

Установка цепочки серверов сертификации как часть внедрения PKI в домене

Часть 1

Станислав Шпак

Электронные подписи, шифрование данных, IPSec, вход в систему по смарт-картам, и все это с использованием цифровых сертификатов – возможно практически в любом домене. Нужно лишь спланировать и внедрить инфраструктуру открытого ключа. А установка серверов сертификации – наиболее важная часть этого процесса. От того, как вы проведете ее, зависит бесперебойность работы всей инфраструктуры PKI в целом.

Инфраструктура открытого ключа (Public Key Infrastructure) не является жизненно необходимой для работы домена. Вы можете годами не внедрять ее на предприятии и не испытывать никаких проблем. Но когда вы начинаете задумываться о безопасности, о тех возможностях, которые дает внедрение PKI, то рано

или поздно вы придете к идее развернуть ее в масштабах поддерживаемого вами домена. PKI – это комбинация из ряда совместно работающих служб и компонентов. Одним из ключевых является центр сертификации (Certificate Authority – CA) – доверенный субъект или служба для выдачи и управления цифровыми сертификатами. В сети

Microsoft Windows центром сертификации становится компьютер с серверной операционной системой, на котором установлены и запущены службы сертификации (Certificate Services). В статье будут рассматриваться CA, работающие на Windows 2003 Server.

Microsoft рекомендует тщательно спланировать PKI, прежде чем при-

ступать к действиям по развертыванию компонентов. Что касается СА, то нужно решить, будет ли использоваться только свой собственный центр сертификации либо же придется прибегать к услугам и открытым (публичным) СА, таких как VerySign. Особую роль имеет планирование расположения, количества и типа СА. Существует два основных типа СА: СА предприятия (enterprise CA) и изолированный СА (stand-alone CA). В свою очередь они подразделяются на два подтипа: корневой (root) и подчиненный (subordinate). Тип СА определяет, где хранится база сертификатов (локально или в Active Directory), как издаются сертификаты (автоматически по шаблонам или вручную) и т. п. Кроме того, издающим (issuing) называется СА, который обрабатывает запросы конечных пользователей.

Выбор структуры СА

Необходимо спланировать многоуровневую структуру СА. Теоретически возможно использование одного центра сертификации одновременно в качестве корневого СА предприятия и издающего одновременно, но такая конфигурация настоятельно не рекомендуется как из соображений безопасности, так и из соображений дальнейшей масштабируемости.

Microsoft рекомендует использовать число уровней СА от 2 до 4: использование более глубокой структуры становится трудным в управлении.

Можно назвать «классической» схему из трех уровней СА (см. рис. 1):

- первый уровень: изолированный корневой СА;
- второй уровень: изолированный подчиненный СА (еще он называется промежуточным, (intermediate), или policy СА);
- третий уровень: подчиненный СА уровня предприятия, он же выпускающий СА.

Развертывание именно такой структуры и будет рассматриваться в этой статье. Что она дает: изолированный СА первого уровня (RootCA) выпускает самоподписанный сертификат сам себе и используется в качестве корня структуры. Изолированный подчиненный СА второго уровня (SubCA) получает сертификат от корневого СА

и используется, во-первых, для усиления безопасности всей структуры, а во-вторых, в случае, когда на втором уровне больше чем один СА, для назначения различных операционных политик или политик безопасности для СА нижних уровней. В рассматриваемой схеме введение промежуточного второго уровня не является обязательным и используется с целью приведения к «классическому» виду и для возможности масштабируемости в дальнейшем. По рекомендации Microsoft из соображений безопасности, СА первых двух уровней должны быть изолированы от сети, а после установки и первичной настройки – храниться в надежном, защищенном от доступа посторонних месте в выключенном состоянии. Выполнению этого требования может помочь применение виртуальных машин – использование VMware или Virtual Server идеально подходит как для обеспечения безопасности на этапе развертывания инфраструктуры, так и для последующей физической изоляции серверов.

И наконец, подчиненный СА уровня предприятия (EntCA) получает сертификат от промежуточного СА, находится в домене Active Directory и выпускает сертификаты по запросам конечных пользователей либо в ручном, либо в автоматическом режиме по шаблонам (рекомендуется). Для отказоустойчивости нужно иметь как минимум два выпускающих СА на каждый промежуточный СА, однако мы будем рассматривать установку только одного сервера.

Определение функциональных параметров для СА

Когда структура СА определена, нужно учесть еще ряд важных параметров, влияющих на работу каждого из СА. К таковым параметрам относятся:

- **Срок жизни сертификатов.** Здесь надо учитывать баланс между соображениями безопасности (меньший срок действия) и соображениями легкости обслуживания (большой срок действия). Мы выберем для сертификатов корневого СА срок действия 20 лет, для подчиненного СА – 10 лет, выпускающего СА – 5 лет и для сертификатов пользователей – 1 год.

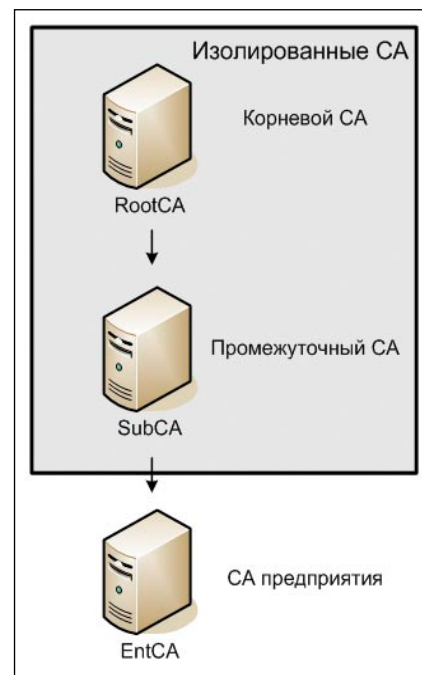


Рисунок 1. Структура из трех СА

Списки отзыва сертификатов и интервал их публикации.

В случае если сертификат стал ненужным или недействительным до истечения срока его жизни, его можно отозвать вручную (пометить как недействительный). При этом его номер попадает в список отзыва (Certificate Revocation List – CRL). Этот список должен периодически обновляться и быть всегда доступным для проверки. Когда приложение проверяет действительность сертификата, происходит не только проверка даты и срока действия сертификата, но и отсутствие его номера в списке отзыва. Сертификат считается недействительным, если его номер содержится в CRL либо CRL недоступен. Список отзыва кэшируется на стороне клиента и обновляется в соответствии с временем жизни CRL, поэтому возможны ситуации, когда сертификат отозван, опубликован в CRL, но какое-то время еще может считаться действительным. Это надо учитывать при определении интервала публикации CRL. Для выпускающего СА интервал оставим по умолчанию в 1 неделю, для промежуточного – 3 месяца, для корневого – полгода. Для самоподписанного сертификата корневого СА этот параметр неприменим.

■ **Сведения о доступе к CA (Authority Information Access – AIA).** В точке публикации AIA располагается сертификат CA, который также должен быть доступен для клиента. Клиент использует сертификаты CA как часть проверки действительности сертификата.

После выбора предполагаемых рабочих параметров каждого из CA можно перейти непосредственно к их установке. Надо иметь в виду, что имя компьютера и доменную принадлежность после установки служб сертификации менять уже будет нельзя. В качестве доменного окружения будем рассматривать лес, состоящий из одного дерева и двух доменов. Домен Dedicated.Root представляет собой корневой домен, домен Res.Dom – дочерний (ресурсный). Службы сертификации на третьем уровне будем разворачивать на компьютере EntCA – члене домена Dedicated.Root.

Установка корневого CA

Поскольку корневой CA будет изолированный, то перед установкой убедитесь, что компьютер не включен в домен, а также имеет имя, которое впоследствии не планируется менять – в нашем случае RootCA.

Далее надо подготовить специальный файл capolicy.inf, который должен быть помещен в %Systemroot%. Наличие этого файла для установки корневого CA очень важно, поскольку в нем задаются все исходные параметры для CA. Более того, мастер установки служб сертификации не только не пре-

дупредит вас об отсутствии этого файла, но и не будет проверять его корректность.

Отсутствие файла capolicy.inf или его неправильное конфигурирование приведет к тому, что CA будет установлен с параметрами по умолчанию, поскольку для него нет родительского CA, от которого можно было бы их унаследовать. Изменить некоторые из них после установки будет невозможно, и, как следствие, придется переустанавливать службы сертификации заново. Это не так страшно, пока CA единственный в структуре, но практически невыполнимо после развертывания CA нижележащих уровней.

Значения параметров в разделе [Certsrv_Server] должны быть не меньше, чем те, которые будут запрашиваться мастером установки.

Как уже было сказано, корневой CA издает самоподписанный сертификат, который не имеет списка отзывать. Поэтому очень важно разделы [CRLDistributionPoint] и [AuthorityInformationAccess] указать в явном виде и оставить пустыми.

В итоге у нас получается вот такое содержимое файла capolicy.inf:

```
[Version]
Signature= "$Windows NT$"
[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
[CRLDistributionPoint]
[AuthorityInformationAccess]
```

Также перед установкой служб сертификации имеет смысл установить службы Internet Information Services и поддержку ASP.NET. Для работы корневого и промежуточного CA их наличие совсем не обязательно, но это может несколько облегчить дальнейший выпуск сертификатов для CA нижних уровней, несмотря на то что почти все действия, доступные через веб-интерфейс, можно продублировать и через консоль управления службами сертификации.

Теперь можно открыть «Панель управления → Установка и удаление программ → Установка компонентов Windows» и выбрать Certificate Services (службы сертификации). Будет показано предупреждение о том, что после завершения установки изменить имя компьютера будет уже нельзя. Далее будет предложено сделать выбор типа

CA. Обратите внимание, что enterprise-типы CA будут недоступны (компьютер – не член домена). Выбираем Stand-Alone root CA, устанавливаем галку Use custom setting to generate the key pair and CA certificate и нажимаем «Далее». При этом на следующем шаге можно будет выбрать поставщика служб криптографии (Cryptographic Service Provider – CSP) (по умолчанию Microsoft), хэш-алгоритм и длину ключа. Для нашего типа CA выберем длину ключа в 4096 бит, остальные параметры оставим без изменений (параметр Allow this CSP to interact with the desktop нужен, например, при использовании смарт-карт).

На следующем шаге нас попросят указать имя нашего CA и отличительное имя (distinguished name). В последнем случае надо указать правильное имя по отношению к контексту Active Directory, несмотря на то что этот CA не является CA уровня предприятия. Итак, в качестве имени CA используем RootCA, в качестве отличительного имени вводим DC=dedicated, DC=root. Значение Validity Period указывает на время жизни сертификата. Как было указано выше, срок службы для корневого CA сделаем равным в 20 лет. Далее происходит генерация криптоматериала, и нужно немного подождать окончания этого процесса.

Заключительным шагом является указание расположения файлов баз данных сертификатов, журналов регистрации и общей папки для расположения информации, требуемой для клиентов (по умолчанию это C:\CACConfig). Несмотря на то что это изолированный CA, все равно локальная папка будет создана и, в случае наличия сетевого интерфейса, открыта для общего доступа.

Проверка и настройка RootCA

Поскольку корневой CA является отправной точкой для всей цепочки CA, очень важно внимательно проверить и сконфигурировать его. Первое, что необходимо сделать, это просмотреть сертификат, который CA выдал сам для себя (см. рис. 2). Это можно сделать, заглянув в папку C:\CACConfig. Там уже должен лежать файл <имя_сервера>_<имя_CA>.crt. В нашем случае это файл RootCA_RootCA.crt.

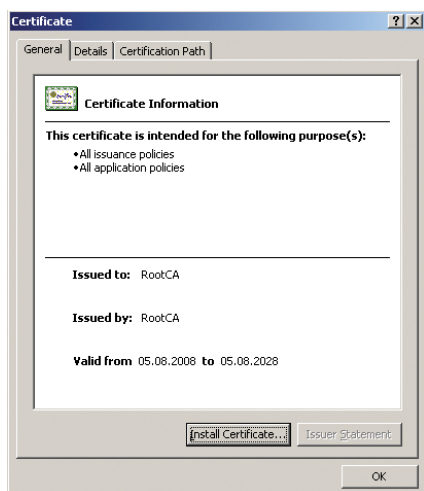


Рисунок 2. Самоподписанный сертификат корневого CA

Что должно быть в сертификате:

- **на вкладке General:** значения полей Issued by и Issued to должны совпадать и указывать на только что установленный CA (в нашем случае это RootCA). Диапазон времени, в течение которого сертификат считается действительным, должен быть верен и соответствовать тому, что задавали при установке;
- **на вкладке Details:** в перечне атрибутов сертификата должны отсутствовать атрибуты CRL Distribution Points и Authority Information Access;
- **на вкладке Certification Path:** в нижнем поле должна быть надпись This certificate is OK.

Посмотреть сертификат можно и другим методом – воспользоваться оснасткой Certification Authority, которая доступна в разделе Administrative Tools панели управления.

После ее запуска должно автоматически произойти подключение к текущему серверу, при этом в дереве слева он должен быть помечен зеленой галочкой. Щелкнув на нем правой кнопкой мыши и выбрав Properties на вкладке General, можно обнаружить кнопку View Certificate. Этот метод лучше, так как сразу позволяет убедиться в том, что службы сертификации успешно запустились, иначе возникла бы ошибка подключения к CA. К тому же именно тут мы и продолжим конфигурирование CA и перейдем к указанию точек распространения CRL и AIA.

Напомню еще раз про важность CRL для проверки действительности сертификата. Задать точки распространения CRL (CRL Distribution Points – CDP) можно перейдя на вкладку Extensions (Расширения) в окне свойств CA. Выпадающий список в верхней части окна содержит всего два параметра: CRL и AIA. Оставим предложенный по умолчанию CRL и обратимся к следующему полю, где перечислены места расположения для CRL.

Здесь надо быть очень осторожным – во-первых, указанные тут точки распространения CRL могут включать во все издаваемые этим CA сертификаты. То есть теоретически возможно изменить или дополнить этот список и после того, как CA начнет работать, на практике же это будет означать не-

обходимость перевыпустить все сертификаты, которые были выпущены до того, как этот список изменился.

Во-вторых, недоступность CRL означает недействительность сертификата, поэтому надо предусмотреть как минимум два разных места расположения CRL.

В-третьих, не рекомендуется оставлять в списке неиспользуемые точки распространения.

В-четвертых, порядок просмотра CDP тоже важен – первыми в списке должны быть те точки, которые смогут обслуживать больше всего клиентов и быть доступными как можно чаще. Хорошим решением считается расположение одной из CDP на корпоративном сайте, с тем чтобы она была доступна из Интернета.

Если посмотреть на предлагаемые по умолчанию варианты, то без труда можно сделать вывод, что в качестве CDP может выступать: Active Directory, локальная файловая система, UNC-путь и http-путь. Каждый из этих вариантов имеет свои плюсы и минусы. Например, как уже было сказано, http удобно использовать когда требуется обеспечить доступ к CRL клиентов снаружи корпоративной сети. Active Directory удобна внутри сети, но нужно учитывать интервалы репликации AD и публикации CRL – если CRL публикуется чаще, чем время полной репликации внутри домена, то использовать AD не рекомендуется.

Кроме того, к каждой из CDP можно указать дополнительные опции:

- **Publish CRL in this location** – указывает на то, что CA будет автоматически пытаться произвести публикацию CRL в этой точке. Для изолированного CA эту опцию стоит устанавливать только для локальной CDP;
- **Include in all CRLs** – активно только для LDAP CDP;
- **Include in CRLs** – добавляет эту CDP к атрибутам CRL, для того чтобы клиенты могли находить delta-CRL (об этом чуть ниже);
- **Include in the CDP extension of issued certificates** – указывает на необходимость включения этой CDP в список атрибутов выпускаемых этим CA сертификатов;
- **Publish delta CRLs to this location** – для публикации delta-CRL.

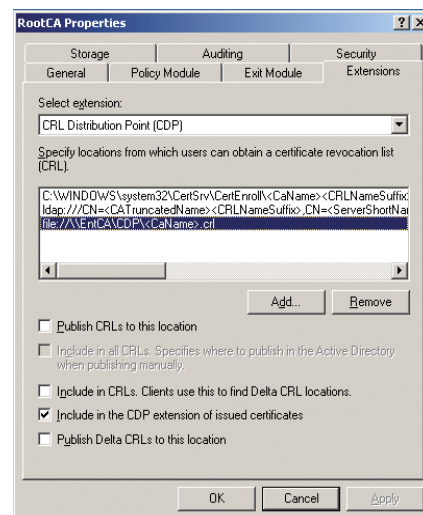


Рисунок 3. Задание CDP на корневом CA

Delta-CRL относится к новшествам, появившимся в Windows 2003 Server (и, кстати, не поддерживающимся клиентами ниже Windows XP). Если вы ожидаете активного использования сертификатов и их частых отзывов, то вам нужно устанавливать более частый интервал обновления CRL. При этом сам список отзывов будет все более и более увеличиваться в размерах, что может затруднять его загрузку клиентами. В таких случаях можно использовать delta-CRL для минимизации трафика. Клиент загружает сам список CRL и до истечения его срока действия загружает изменения, произошедшие в CRL после его публикации.

Таким образом, можно делать интервал публикации CRL более длинным, а delta-CRL публиковать чаще. Однако это имеет смысл делать только на выпускающем CA и только при вышеназванных условиях, поэтому для данного и последующих CA везде отключаем опции, связанные с delta-CRL.

Вернемся к заданию точек распространения CRL. Поскольку наш CA будет отключен от сети, то необходимо оставить локальную точку распространения, которая идет в списке первой и по умолчанию указывает в папку C:\WINDOWS\system32\CertSvc\CertEnroll. Обратите внимание, что для этой CDP помечена опция Publish CRL in this location. Для обеспечения доступности CRL мы оставим также LDAP-точку (указав опции Include in all CRLs и Include in the CDP extension of issued certificates) и создадим новую точку,

