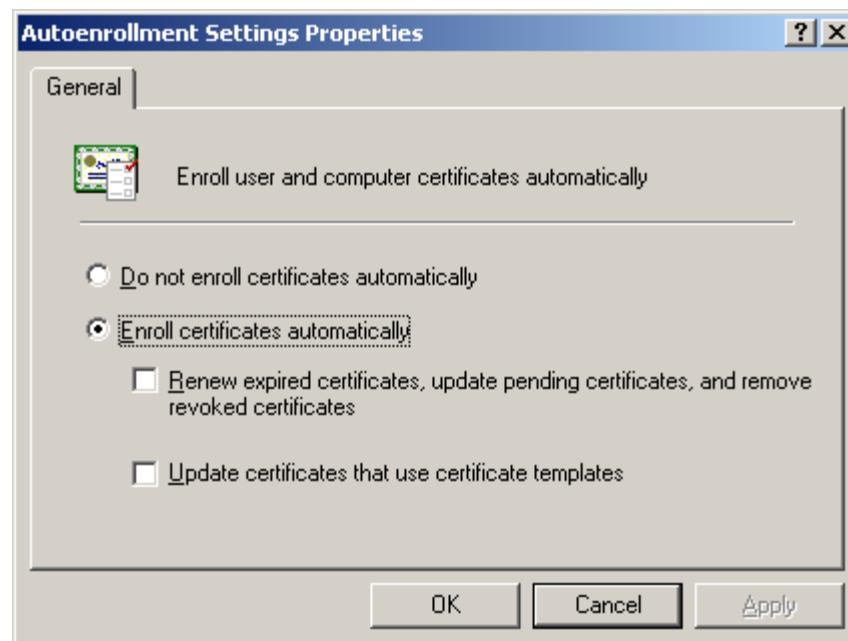
Автоматическая регистрация:

- ЦС определяет, действителен или нет Запроса на сертификат и, соответственно, выдает или отрицает сертификатов.

Ручная выдача:

- Администратор ЦС отслеживает входящие запросы и определяет, должен ли сертификат быть выдан по запросу.

Использование Автоматической выдачи



Использование Ручной выдачи

- При использовании автономных центров сертификации, администратор должен разрешить или запретить запросы на сертификаты.
- Входящие запросы заявки на сертификат появляется в папке **Запросы в ожидании**.
- Администратор должен проверять папку на регулярной основе.

Использование оснастки Сертификаты

