

# Установка цепочки серверов сертификации как часть внедрения PKI в домене

## Часть 2

Станислав Шпак

В первой части статьи мы говорили о типах центров сертификации (Certificate Authority, CA), их операционных параметрах и рассматривали установку и настройку корневого сервера сертификации. Сегодня мы займемся установкой промежуточного и выпускающего CA – для них процесс имеет свои особенности, которые надо учитывать при развертывании всей цепочки серверов.

### Установка промежуточного CA (SubCA)

Так же, как и корневой, этот CA является изолированным, поэтому не должен быть членом домена. Убедитесь, что вы окончательно определились с именем сервера (в нашем случае это SubCA), поскольку после установки служб сертификации изменить его будет также нельзя. Несмотря на то что промежуточный CA является подчиненным по отношению к корневому и наследует многие параметры, нам все равно потребуются перед установкой подготовить файл `capolicy.inf` и поместить его в `%Systemroot%`. Сделать это необходимо для того, чтобы позволить промежуточному CA использовать политики выпуска сертификатов (issuing policies). По умолчанию такая возможность отсутствует. Поэтому содержимое файла будет несколько отличаться

от того, который использовался для установки корневого CA.

В первой части статьи было сказано, что промежуточный CA используется, в частности, для назначения операционных политик. В сертификатах конечных субъектов политика указывает на условия, при которых сертификат был выпущен, и на цели, для которых он может быть использован. Вы можете задавать для различных CA различные политики выпуска сертификатов, которые определяются посредством их OID (object identifier). OID представляет собой серию разделенных точками чисел, например 2.5.29.32.0, и используется для однозначной идентификации объекта в каталогах, организуемых в соответствии с международными рекомендациями X.501, которые регламентируют построение каталогов при взаимодействии открытых систем. Свой OID для предприя-

тия нужно регистрировать, если возникает необходимость занесения в сертификаты открытых ключей сведений о правовых отношениях, при которых электронный документ имеет юридическую силу. Зарегистрировать свой OID можно или на сайте [iana.org](http://iana.org) (при этом OID вашей организации будет начинаться на 1.3.6.1.4.1) или обратиться в ЗАО «Центральный телеграф», который является регистрирующей организацией для российской ветви международных идентификаторов объектов (OID префикс 1.2.643). Примечательно, что на сайте телеграфа я не нашел упоминания о такой услуге, однако по ссылке из [1] можно найти нужные контакты. Список уже зарегистрированных в российской ветке OID можно посмотреть по той же ссылке. Кроме того, существуют и зарезервированные (или «общие») OID (как в примере выше).

Несмотря на то что в нашем примере мы не будем использовать никаких операционных политик, все же надо разрешить промежуточному CA обрабатывать политики выпуска сертификатов, чтобы можно было в дальнейшем применять их на нижележащих CA в случае необходимости. Для этого существует политика с OID=2.5.29.32.0. Поэтому наш файл `carpolicy.inf` будет выглядеть следующим образом:

```
[Version]
Signature= "$Windows NT$"
[PolicyStatementExtension]
Policies = AllIssuancePolicy
Critical = FALSE
[AllIssuancePolicy]
OID = 2.5.29.32.0
```

Если вы обратитесь к первой части статьи [1] и посмотрите на рисунок 2 (пример самоподписанного сертификата корневого CA), то в информации о сертификате в разделе «This certificate is intended for the following purpose(s):» (этот сертификат предназначен для следующих целей) можно увидеть два пункта: All issuance policies и All application policies. Корневой CA всегда выпускает сертификат, который разрешает применение операционных политик; вышеприведенный текст файла `carpolicy.inf` позволяет сделать это и для подчиненного CA.

Для установки служб сертификации нам потребуется сертификат корневого CA и его CRL. Их надо забрать с компьютера RootCA (напомню, что файл сертификата `RootCA_RootCA.crt` находится в папке `C:\CACConfig`, а файл `RootCA.crl` в папке `C:\WINDOWS\system32\CertSrv\CertEnroll`), перенести на компьютер SubCA и импортировать в локальное хранилище сертификатов. Импорт делается командой:

```
certutil -addstore -f Root RootCA_RootCA.crt
certutil -addstore -f Root RootCA.crl
```

Можно воспользоваться оснасткой Certificates (сертификаты). В меню «Администрирование» панели управления она отсутствует, и запустить ее можно, только добавив через консоль `mmc.exe`, выбрав при инициализации раздел «computer account» (учетная запись компьютера). Выбрав в дереве слева ветвь Certificates надо в меню «View → Options» («Вид → Параметры») в разделе Show the following (также показывать) включить опцию Physical certificate stores (физические хранилища). Затем раскрыть ветки «Trusted root certification authorities → Registry → Certificates» («Доверенные корневые центры сертификации → Реестр → Сертификаты»). Нажать в правом окне правую кнопку мыши, из контекстного меню выбрать «All Task → Import» («Все задачи → Импорт») и далее следовать указаниям мастера. В появившемся окне обратите внимание на тип отображаемых файлов. Получившийся результат представлен на рис. 1. Обратите внимание, что импортированный CRL тут

не отображается. Чтобы проверить его наличие в локальном хранилище, можно воспользоваться командой:

```
certutil -verifystore root
```

После перечисления хранящихся локально сертификатов идет перечисление CRL – там мы должны увидеть информацию о нашем CRL:

```
===== CRL 0 =====
Issuer:
  CN=RootCA
  DC=dedicated
  DC=root
CA Version: V0.0
CRL Number: CRL Number=4
CRL Hash(sha1): f8 ca 01 04 b7 fb 38 02 61 14 32 6f e3 84 19 04 97 12 52 eb
```

**Важно:** процедуру импорта нужно будет повторять каждый раз при обновлении CRL и сертификата вышестоящего CA.

Теперь можно приступить непосредственно к установке служб сертификации. Так же, как и для RootCA, сначала имеет смысл установить компоненты IIS и ASP.NET, чтобы иметь возможность в случае необходимости воспользоваться выпуском сертификатов через веб-интерфейс.

Установка во многом будет похожа на установку корневого CA. На первом шаге надо будет выбрать тип CA – в нашем случае это Stand-Alone Subordinate CA (изолированный подчиненный центр сертификации) – и установить опцию use custom setting to generate the key pair and CA certificate (использовать специальные параметры для генерации пары ключей и сертификата ЦС). На следующем шаге оставляем все без изменений, кроме длины ключа шифрования – его стоит выбрать в 2048 бит. В качестве имени CA на следующем шаге вводим имя SubCA, в поле Distinguished name suffix (суффикс отличительного имени) вводим информацию об операционном домене – в нашем случае это, так же как и для RootCA, будет DC=Dedicated,DC=Root. Обратите внимание, что поле Validity Period (период действия) затенено и в нем содержится Determined by parent CA (определяется вышестоящим CA). Шаг Certificate Database Setting (параметры базы данных для сертификатов) оставляем без изменений, а вот на следующем шаге мы должны решить, на какой CA отправлять запрос сертификата (ведь мы устанавливаем подчиненный CA) или же сохранить его в файл для дальнейшей ручной обработки. Поскольку и установ-

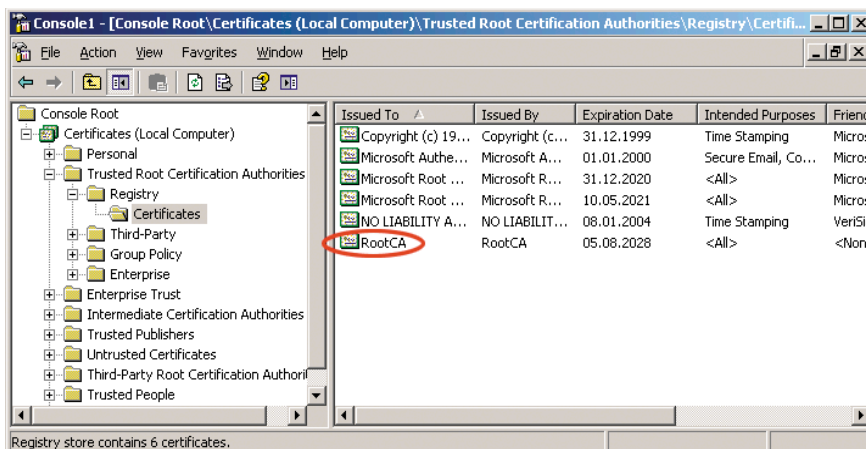


Рисунок 1. Сертификат корневого CA в локальном хранилище сертификатов

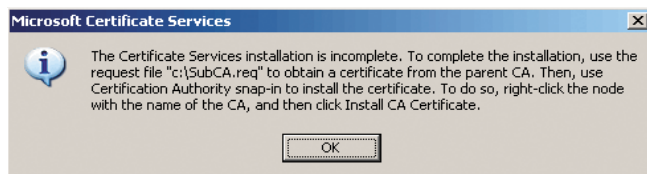


Рисунок 2. Сообщение с инструкциями для завершения процесса установки СА

ливаемый, и корневой СА предполагаются отключенными от сети, то мы выбираем второй вариант и сохраняем запрос в файл c:\SubCA.req. Нажав «Далее» и согласившись на временную остановку служб IIS, мы наблюдаем за установкой компонентов, которая оканчивается сообщением, представленным на рис. 2. В нем говорится о том, что установка не будет завершена до тех пор, пока по сохраненному в файле c:\SubCA.req запросу не будет выпущен сертификат родителем СА (в нашем случае это RootCA). Этот сертификат затем надо будет установить через оснастку Certification Authority (центр сертификации). Нажимаем «OK» и ждем окончания процесса.

Теперь открываем диск C:\ и видим там файл SubCA.req. Этот файл содержит запрос сертификата, и с ним можно поступить двумя способами:

- физически перенести на RootCA, где обработать через оснастку Certification Authority;
- скопировать из него данные запроса и воспользоваться веб-интерфейсом, если на корневом СА установлены службы IIS. Для этого на RootCA нужно в браузере открыть адрес <http://localhost/certsrv> и далее следовать указаниям на странице. Если для развертывания структуры вы пользуетесь виртуальными машинами и есть возможность сетевого взаимодействия, то можно открыть веб-страницу непосредственно с SubCA. Разумеется, заменив localhost на нужное имя.

Воспользуемся первым способом. Итак, переносим любым доступным способом файл запроса на RootCA и запускаем оснастку Certification Authority. Выбрав слева RootCA,

нажимаем на нем правой кнопкой мыши и выбираем «All Task → Submit new request» («Все задачи → Выдать новый запрос»). Далее открываем сформированный чуть выше файл запроса и переходим в ветку Pending Request (запросы в ожидании) в левой части окна. При этом в правой части отображаются все запросы, ожидающие обработки. Поскольку наш СА – изолированный, то он не производит выпуск сертификатов автоматически – все запросы должны быть обработаны вручную. Поэтому в правой части окна на запросе надо нажать правую кнопку мыши и выбрать «All Tasks → Issue» («Все задачи → Выпустить»). Тем самым мы выпускаем сертификат, запрос исчезает из ветки Pending Request, а выпущенный сертификат помещается в ветку Issued certificates (выданные сертификаты). Перейдя в эту ветку в правой части, мы видим, что сертификат выпущен, нам остается теперь только просмотреть его (на предмет корректности срока действия), экспортировать и доставить на подчиненный СА. При просмотре сертификата перейдите на вкладку Details (состав) и нажмите внизу кнопку Copy to file (копировать в файл). Запустится мастер экспорта сертификата, в котором в качестве типа экспортируемого сертификата следует выбрать Cryptographic Message Syntax Standard – PKCS#7 Certificates (.P7B), установить опцию the Include all certificates in the certification path if possible (включить по возможности все сертификаты в путь сертификата), указать место, куда будет сохранен файл сертификата и его имя. В конце работы мастера в сводной информации обратите внимание на строку Export keys: No (экспорт ключей: нет). Это говорит о том, что файл сертификата не будет содержать закрытый ключ. Этот ключ сформирован и хранится на том СА, с которого получен файл запроса сертификата. Поэтому о безопасности файла сертификата можно не беспокоиться. Полученный файл теперь нужно перенести на SubCA, а RootCA можно выключить – он больше не понадобится до тех пор, пока не наступит время обновления CRL. На SubCA теперь надо запустить оснастку Certification Authority. Как видим, в дереве оснастки сервер SubCA помечен как неработающий, поскольку он пока еще не содержит собственного сертификата. Нажимаем

на нем правой кнопкой мыши и выбираем «All Tasks → Install CA certificate» («Все задачи → Установить сертификат ЦС»). Указываем файл с сертификатом, после чего можно из контекстного меню выбрать «All Tasks → Start service» («Все задачи → Запуск службы»). Если все прошло удачно, службы сертификации должны запуститься и в оснастке SubCA станет помечен зеленым значком.

На этом установку можно считать законченной. Но перед тем как начать использовать установленный СА, следует провести его конфигурирование. Процесс практически ничем не отличается от описанной в первой части статьи настройки корневого СА за исключением сроков: для подчиненного СА

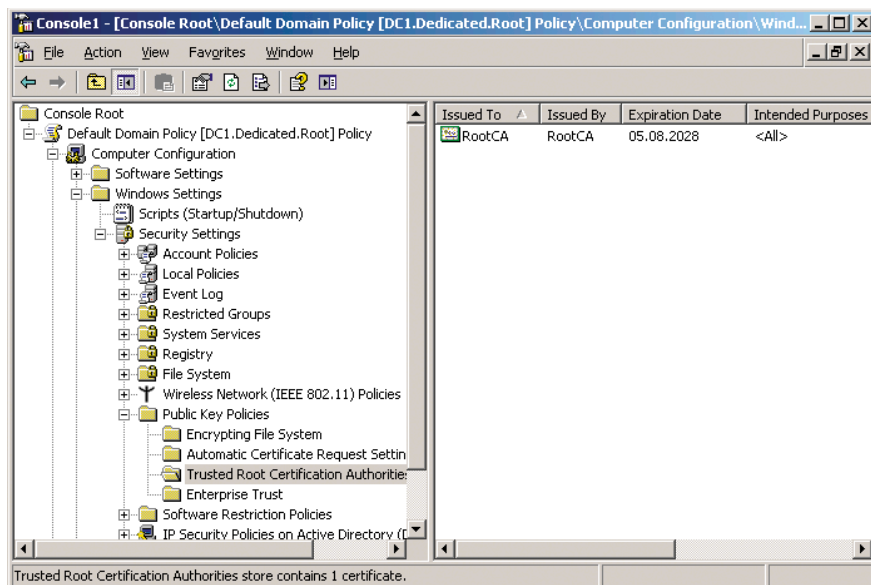


Рисунок 3. Распространение в домене сертификата корневого СА через групповую политику



можно задать несколько меньший интервал публикации CRL и в реестре значение ValidityPeriodUnits сделать равным 5, чтобы SubCA мог выдавать сертификаты со сроком действия в 5 лет. После завершения всех настроек не забудьте перезапустить службу сертификации на компьютере.

## Установка СА предприятия (EntCA)

Теперь мы подошли к конечному звену в цепочке серверов сертификации. До сих пор никаких изменений в Active Directory сделано не было, и еще есть возможность безболезненно что-то поправить. Это будет весьма сложно после того, как мы закончим установку СА предприятия и он начнет функционировать. Надо также иметь в виду то, что с появлением корпоративного сервера сертификации поведение контроллеров домена при различных режимах функционирования домена Windows 2000 и Windows 2003 отличается. В первом случае контроллеры домена автоматически начинают пытаться получить сертификат контроллера домена, а во втором – подчиняются настройкам групповой политики, в которой по умолчанию автоматическое получение сертификата контроллера домена отключено.

Перед установкой служб сертификации компьютер должен быть членом домена, желательно, чтобы это был корневой домен и компьютер имел статический IP-адрес, а служба доступа к файлам и принтерам была включена. Если домен работает под управлением Windows 2000, на контроллерах домена должен быть установлен Service Pack 3 и, кроме того, потребуется сделать апгрейд схемы до уровня функциональности Windows Server 2003. Настоятельно не рекомендуется размещать службы сертификации на компьютере, уже выполняющем какие-либо функции в домене – например, на файловом сервере или контроллере домена. Установка выполняется из-под учетной записи пользователя, имеющего права Enterprise Admin. Для установки потребуются сертификаты и файлы CRL с вышележащих СА. Как их получить, было рассмотрено в предыдущем разделе.

Сначала надо распространить в домене сертификат корневого СА. Члены домена затем автоматически добавят его в локальное хранилище доверенных сертификатов. Во время установки SubCA мы это делали вручную, в домене же можно воспользоваться доменными политиками. Обратите внимание на то, что здесь требуется лишь сертификат корневого СА, а не промежуточного. Чтобы сделать это, в том домене, где будет впоследствии установлен СА предприятия, откройте доменную политику по умолчанию (Default Domain Policy). Раскройте последовательно узлы: «Default Domain Policy → Computer Configuration → Windows Settings → Security Settings → Public Key Policies» («Политика Default Domain Policy → Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики открытого ключа»). Щелкните правой кнопкой мыши на Trusted Root Certification Authorities (доверенные корневые центры сертификации) и выберите Import (импорт). С помощью мастера импортируйте сертификат корневого СА, который должен появиться в списке справа (см. **рис. 3**).

Как вы помните, на этапе конфигурирования корневого и подчиненного СА мы задавали точки распространения CRL и AIA. Если посмотреть на рисунок 3 в первой

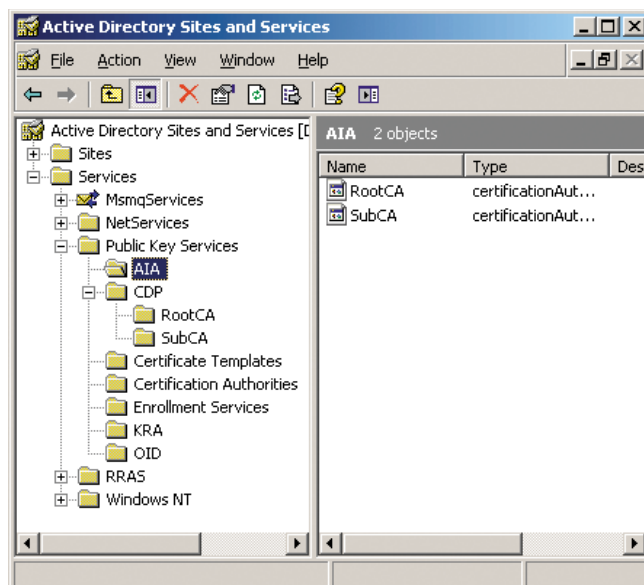


Рисунок 4. Сертификаты вышестоящих СА и их CRL импортированы в Active Directory

части статьи, то видно, что в качестве таковых мы использовали LDAP-точку и общую папку. Теперь надо позаботиться, чтобы в этих точках были доступны сертификаты СА и файлы с CRL (файлы RootCA\_RootCA.crt, RootCA.crl, SubCA\_SubCA.crt, SubCA.crl).

Начнем с более простого – с общей папки. На компьютере EntCA создаем папку с именем CDP, помещаем в нее вышеназванные файлы и открываем ее для общего доступа. Причем уровень доступа должен разрешать чтение для группы Everyone (все) (не забывая и про NTFS-разрешения тоже).

Импорт этих файлов в Active Directory проводится с помощью команды certutil.exe с компьютера EntCA следующим образом:

```
certutil -dspublish -f RootCA RootCA.crt RootCA
certutil -dspublish -f SubCA SubCA.crt SubCA
certutil -dspublish -f RootCA.crl RootCA RootCA
certutil -dspublish -f SubCA.crl SubCA SubCA
```

Разумеется, команды выполняются из той папки, где находятся файлы сертификатов и CRL. Обратите внимание, что в первых двух командах последний параметр RootCA и SubCA обозначают хранилище и совпадение с именами компьютеров случайно. Во вторых двух командах параметры RootCA RootCA и SubCA SubCA обозначают соответственно имя компьютера СА и короткое имя СА (CA sanitized name). В нашем случае эти имена совпадают, а узнать их можно с помощью команды:

```
certutil.exe -cainfo
```

выполненной на соответствующем СА.

Чтобы убедиться, что импорт прошел успешно, можно открыть оснастку Active Directory Sites and Services (Active Directory – сайты и службы), в меню View (вид) включить пункт Show Services Node (показать узел служб) и в дереве слева развернуть узел «Services → Public Key Services». При этом в подразделе AIA должны содержаться сертифи-

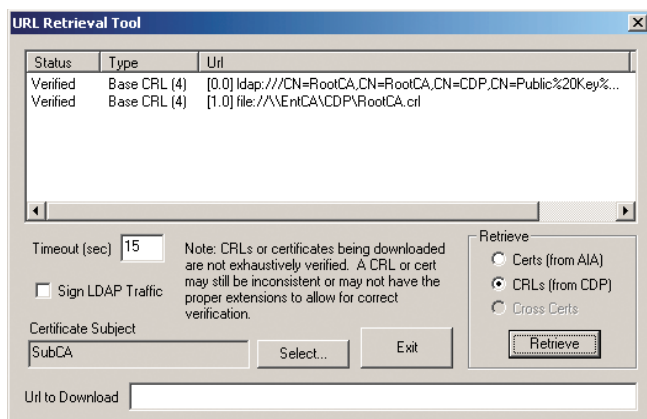


Рисунок 5. Проверка сертификата с помощью URL Retrieval Tool

каты родительских CA, а в подразделе CDP – созданы подпапки с именами, соответствующими корневому и подчиненному CA (см. рис. 4).

Теперь надо убедиться, что указанные в сертификате подчиненного CA точки CDP доступны. Для этого используется команда:

```
certutil.exe -url SubCA_SubCA.crt
```

По этой команде запустится графическое средство URL Retrieval Tool (инструмент извлечения URL) (см. рис. 5). В поле Retrieve (загрузить) выбираем, что мы хотим проверить – доступность сертификата (из AIA) или доступность CRL (из CDP), и нажимаем кнопку Retrieve (загрузить). Если все в порядке, то в верхнем поле должен появиться статус Verified (проверено) напротив каждой из указанных в сертификате AIA или CDP. Если в каком-то поле появится статус Failed (ошибка), то надо принять меры. Например, если у вас файл сертификата называется SubCA\_SubCA.crt, а происходит поиск файла SubCA.crt, то можно переименовать исходный файл.

На этом подготовительный этап завершен.

**Внимание!** Вышеприведенные процедуры должны будут повторяться по мере обновления сертификатов и CRL-файлов родительских CA.

Теперь можно приступить непосредственно к установке служб сертификации. Файл `capolicy.inf` нам не потребуется, так как мы не собираемся указывать для CA никаких операционных политик. Однако установка служб IIS и ASP.NET настоятельно рекомендуется для возможности проводить выпуск сертификатов посредством веб-интерфейса.

Процесс установки уже нам знаком. Обратите внимание, что теперь при выборе типа CA нам доступны все 4 типа, из которых мы выбираем Enterprise Subordinate CA (подчиненный ЦС предприятия) и, как и раньше, устанавливаем опцию `use custom setting to generate the key pair and CA certificate`. На следующем шаге выбираем желаемую длину ключа и не устанавливаем опцию `Allow this CSP to interact with the desktop` (если используете стандартный Microsoft CSP). Далее задаем имя нашему CA (EntCA) и обращаем внимание, что поскольку компьютер является членом домена, поле `distinguished name suffix` уже заполнено. На следующем шаге мы видим, что опция `stores configuration information in shared folder` (хранить информацию о конфигурации в об-

щей папке) не выбрана. Она нужна в случае, если клиент не может получить сертификат через групповую политику или веб-интерфейс. Поскольку у нас на этом сервере уже есть общая папка, то на всякий случай имеет смысл указать ее в качестве места хранения конфигурационной информации. На следующем шаге сохраняем запрос сертификата в файл `EntCA.req` и завершаем установку.

Теперь мы должны вручную выпустить сертификат для нашего корпоративного CA по файлу запроса. Процедура полностью идентична рассматриваемой выше, только запрос должен быть обработан не на корневом CA, а на подчиненном (SubCA). В результате мы должны получить файл сертификата для EntCA и установить его. Перед установкой имеет смысл проверить файл сертификата командой:

```
certutil.exe -url <имя файла сертификата>
```

Конфигурирование CA практически идентично тому, что мы делали ранее. Необходимо задать точки распространения CRL и AIA, выбрать период публикации CRL и определиться, нужны ли нам delta-CRL. При выборе интервалов публикации для CRL стоит вспомнить о рекомендациях, которые давались по этому поводу в первой части статьи. В качестве точек публикации CRL и AIA задаются те же самые места, что и в CA уровнями выше, однако следует задать еще одно расположение, которое будет совпадать с местом `\\EntCA\CDP`, но указывать на него локально. То есть если папка CDP лежит в корне диска C, то вариант точки публикации будет следующим:

```
C:\CDP\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
```

При этом для этого расположения надо сбросить все опции, кроме `Publish CRL in this location` (опубликовать CRL по данному адресу). Поскольку CRL публикуются автоматически, мы избавляем себя от необходимости вручную перекладывать каждый раз новый CRL из папки `CertEnroll` в папку `C:\CDP`.

По умолчанию CA будет выпускать сертификаты сроком действия в 1 год, и изменять это положение не нужно. После того как вы сделаете все необходимые настройки и перезапустите службы сертификации, CA будет готов к работе и обслуживанию клиентов. Если вы работаете в домене под управлением Windows 2000, то контроллеры домена автоматически получают сертификат, как только обнаружат присутствие центра сертификации в домене, для домена Windows 2003 ничего не произойдет.

В последней части статьи мы рассмотрим, как настроить доменные политики на запрос сертификатов и как настраивать шаблоны сертификатов на корпоративном CA. Кроме того, в заключение немного поговорим о типичных проблемах, которые могут возникнуть во время процесса установки всей цепочки и вариантах их решения. ●

1. Шлак С. Установка цепочки серверов сертификации как часть внедрения PKI в домене. Часть 1. // «Системный администратор», №8, 2008 г. – С. 54-58.
2. Российский сегмент мирового пространства идентификаторов объектов – <http://www.tel-inform.ru/x500/OIDS/inform.htm>.