Лабораторная работа №5

Цель работы:

- создание мостового удостоверяющего центра для построения «ограниченных» доверительных отношений между различными доменами доверия;
- ознакомление с технологиями построения и проверки путей сертификации и их реализацией в ОС Microsoft Windows 2003 Server и XP.

Легенда

Для выполнения совместных исследований в области математических методов криптологии возникла необходимость организовать защищенный обмен сообщениями электронной почты между Московским государственным университетом (МГУ) и Московским инженерно-физическим институтом (МИФИ). При этом в обоих научно-образовательных учреждениях уже развернуты инфраструктуры открытых ключей, использующиеся, в том числе, для защиты обмена сообщениями электронной почты и функционирующие в соответствии с определенным набором политик.

Задача, таким образом, заключается в организации доверительных отношений между двумя доменами, включая согласование политик, действующих в различных доменах. Кроме того, было принято решение не устанавливать доверительные отношения только между доменами МГУ и МИФИ, а создать специализированный мостовой удостоверяющий центр, который впоследствии мог бы использоваться для организации доверительных отношений с другими образовательными учреждениями.

1 Введение

2 Описание лабораторного стенда

Для выполнения лабораторной работы используются 3 виртуальные машины, запускаемые на одной физической машине и работающие в режиме Host-only (замкнутая сеть в рамках локальной машины). На физической (базовой) машине установлено следующее ПО:

- ОС Microsoft Windows Server 2003 Enterprise Edition;
- VMware Workstation 4.5.2;
- Adobe Acrobat Reader 6.0.

2.1 Назначение виртуальных машин и предустановленное/устанавливаемое ПО

VM	Назначение	Предустановленное/устанавливаемое ПО
1	Удостоверяющий центр МГУ	ОС Microsoft Windows Server 2003 Enterprise Edition, Service Pack 1; Domain Controller/Active Directory; Internet Information Services (с поддержкой ASP.NET); MS Certificate Cervices (в режиме Enterprise)
2	Удостоверяющий центр МИФИ	ОС Microsoft Windows Server 2003 Enterprise Edition, Service Pack 1; RSA Keon CA 6.5.1; Sun ONE Directory Server 5.2
3	Мостовой удостоверяющий центр	ОС Microsoft Windows Server 2003 Enterprise Edition, Service Pack 1; RSA Keon CA 6.5.1; Sun ONE Directory Server 5.2

2.2 Программная архитектура лабораторного стенда

Схема размещения ПО лабораторного стенда представлена на Рисунке 1.

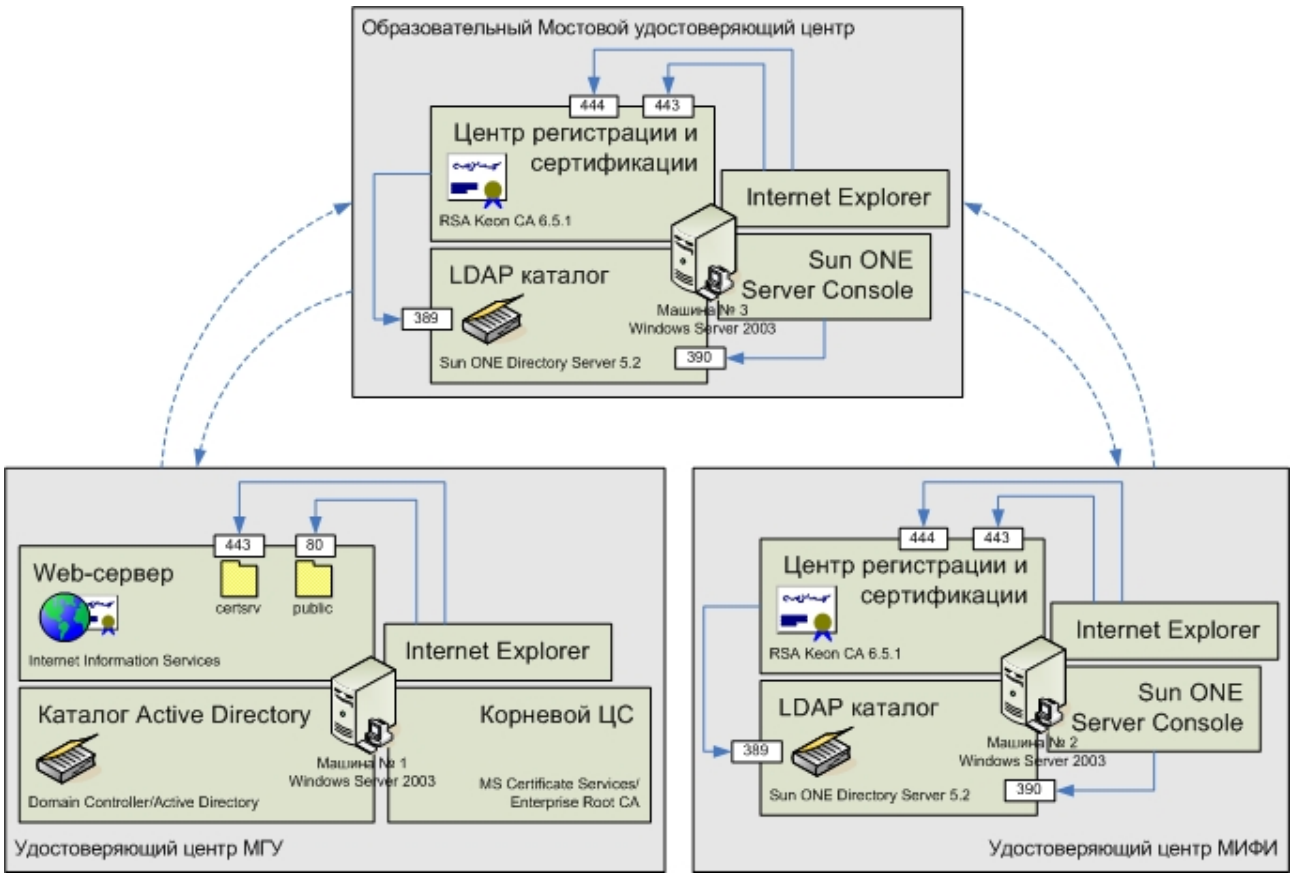


Рисунок 1 – Схема размещения ПО лабораторного стенда

Примечание. На схеме указаны подключения и сервисы, существенные с точки зрения выполнения лабораторной работы.

2.3 Логическая архитектура лабораторного стенда

На Рисунке 2 представлена логическая архитектура, используема в работе. В качестве примера, серым цветом указаны сертификаты, входящие в путь сертификации от Пользователя 2 до точки доверия Пользователя 1. Данная последовательность сертификатов, таким образом, позволяет установить ограниченное доверие между Пользователями 1 и 2, находящимися в разных доменах доверия.

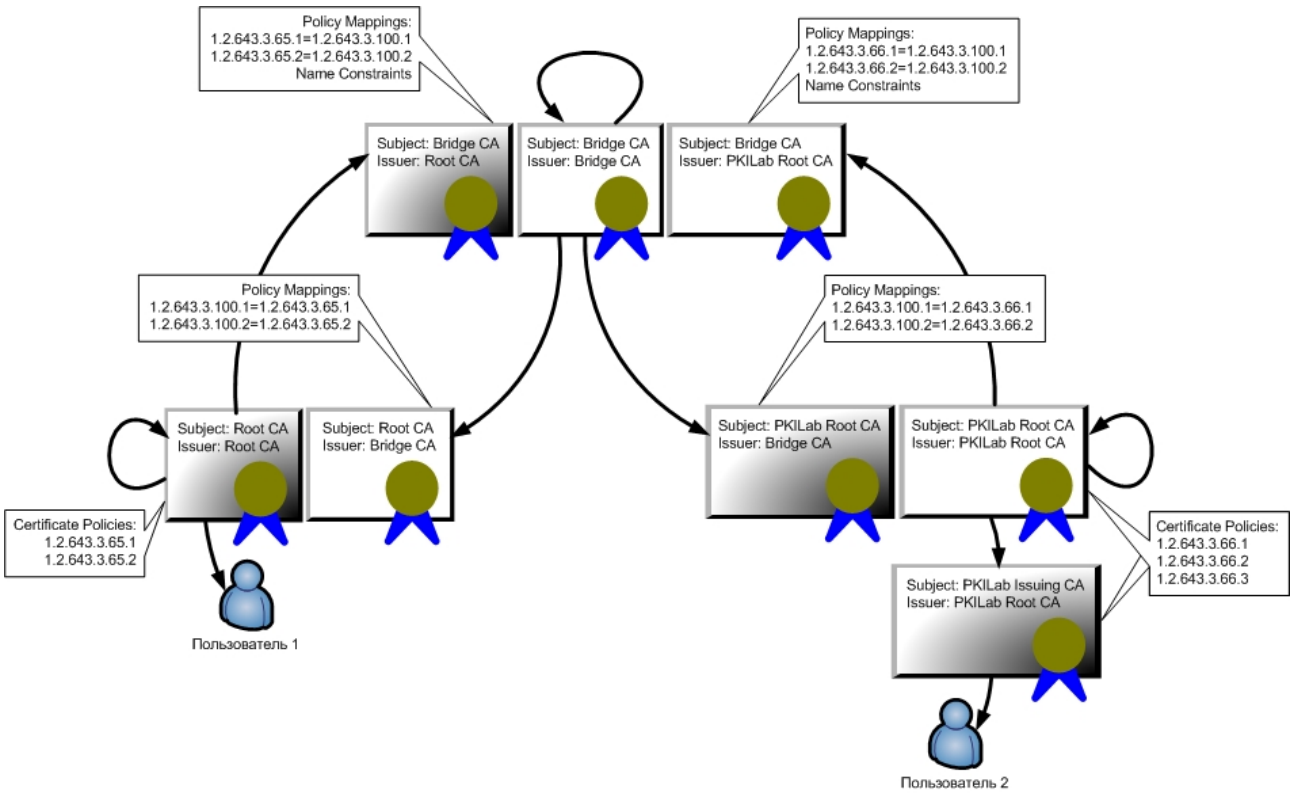


Рисунок 2 – Логическая архитектура лабораторного стенда

3 Порядок выполнения работы

ВНИМАНИЕ! Перед выполнением работы необходимо синхронизировать время и проверить сетевое взаимодействие между всеми виртуальными машинами! Для этого необходимо:

1. запустить все три виртуальные машины (d:\labs_2006\lab5\);
2. выяснить IP-адрес и имя каждой виртуальной машины:

   ```
   ipconfig /all
   ```

3. проверить сетевое взаимодействие между машинами:

   ```
   ping <IP_адрес_виртуальной_машины>
   ```

4. синхронизировать время с помощью команды:

   ```
   net time \\<IP_адрес_виртуальной_машины_3>
   ```

   в качестве источника для синхронизации взять виртуальную машину № 3 (Мостовой УЦ)

Примечание. При выполнении работы, в целях повышения производительности системы, рекомендуется запускать соответствующие виртуальные машины по мере необходимости.

3.1 Создание Мостового УЦ на машине №3

Машина №3 используется для построения Мостового удостоверяющего центра, связывающего существующие домены доверия Московского государственного университета и Московского инженерно-физического института (государственного университета). Характеристики доменов доверия приведены в разделе 2 (Описание лабораторного стенда).

Для реализации функционала Мостового УЦ используется ПО RSA Keon CA 6.5.1 и Sun ONE Directory Server 5.2, устанавливаемое на одну машину. Администрирование установленного ПО производится локально.

Далее приведены указания по настройке ПО Мостового УЦ. Описание конкретных действий можно взять из Лабораторной работы №3.

3.1.1 Предварительная настройка машины №3

К имени машины №3 добавить DNS-суффикс pki.edu и перезагрузить машину.

В дальнейшем, для доступа к машине Мостового УЦ по полному доменному имени (вместе с DNS-суффиксом), необходимо прописать соответствие между доменным именем и IP-адресом машины №3 в файле %systemroot%\system32\drivers\etc\hosts той машины, с которой необходим доступ.

3.1.2 Установка и настройка ПО Сетевого справочника

Все компоненты Sun ONE Directory Server 5.2 (непосредственно Directory Server и

Administration Console) устанавливаются на одну машину.

1. Произвести установку всех компонент Sun ONE Directory Server 5.2 с помощью дистрибутива на рабочем столе. В качестве основного порта взаимодействия указать стандартный порт LDAP (389), остальные параметры оставить по умолчанию. В окне Populate Suffix установить флаг Don't populate для исключения заполнения основного дерева каталога.
2. Произвести модификация схемы созданного каталога, добавив класс pkiCA, включающий следующие атрибуты (Allowed atributes): authorityRevocationList, cACertificate, certificaterevocationlist, crosscertificatepair.
3. В корне DC=pki,DC=edu создать следующее дерево каталога Мостового УЦ: O=Bridge CA,C=RU,DC=pki,DC=edu.
4. Включить созданный объект O=Bridge CA,C=RU,DC=pki,DC=edu в класс pkiCA.

3.1.3 Установка и первичная настройка ПО RSA Keon CA

Обе фазы установки RSA Keon CA (файловую и браузерную) необходимо проводить на одной машине. Администрирование инсталляции также будет проводиться локально.

1. Инициировать установку RSA Keon CA с помощью дистрибутива на рабочем столе.
2. При первой фазе установки оставить параметры по умолчанию.
3. При второй фазе установки заменить занятый LDAP-каталогом порт 389 на любой другой (не занятый). Список занятых портов можно посмотреть с помощью команды:

   ```
   netstat -a
   ```

4. Имя почтового SMTP-сервера оставить по умолчанию, отключить проверку доступности почтового сервера.
5. Произвести установку сертификата администратора.
6. После завершения установки подключиться к административной консоли RSA Keon CA (https://<имя_машины>:444) и включить полное протоколирование всех событий.
7. Перезагрузить виртуальную машину.

3.1.4 Создание Мостового центра сертификации на машине №3

В составе Мостового УЦ может быть создано несколько центров сертификации для различных целей. В работе создается один Мостовой центр сертификации, участвующий в кроссертификации с выделенными ЦС (CA Principal) связываемых доменов доверия.

Мостовой УЦ функционирует в соответствии с собственными политиками, являющимися универсальными и использующимися для построения соответствий между политиками различных доменов. В работе универсальным политикам Мостового УЦ назначены следующие идентификаторы:

1.2.643.3.100.1 (Educational Bridge CA General Certificate Policy)

1.2.643.3.100.2 (Educational Bridge CA Limited Liability Certificate Policy)

1.2.643.3.100.3 (Educational Bridge CA Low Assurance Certificate Policy)

1. Создать самоподписанный ЦС с сертификатом следующего вида:

```
X509 Certificate:
Version: 3
```

```
Serial Number: d085612b4a377d3b6aef78b1dffcddd2
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    O=Bridge CA
    C=RU

NotBefore: 09.12.2006 16:22
NotAfter: 06.12.2009 21:12

Subject:
    O=Bridge CA
    C=RU

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 b1 ab 0d 06 21 70 04
    0010  bc e9 5a 82 db 94 95 cd  10 9f ca 5a 0b f3 07 d3
    0020  a8 d4 a7 ba a6 8d ea 66  b1 ca b0 f8 87 3c dc 2e
    0030  f5 35 2b ad 24 b8 bb 7a  89 bc 45 41 90 a4 75 8c
    0040  f8 b5 e6 53 ba c2 f8 e1  24 1e 3b cb e9 b3 24 28
    0050  ef 8d 6c 1b 54 2f 7a 68  6a 95 26 00 d9 94 26 bc
    0060  ed 81 82 de 65 dd dd 8b  e4 75 ae e8 1f 59 72 21
    0070  89 53 bc 13 9a 65 00 c1  0b 6a e3 1d 60 71 66 62
    0080  f7 3a e3 fc 17 08 1b db  d6 1b 8a bd 9d 43 c2 18
    0090  66 23 32 73 3a 24 56 00  78 9e ec 9c 35 92 6f c1
    00a0  f4 79 76 46 b8 6b a4 9e  ed 23 cc f3 ca ca fc c4
    00b0  f4 f6 3d 3c ca c1 7e 94  fc 83 85 c1 7a af 92 91
    00c0  f2 23 d6 a7 d6 b6 31 4a  45 65 db a6 dd 00 4c e8
    00d0  eb 9f b2 bc 4d 8c 30 ae  d5 86 ac d0 05 56 49 e1
    00e0  2b e5 a0 b4 78 2c 24 9f  66 18 d7 06 06 36 71 bf
    00f0  ee 00 09 b0 25 3c 5b fd  51 56 52 a4 15 f9 3c 90
    0100  6f 69 80 d4 c9 cb 47 71  75 02 03 01 00 01

Certificate Extensions: 6
    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.32: Flags = 0, Length = 129
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.2.643.3.100.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                             Notice Text=Educational Bridge Certification Authority General Policy
Statement
        [2]Certificate Policy:
             Policy Identifier=1.2.643.3.100.2
             [2,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                             Notice Text=Educational Bridge Certification Authority Limited Policy
Statement
        [3]Certificate Policy:
             Policy Identifier=1.2.643.3.100.3
             [3,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Educational Bridge Certification Authority Low Trust Level Policy
Statement

    2.5.29.15: Flags = 1(Critical), Length = 4
    Key Usage
        Certificate Signing, Off-line CRL Signing, CRL Signing (06)

    2.5.29.17: Flags = 0, Length = 14
    Subject Alternative Name
        DNS Name=bridgeca.pki.edu
```

```
    2.5.29.35: Flags = 0, Length = 18
    Authority Key Identifier
        KeyID=82 ba d9 12 88 d8 0e c8 21 42 d0 fd de 89 6b a6 18 3d c8 c7

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        82 ba d9 12 88 d8 0e c8 21 42 d0 fd de 89 6b a6 18 3d c8 c7

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  6b 93 3f 29 80 12 e6 c1  d8 27 88 e0 39 4b 79 23
    0010  4d 3d 2e bd cb 2d fa a7  c9 03 99 d7 e0 c6 f3 87
    0020  a0 31 ad 6d cc 80 86 f7  5d f4 db c2 2b 78 f5 0c
    0030  e9 01 c5 0b f1 2c e6 06  1d c9 6f a7 9b ee e1 52
    0040  79 73 41 0d 8d d9 1e 68  8f 0e b8 ac 79 ad a8 84
    0050  68 96 a1 77 36 e7 eb 54  ad d3 25 4f 27 d5 70 2d
    0060  71 70 a6 4a dc 35 87 59  92 d0 2b 9d 7f c6 ac 54
    0070  be ff 17 10 bc 15 28 0b  cc b7 1f e6 10 02 fc de
    0080  32 54 31 8b 2e 68 70 84  45 2f 0e f8 a9 84 01 3a
    0090  50 30 63 be a7 93 bd 0a  59 85 7e aa 4b 84 93 13
    00a0  75 a6 db 65 42 fc 14 dc  a7 7b cc ec 99 35 ff 92
    00b0  7d 83 11 9f 38 0e 89 99  c1 0a 0f f7 aa 22 72 6d
    00c0  09 b1 bb 55 44 b9 6b 6d  14 43 ac c4 f3 90 17 df
    00d0  42 d2 9b ba 12 69 35 a8  ad e1 1a 09 8e 40 53 dd
    00e0  14 f4 0d 6c de b1 30 79  76 b2 dc ae d1 25 06 4b
    00f0  43 08 80 4e cc cd cf 10  cd aa 43 ba f7 a6 eb b0
```

2. Для этого подключиться к административной консоли RSA Keon CA и в разделе CA Operations выбрать ссылку create в левой части.
3. Далее произвести настройку юрисдикции по умолчанию для создаваемого ЦС. В разделе Certificate Attributes добавить два атрибута типа DC с соответствующими значениями по умолчанию (DC=pki,DC=edu). При этом добавленные атрибуты не включать в состав сертификатов.
4. В разделе Publishing Configuration настроить публикацию сертификата ЦС (Publish Authorities), СОС (Publish Complete CRLs) и пары кроссертификатов (Publish Cross-Certificates) в объект, созданный в LDAP-каталоге (O=Bridge CA,C=RU,DC=pki,DC=edu). Более подробную информацию о настройке публикации см. в Лабораторной работе №3.
5. В разделе Extension Profiles выбрать профиль Custom CA и отметить флаг Vettor can override.
6. Нажать Save and Exit.
7. Далее на странице Create a New CA заполнить поля Subject DN для соответствия приведенному выше шаблону сертификата.
8. В качестве профиля указать Custom CA и выбрать расширения из списка согласно приведенному шаблону сертификата (см. п. 1).
9. Далее необходимо настроить содержание сертификата в соответствии с шаблоном, приведенном в пункте 1. При настройке содержания расширения Certificate Policies установить количество политик равным 3 и количество определителей (qualifier) для каждой политики равным 1. В качестве типа определителей указать UserNotice, установить флаг UserNotice/explicitText object и ввести текст примечаний в соответствии с приведенным шаблоном.
10. После создания ЦС проверить соответствие сформированного сертификата ЦС приведенному шаблону с помощью утилиты:

    ```
    certutil –dump
    ```

11. Опубликовать сертификат и СОС сформированного ЦС в LDAP-каталог. Проверить корректность опубликования с помощью LDAP-браузера.

3.2 Кроссертификация Мостового УЦ с доменом МИФИ

С технической точки зрения, кроссертификация подразумевает издание одного (двух) специальных сертификатов (кроссертиификатов) одним ЦС другому. Для проведения кроссертификации в домене обычно выделяется специальный ЦС (CA Principal). В работе для кроссертификации с Мостовым УЦ используется корневой ЦС двухуровневой иерархии домена МИФИ.

Однако необходимо учитывать тот факт, что кроссертификация – это не только технический процесс издания специальных сертификатов. Кроссертификация также включает в себя согласование политик, действующих в различных доменах. Результатом согласования политик является включение в кроссертификаты специальных расширений, ограничивающих распространение доверия при переходе из одного домена доверия в другой.

В работе используются следующие ограничивающие расширения, включаемые в состав кроссертификатов:

- Basic Constraints – устанавливает ограничения на тип субъекта сертификата и длину пути сертификации;
- Name Constraints – устанавливает ограничения на пространство имен;
- Policy Mappings – устанавливает отображение политик одного домена на аналогичные политики другого домена.

3.2.1 Анализ домена МИФИ

1. Изучить архитектуру PKI домена МИФИ и содержание сертификатов ЦС, входящих в иерархию (см. Приложение А):
   - Корневой ЦС МИФИ (PKILab Root CA);
   - Издающий ЦС МИФИ (PKILab Issuing CA).
2. Определить политики, действующие в домене, и их соответствие политикам Мостового УЦ.

3.2.2 Издание сертификата Корневым ЦС МИФИ Мостовому ЦС

При издании кроссертификата необходимо обеспечить отображение политик, действующих в домене МИФИ в универсальное множество политик Мостового УЦ. В работе используется следующее отображение:

	Отображаемая политика	**Отображение в политику Мостового УЦ**
1	1.2.643.3.66.1 (MEPhI Common Certificate Policy)	1.2.643.3.100.1 (Educational Bridge CA General Certificate Policy)
2	1.2.643.3.66.2 (MEPhI Restricted Policy)	1.2.643.3.100.2 (Educational Bridge CA Limited Liability Certificate Policy)
3	1.2.643.3.66.3 (MEPhI Low Assurance Test Policy)	*не отображается*, т.к. в соответствии с данной политикой издаются только тестовые сертификаты внутри домена

1. На Мостовом УЦ (машина №3) сформировать PKCS#10-запрос от лица Мостового ЦС (Bridge CA). Для этого подключиться к административной консоли RSA Keon CA на машине №3, войти в раздел CA Operations, выбрать в левой части созданный самоподписанный мостовой ЦС и нажать кнопку Generate PKCS#10 в окне отображения параметров ЦС.
2. Перенести сформированный PKCS#10-запрос на машину №2 (УЦ МИФИ) и импортировать его в юрисдикцию Корневого ЦС через Enrollment Server (https://<имя_машины_2>) с использованием соответствующей ссылки (Make a PKCS#10 Cross-Certificate Request).
3. Произвести изменения в настройках юрисдикции Корневого ЦС МИФИ. Для этого подключиться к административной консоли RSA Keon CA на машине №2 (https://<имя_машины_2>:444) и войти в раздел CA Operations.
4. Далее в левой части выбрать для просмотра Корневой ЦС МИФИ (PKILab Root CA), нажать кнопку Configure в разделе Jurisdiction Configuration и в разделе настроек Extension Profiles установить флаг Vettor can override.
5. В разделе настроек External Publishing включить опубликование кроссертификатов (Publish Cross-Certificates) и указать соответствующий атрибут объекта, в который будет происходить опубликование. Сохранить изменения.
6. Выбрать в левой части Корневой ЦС МИФИ (PKILab Root CA) и перейти по ссылке cross-certificates. Откроется окно управления кроссертификатами Корневого ЦС.
7. Выбрать для обработки импортированный ранее запрос.
8. Выбрать профиль Custom CA. Отобразится список доступных расширений.
9. Из расширений, присутствующих в PKCS#10-запросе взять Subject Alternative Names. Из списка Available Extensions выбрать следующие расширения:
   - Authority Key Identifier
   - Basic Constraints
   - Key Usage
   - Name Constraints
   - Policy Mappings
   - Subject Key Identifier
10. При издании сертификата для расширения Name Constraints установить следующие параметры:

Permitted subtrees	rfc822Name	*
Excluded subtrees	rfc822Name	@mephi.ru
	dnsName	mephi.ru
	directoryName	organizationalName: MEPhI countryName: RU

Включение в состав кроссертификата подобного расширения позволит избежать издания сертификатов в другом домене, содержащих поля из пространства имен МИФИ (включая адреса электронной почты, DNS-имена серверов и имена пользователей в директории).

---

11. Расширение Policy Mappings настроить в соответствии с используемым в работе отображением политик (см. ранее).

---

12. Расширения Basic Constraints и Key Usage сделать критичными. Ограничения на длину пути сертификации не устанавливать.
13. Изданный сертификат перенести на Мостовой УЦ (машина №3) и импортировать. Для этого воспользоваться кнопкой Import Forward Certificate, расположенной на странице управления кросс-сертификатами Мостового ЦС (Bridge CA).

3.2.3 Издание сертификата Мостовым ЦС Корневому ЦС МИФИ

1. Аналогичным образом провести кроссертификацию в обратную сторону. При этом в состав кроссертификата включить тот же набор расширению за исключением Name Constraints. В расширение Policy Mappings включить отображение политик Мостового УЦ во множество политик домена МИФИ.
2. После проведения кроссертификации опубликовать пару кроссертификатов как в LDAP-каталоге МИФИ, так и в LDAP-каталоге Мостового УЦ с помощью страницы управления кросс-сертификатами.
3. Проверить корректность опубликования пары кроссертификатов (crossCertificatePair) с помощью LDAP-браузера.

3.3 Кроссертификация Мостового УЦ с доменом МГУ

3.3.1 Анализ домена МГУ

1. Изучить архитектуру PKI домена МГУ, содержание сертификата ЦС (Root CA), а также настройки службы сертификатов (см. Приложение Б).
2. Определить политики, действующие в домене, и их соответствие политикам Мостового УЦ.

3.3.2 Издание кроссертификата Корневым ЦС МГУ Мостовому ЦС

Реализация кроссертификации в решении MS Certificate Services (возможность проведения которой появилась, начиная с MS Windows 2003 Server) имеет некоторые особенности. Для проведения кроссертификации (издания кроссертификата Центром сертификации MS) необходимо выполнить следующую последовательность действий:

- Издать специальный сертификат Qualified Subordination Signing, необходимый для одобрения акта издания кроссертификата;
- Сформировать специальный файл Policy.inf, определяющий параметры устанавливаемого кроссертификационного отношения;
- На основании запроса (или сертификата) ЦС, которому необходимо издать кроссертификат, и файла Policy.inf сформировать специальный запрос на кроссертификат (Qualified Subordination Request); при формировании данного запроса также используется специальный сертификат Qualified Subordination Signing, сформированный ранее;
- Отправить сформированный запрос в ЦС Microsoft и издать кроссертификат.

---

1. Сформировать специальный шаблон Qualified Subordination Signing. Для этого войти на машину №1 под учетной записью администратор и открыть консоль Certificate Templates.
2. Скопировать шаблон Enrollment Agent.
3. В окне свойств нового шаблона перейти на вкладку General и в поле Template display name ввести Qualified Subordination Signing.
4. На вкладке Request Handling указать цель использования ключа Signature.

---

5. Нажать кнопку CSPs и в окне выбора криптопровайдера оставить выбранным только Microsoft Enhanced Cryptographic Provider 1.0.
6. На вкладке Subject Name убедиться, что выбран режим Build from this AD information, формат имени Fully distinguished name и установлен только флаг User principal name (UPN).
7. На вкладке Issuance Requirements убедиться, что флаг CA certificate manager approval установлен. В поле Require the following for reenrollment должна быть выбрана опция Valid existing certificate.
8. На вкладке Extensions настроить расширения таким образом, чтобы расширение Application policies включало только значение Qualified Subordination.
9. На закладке Security убедиться, что только члены групп Domain Admins и Enterprise Admins имеют разрешение Enroll для данного шаблона сертификатов.
10. Сохранить изменения.
11. После создания шаблона сертификата Qualified Subordination Signing необходимо произвести соответствующие изменения в шаблоне кроссертификата Cross-Certification Authority. Для этого в консоли Certificate Templates открыть шаблон Cross Certification Authority.
12. В свойствах шаблона Cross-Certification Authority на вкладке Issuance Requirements сделать следующие изменения. В поле This number of authorized signatures установите значение 1 (это поле указывает количество подписей, необходимое для выпуска сертификата). В поле Application Policy указать Qualified Subordination.
13. Сохранить изменения.
14. Далее необходимо настроить ЦС Root CA для издания сертификатов в соответствии с настроенными шаблонами: Консоль управления ЦС, Certificate Templates→New Certificate Template to Issue... и выбрать оба шаблонаю .
15. Запросить и установить сертификат в соответствии с шаблоном Qualified Subordination Signing, подключившись к WEB-интерфейсу ЦС (https://<имя_машины_1>/certsrv) с использованием учетной записью Administrator.
16. Проверить корректность полученного сертификата – убедиться, что в полях Extended key Usage и Key Usage стоят правильные значения (Qualified Subordination и Digital Signature соответственно).

Далее необходимо непосредственно сформировать запрос на кроссертификат в соответствии с процедурой, описанной выше.

---

17. На машине №3 сформировать PKCS#10-запрос от лица Мостового УЦ аналогично тому, как это делалось ранее и перенести запрос на машину №1.
18. Сформировать файл Policy.inf следующим образом. Создать текстовый файл и добавить в него заголовок:

```
[Version]
Signature="$WindowsNT$"
```

19. Добавить в файл информацию об отображении политик домена МГУ на множество политик Мостового УЦ:

```
[PolicyMappingsExtension]
1.2.643.3.65.1 = 1.2.643.3.100.1
1.2.643.3.65.2 = 1.2.643.3.100.2
critical = yes
```

20. Включить в файл информацию об ограничениях, накладываемых на пространство имен:

```
[NameConstraintsExtension]
Include = NameConstraintsPermitted
Exclude = NameConstraintsExcluded
Critical = TrUe
[NameConstraintsPermitted]
[NameConstraintsExcluded]
DirectoryName = "DC=msu, DC=su"
email = @msu.su
DNS = .msu.su
```

21. Сохранить файл в каталоге %systemroot% (по умолчанию C:\Windows) с именем Policy.inf.
22. Сформировать специальный запрос на выпуск кроссертификата (Qualified Subordination Request) с помощью следующей команды:

    ```
    certreq –policy –attrib CertificateTemplate:CrossCA
    ```

    на вход подать PKCS#10-запрос Мостового ЦС, файл Policy.inf и указать полученный ранее сертификат Qualified Subordination Signing.
23. Перед изданием кроссертификата отключить добавление в издаваемые сертификаты расширений CDP и AIA (см. Лабораторную работу №2).
24. Сформированный специальный запрос отправить в ЦС с помощью WEB-интерфейса (https://<имя_машины_1>/certsrv), указав при отправке шаблон Cross Certificate Authority.
25. Проверить корректность изданного сертификата и его соответствие файлу политики (Policy.inf).
26. Изданный сертификат импортировать на Мостовой УЦ. Для этого на машине №3 подключиться к административной консоли RSA Keon CA, войти в раздел CA Operations, выбрать в левой части Мостовой ЦС и импортировать созданный кроссертификат с помощью кнопки Import Forward Certificate на странице управления кроссертификатами.

3.3.3 Издание кроссертификата Мостовым ЦС Корневому ЦС МГУ

Полноценная двухсторонняя кроссертификация с использованием механизма Qualified Subordination, описанного выше, поддерживается только между двумя ЦС, основанными на MS Certificate Cervices. Это связано с тем, что формируемый запрос (Qualified Subordination Request) имеет специальный формат, не поддерживаемый решениями сторонних производителей и, в частности RSA Keon. Кроме того, в MS Certificate Cervices отсутствуют штатные средства генерирования стандартного PKCS#10-запроса от лица ЦС.

В связи с этим, для проведения кроссертификации в обратную сторону (издания кроссертификата Мостовым ЦС Корневому ЦС МГУ) необходимо использовать дополнительную возможность ПО RSA Keon CA, позволяющую переподписывать произвольный сертификат с использованием локально созданных ЦС.

1. Сохранить сертификат Корневого ЦС домена МГУ (Root CA) в файл в виде кодировке Base-64 и перенести его на Мостовой УЦ (машина №3).
2. На машине №3 подключиться к административной консоли RSA Keon CA и войти в раздел CA Operations.

3. В левой части под заголовком External CAs выбрать пункт re-sign external CA certificate.
4. Скопировать сертификат Корневого ЦС МГУ (Root CA) в текстовое поле.
5. В качестве издателя выбрать Мостовой ЦС (Bridge CA).
6. Далее выбрать пункт specify a new set of extensions, для включения в переиздаваемый сертификат нового набора расширений:
   - Authority Key Identifier
   - Basic Constraints
   - Key Usage
   - Policy Mappings
   - Subject Key Identifier
7. В расширение Policy Mappings включить отображение политик Мостового УЦ во множество политик домена МГУ.

Примечание. Переизданный сертификат не сохраняется во внутренней БД RSA Keon CA. Таким образом, в случае перехода с финальной страницы переиздания сертификата (закрытия браузера) без сохранения нового сертификата в файл переизданный сертификат не сохранится, и процесс переиздания придется повторить.

8. После завершения процесса переиздания сохранить новый сертификат в файл, воспользовавшись возможностью его отображения в формате PEM.

3.4 Тестирование решения

Для полноценного тестирования получившейся связи между доменами МИФИ и МГУ, организованной с помощью Мостового УЦ, необходимо в каждом домене издать сертификаты как удовлетворяющие требованиям распространения доверия, так и не удовлетворяющие.

Поскольку в нашем случае процесс построения пути сертификации через Мостовой УЦ не автоматизирован, необходимо ручным способом перенести и установить сертификаты, необходимые для построения правильного пути сертификации (см. раздел 2.3). При этом необходимо учитывать тот факт, что в каждом домене доверенным (установленным в хранилище Trusted Root Certification Authorities) является только один ЦС – Корневой ЦС домена и все пути сертификации должны заканчиваться (начинаться) на самоподписанном сертификате данного ЦС.

3.4.1 Проверка сертификатов МИФИ в домене МГУ

1. В домене МИФИ издать сертификат, удовлетворяющий требованиям распространения доверия, т.е.
   - сертификат издан в соответствии с политикой, для которой настроено отображение через мост (должен иметь соответствующее расширение Certificate Policies);
   - сертификат не содержит имен из пространства имен МГУ.
2. Издание сертификата осуществлять ручным способом в два этапа:
   - формирование запроса через Enrollment Server (https://<имя_машины_2>);
   - обработка запроса администратором в разделе Certificate Operations.

3. Для задания расширений сертификата использовать стандартный профиль Custom End-entity, позволяющий включать в сертификат практически все доступные расширения. В сертификат пользователя включить следующие расширения:
   - Authority Key Identifier
   - Key Usage (произвольное значение)
   - Extended Key Usage (произвольное значение)
   - Certificate Policies (включить значение отображаемой политики)
   - Subject Key Identifier
4. В домене МИФИ издать сертификат, не удовлетворяющий требованиям распространения доверия по причине присутствия в сертификате имени из запрещенного пространства имен. Данный сертификат должен быть издан в соответствии с политикой, для которой настроено отображение через мост (должен иметь соответствующее расширение Certificate Policies).
5. В домене МИФИ издать сертификат, не удовлетворяющий требованиям распространения доверия по причине отсутствия отображения для политики, в соответствии с которой он был издан (1.2.643.3.66.3 – MEPhI Low Assurance Test Policy).
6. Сохранить изданные сертификаты в файл формата PKCS#7 вместе с цепочкой до Корневого ЦС МИФИ (PKILab Root CA) с помощью стандартных средств RSA Keon CA, доступных при нажатии на кнопку Download в окне отображения сертификата.
7. Перенести сформированные контейнеры в домен МГУ (машина №1).
8. Перенести и установить на машине №1 сертификаты, необходимые для построения пути сертификации от Корневого ЦС МИФИ (PKILab Root CA) до Корневого ЦС МГУ (Root CA), являющегося точкой доверия для пользователей домена МГУ.
9. Открыть PKCS#7-контейнеры с сертификатами МИФИ. Проанализировать результаты.

3.4.2 Проверка сертификатов МГУ в домене МИФИ

Аналогичным образом произвести проверку сертификатов МГУ в домене МИФИ. Для издания сертификатов, содержащих необходимые поля, при необходимости, создать специальный профиль.

4 Контрольные вопросы

1. Каким образом можно организовать распространение доверия к открытому ключу некоторого субъекта? С помощью какого математического аппарата можно описать систему распространения доверия?
2. Каковы основные понятия, связанные с распространением доверия?
3. Каковы основные модели доверия? В чем их особенности? Провести краткий сравнительный анализ.
4. Для чего используется мостовой удостоверяющий центр? Каковы достоинства и недостатки использования данного подхода?
5. Что представляет собой путь сертификации? Каким образом происходит построение пути сертификации? Каковы входные и выходные данные процесса построения и проверки пути сертификации?
6. Какие существуют механизмы для ограничения распространения доверия?
7. Что собой представляет Qualified Subordination (в терминологии Microsoft)? Какова общая процедура организации таких отношений?

Приложение А

Сертификат Корневого ЦС МИФИ

```
X509 Certificate:
Version: 3
Serial Number: 5479ee8c0a5f071b57a7a8c104ead0d9
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=PKILab Root CA
    OU=Dept. 42
    O=MEPhI
    C=RU
    DC=mephi
    DC=ru

NotBefore: 08.12.2006 18:06
NotAfter: 08.12.2011 17:47

Subject:
    CN=PKILab Root CA
    OU=Dept. 42
    O=MEPhI
    C=RU
    DC=mephi
    DC=ru

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 c8 90 dd 7b 64 42 85
    0010  b2 e8 06 3f fe ea 78 2f  32 92 fd 3b 75 01 eb f8
    0020  e8 05 27 72 f3 d3 29 ca  ce d0 55 fb b2 4e f6 83
    0030  96 8d da c2 78 af 4b 9f  69 dd a2 28 6e e9 de b7
    0040  b8 fe e8 ef 24 57 e9 99  4c a5 4e ad e3 2b 96 84
    0050  2f 3b 6e eb b7 eb 49 99  78 71 26 bf 83 b0 52 8d
    0060  09 12 ba 9d 20 28 e8 f9  32 52 b0 17 cc c9 dc 37
    0070  eb 2b 70 ba f0 23 ed aa  aa 89 03 56 29 c0 e3 36
    0080  0f 69 f1 1c c4 db fd 13  75 b3 28 35 10 d0 19 99
    0090  49 52 0f 06 cb ac 63 bf  2d 45 1e 28 5e 98 49 69
    00a0  2e 4f 84 60 b9 0d c7 f5  c9 b9 d2 3a b4 a4 75 4f
    00b0  56 92 ee 01 92 f0 33 fc  bd d7 4e a1 57 d8 31 4e
    00c0  fd c3 6c 82 02 c4 22 66  80 8e 4d 4c f7 ed bb a6
    00d0  a9 c2 bb 84 9e fe 29 67  2c 9c 30 0e 36 8e 03 91
    00e0  c5 76 b0 a2 20 cc 22 fc  b2 63 1b bd 6b cb d6 37
    00f0  4d 45 d3 aa 93 b5 69 de  e1 de 54 dc f4 2e 88 d8
    0100  ea 14 b5 fb 66 fb 89 f6  dd 02 03 01 00 01

Certificate Extensions: 5
    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.32: Flags = 0, Length = 141
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.2.643.3.66.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://keonca.mephi.ru:447/rfc3647.htm
             [1,2]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Moscow Engineering-Physics Institute Common Certificate Policy
        [2]Certificate Policy:
             Policy Identifier=1.2.643.3.66.2
             [2,1]Policy Qualifier Info:
```

```
                    Policy Qualifier Id=User Notice
                    Qualifier:
                         Notice Text=Moscow Engineering-Physics Institute Restricted Policy
          [3]Certificate Policy:
               Policy Identifier=1.2.643.3.66.3
               [3,1]Policy Qualifier Info:
                    Policy Qualifier Id=User Notice
                    Qualifier:
                         Notice Text=Moscow Engineering-Physics Institute Low Assuarance Test Policy

    2.5.29.15: Flags = 1(Critical), Length = 4
    Key Usage
        Certificate Signing, Off-line CRL Signing, CRL Signing (06)

    2.5.29.35: Flags = 0, Length = 18
    Authority Key Identifier
        KeyID=8a fc 35 7a ad 3c a5 23 ac 94 2e 8a 62 22 02 84 88 b5 22 78

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        8a fc 35 7a ad 3c a5 23 ac 94 2e 8a 62 22 02 84 88 b5 22 78

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  ec b4 36 a5 9e ec 2a 6c  e0 2b b0 fa 0f 88 75 f7
    0010  e1 ee c9 3a 9f f4 80 7f  a9 b1 33 81 47 e6 20 79
    0020  94 7d b1 82 36 fb 76 ea  52 86 fe 4b a6 0a 82 d6
    0030  42 91 4b 2c 68 fd 7b b1  50 f5 3f c5 4e d5 28 e4
    0040  3c a7 c5 a3 ed f2 7c cd  b2 14 84 58 68 b5 a4 08
    0050  4d fe f3 0c 50 22 97 fe  61 06 39 49 c8 a7 b7 58
    0060  fc 22 37 42 b4 46 10 9b  30 aa 22 8f b0 d8 7b 56
    0070  d4 ee a6 23 76 3a f0 80  f2 bf 11 ed 22 7d 7e 7a
    0080  4b 07 37 e1 9a e6 7f b1  f0 5e da 34 56 e9 45 b1
    0090  94 5d 5a da 9c 08 8a 04  c9 3d 64 ba d5 59 e7 4c
    00a0  c8 c8 c9 5a 46 bb c2 4e  84 e6 14 b1 ae ce 10 e3
    00b0  62 07 97 8a 7c 0d 67 52  de b6 f2 9e 5d ce b1 c7
    00c0  24 9c f1 b4 e8 25 e7 f3  fe 04 e2 f1 cc 85 be ec
    00d0  26 f0 af 54 4e 27 e1 73  3e 7c 42 0b 9e f9 c2 51
    00e0  5d 88 89 64 fb ff 72 67  b0 67 21 50 00 cf b9 4c
    00f0  5d 1b bd e6 4e 15 ce 66  94 42 63 e0 39 e1 48 7c
```

Сертификат Издающего ЦС МИФИ

```
X509 Certificate:
Version: 3
Serial Number: 799b9850609066e6df581657fb92f0ff
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=PKILab Root CA
    OU=Dept. 42
    O=MEPhI
    C=RU
    DC=mephi
    DC=ru

NotBefore: 08.12.2006 18:38
NotAfter: 08.12.2009 17:56

Subject:
    CN=PKILab Issuing CA
    OU=Dept. 42
    O=MEPhI
    C=RU
    DC=mephi
    DC=ru

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
```

```
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 c2 c7 3a 05 4d d6 87
    0010  d2 e0 56 a4 f2 1f 83 00  d4 ef f9 9c 99 d9 e4 43
    0020  bc d0 9b c1 4f 77 2a 18  b0 83 cd 35 8c 83 52 c3
    0030  b7 62 96 64 46 77 58 42  ab 86 f1 db 41 a8 92 61
    0040  61 dc 2b a0 98 74 6a 89  40 9a 1e 9e df 8f bc 34
    0050  72 e5 8b 57 c2 88 13 72  18 00 cc 88 86 21 04 fe
    0060  48 0c 38 6a 35 4d c2 f4  f0 2f 25 fe bc 56 18 be
    0070  40 85 b9 ce e6 c5 fe f0  14 b4 b1 b4 fe 6f 7c 29
    0080  d8 94 d0 9c cf 29 76 f7  ca eb 71 70 89 01 71 ec
    0090  83 98 cd 84 6f bc af cf  76 a0 18 4e 4c fc a1 61
    00a0  62 fc c7 00 ea ff 1f 78  7b 85 2f e3 e4 68 2f 83
    00b0  63 20 28 d8 8a 2c 75 4f  90 43 30 ce 34 bf a3 04
    00c0  1d 11 8d eb 18 2d 19 af  f0 25 f3 21 a9 c6 03 a2
    00d0  de e9 c6 33 45 35 7a 28  85 f5 1c d4 6c a7 83 d5
    00e0  bd 26 d6 ab f6 cf 87 64  85 13 21 7f 24 c9 ba f9
    00f0  da e3 16 58 d0 87 11 f9  c0 13 60 77 44 0f 1c 15
    0100  cf 32 ee 31 bd 46 ef d3  c9 02 03 01 00 01

Certificate Extensions: 8
    1.3.6.1.5.5.7.1.1: Flags = 0, Length = 50
    Authority Information Access
        [1]Authority Info Access
             Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
             Alternative Name:
                  URL=ldap://keonca.mephi.ru/o=MEPhI,c=RU,dc=mephi,dc=ru?cACertificate

    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.32: Flags = 0, Length = f0
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.2.643.3.66.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://keonca.mephi.ru:447/rfc3647.htm
        [2]Certificate Policy:
             Policy Identifier=1.2.643.3.66.2
             [2,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Moscow Engineering-Physics Institute Restricted Policy
        [3]Certificate Policy:
             Policy Identifier=1.2.643.3.66.3
             [3,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Moscow Engineering-Physics Institute Low Assuarance Test Policy

    2.5.29.31: Flags = 0, Length = 56
    CRL Distribution Points
        [1]CRL Distribution Point
             Distribution Point Name:
                  Full Name:
URL=ldap://keonca.mephi.ru/o=MEPhI,c=RU,dc=mephi,dc=ru?certificateRevocationList

    2.5.29.15: Flags = 1(Critical), Length = 4
    Key Usage
        Certificate Signing, Off-line CRL Signing, CRL Signing (06)

    2.5.29.17: Flags = 0, Length = 15
    Subject Alternative Name
        RFC822 Name=ca_admin@mephi.ru

    2.5.29.35: Flags = 0, Length = 18
    Authority Key Identifier
        KeyID=8a fc 35 7a ad 3c a5 23 ac 94 2e 8a 62 22 02 84 88 b5 22 78

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
```

```
        58 d6 ed 79 2c 1f 83 a9 79 5b 44 cd ac 38 11 7c 59 28 9a b4

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  a8 bb d3 f4 a7 0b 8d 77  19 ac 72 ae 20 c3 5d b5
    0010  d1 68 89 37 0b 95 1a 6a  97 b3 53 79 36 c7 b3 ae
    0020  ce 6e 0d 41 21 14 d5 d5  25 bc 57 e2 7f 59 2d ac
    0030  87 40 dc f6 b0 b8 45 c1  80 c6 aa 80 13 e5 c7 85
    0040  28 f0 e4 a0 69 aa 40 b1  5e bf fd aa b5 20 13 4d
    0050  f5 1f 31 96 08 4b 47 8e  56 50 eb 5e e0 6f 3d 1c
    0060  83 40 dd ea a6 8b 2a 6a  0a 2d 82 9b 18 0d 7d 7e
    0070  72 d9 b5 f2 c2 5b a4 a0  12 70 84 d8 e3 bc c7 83
    0080  ff 58 bf f5 f8 9d 7d 6d  59 0d 2d 39 43 e0 31 c0
    0090  c3 ec 64 40 fe cf 48 a3  e8 19 ed 82 4b fd 51 14
    00a0  88 fc 99 d6 6f e2 31 8c  0b e6 e7 de f6 a9 58 c5
    00b0  32 c1 8b f4 76 50 b9 29  e3 6b 9b 25 5e b5 36 fc
    00c0  ab 80 7e 7d e9 84 0e 4a  55 ea 50 3b fc dd bd 01
    00d0  6e de 8a 37 97 2e a1 8d  b1 5a 20 eb 93 c4 f0 10
    00e0  fb b2 01 f3 b2 d0 5c 53  62 8c c0 77 93 82 2d 94
    00f0  1b 29 90 89 78 e9 29 e5  b8 9f 94 ee 9d 16 91 3c
```

Сертификат Корневого ЦС МГУ

```
X509 Certificate:
Version: 3
Serial Number: 7c7fbe295cb12abd48692c9fe8b17829
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=RootCA
    O=MSU
    C=RU
    DC=msu
    DC=su

NotBefore: 08.12.2006 15:54
NotAfter: 08.12.2011 15:59

Subject:
    CN=RootCA
    O=MSU
    C=RU
    DC=msu
    DC=su

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 b0 79 66 91 60 b4 c3
    0010  2b fd a2 61 9a be 2d eb  3c 99 e9 0b 6a 1c 2b 57
    0020  ae 7b f4 aa 60 63 c2 68  39 27 43 6d 53 8c 69 7a
    0030  52 d7 d7 17 64 62 25 d7  51 26 0e 23 31 05 3d 00
    0040  98 4d d1 af 74 ae b3 40  ce 84 22 1e 6b d1 2c 53
    0050  cc 54 c1 db 4f 04 63 a4  d5 ac 48 7a 29 ce 4b 3b
    0060  ae 75 a2 4d ad a3 5c 35  17 56 f8 fb d7 ed 0e 29
    0070  89 6c 8d d4 e6 a9 8f ee  03 0a f0 96 ee 31 d3 01
    0080  cb 2b 3f c9 c4 1a 5d 4e  89 1a 8d 3d cb bc a4 02
    0090  56 d5 6c a3 62 f4 f2 6c  72 67 e6 b8 19 10 58 56
    00a0  28 ff 04 66 03 13 0c 0b  15 38 e7 c5 9e 2f d3 df
    00b0  c8 10 7d 37 11 38 7a 7f  c7 fa fc d6 2a 9a 9a ba
    00c0  47 59 54 01 5d bc dc 44  65 4f 5d 18 7e 26 a3 a3
    00d0  1b db 4a ba 97 0e 34 c5  5f 5c dd eb 01 bd 41 82
    00e0  6a 84 a8 77 67 bf 31 ef  0f 40 63 47 29 53 f8 f9
    00f0  fc 40 2f a5 f8 a6 c0 5c  40 08 c9 97 f6 5a 07 ed
    0100  10 3a 0c fb 80 83 37 41  f3 02 03 01 00 01

Certificate Extensions: 5
    2.5.29.15: Flags = 0, Length = 4
    Key Usage
        Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        63 f1 16 2a 71 d5 cb f8 5f 88 cc ff 0d 68 ca 50 ed 8e be 3a

    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V0.0

    2.5.29.32: Flags = 0, Length = 14a
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.2.643.3.65.1
             [1,1]Policy Qualifier Info:
```

```
                    Policy Qualifier Id=CPS
                    Qualifier:
                         http://msca.msu.su/public/rfc3647.htm
               [1,2]Policy Qualifier Info:
                    Policy Qualifier Id=User Notice
                    Qualifier:
                         Notice Text=Moscow State University General Legal Policy Statement.
          [2]Certificate Policy:
               Policy Identifier=1.2.643.3.65.2
               [2,1]Policy Qualifier Info:
                    Policy Qualifier Id=User Notice
                    Qualifier:
                         Notice Text=Moscow State University Limited Use Policy Statement.

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  b6 62 21 97 1f cb 13 c9  98 ef 03 93 08 4a 2b 2d
    0010  89 51 3d d8 03 b1 80 43  f5 e3 7e 49 8a f0 19 3e
    0020  8e 17 13 b2 ba d3 1a 53  a7 df 2f 08 2d 03 ba 50
    0030  3a 70 0c 78 7f 39 9d a8  d1 f2 aa 49 03 1c 01 81
    0040  ee 4c af 59 c3 26 9d 14  a7 07 45 5a 0b 38 10 3f
    0050  50 fc 19 6b d5 1c 91 dc  cd 87 95 9c 41 a5 9e 18
    0060  84 6a cf 30 27 7c 52 e9  78 ef e2 17 8c 0a df 50
    0070  82 0e e7 f8 e1 57 e2 1c  b4 6b 05 2b 8c 30 c6 20
    0080  e4 a4 88 3d 35 57 9a 76  04 fe 9c d7 2c 3a d0 85
    0090  bb 92 ca f9 7b c2 29 ea  c7 22 f0 97 07 5e 2e 71
    00a0  f5 12 07 2f c1 24 b5 a5  a7 55 d3 c2 33 1b 9b fd
    00b0  8a aa 88 56 cb 12 de a6  9e cf f4 31 32 4a e7 32
    00c0  8b df 06 38 45 31 68 60  1a f6 a2 7d e6 74 03 0b
    00d0  21 ce 68 a1 4b 0e 31 a1  04 7e fe 9d 38 52 0e 28
    00e0  85 03 35 42 bd de be fe  38 4c 99 44 fd 65 23 c8
    00f0  d4 3a b2 46 88 c8 28 7a  b6 cd af 5c 9e 62 37 51
```

Файл конфигурации CAPolicy.inf Корневого ЦС МГУ

```
[Version]
Signature= "$Windows NT$"

[PolicyStatementExtension]
Policies = MSULegalPolicy, MSULimitedUsePolicy
Critical = 0

[MSULegalPolicy]
OID = 1.2.643.3.65.1
URL = "http://msca.msu.su/public/rfc3647.htm"
Notice = "Moscow State University General Legal Policy Statement."

[MSULimitedUsePolicy]
OID = 1.2.643.3.65.2
Notice = "Moscow State University Limited Use Policy Statement."

[AuthorityInformationAccess]

[CRLDistributionPoint]

[basicconstraintsextension]
criticaL=true

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=0x18
RenewalValidityPeriod=years
CRLPeriod = days
CRLPeriodUnits = 2
CRLDeltaPeriod = hours
CRLDeltaPeriodUnits = 4
```