Внедрение служб сертификации

Лаштанов И.Г.

Общие сведения о сертификатах

Сертификат (цифровой сертификат, сертификат открытого ключа) представляет собой цифровой документ, подтверждающий соответствие открытого ключа объекту. Основное назначение сертификатов — гарантировать, что открытый ключ, содержащийся в сертификате, действительно принадлежит объекту, указанному *к* сертификате. Сертификаты играют главную роль в инфраструктуре открытого ключа.

Сертификат может состоять из открытого ключа, подписанного доверенным объектом. Наиболее широко используемые структура и синтаксис цифровых сертификатов определены в документе ITU-T Recommendation X.509. На рис. 13-2 показан сертификат, используемый для проверки подлинности отправителя сообщения электронной почты.

- Сертификат X.509 содержит информацию, определяющую пользователя, организацию, выпустившую сертификат, серийный номер сертификата, срок его действия, ими и подпись запрашивающей стороны и имя субъекта (или польюватсля). В качестве субъекта могут выступать физическое лицо, школа, коммерческая или другая организация, *в* том числе ЦС.

Служба сертификации, интегрированная с Active Directory с распределенной службой безопасности

Создание сертификата

Сертификаты изготавливаются центром сертификации, который может быть любой доверяемой службой или объектом, желающим проверить подлинность того, для кого сертификат выпушен, и его связь с конкретным ключом. Компании вправе выпускать сертификаты для своих работников, школы — для своих учащихся, и т. п. Необходимо, чтобы достоверность открытого ключа центра сертификации была полностью определена, иначе не будет доверия к выпускаемым им сертификатам. Так как UC может создать кто угодно, степень доверия к нему определяется степенью доверия к организации, выдавшей ему ключ. Ниже описаны шесть этапов процесса запроса и выпуска сертификата.

Этапы процесса запроса и выпуска сертификата

1. Генерация пары ключей. Претендент генерирует пару из открытого и закрытого ключа или назначает автора пары ключей из своей организации.

2. Сбор требуемой информации. Претендент собирает всю информацию, необходимую ЦС для выдачи сертификата. Она может включать адрес электронной почты претендента, свидетельство о рождении, отпечатки пальцев или другие нотариально заверенные документы, подтверждающие подлинность претендента. ЦС со строгими идентификационными требованиями выпускают сертификаты с высокой степенью доверия. О самих ЦС говорят, что они имеют высокую, среднюю или низкую степень доверия.

3. Запрос сертификата. Претендент посылает в ЦС запрос на сертификат, состоящий из своего открытого ключа и необходимой дополнительной информации. Запрос на сертификат может быть зашифрован с использованием открытого ключа ЦС. Запросы разрешается посылать по электронной почте, посредством обычной почты или курьерской службы, например при необходимости нотариального заверения самого запроса.

4. Проверка информации. Чтобы удостовериться в том. что претендент получит сертификат, ЦС применяет любые необходимые правила политик. В соответствии с идентификационными требованиями политика и процедуры верификации ЦС влияют на степень доверия выпускаемых им сертификатов.

5. Создание сертификата. ЦС создает и подписывает цифровой документ, содержащий открытый ключ претендента и другую необходимую информацию. Подпись ЦС подтверждает привязку имени субъекта к его открытому ключу. Подписанный документ и является сертификатом.

6. Отправка или рассылка сертификата**.** ЦС отправляет претенденту сертификат или помещает его в каталог.

Классы центров сертификации

Службы сертификации предусматривают два варианта политик, разрешающих использование двух классов ЦС: корпоративного и изолированного. В каждый класс входят два типа ЦС: корневой и подчиненный. Модули политики определяют изменяемый при необходимости порядок действий, предпринимаемый ЦС при получении запроса на сертификат.

ЦС организованы иерархически: наиболее доверенный ЦС находится ближе к вершине. Windows 2000 PKI поддерживает иерархическую модель ЦС. В ней может быть множество не связанных между собой иерархий. Совместное использование всеми ЦС общего родителя верхнего уровня не требуется.

Корпоративный ЦС

На предприятии корневые ЦС обладают самой высокой степенью доверия. В домене Windows 2000 может быть несколько корпоративных корневых ЦС. но только одному из них разрешено основать иерархию. Остальные являются корпоративными подчиненными ЦС.

Организация устанавливает корпоративный ЦС для выдачи сертификатов своим пользователям или компьютерам. Нет необходимости устанавливать ЦС в каждом домене организации. Например, пользователи дочернего домена могут обратиться к ЦС в родительском домене. Модуль политики корпоративного ЦС предписывает порядок обработки и выпуска сертификатов. Необходимая этим модулям информация о политике хранится централизованно в Windows 2000 Active Directory.

Изолированный ЦС

Организация, которая предполагает выпускать сертификаты для пользователей или компьютеров, расположенных за ее пределами, должна установить изолированный ЦС. Их может быть несколько, но в каждой иерархии допустимо существование только одного изолированного ЦС. Остальные ЦС в иерархии считаются изолированными или корпоративными подчиненными ЦС.

Автономный ЦС имеет относительно простой заданный по умолчанию модуль политики и не хранит информацию удаленно. Поэтому изолированному ЦС не нужна служба Active Directory.

Типы центров сертификации

Корпоративный корневой ЦС

Считается корнем иерархии ЦС в организации. Его устанавливают, если ЦС предполагает выпускать сертификаты для пользователей и компьютеров своей организации. В больших организациях корпоративный корневой ЦС применяется только для выпуска сертификатов подчиненным ЦС, которые генерируют сертификаты для остальных пользователей и компьютеров.

Корпоративный подчиненный ЦС

Выпускает сертификаты, действующие в пределах организации. Не является самым доверенным ЦС в организации и подчинен другому ЦС в иерархии.

Изолированный корневой ЦС

Является корнем доверительной иерархии ЦС. Для него требуются административные полномочия на локальном сервере. Организации необходимо установить изолированный корневой ЦС, если он будет выпускать сертификаты за пределы корпоративной сети организации, и необходимо, чтобы он был корневым.

Изолированный подчиненный ЦС

Функционирует как отдельный сертификационный сервер или .в составе доверительной иерархии ЦС. Устанавливается для выдачи сертификатов объектам за пределами организации.

Развертывание центра сертификации

Ключевые этапы:

- **Установка домена Windows 2000;**
- **Интеграция службы Active Directory;**
- **Выбор несущего сервера;**
- **Назначение имен;**
- **Генерация ключей;**
- **Сертификация ЦС;**
- **Политика выпуска.**

После установки корневого ЦС разрешается установить промежуточный или подчиненный ЦС.

Защита центра сертификации

• Физическая зашита. ЦС на предприятии являются объектами с высоким доверием, поэтому их необходимо защищать от вмешательства извне. Это требование зависит от значимости сертификатов, выдаваемых ЦС. Физическая изоляция сервера ЦС в месте, доступном только администраторам безопасности, может значительно уменьшить возможность таких физических атак.

• Управление ключами. Закрытый ключ ЦС является основой для доверия в процессе сертификации. Его необходимо защищать от внешних вторжений. Криптографические аппаратные модули (доступ к службам сертификации при помощи CryptoAPI CSP) обеспечивают надежное хранение ключей и отделение выполнения криптографических операций от работы остального ПО сервера. Это существенно уменьшает вероятность компрометации ключа ЦС.

• Восстановление. Выход из строя ЦС (например, из-за отказа оборудования) создает ряд административных и оперативных проблем и предотвращает аннулирование существующих сертификатов. Службы сертификации поддерживают резервное копирование экземпляра IJC в целях его восстановления. Это важная часть всего процесса управления ЦС.

Регистрация сертификата

Процесс получения цифрового сертификата называют его регистрацией. Инфраструктура открытых ключей (PKI) Windows 2000 поддерживает регистрацию сертификатов в корпоративных, автономных и сторонних ЦС. Регистрация не зависит от транспорта и основана на использовании промышленных стандартов шифрования с открытым ключом PKCS #10 (Сообщения с запросом сертификата) и PKCS #7 (Ответы, содержащие выданный сертификат или последовательность сертификатов).

Обновление сертификата

Концепция обновления сертификатов похожа на регистрацию и использует преимущество доверительных отношений, которым отличаются существующие сертификаты. Обновление преаполагает, что запрашивающему объекту нужен новый сертификате теми же атрибутами, что и у существующего, но с продленным сроком действия. При обновлении используется существующий или новый открытый ключ.

Обновление идет в основном на ЦС. Запрос на обновление обрабатывается более эффективно, потому что нет необходимости проверять уже существующий сертификат. В настоящий момент обновление поддерживается в Windows 2000 PKI для автоматически зарегистрироаанных сертификатов. В других системах обновление рассматривается как новый запрос на регистрацию.

Восстановление сертификата и ключа

Пары открытых ключей и сертификаты имеют большое значение. При утрате в результате сбоя системы их замена отнимает много времени и денег. Для решения данной проблемы в Windows 2000 PKI встроена возможность архивирования и восстановления сертификатов и связанных с ними пар ключей, используя административные инструменты управления сертификатами.

При экспорте сертификата средствами диспетчера пользователь вправе также экспортировать и связанную с ним пару ключей. При этом информация экспортируется в зашифрованном (наосноне пароля пользователя) сообщении PKCS #12. Затем его можно импортировать в свою или другую систему или восстановить сертификат и ключи.

Пару ключей можно экспортировать средствами CSP, например, на базе Microsoft, если во время генерации набора ключей пометить флажок экспорта. CSP сторонних фирм могут поддерживать или не поддерживать экспорт закрытого ключа.

Для программных CSP с неэкспортируемыми ключами альтернативой служит полное резервное копирование образа системы, включая всю информацию реестра.

Процедура выдачи сертификата

После представления объекту сертификата как средства его (субъекта сертификата) идентификации объект должен выразить доверие выдавшему сертификат ЦС. Выпуск сертификатов происходит в несколько этапов.

• **Генерация** ключа. Претендент, запрашивающий сертификат, генерирует пару из открытого и закрытого ключей. Исключением является создание персональных цифровых сертификатов, для которых ЦС сам генерирует открытый и закрытый ключи и рассылает их.конечным пользователям.

• **Проверка соответствия политике.** Претендент предоставляет дополнительные сведения, необходимые для выдачи сертификата (например, удостоверение личности, номер налогоплательщика, адрес электронной почты и т. п.). Требуемые для выдачи сертификата данные определяются ЦС.

• **Рассылка открытых ключей и информации.** Претендент высылает в адрес ЦС открытые ключи и необходимую информацию (часто зашифрованную открытым ключом ЦС).

• **Проверка информации.** Для проверки возможности приема претендентом сертификата ЦС применяет любые требуемые правила политики.

• **Создание сертификата.** ЦС создает цифровой документ со всей необходимой HHI формацией (открытые ключи, дата истечения срока действия и другие данные) и подписывает его своим закрытым ключом.

• **Рассылка сертификата.** ЦС посылает сертификат претенденту или публикует его в хранилище. Сертификат загружается в систему пользователя.

Отзыв сертификата

ЦС публикует CRL, содержащие отозванные им сертификаты. Закрытый ключ владельца сертификата может быть скомпрометирован, либо для запроса на сертификат использовалась неверная информация. CRL позволяет удалить сертификат после его выпуска. CRL доступны для загрузки и интерактивного просмотра клиентскими приложениями.

Для проверки сертификата необходимы открытый ключ ЦС и доступ к списку отзыва, опубликованного этим ЦС. Сертификаты и ЦС устраняют проблемы распространения открытых ключей и использования нескольких открытых ключей одним субъектом. Если открытый ключ ЦС не вызывает подозрений, на него можно полагаться для проверки других сертификатов.