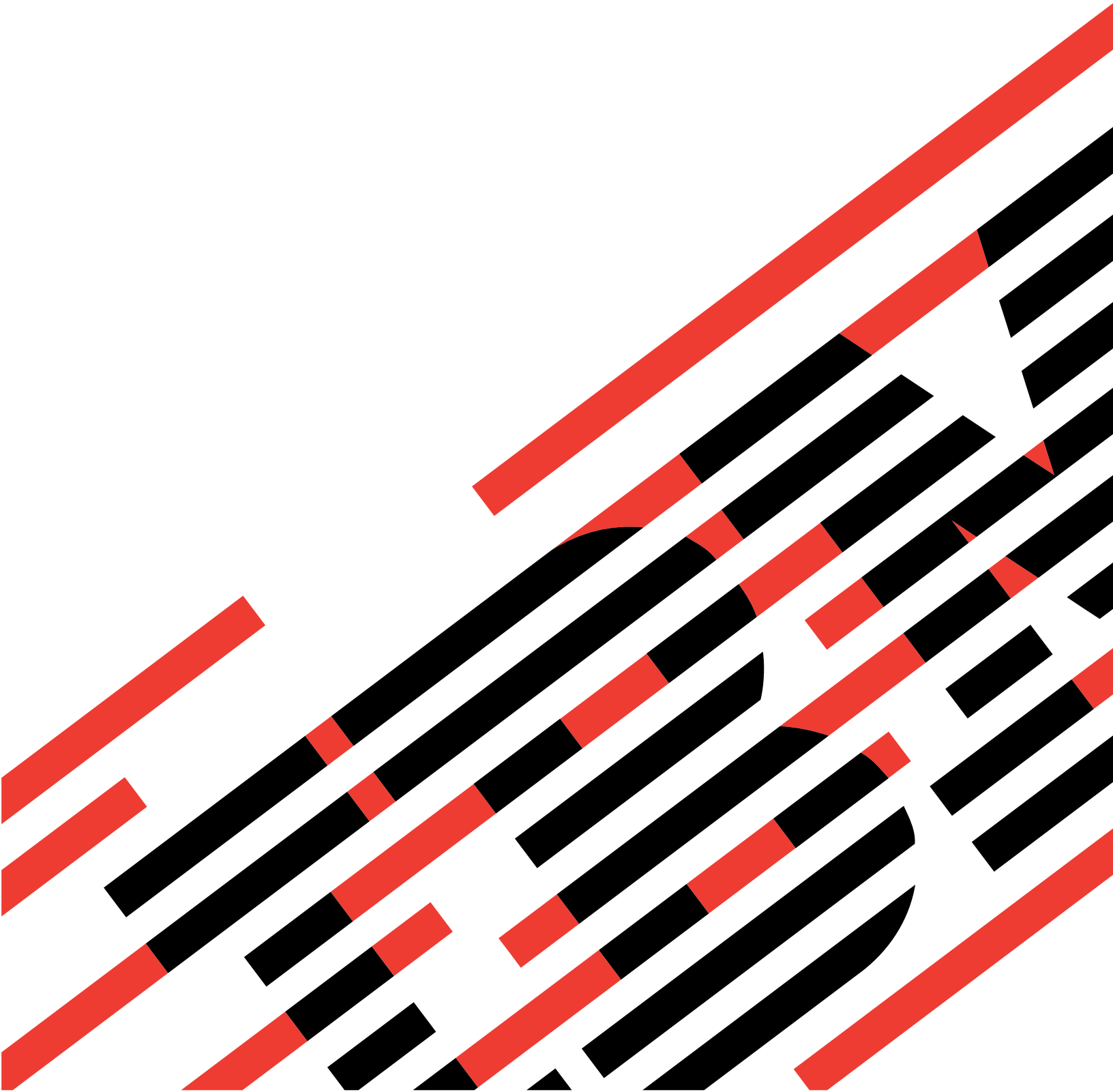
IBM

eserver

iSeries

Диспетчер цифровых сертификатов



IBM

@server

iSeries

Диспетчер цифровых сертификатов

Содержание

Часть 1. Диспетчер цифровых сертификатов 1

Глава 1. Новое в версии V5R2 3

Глава 2. Как напечатать этот раздел . . 5

Глава 3. Переход от предыдущей версии DCM 7

Глава 4. Сценарии DCM 9
Сценарий: Защита доступа к внешним приложениям и ресурсам с помощью сертификатов 9
Подробные сведения о настройке 13
Сценарий: Защита доступа к внутренним приложениям и ресурсам с помощью сертификатов . 16
Подробные сведения о настройке 20

Глава 5. Принципы применения цифровых сертификатов 25
Отличительное имя 25
Цифровые подписи 26
Общий и личный ключи 27
Сертификатная компания (CA) 27
Определения списка аннулированных сертификатов (CRL) 28
Хранилища сертификатов 29
Шифрование 30
Secure Sockets Layer (SSL) 31

Глава 6. Планирование работы с DCM 33
Требования для установки DCM 33
Типы цифровых сертификатов 34
Сравнение общих и частных сертификатов 35
Применение цифровых сертификатов в защищенных соединениях SSL 37
Применение цифровых сертификатов для идентификации пользователей 38
Применение цифровых сертификатов в соединениях VPN 39
Цифровые сертификаты подписи объектов 40
Применение цифровых сертификатов для проверки подписей объектов 41

Глава 7. Настройка DCM 43
Запуск Диспетчера цифровых сертификатов 44
Первая настройка сертификатов 44
Создание и управление локальной сертификатной компанией (CA) 45
Управление пользовательскими сертификатами 47
Создание пользовательского сертификата 48
Присвоение пользовательского сертификата 49
Выдача сертификатов пользователям других систем с помощью API 50
Получение копии сертификата частной сертификатной компании 50
Управление сертификатами, полученными от общественной сертификатной компании 51
Управление общими сертификатами Internet для сеансов SSL 52
Управление общими сертификатами Internet для подписания объектов 54
Управление сертификатами проверки подписей объектов 56

Глава 8. Управление DCM 59
Выдача сертификатов другим системам iSeries с помощью локальной сертификатной компании . . . 59
Применение частных сертификатов в соединениях SSL в целевой системе V5R2 63
Применение частных сертификатов в соединениях SSL в целевой системе V5R1 68
Применение частных сертификатов для подписания объектов в целевой системе V5R2 или V5R1 73
Применение частных сертификатов в соединениях SSL в целевой системе V4R5 или V4R4 77
Управление приложениями в DCM 82
Создание определения приложения 83
Управление присвоением сертификатов приложениям 84
Определение списка уполномоченных сертификатных компаний для приложения . . . 85
Проверка сертификатов и приложений. 86
Присвоение сертификата приложениям 86
Управление определениями CRL 87
Хранение ключей сертификатов в Шифровальном сопроцессоре IBM 4758. 88
Хранение личного ключа сертификата непосредственно в сопроцессоре 89
Шифрование личного ключа сертификата с помощью главного ключа. 89
Управление расположением сертификатной компании PKIX 90
Подписание объектов 91
Проверка подписей объектов 92

Глава 9. Устранение неполадок в DCM 95
Устранение общих неполадок и неполадок, связанных с паролями 95
Устранение неполадок хранилищ сертификатов и баз данных ключей 97
Устранение неполадок браузера 98
Устранение неполадок HTTP Server для iSeries . . . 99
Исправление ошибок, возникших при переходе к другой версии 100

Устранение неполадок, возникших при регистрации пользовательского сертификата 103

Глава 10. Связанная информация о DCM 105

Часть 1. Диспетчер цифровых сертификатов

Цифровой сертификат - это электронный документ, который может использоваться в электронных транзакциях в качестве удостоверения личности. Сфера применения цифровых сертификатов в целях повышения эффективности защиты сети постоянно расширяется. Например, цифровые сертификаты играют важную роль в соединениях Secure Sockets Layer (SSL). Применение SSL позволяет создавать защищенные соединения между пользователями и приложениями сервера в незащищенной сети, например Internet. Это один из лучших способов защиты передаваемых по Internet конфиденциальных данных, таких как имена пользователей и пароли. В настоящее время SSL поддерживается многими службами и приложениями iSeries: FTP, Telnet, HTTP Server для iSeries и др.

В iSeries предоставляется расширенная поддержка цифровых сертификатов, позволяющая применять сертификаты в качестве удостоверений личности в различных приложениях защиты. Помимо соединений SSL, сертификаты могут применяться для идентификации клиентов в транзакциях SSL и виртуальной частной сети (VPN). Кроме того, с помощью цифровых сертификатов и связанных с ними ключей шифрования можно подписывать объекты. Подписание объектов позволяет обнаруживать непредвиденные изменения в них; таким образом, цифровые подписи гарантируют целостность объектов.

Воспользоваться преимуществами поддержки сертификатов в iSeries позволяет Диспетчер цифровых сертификатов (DCM) - бесплатная программа iSeries, обеспечивающее централизованное управление сертификатами для приложений. DCM обеспечивает управление сертификатами, полученными от всех типов сертификатных компаний (CA). Кроме того, DCM позволяет вам создать собственную, частную локальную сертификатную компанию и с ее помощью выдавать частные сертификаты приложениям и пользователям в вашей организации.

Эффективность применения сертификатов напрямую связана с правильным планированием конфигурации и учетом особенностей конкретной системы. Дополнительная информация о работе с сертификатами и использующими их приложениями с помощью DCM приведена в следующих разделах:

Новое в версии V5R2
Здесь описаны изменения, внесенные в программу Диспетчер цифровых сертификатов и в соответствующие разделы документации.

Как напечатать этот раздел
Здесь указано, как можно напечатать этот раздел в виде PDF-файла.

Переход от предыдущей версии DCM
Здесь приведены инструкции по переходу от предыдущей версии DCM, а также прочая связанная информация.

Сценарии DCM
Здесь указаны примеры двух сценариев, которые помогут вам в разработке собственной схемы применения сертификатов в рамках стратегии защиты сервера iSeries. В каждом сценарии, кроме того, описаны все операции по настройке, необходимые для его реализации.

Принципы применения цифровых сертификатов
Здесь рассмотрены основные понятия, связанные с цифровыми сертификатами, и приведены ссылки на более подробную информацию. Раздел содержит информацию о различных типах сертификатов и их роли в стратегии защиты.

Планирование работы с DCM
Здесь приведены сведения об обеспечении защиты данных с помощью цифровых сертификатов. Также перечислены требования к установке DCM.

Настройка DCM
Здесь содержится информация о действиях по настройке, которые необходимо выполнить для управления сертификатами и их ключами с помощью DCM.

Управление DCM
Здесь приведена информация об управлении сертификатами и применяющими их приложениями с помощью DCM. Кроме того, раздел содержит сведения о добавлении цифровых подписей к объектам и создании собственной сертификатной компании.

Устранение неполадок DCM
Здесь приведены инструкции по устранению неполадок при работе с DCM.

Связанная информация о DCM
Здесь перечислены ссылки на дополнительные источники информации о цифровых сертификатах, инфраструктуре общих ключей, Диспетчере цифровых сертификатов и прочих связанных понятиях.

Глава 1. Новое в версии V5R2

В версии V5R2 в Диспетчере цифровых сертификатов (DCM) и поддержке цифровых сертификатов в iSeries появились следующие новые возможности:

- **Функция Присвоить сертификат**
  Это новая задача DCM, которая позволяет сократить и упростить процесс присвоения сертификата одному или нескольким приложениям. Эту задачу можно вызвать либо из списка задач **Управление сертификатами**, либо со страниц быстрого доступа **Работа с сервером и сертификатами** и **Работа с сертификатами подписи объектов**. Функция применима только к хранилищам сертификатов *SYSTEM и *OBJECTSIGNING.
- **Добавление подписей к командам (*CMD)**
  DCM теперь позволяет добавлять подписи к объектам команд (*CMD) для контроля их целостности. Кроме того, эта функция позволяет выбрать подписываемую часть объекта *CMD; подпись может быть добавлена либо ко всему объекту *CMD, либо только к его базовым компонентам. При просмотре подписей объектов типа *CMD с помощью DCM отображается и эта информация о подписанной части объекта.
- **API для создания пользовательских сертификатов, подписанных локальной сертификатной компанией, без помощи DCM**
  В новой версии добавлено два новых API, позволяющих выдавать сертификаты, подписанные локальной сертификатной компанией, пользователям систем, отличных от iSeries. С помощью этих API можно выдавать сертификаты пользователям, не имеющим пользовательских профайлов iSeries, причем без использования DCM.

Новая и дополненная информация в этом разделе:

- Два новых сценария, которые помогут вам выбрать оптимальный способ работы с сертификатами.
- Измененная структура информации упрощает поиск сведений по нужному вопросу, связанному с DCM.

Дополнительная информация об изменениях и нововведениях в текущем выпуске приведена в разделе Информация для пользователей  .

Глава 2. Как напечатать этот раздел

Для просмотра или загрузки документа в формате PDF выберите Диспетчер цифровых сертификатов  (размер файла - примерно 468 Кб или 110 страниц).

Для сохранения файла в формате PDF на персональном компьютере выполните следующие действия:

1. Откройте файл PDF в браузере (щелкните на приведенной выше ссылке).
2. В меню браузера выберите **Файл**.
3. Щелкните на **Сохранить как...**
4. Укажите каталог, в котором вы хотите сохранить документ.
5. Нажмите кнопку **Сохранить**.

Программу Adobe Acrobat Reader, необходимую для просмотра этого документа в формате PDF, можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Глава 3. Переход от предыдущей версии DCM

При переходе от Диспетчера цифровых сертификатов (DCM) версии V4R3 к DCM версии V5R2 локальная сертификатная компания (CA) и файлы наборов ключей сертификатов системы обновляются автоматически. DCM преобразует эти файлы, `default.kyr`, в соответствующие хранилища сертификатов, `default.kdb`. DCM также обновляет все действительные сертификаты в файлах наборов ключей, связанных с серверами Протокола передачи гипертекстовой информации (HTTP) и Простого протокола доступа к каталогам (LDAP). DCM переносит действительные сертификаты в хранилище сертификатов *SYSTEM (`default.kdb`).

Примечание: При переходе от DCM версии V4R4, V4R5 или V5R1 к версии V5R2 никаких дополнительных действий выполнять не требуется, так как файлы сертификатов этих версий совместимы.

Преобразование набора ключей в хранилище сертификатов – переход от версии V4R3

Во время установки DCM версии V5R2 система преобразует следующие файлы наборов ключей:
- Файлы наборов ключей DCM по умолчанию
- Наборы ключей, применяемые в файлах конфигурации HTTP Server
- Наборы ключей, применяемые в файлах конфигурации сервера LDAP

Если вы работаете с файлом `.kyr`, который не был автоматически обновлен DCM, то он будет преобразован в файл `kyr.kdb` при первом обращении к файлу в DCM. Например, когда вы впервые укажете файл `secure.kyr` в пользовательском интерфейсе DCM, он будет преобразован в новое хранилище сертификатов с именем `secure.kyr.kdb`.

Примечание: Структура наборов ключей не совпадает со структурой хранилищ сертификатов, поэтому файлы, не преобразованные автоматически Диспетчером цифровых сертификатов, необходимо обновить с помощью пользовательского интерфейса DCM. Не изменяйте расширение файлов на `.kdb` вручную - это вызовет ошибки при обращении к этому файлу из пользовательского интерфейса DCM.

Если вы попытаетесь удалить файл `secure.kyr` при работе с DCM, то этот файл будет автоматически сохранен в архиве, а удален будет файл `secure.kyr.kdb`.

Пароль хранилища сертификатов по умолчанию

Если в системе есть файл набора ключей `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR`, то он также будет преобразован в хранилище сертификатов *SYSTEM. При этом для последнего будет установлен тот же пароль, что и для файла `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR`.

Если в системе нет файла `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR`, но есть другие файлы наборов ключей (например те, что указаны в файлах конфигурации сервера HTTP), то система создаст хранилище сертификатов *SYSTEM с паролем `DEFAULT` (прописными буквами).

Ошибки, которые могут возникнуть при обновлении файлов, и способы их устранения рассмотрены в разделе Ошибки при обновлении и их устранение.

Глава 4. Сценарии DCM

Диспетчер цифровых сертификатов и поддержка цифровых сертификатов на сервере iSeries позволяют различными способами усовершенствовать стратегию защиты за счет применения цифровых сертификатов. Конкретный способ применения цифровых сертификатов зависит от ваших целей и требований к защите.

Цифровые сертификаты лежат в основе множества различных приемов по защите системы. Например, цифровые сертификаты позволяют устанавливать защищенные соединения по протоколу Secure Sockets Layer (SSL) с Web-сайтами и другими службами Internet. С помощью цифровых сертификатов вы можете настраивать соединения частной виртуальной сети (VPN). Кроме того, с помощью ключа сертификата можно добавлять и проверять цифровые подписи объектов. Цифровые подписи гарантируют подлинность и целостность объектов.

Применение цифровых сертификатов вместо имен и паролей, обычно используемых для идентификации удаленного сервера или пользователя, еще больше повышает защищенность системы. DCM позволяет связать сертификат пользователя с его пользовательским профайлом iSeries. В этом случае у сертификата будут те же права доступа, что и у связанного с ним пользовательского профайла.

Таким образом, выбор способа применения сертификатов непрост и зависит от множества факторов. Сценарии, приведенные в этом разделе, описывают некоторые наиболее распространенные способы применения цифровых сертификатов в типичной стратегии защиты. Каждый из сценариев, кроме того, содержит описание всех предварительных требований к системе и программному обеспечению, а также необходимых действий по настройке. Ознакомьтесь с этими сценариями, чтобы определить оптимальный способ применения цифровых сертификатов для повышения надежности защиты:

Сценарий: Защита доступа к внешним приложениям и ресурсам с помощью сертификатов
В этом сценарии показано, когда и как следует применять сертификаты для защиты и ограничения доступа внешних пользователей к внешним ресурсам и приложениям или приложениям и ресурсам в сети Extranet.

Сценарий: Защита доступа к внутренним приложениям и ресурсам с помощью сертификатов
В этом сценарии показано, когда и как следует применять сертификаты для защиты и запрета доступа внутренних пользователей к ресурсам и приложениям на внутренних серверах.

Сценарий: Защита доступа к внешним приложениям и ресурсам с помощью сертификатов

Ситуация

Вы работаете в страховой компании (MyCo., Inc), и в ваши обязанности входит обслуживание различных приложений на внутренних и внешних серверах компании. Одним из них является приложение, которое выдает расценки на услуги. Это приложение используется сотнями независимых страховых агентов для обслуживания клиентов. Так как информация, предоставляемая этим приложением, является конфиденциальной, приложение должно быть доступно только зарегистрированным агентам. Кроме того, в дальнейшем вы планируете заменить текущий метод

предоставления доступа к приложению, основанный на именах пользователей и паролях, на более защищенный метод. Вы обеспокоены возможностью перехвата этой информации при ее передаче по незащищенным сетевым каналам. Более того, различные агенты могут обмениваться этой информацией без вашего ведома и разрешения, что нежелательно.

Проанализировав ситуацию, вы пришли к выводу, что необходимый уровень защиты можно обеспечить с помощью цифровых сертификатов. Сертификаты позволяют использовать протокол Secure Sockets Layer (SSL) для защиты передаваемых данных. Хотя в будущем вы планируете перейти на идентификацию всех агентов, применяющих это приложение, с помощью цифровых сертификатов, вы понимаете, что для достижения этой цели требуется определенное время. На сегодняшний день вы решили сохранить текущий метод идентификации агентов, поскольку SSL обеспечивает конфиденциальность передаваемых данных.

Исходя из типа приложения, контингента пользователей и своего намерения ввести в будущем идентификацию клиентов на основе сертификатов, вы решили использовать для настройки сеансов SSL в вашем приложении общие цифровые сертификаты, полученные от общеизвестной сертификатной компании (CA).

Преимущества сценария

Этот сценарий обладает следующими преимуществами:

- Применение цифровых сертификатов для настройки доступа к приложению, предназначенному для расчета страховых премий, по протоколу SSL обеспечивает защиту информации, передаваемой между клиентом и сервером, и гарантирует ее конфиденциальность.
- Применение цифровых сертификатов для идентификации клиентов (в тех случаях, когда это возможно) обеспечивает более надежную идентификацию пользователей с правами доступа. Даже если этот способ невозможен, для идентификации клиента с помощью имени пользователя и пароля применяется сеанс SSL, что повышает надежность защиты этих конфиденциальных данных при их передаче.
- С помощью *общих* сертификатов удобно управлять доступом к приложениям и данным в следующих случаях:
  - Для данных и приложений требуется различная степень защиты.
  - В вашей компании большая текучесть кадров.
  - Вы предоставляете глобальный доступ к приложениям и данным, например путем создания Web-сайта в сети Internet или приложения для внешней сети.
  - Вы не хотите создавать собственную сертификатную компанию (CA) из-за большого числа пользователей, работающих с приложением и ресурсами, или по другим причинам административного характера.
- Применение в этом сценарии сертификата общедоступной сертификатной компании для настройки SSL в приложении вычисления ставки страховой премии сокращает процедуру соответствующей настройки для пользователей этого приложения. В клиентских программах, как правило, уже установлены сертификаты многих общеизвестных сертификатных компаний.

Цели

В этом сценарии компания MyCo., Inc. планирует применять цифровые сертификаты для защиты информации о ставках страховых премий, предоставляемой ее приложением внешним пользователям с правами доступа. Кроме того, компания собирается ввести более защищенный метод идентификации пользователей приложения.

Цели этого сценария следующие:
- Приложение расчета страховых премий должно применять протокол SSL для защиты предоставляемых им пользователям конфиденциальных данных.
- Настройку SSL необходимо выполнить с помощью сертификатов, полученных от общеизвестной сертификатной компании (CA), действующей в сети Internet.
- Пользователи с правами доступа должны вводить имя пользователя и пароль для работы с приложением в режиме SSL. В конечном счете, у пользователей должна быть возможность применять один из двух защищенных методов идентификации. Агенты должны представлять либо цифровой сертификат, полученный от общедоступной сертификатной компании (CA), либо действительные имя пользователя и пароль.

Подробности

На следующем рисунке представлена конфигурация сети для данного сценария:

На рисунке представлена следующая информация об этом сценарии:

Общий сервер компании – iSeries A
- iSeries A - сервер, на котором расположено приложение расчета ставок страховых премий компании.
- На сервере iSeries A установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- На сервере iSeries A установлена программа шифрования Cryptographic Access Provider (5722–AC3).
- На сервере iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 операционной системы OS/400) и IBM HTTP Server для iSeries (5722–DG1).
- На сервере iSeries A работает приложение расчета ставок страховых премий, настроенное следующим образом:
  – Требует режим SSL.
  – Применяет для настройки SSL сертификат, полученный от общеизвестной сертификатной компании (CA).
  – Требует идентификации клиентов по имени пользователя и паролю.
- Сервер iSeries A предъявляет свой сертификат для инициализации сеанса SSL, когда клиенты B и C обращаются к приложению.
- После инициализации сеанса SSL сервер iSeries A запрашивает у клиентов B и C имена пользователей и пароли, перед тем как предоставить им доступ к приложению.

Клиентские системы агентов – клиент B и клиент C

- Клиенты B и C - независимые агенты, обращающиеся к приложению расчета ставок.
- У клиентов B и C есть копии сертификата общеизвестной сертификатной компании, выдавшей сертификаты приложения, установленные в их клиентском программном обеспечении.
- Клиенты B и C обращаются к приложению расчета ставок страховых премий на сервере iSeries A, который предъявляет свой сертификат клиентскому программному обеспечению для идентификации и инициализации сеанса SSL.
- Клиентское программное обеспечение клиентов B и C принимает сертификат сервера iSeries A, и сеанс SSL запускается.
- После запуска сеанса SSL клиенты B и C должны предоставить действительные имена пользователей и пароли, чтобы сервер iSeries A разрешил им доступ к приложению.

Предварительные требования и допущения

Этот сценарий зависит от выполнения следующих предварительных требований и допущений:

1. Приложение расчета ставок страховых премий, расположенное на сервере iSeries A, является стандартным приложением, поддерживающим SSL. Большинство приложений, включая приложения iSeries, обеспечивают поддержку SSL. Действия по настройке SSL различаются в зависимости от конкретного приложения. По этой причине, сценарий не содержит инструкций по настройке поддержки SSL в приложении расчета ставок. В этом сценарии приведены инструкции по настройке и управлению сертификатами, которые необходимы для всех приложений, применяющих протокол SSL.
2. *В дополнение* к вышеуказанным условиям, приложение расчета ставок страховых премий может поддерживать идентификацию клиентов на основе цифровых сертификатов. Этот сценарий содержит инструкции по настройке с помощью Диспетчера цифровых сертификатов (DCM) списка уполномоченных сертификатных компаний в приложениях с такой поддержкой. Так как действия по настройке идентификации клиентов зависят от конкретного приложения, сценарий не содержит инструкций по настройке функции идентификации клиентов в приложении расчета ставок.
3. Сервер iSeries A отвечает требованиям, необходимым для установки и применения Диспетчера цифровых сертификатов (DCM).
4. Ранее DCM на сервере iSeries A не устанавливался и не применялся.
5. Задачи этого сценария выполняются с помощью DCM пользователем, обладающим специальными правами доступа *SECADM и *ALLOBJ.
6. На сервере iSeries A не установлен Шифровальный сопроцессор IBM 4758-023 PCI.

Этапы выполнения

Для реализации этого сценария выполните следующие задачи на сервере iSeries A:

1. Установите и настройте все необходимые продукты iSeries.
2. С помощью Диспетчера цифровых сертификатов (DCM) создайте запрос на сертификат сервера.
3. Настройте в приложении поддержку Secure Sockets Layer (SSL).
4. С помощью DCM импортируйте и присвойте подписанный сертификат сервера или клиента ИД вашего приложения.
5. При необходимости, запустите приложение в режиме SSL.

6. *Необязательная задача*: С помощью DCM задайте список уполномоченных сертификатных компаний, чтобы включить функцию идентификации клиентов на основе сертификатов в приложениях, поддерживающих такую функцию.

   Примечание: Ситуация, описанная в этом сценарии, не требует идентификации клиентов на основе сертификатов в приложении расчета ставок страховых премий. Многие приложения поддерживают функцию идентификации клиентов на основе цифровых сертификатов; действия, необходимые для настройки этой функции, определяются конкретным приложением. В этой дополнительной задаче описана процедура создания списка уполномоченных сертификатных компаний с помощью DCM, которая необходима для настройки в приложении функции идентификации клиентов на основе цифровых сертификатов.

Подробные сведения о настройке

Для настройки внешнего доступа к приложениям и ресурсам, защищенного с помощью сертификатов, в соответствии с этим сценарием выполните следующие действия.

Шаг 1: Выполните предварительные задачи по установке всех необходимых продуктов iSeries

Перед непосредственным выполнением задач по реализации этого сценария вы должны выполнить все предварительные задачи, установив и настроив все необходимые продукты iSeries.

Шаг 2: Создайте запрос на сертификат клиента или сервера

Перед тем, как вы начнете настройку защиты приложения с помощью SSL в соответствии с этим сценарием, вы должны получить цифровой сертификат от общественной сертификатной компании (CA). С помощью Диспетчера цифровых сертификатов (DCM) создайте информацию, которая необходима этой CA для выдачи сертификата.

Для того чтобы начать процедуру получения сертификата, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать хранилище сертификатов**, чтобы запустить пошаговую задачу и заполнить несколько форм. Выполните показанные инструкции по созданию хранилища сертификатов и сертификата, с помощью которых приложения смогут устанавливать сеансы SSL.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
3. Выберите хранилище сертификатов ***SYSTEM** и нажмите **Продолжить**.
4. Выберите **Да**, чтобы создать сертификат вместе с хранилищем сертификатов *SYSTEM, и нажмите **Продолжить**.
5. Выберите **VeriSign или другая сертификатная компания Internet** в качестве сертификатной компании, которая подпишет новый сертификат, и нажмите **Продолжить**. Появится форма, в которой следует указать идентифицирующую информацию о новом сертификате.
6. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения. Она содержит данные о сертификате, которые необходимо

предоставить общественной сертификатной компании для получения сертификата. Эти данные называются данными Запроса на подписание сертификата (CSR) и содержат общий ключ и другую информацию, указанную вами для нового сертификата.
7. Аккуратно скопируйте и вставьте данные CSR в форму запроса сертификата или в отдельный файл, необходимый для получения сертификата от общей сертификатной компании. Необходимо скопировать все данные CSR, включая строки Begin и End New Certificate Request. После завершения работы с этой страницей данные будут потеряны и не смогут быть восстановлены.
8. Отправьте форму запроса или файл в выбранную сертификатную компанию.
9. Перед тем, как перейти к следующему этапу этого сценария, дождитесь возвращения сертификатной компанией подписанного сертификата.

После того, как сертификатная компания выдаст подписанный сертификат, можно настроить поддержку SSL в приложении, импортировать сертификат в хранилище сертификатов *SYSTEM и присвоить его приложению, применяющему функцию SSL.

Шаг 3: Настройте поддержку SSL в приложении

Получив подписанный сертификат от общественной сертификатной компании (CA), вы можете продолжить настройку поддержки протокола Secure Sockets Layer (SSL) в приложении. Вы должны настроить поддержку SSL до того, как начнете применять сертификат. Некоторые приложения, например HTTP Server для iSeries, при настройке поддержки SSL создают уникальный ИД приложения и регистрируют его в Диспетчере цифровых сертификатов (DCM). Вы должны узнать этот ИД, чтобы с помощью DCM присвоить ему подписанный сертификат и выполнить процедуру настройки SSL.

Способ настройки поддержки SSL зависит от конкретного приложения. В этом сценарии не указан конкретный источник приложения расчета ставок страховых премий, так как компания MyCo., Inc. может предоставлять его агентам различными способами.

При настройке поддержки SSL в приложении следуйте инструкциям, приведенным в документации по приложению. Информация о настройке поддержки SSL в наиболее распространенных приложениях фирмы IBM приведена в разделе Защита приложений с помощью SSL справочной системы Information Center.

Шаг 4: Импортируйте и присвойте приложению подписанный общий сертификат

Настроив поддержку SSL в приложении, вы можете с помощью Диспетчера цифровых сертификатов (DCM) импортировать подписанный сертификат и присвоить его приложению.

Для того чтобы импортировать сертификат, присвоить его приложению и завершить процедуру настройки SSL, выполните следующие действия:
1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
3. На странице Хранилище сертификатов и пароль укажите пароль, заданный при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.

5. В списке задач выберите **Импортировать сертификат**, чтобы начать импортирование подписанного сертификата в хранилище сертификатов *SYSTEM.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
6. Затем выберите **Присвоить сертификат** в списке задач **Управление сертификатами**, чтобы просмотреть список сертификатов в текущем хранилище сертификатов.
7. Выберите сертификат из списка и нажмите кнопку **Присвоить приложениям**, чтобы просмотреть список определений приложений для текущего хранилища сертификатов.
8. Выберите в списке свое приложение и нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного выполнения операции, либо, в случае возникновения неполадки, - с информацией об ошибках.

Выполнив эти задачи, вы можете запустить приложение в режиме SSL, что обеспечит конфиденциальность данных, предоставляемых приложением.

Шаг 5: Запустите приложение в режиме SSL

После импортирования сертификата и его присвоения приложению вам, возможно, потребуется завершить работу приложения и перезапустить его в режиме SSL. Это необходимо в некоторых случаях, когда приложение не может обнаружить назначенный ему сертификат в процессе работы. Информация о том, нужно ли перезапускать приложение, а также сведения о запуске приложения в режиме SSL приведены в документации по приложению.

Необязательный шаг 6: Задайте список уполномоченных сертификатных компаний для приложения, идентифицирующего клиентов на основе сертификатов

Приложения, поддерживающие применение сертификатов для идентификации клиентов во время сеансов Secure Sockets Layer (SSL), определяют, может ли сертификат быть принят в качестве удостоверения личности. Один из критериев идентификации сертификата основан на том, является ли сертификатная компания, выдавшая этот сертификат, уполномоченной.

Ситуация, описанная в этом сценарии, не требует идентификации клиентов на основе сертификатов в приложении расчета ставок страховых премий. Многие приложения поддерживают функцию идентификации клиентов на основе цифровых сертификатов; действия, необходимые для настройки этой функции, определяются конкретным приложением. В данной дополнительной задаче описана процедура создания списка уполномоченных сертификатных компаний с помощью DCM, которая необходима для настройки идентификации клиентов на основе цифровых сертификатов в приложении.

Для того чтобы вы могли определить список уполномоченных сертификатных компаний для приложения, должны быть выполнены несколько условий:
- Приложение должно поддерживать идентификацию клиентов на основе сертификатов.
- В определении приложения DCM должно быть указано, что приложение применяет список уполномоченных сертификатных компаний.

Если в определении приложения указано, что приложение применяет список уполномоченных сертификатных компаний, то для успешной идентификации

клиентов с помощью сертификатов необходимо определить этот список. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

Для того чтобы с помощью DCM определить список уполномоченных сертификатных компаний для приложения, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
3. На странице Хранилище сертификатов и пароль укажите пароль, заданный при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
5. В списке задач выберите **Задать состояние CA**, чтобы просмотреть список сертификатов CA.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
6. Выберите из списка сертификат CA, сертификаты которой должно принимать ваше приложение, и нажмите кнопку **Включить**, чтобы просмотреть список приложений, применяющих список уполномоченных сертификатных компаний.
7. Выберите из списка приложение, в список уполномоченных CA которого необходимо добавить выбранную сертификатную компанию, и нажмите кнопку **OK**. В верхней части страницы будет показано сообщение о том, что выбранные приложения будут принимать сертификаты, выданные этой сертификатной компанией.

Теперь в приложении можно настроить идентификацию клиентов на основе цифровых сертификатов. Выполните инструкции по настройке, приведенные в документации по приложению.

Сценарий: Защита доступа к внутренним приложениям и ресурсам с помощью сертификатов

Ситуация

Вы являетесь администратором сети в компании (MyCo., Inc.), и ее отдел кадров столкнулся с проблемой защиты конфиденциальных данных о сотрудниках. Работники компании хотят, чтобы у них была возможность получать информацию о своей медицинской страховке и льготах по электронным каналам связи. В ответ на эту просьбу компания создала внутренний Web-сайт, предоставляющий эту информацию работникам. Вы выполняете роль администратора этого внутреннего Web-сайта.

Так как офисы компании расположены в двух городах, то сотрудники часто путешествуют, и перед вами стоит задача обеспечения конфиденциальности информации при ее передаче по сети Internet. Идентификация пользователей выполняется по именам и паролям. Поскольку информация конфиденциальная, вы считаете, что защиты паролем недостаточно. Всегда существует вероятность, что пароль будет забыт, украден или непреднамеренно сообщен другому пользователю.

Проанализировав ситуацию, вы пришли к выводу, что необходимый уровень защиты можно обеспечить с помощью цифровых сертификатов. Сертификаты позволяют использовать протокол Secure Sockets Layer (SSL) для защиты передаваемых данных. Кроме того, применение сертификатов вместо паролей позволяет надежнее идентифицировать пользователей и контролировать доступ к информации о кадрах компании.

Таким образом, вы решаете создать частную локальную сертификатную компанию (CA), выдать сертификаты всем сотрудникам и потребовать, чтобы сотрудники связали полученные сертификаты со своими пользовательскими профайлами iSeries. Описанные меры позволят ужесточить контроль над доступом к секретным данным и обеспечить конфиденциальность данных с помощью SSL. Если вы будете выдавать сертификаты с помощью своей собственной сертификатной компании, то вероятность несанкционированного доступа значительно снизится.

Преимущества сценария

Этот сценарий обладает следующими преимуществами:
- Настройка SSL-доступа к Web-серверу, содержащему информацию о персонале компании, с помощью цифровых сертификатов гарантирует конфиденциальность передаваемой информации.
- Идентификация клиентов на основе цифровых сертификатов обеспечивает более надежную идентификацию пользователей с правами доступа.
- Контроль доступа к приложениям и данным с помощью *частных* цифровых сертификатов удобен в следующих случаях:
  - Необходимо обеспечить высокий уровень защиты, особенно при идентификации пользователей.
  - Сертификаты выдаются только доверенным лицам.
  - Доступ к приложениям и данным уже контролируется с помощью пользовательских профайлов iSeries.
  - Вы собираетесь создать локальную сертификатную компанию (CA).
- Применение частных сертификатов для идентификации клиентов упрощает процедуру присвоения сертификата пользовательскому профайлу iSeries. Сопоставление сертификата с пользовательским профайлом позволяет серверу HTTP определить пользовательский профайл владельца сертификата при идентификации. Сервер HTTP может переключиться на пользовательский профайл и под его управлением выполнять операции для пользователя.

Цели

В этом сценарии компания MyCo., Inc. планирует применять цифровые сертификаты для защиты конфиденциальной информации о сотрудниках компании, предоставляемой ее внутренним Web-сайтом. Кроме того, компания собирается внедрить более надежный метод идентификации пользователей этого Web-сайта.

Цели этого сценария следующие:
- Внутренний Web-сайт персонала компании должен применять протокол SSL для защиты предоставляемых им конфиденциальных данных.
- Настройку SSL необходимо выполнить с помощью сертификатов, полученных от внутренней локальной сертификатной компании (CA).
- Пользователи с правами доступа должны предъявлять действительный сертификат для работы с Web-сайтом в режиме SSL.

Подробности

На следующем рисунке представлена конфигурация сети для данного сценария:

На рисунке представлена следующая информация об этом сценарии:

Web-сервер отдела кадров компании – iSeries A

- iSeries A - это сервер, на котором расположено Web-приложение отдела кадров.
- На сервере iSeries A установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- На сервере iSeries A установлена программа шифрования Cryptographic Access Provider (5722–AC3).
- На сервере iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 операционной системы OS/400) и IBM HTTP Server для iSeries (5722–DG1).
- На сервере iSeries A работает приложение отдела кадров, настроенное следующим образом:
  - Требует режим SSL.
  - Применяет для настройки SSL частный сертификат, полученный от локальной сертификатной компании (CA).
  - Выполняет идентификацию клиентов на основе сертификатов.
- Сервер iSeries A предъявляет свой сертификат для инициализации сеанса SSL, когда клиенты B, C и D обращаются к приложению.
- После инициализации сеанса SSL сервер iSeries A запрашивает у клиентов B, C и D действительные сертификаты, перед тем как предоставить им доступ к приложению. Об этом обмене сертификатами уведомляются пользователи клиентов B, C и D.

Клиентские системы сотрудников компании – клиент B, клиент C и клиент D

- Клиент B работает в главном офисе компании MyCo, где расположен сервер iSeries A.
- Клиент C работает в дополнительном офисе компании MyCo, находящемся в другом городе.
- Клиент D работает удаленно. Он часто ездит в командировки, и независимо от того, где он находится, ему необходим защищенный доступ к Web-сайту отдела кадров.
- Клиенты B, C и D - это сотрудники, работающие с приложением отдела кадров.
- У клиентов B, C и D есть копии сертификата локальной сертификатной компании, выдавшей сертификат приложения, установленный в их клиентском программном обеспечении.
- Клиенты B, C и D обращаются к приложению отдела кадров на сервере iSeries A, который предъявляет свой сертификат клиентскому программному обеспечению для идентификации и инициализации сеанса SSL.

- Клиентское программное обеспечение клиентов B, C и D принимает сертификат сервера iSeries A, и сеанс SSL запускается.
- После запуска сеанса SSL клиенты B, C и D должны предоставить действительные сертификаты, чтобы сервер iSeries A разрешил им доступ к приложению и его ресурсам.

Предварительные требования и допущения

Этот сценарий зависит от выполнения следующих предварительных требований и допущений:

1. В системе iSeries A на сервере IBM HTTP Server для iSeries работает приложение отдела кадров. В настоящее время существует два типа серверов HTTP Server для iSeries: стандартный и на основе Apache; после опубликования этой документации появится новая, значительно переработанная версия сервера HTTP. По этой причине сценарий не содержит *конкретных* инструкций по настройке поддержки SSL на сервере HTTP. В этом сценарии приведены инструкции по настройке и управлению сертификатами, которые необходимы для всех приложений, применяющих протокол SSL.
2. Сервер HTTP обеспечивает возможность идентификации клиентов на основе цифровых сертификатов. Этот сценарий содержит инструкции по всем необходимым операциям настройки сертификатов с помощью Диспетчера цифровых сертификатов (DCM). Однако этот сценарий не содержит *конкретных* инструкций по настройке идентификации клиентов на основе сертификатов на сервере HTTP.
3. На сервере HTTP отдела кадров в системе iSeries A уже настроена защита паролем.
4. Сервер iSeries A отвечает требованиям, необходимым для установки и применения Диспетчера цифровых сертификатов (DCM).
5. Ранее DCM на сервере iSeries A не устанавливался и не применялся.
6. У пользователя, выполняющего задачи этого сценария с помощью DCM, есть специальные права доступа *SECADM и *ALLOBJ.
7. На сервере iSeries A не установлен Шифровальный сопроцессор IBM 4758-023 PCI.

Этапы выполнения

Для реализации этого сценария необходимо выполнить два набора задач. Первый предполагает настройку поддержки SSL и идентификации клиентов на основе сертификатов в приложении отдела кадров на сервере iSeries A. Второй позволит пользователям настроить поддержку SSL на клиентах B, C и D и получить сертификаты для идентификации.

Выполнение задач для Web-сервера приложения отдела кадров

Для реализации этого сценария выполните следующие задачи на сервере iSeries A:

1. Установите и настройте все необходимые продукты iSeries.
2. Настройте поддержку SSL на сервере HTTP отдела кадров и запишите ИД приложения экземпляра сервера.
3. В Диспетчере цифровых сертификатов (DCM) создайте локальную сертификатную компанию (CA) и с ее помощью выдайте сертификат серверу HTTP отдела кадров. Кроме того, в процессе выполнения этой пошаговой задачи вы присвоите сертификат приложению Web-сервера и добавите локальную сертификатную компанию в список уполномоченных сертификатных компаний.
4. Настройте на Web-сервере отдела кадров идентификацию клиентов на основе цифровых сертификатов.
5. Запустите сервер HTTP отдела кадров в режиме SSL.

Выполнение задач настройки клиентов

Для реализации этого сценария каждый из пользователей (клиенты B, C и D), работающих с Web-сервером отдела кадров на сервере iSeries A, должен выполнить следующие действия:
6. Установить копию сертификата локальной сертификатной компании в браузере.
7. Запросить сертификат от локальной сертификатной компании.

Подробные сведения о настройке

Для настройки доступа к внутренним приложениям и ресурсам, защищенного с помощью сертификатов, в соответствии с этим сценарием выполните следующие действия.

Шаг 1: Выполните предварительные задачи по установке всех необходимых продуктов iSeries

Перед непосредственным выполнением задач по реализации этого сценария вы должны выполнить все предварительные задачи, установив и настроив все необходимые продукты iSeries.

Шаг 2: Настройте поддержку SSL на сервере HTTP отдела кадров

Конкретные действия по настройке поддержки протокола Secure Sockets Layer (SSL) на сервере HTTP отдела кадров в системе iSeries A зависят от применяемой версии сервера HTTP (стандартный или на основе Apache).

Информация о настройке поддержки SSL на сервере HTTP стандартной версии приведена в разделе Настройка защищенного сервера HTTP.

Информация о настройке поддержки SSL на сервере HTTP на основе Apache приведена в разделе Сценарий: JKL настраивает защиту Secure Sockets Layer (SSL) на своем сервере HTTP (на основе Apache). В этом сценарии описаны все действия, необходимые для создания виртуального хоста и настройки на нем поддержки SSL. Подробные сведения о настройке SSL приведены в разделе ″Настройка SSL на виртуальном хосте.″

Дополнительная информация о настройке текущей и будущих версий сервера HTTP Server для iSeries (стандартного и на основе Apache) приведена в разделе Web-серверы.

Шаг 3: Создание и управление локальной сертификатной компанией

После настройки поддержки протокола Secure Sockets Layer (SSL) на сервере HTTP необходимо настроить сертификат для инициализации SSL на сервере. Руководствуясь целями данного сценария, вы решили создать локальную сертификатную компанию (CA), чтобы выдать сертификат серверу.

В процессе создания локальной сертификатной компании с помощью Диспетчера цифровых сертификатов (DCM) будут выполнены все необходимые действия по настройке для применения SSL в приложении. Эти действия включают присвоение сертификата, выданного локальной сертификатной компанией, приложению Web-сервера. Кроме того, локальная сертификатная компания будет добавлена в список уполномоченных сертификатных компаний приложения Web-сервера. При этом Web-сервер будет распознавать и идентифицировать пользователей, предъявляющих сертификаты, выданные локальной сертификатной компанией.

Для того чтобы с помощью Диспетчера цифровых сертификатов (DCM) создать локальную сертификатную компанию и выдать сертификат приложению сервера отдела кадров, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать сертификатную компанию (CA)**. Будет показано несколько форм. Эти формы содержат инструкции по созданию локальной сертификатной компании и выполнению других задач, необходимых для применения цифровых сертификатов в соединениях SSL, подписания объектов и проверки подписей.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
3. Заполните все необходимые формы. В процессе настройки локальной сертификатной компании (CA) путем заполнения этих форм вы должны выполнить следующие задачи:
   a. Предоставить идентификационную информацию для локальной CA.
   b. Установить сертификат локальной CA на PC или в браузере, чтобы соответствующая программа могла распознавать эту локальную сертификатную компанию и проверять выдаваемые ей сертификаты.
   c. Выбрать полномочия локальной CA.

      Примечание: Выбранные полномочия должны предусматривать возможность выдачи сертификатов пользователям.
   d. С помощью новой локальной сертификатной компании создать сертификат клиента или сервера, с помощью которого приложения будут устанавливать соединения SSL.
   e. Выбрать приложения, которые будут с помощью сертификата клиента или сервера устанавливать соединение SSL.

      Примечание: Обязательно выберите ИД приложения сервера HTTP отдела кадров.
   f. С помощью новой локальной сертификатной компании создать сертификат подписи объектов, с помощью которого приложения будут подписывать объекты. Эта подзадача включает создание хранилища сертификатов *OBJECTSIGNING, предназначенного для управления сертификатами подписи объектов.

      Примечание: Хотя в данном сценарии не применяются сертификаты подписи объектов, обязательно выполните этот шаг. Если вы отмените задачу на этом этапе, то она будет завершена, и вам придется заново выполнять отдельные задачи для настройки сертификата SSL.
   g. Выбрать приложения, которые будут принимать сертификаты локальной сертификатной компании.

      Примечание: Обязательно выберите ИД приложения сервера HTTP отдела кадров.

Выполнив настройку сертификатов, необходимую для поддержки SSL на Web-сервере, вы можете настроить в приложении Web-сервера идентификацию клиентов на основе цифровых сертификатов.

Шаг 4: Настройте идентификацию клиентов на основе цифровых сертификатов на Web-сервере

Конкретные действия по настройке поддержки протокола Secure Sockets Layer (SSL) для идентификации клиентов с помощью сертификатов на сервере HTTP отдела кадров в системе iSeries A зависят от применяемой версии сервера HTTP.

Более подробная информация о настройке идентификации клиентов с помощью сертификатов на сервере HTTP стандартной версии приведена в разделе Создание конфигураций защиты на сервере HTTP стандартной версии.

Информация о настройке поддержки идентификации клиентов с помощью сертификатов на сервере HTTP на основе Apache приведена в разделе Сценарий: JKL настраивает защиту Secure Sockets Layer (SSL) на своем сервере HTTP на основе Apache. В этом сценарии, относящемся к серверу HTTP, описаны все действия, необходимые для создания виртуального хоста и настройки на нем поддержки SSL и идентификации клиентов с помощью сертификатов. Подробные сведения о настройке SSL и идентификации клиентов с помощью сертификатов приведены в разделе ″Настройка SSL на виртуальном хосте.″

Дополнительная информация о настройке текущей и будущих версий сервера HTTP Server для iSeries (стандартного и на основе Apache) приведена в разделе Web-серверы.

Шаг 5: Запустите Web-сервер отдела кадров в режиме SSL

Возможно, вам потребуется перезапустить сервер HTTP, чтобы сервер смог обнаружить присвоенный сертификат и применять его для инициализации сеансов SSL.

Для перезапуска сервера HTTP (стандартной версии) воспользуйтесь формами Настройка и Администрирование и выполните следующие действия:
1. Выберите **Администрирование**.
2. Выберите **Управление серверами HTTP**.
3. Выберите сервер.
4. Введите параметры запуска в соответствующем поле формы, если это необходимо.
5. Нажмите кнопку **Запустить**.

Примечание: Если в момент присвоения сертификатов сервер работал, необходимо остановить, а затем запустить его. Простое нажатие кнопки **Перезапустить** не всегда гарантирует, что сервер обнаружит изменения в конфигурации сертификатов, произошедшие во время его работы.

Для перезапуска сервера HTTP (на основе Apache) воспользуйтесь формами Настройка и Администрирование и выполните следующие действия:
1. Выберите **Администрирование**.
2. В левом меню выберите **Управление серверами HTTP** в категории **Общее администрирование серверов**.
3. Выберите необходимый сервер и нажмите кнопку **Запустить** или **Остановить**. Дополнительная информация о параметрах запуска приведена в электронной справке.

Дополнительная информация об управлении текущей и будущими версиями сервера HTTP Server для iSeries (стандартной версии и на основе Apache) приведена в разделе Web-серверы.

Выполнив эти задачи, вы можете запустить приложение отдела кадров в режиме SSL, что обеспечит конфиденциальность данных, предоставляемых приложением.

Шаг 6: Предложите пользователям установить копию сертификата локальной сертификатной компании в браузере.

Когда пользователь отправляет запрос на сервер по соединению SSL, сервер предъявляет клиентской программе пользователя сертификат в качестве своего удостоверения. Клиентская программа должна проверить этот сертификат, прежде чем будет установлен сеанс. Для проверки сертификата у программы должен быть доступ к локальной копии сертификата сертификатной компании, выдавшей сертификат серверу. Если сервер предъявляет сертификат, полученный от общественной сертификатной компании Internet, то в браузере пользователя или другом клиентском приложении уже должна быть копия сертификата этой сертификатной компании. Если же, как в этом сценарии, сервер предъявляет сертификат, полученный от частной локальной сертификатной компании, то все пользователи должны установить копии сертификата этой сертификатной компании с помощью Диспетчера цифровых сертификатов (DCM).

Для установки копии сертификата локальной сертификатной компании на PC каждого из пользователей (клиентов B, C и D) выполните следующие действия:
1. Запустите DCM.
2. В окне навигации выберите **Установить сертификат локальной CA на PC**. Будет показана страница, позволяющая загрузить сертификат локальной сертификатной компании в браузер или сохранить его в файле.
3. Выберите опцию установки сертификата. Сертификат локальной сертификатной компании будет загружен в браузер в качестве надежного базового сертификата. После этого браузер сможет устанавливать защищенные соединения с серверами, которые применяют сертификат, полученный от этой локальной сертификатной компании. Браузер выдаст последовательность окон с инструкциями по установке сертификата.
4. Нажмите кнопку **OK** для возврата к главному окну Диспетчера цифровых сертификатов.

Шаг 7: Предложите пользователям получить сертификаты от локальной сертификатной компании

На предыдущих этапах вы настроили на Web-сервере отдела кадров идентификацию клиентов на основе цифровых сертификатов. Теперь для получения доступа к Web-серверу пользователи должны предъявлять действительный цифровой сертификат, выданный локальной сертификатной компанией. Каждому пользователю необходимо получить сертификат, выполнив задачу **Создать сертификат** Диспетчера цифровых сертификатов (DCM). Для получения сертификата от локальной сертификатной компании необходимо, чтобы стратегия сертификатной компании позволяла ей выдавать пользовательские сертификаты.

Для получения сертификата выполните следующие действия на PC клиентов B, C и D:
1. Запустите DCM.
2. В окне навигации выберите **Создать сертификат**.
3. Выберите тип сертификата **Пользовательский сертификат**. Будет показана форма для ввода информации о сертификате.
4. Заполните форму и нажмите кнопку **Продолжить**.

Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.

5. На этом этапе DCM с помощью браузера создает общий и личный ключи для сертификата. Появится окно браузера с инструкциями по выполнению этой задачи. Выполните описанные действия. После того, как браузер создаст ключи, будет показано подтверждающее сообщение о создании сертификата.
6. Установите новый сертификат в программном обеспечении браузера. Появится окно браузера с инструкциями по выполнению этой задачи. Выполните описанные действия.
7. Нажмите кнопку **OK** для завершения задачи.

Диспетчер цифровых сертификатов автоматически свяжет сертификат с вашим пользовательским профайлом iSeries.

Глава 5. Принципы применения цифровых сертификатов

Перед тем, как начать применение цифровых сертификатов для защиты системы и сети, необходимо уяснить, что такое цифровые сертификаты и какие преимущества в сфере защиты они предоставляют.

Цифровой сертификат - это электронный документ, удостоверяющий личность своего владельца. Его можно сравнить с паспортом. Специальная уполномоченная организация, называемая сертификатной компанией (CA), выдает цифровые сертификаты пользователям и серверным и клиентским приложениям. Полномочия CA служат гарантией подлинности сертификатов, которые она выдает.

Дополнительная о информация о работе с цифровыми сертификатами приведена в следующих разделах:

Отличительное имя
Этот раздел содержит информацию об идентификационных характеристиках цифровых сертификатов.

Цифровые подписи
Этот раздел содержит информацию об обеспечении целостности объектов с помощью цифровых подписей.

Общий и личный ключи
Этот раздел содержит дополнительную информацию о ключах шифрования, связанных с цифровыми сертификатами.

Сертификатная компания (CA)
Здесь приведена дополнительная информация о сертификатных компаниях, выдающих цифровые сертификаты.

Определения CRL
Здесь приведена информация о том, что такое Списки аннулированных сертификатов и как они применяются при проверке сертификатов.

Хранилища сертификатов
Здесь приведена информация о хранилищах сертификатов и работе с ними с помощью Диспетчера цифровых сертификатов (DCM).

Шифрование
Здесь приведена информация о том, что такое шифрование и каким образом обеспечивается защита с помощью функций шифрования сертификатов.

Secure Sockets Layer (SSL)
Этот раздел содержит краткое описание SSL.

Отличительное имя

У каждой CA есть стратегия, определяющая идентификационную информацию, которую необходимо предоставить для получения сертификата. Для некоторых общественных сертификатных компаний достаточно указать только имя и электронный адрес. Другие общественные CA могут требовать более развернутую информацию и более надежное подтверждение истинности этой информации. Например, сертификатные компании, поддерживающие стандарты Инфраструктуры общих ключей (PKIX), могут требовать от инициатора подтверждения идентификационной информации с помощью регистрационной компании (RA). Таким образом, если вы собираетесь применять сертификаты в качестве

удостоверений личности, то необходимо определить, насколько идентификационные требования сертификатной компании соответствуют требованиям защиты вашей системы.

Отличительное имя (DN) - это термин, обозначающий идентификационную информацию о личности владельца сертификата. Отличительное имя входит в состав сертификата. В зависимости от стратегии CA, выдающей сертификат, DN может содержать различную информацию. Диспетчер цифровых сертификатов позволяет создать частную сертификатную компанию для выдачи сертификатов. Кроме того, DCM позволяет создавать информацию DN и пару ключей для сертификатов, получаемых от общественной сертификатной компании. Независимо от типа сертификата, вы можете предоставить следующую информацию DN:
- Обычное имя владельца сертификата
- Организация
- Подразделение
- Город
- Область
- Страна

При выдаче частных сертификатов с помощью DCM для сертификата может быть предоставлена дополнительная информация отличительного имени:
- IP-адрес версии 4
- Полное имя домена
- Электронный адрес

Эта дополнительная информация полезна, если вы собираетесь настраивать соединение виртуальной частной сети (VPN) с помощью сертификата.

Цифровые подписи

Цифровая подпись в электронном документе или другом объекте аналогична обычной подписи в напечатанном документе и создается с помощью одного из видов шифрования. Она подтверждает подлинность источника и целостность объекта. Владелец цифрового сертификата ″подписывает″ объект с помощью личного ключа сертификата. Получатель объекта расшифровывает подпись, подтверждающую целостность объекта и идентифицирующую отправителя, с помощью соответствующего общего ключа сертификата.

Сертификатная компания (CA) всегда подписывает свои сертификаты. Эта подпись состоит из символьной строки, зашифрованной с помощью личного ключа сертификатной компании. Пользователь может проверить подпись на сертификате, расшифровав ее с помощью общего ключа сертификатной компании.

Цифровая подпись - это электронная подпись, добавленная к объекту с применением личного ключа цифрового сертификата. Цифровая подпись объекта обеспечивает уникальное связывание владельца подписи (владельца ключа) с источником объекта. При обращении к подписанному объекту можно проверить его подпись, чтобы идентифицировать его источник (например, если необходимо убедиться, что загружаемое приложение действительно получено из надежного источника, такого как фирма IBM). Такая проверка позволяет определить, не нарушалась ли целостность объекта с момента его подписания.

Пример работы с цифровыми подписями

Разработчик программного обеспечения создал приложение iSeries и собирается распространять его по сети Internet, так как это удобно для его заказчиков и недорого.

Однако разработчику известно, что заказчики обоснованно опасаются загружать программы из сети Internet из-за увеличения числа объектов, замаскированных под полезные приложения, но содержащих опасные программы, например вирусы.

По этой причине разработчик программного обеспечения принимает решение добавить к своему приложению цифровую подпись, чтобы его покупатели могли проверить подлинность его приложения. Разработчик подписывает свое приложение с помощью личного ключа цифрового сертификата, выданного общеизвестной сертификатной компанией. После этого разработчик размещает приложение на сервере для покупателей. В загрузочный пакет он включает копию цифрового сертификата, с помощью которого был подписан объект. При загрузке пакета заказчик может с помощью общего ключа этого сертификата проверить подпись приложения. Это позволяет заказчику идентифицировать и проверить подпись приложения, а также убедиться, что содержимое объекта приложения не изменялось с момента его подписания.

Общий и личный ключи

С каждым сертификатом связана пара шифровальных ключей. Эта пара состоит из личного ключа и общего ключа. (Исключением является сертификат проверки подписи, с которым связан только общий ключ.)

Общий ключ - общедоступная часть цифрового сертификата владельца. Напротив, личный ключ может применяться только его владельцем. Такое ограничение гарантирует защищенность соединений, в которых применяется этот ключ.

С помощью этих ключей владелец сертификата может выполнять шифрование. Например, с помощью личного ключа владелец сертификата может ″подписывать″ и зашифровывать сообщения, документы, программы и прочие данные, которыми пользователи обмениваются с серверами. Получатель подписанного объекта может расшифровать подпись с помощью общего ключа сертификата владельца подписи. Цифровые подписи гарантируют подлинность и позволяют проверить целостность объектов.

Сертификатная компания (CA)

Сертификатная компания (CA) - это центральный административный орган, уполномоченный выдавать цифровые сертификаты пользователям и серверам. Полномочия CA служат гарантией подлинности сертификатов, которые она выдает. С помощью своего личного ключа CA добавляет к сертификату, идентифицирующему пользователя или систему, цифровую подпись.Другие пользователи могут проверить подлинность сертификатов, выданных и подписанных CA, с помощью общего ключа сертификатной компании.

Вы можете выбрать одну из крупных сертификатных компаний, например, VeriSign, или создать собственную сертификатную компанию, которая будет обслуживать, например, сеть вашей организации. В Internet существует несколько сертификатных компаний. Для управления сертификатами как частных, так и общественных сертификатных компаний служит программа Диспетчер цифровых сертификатов (DCM).

DCM позволяет также выдавать системам и пользователям сертификаты частной сертификатной компании. Когда сертификатная компания выдает пользовательский сертификат, DSM автоматически связывает его с соответствующим профайлом пользователя системы iSeries. Это означает, что сертификату присваиваются те же права доступа, что и его владельцу.

Надежный базовый сертификат

Надежный базовый сертификат - это специальное обозначение сертификата CA. Это обозначение позволяет браузеру или другому приложению идентифицировать и принимать сертификаты, выданные CA.

При загрузке сертификата CA в окно браузера последний позволяет пометить его как надежный базовый сертификат. Другие приложения, поддерживающие работу с цифровыми сертификатами, также необходимо настроить для работы с сертификатами данной CA.

DCM позволяет изменить статус надежности сертификата CA в хранилище сертификатов. Если сертификат CA помечен как надежный, то можно указать приложения, которые будут с его помощью проверять и принимать сертификаты, выданные данной CA. В противном случае, этого сделать нельзя.

Информация о полномочиях сертификатной компании

Когда вы создаете сертификатную компанию с помощью Диспетчера цифровых сертификатов, вы можете указать ее полномочия. В полномочиях CA определяется, есть ли у нее права на подпись сертификатов. В информации о полномочиях задаются следующие параметры:
- Может ли CA выдавать и подписывать пользовательские сертификаты.
- Срок действия сертификатов, выдаваемых CA.

Определения списка аннулированных сертификатов (CRL)

Список аннулированных сертификатов (CRL) - это файл, содержащий список всех недопустимых и аннулированных сертификатов определенной сертификатной компании (CA). Сертификатные компании периодически обновляют свои CRL и предоставляют их внешним пользователям для опубликования в каталогах LDAP. Некоторые сертификатные компании, например SSH в Финляндии, публикуют сами CRL в каталогах LDAP. Если сертификатная компания публикует свой собственный CRL, то это будет отмечено в сертификате: в унифицированный идентификатор ресурсов (URI) будет добавлено расширение узла рассылки CRL.

Диспетчер цифровых сертификатов позволяет создавать и управлять определениями CRL. Применение CRL повышает надежность проверки сертификатов. Определение CRL содержит информацию о расположении и способе доступа к серверу Lightweight Directory Access Protocol (LDAP), на котором хранится CRL.

При идентификации сертификата приложения обращаются к определению CRL (если оно задано), чтобы убедиться, что соответствующая сертификатная компания не аннулировала данный сертификат. DCM позволяет задавать и изменять информацию определения CRL, необходимую приложениям для работы с CRL при идентификации сертификата. Примерами приложений и процессов, которые могут выполнять идентификацию сертификатов с помощью CRL, служат: виртуальная частная сеть (VPN), сервер обмена ключами Internet (IKE), приложения с поддержкой Secure Sockets Layer (SSL) и приложения, подписывающие объекты. Кроме того, если определение CRL связано с сертификатом CA, то DCM применяет CRL при проверке сертификатов, выданных этой CA.

Хранилища сертификатов

Хранилище сертификатов - это специальный файл базы данных, в котором Диспетчер цифровых сертификатов (DCM) хранит цифровые сертификаты. В хранилище сертификатов также хранятся личные ключи сертификатов, если только для этого не был выбран Шифровальный сопроцессор 4758. DCM позволяет создавать несколько типов хранилищ сертификатов и управлять ими. Управление доступом к хранилищам сертификатов осуществляется в DCM с помощью паролей и средств управления доступом к каталогу и файлам IFS, составляющим хранилища сертификатов.

Классификация хранилищ сертификатов основана на типах сертификатов, которые в них хранятся. Набор доступных задач по управлению сертификатами зависит от типа сертификатов в выбранном хранилище сертификатов. В DCM заранее определены следующие хранилища сертификатов:

Локальная сертификатная компания (CA)
В этом хранилище сертификатов DCM хранит сертификат локальной сертификатной компании и его личный ключ, если такая сертификатная компания создана. С помощью этого сертификата подписываются сертификаты, выдаваемые локальной сертификатной компанией. При создании сертификата с помощью локальной сертификатной компании DCM сохраняет копию сертификата сертификатной компании (без личного ключа) в соответствующем хранилище сертификатов (например *SYSTEM) для последующей идентификации. С помощью сертификатов сертификатных компаний приложения проверяют подлинность сертификатов в ходе согласования SSL для предоставления доступа к ресурсам.

***SYSTEM**
Это хранилище сертификатов предназначено для управления сертификатами клиентов и серверов, с помощью которых приложения принимают участие в сеансах Secure Sockets Layer (SSL). Приложения IBM iSeries (и приложения многих других разработчиков программного обеспечения) применяют только сертификаты из хранилища сертификатов *SYSTEM. Это хранилище сертификатов создается в DCM при создании локальной сертификатной компании. Если вы решили получать сертификаты для приложений клиента или сервера от общедоступной сертификатной компании, например VeriSign, то необходимо создать это хранилище сертификатов.

***OBJECTSIGNING**
Это хранилище сертификатов DCM предназначено для управления сертификатами, с помощью которых добавляются цифровые подписи к объектам. Кроме того, задачи, связанные с этим хранилищем сертификатов, позволяют добавлять к объектам цифровые подписи, а также и просматривать и проверять подписи объектов. Это хранилище сертификатов создается в DCM при создании локальной сертификатной компании. Если вы решили получать сертификаты для добавления подписей к объектам от общедоступной сертификатной компании, например VeriSign, то необходимо создать это хранилище сертификатов.

***SIGNATUREVERIFICATION**
Это хранилище сертификатов DCM предназначено для управления сертификатами, с помощью которых проверяется подлинность цифровых подписей объектов. Для проверки цифровой подписи объекта это хранилище сертификатов должно содержать копию сертификата, с помощью которого был подписан объект. Кроме того, в этом хранилище сертификатов должна находиться копия сертификата сертификатной компании (CA), выдавшей сертификат для добавления подписей к объектам. Для получения этих сертификатов необходимо либо экспортировать сертификаты добавления подписей к объектам, находящиеся в данной системе, в хранилище сертификатов, либо импортировать сертификаты, полученные от владельца подписи.

Другое хранилище сертификатов
Это альтернативное хранилище для сертификатов клиентов и серверов, предназначенных для сеансов SSL. Другие хранилища сертификатов являются дополнительными пользовательскими хранилищами сертификатов SSL. Они обеспечивают управление сертификатами, программируемый доступ к которым при настройке соединения SSL осуществляется в пользовательских приложениях с помощью API SSL_Init. Этот API предназначен для применения сертификата по умолчанию. Чаще всего это хранилище сертификатов применяется при переносе сертификатов из предыдущего выпуска DCM или для создания специального подмножества сертификатов для SSL.

Примечание: Если на сервере iSeries установлен шифровальный сопроцессор IBM 4758 PCI, то вы можете задать дополнительные опции хранения личных ключей для сертификатов (кроме сертификатов подписи объекта, которые, как известно, не содержат личных ключей). Кроме того, сопроцессор позволяет зашифровать личный ключ и хранить его в специальном файле ключей, а не в хранилище сертификатов.

Хранилища сертификатов DCM защищены паролями. Кроме того, в DCM паролями защищены каталог в интегрированной файловой системе и файлы, образующие хранилища сертификатов. Пути в интегрированной файловой системе к хранилищам сертификатов Локальная сертификатная компания (CA), *SYSTEM, *OBJECTSIGNING и *SIGNATUREVERIFICATION предопределены и не могут быть изменены. Напротив, Другие хранилища сертификатов могут находиться в произвольном каталоге интегрированной файловой системы.

Шифрование

Шифрование - это преобразование данных с целью защитить их от постороннего доступа. Шифрование позволяет защитить информацию, хранящуюся в системе или передаваемую по сети, от тех, для кого она не предназначена. В результате шифрования обычный текст преобразуется в нечитаемые данные. Процедура восстановления обычного текста из зашифрованных данных называется расшифровкой. Оба процесса основаны на применении сложного математического алгоритма, в котором используется секретная строка символов (ключ).

Существует два типа шифрования:

- **Шифрование с секретным ключом** называется симметричным. В этом случае обе системы, участвующие в обмене данными, применяют один и тот же секретный ключ. Этот ключ служит и для шифрования, и для расшифровки.
- **Шифрование с общим ключом** называется несимметричным. В этом случае для шифрования и расшифровки применяются разные ключи. В каждой системе хранится пара ключей, состоящая из общего ключа и личного ключа. Общий ключ свободно распространяется, обычно вместе с цифровым сертификатом, а личный ключ известен только его владельцу. Эти ключи однозначно определяют друг друга по математическому правилу, однако получить личный ключ, зная общий, возможно лишь теоретически - на практике это занимает слишком много времени. Объект, например сообщение, зашифрованный с помощью общего ключа, можно расшифровать только с помощью соответствующего личного ключа. Кроме того, сервер или пользователь могут подписывать свои документы личным ключом, а получатель может с помощью общего ключа расшифровывать чужие цифровые подписи для проверки подлинности источника и целостности объекта.

Secure Sockets Layer (SSL)

Протокол Secure Sockets Layer (SSL), разработанный фирмой Netscape, является стандартным средством шифрования данных в соединениях между клиентом и сервером. В SSL применяется несимметричное шифрование, или шифрование с общим ключом. Клиент и сервер согласуют между собой ключ сеанса во время обмена цифровыми сертификатами. Срок действия ключа автоматически истекает через 24 часа, после чего для каждого соединения сервера с клиентом процесс SSL создает новый ключ. Следовательно, даже если злоумышленники перехватят и расшифруют ключ сеанса (что маловероятно), они не смогут получить информацию из последующих сеансов.

Глава 6. Планирование работы с DCM

Для эффективного управления цифровыми сертификатами вашей компании с помощью Диспетчера цифровых сертификатов (DCM) в стратегии защиты необходимо отдельно спланировать использование цифровых сертификатов.

Дополнительная информация о планировании работы с DCM и об интеграции цифровых сертификатов в стратегию защиты приведена в следующих разделах:

Требования для работы с DCM
Здесь указаны программное обеспечение и прочая информация, необходимые для настройки системы для работы с DCM.

Типы цифровых сертификатов
Содержит информацию о различных типах цифровых сертификатов, поддерживаемых DCM.

Сравнение общих и частных сертификатов
Здесь приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов, если вы решили улучшить защиту информации с их помощью. Вы можете получать сертификаты от общественной сертификатной компании или создать частную сертификатную компанию для выдачи сертификатов. Выбор между этими двумя способами зависит от того, с какой целью будут применяться сертификаты.

Цифровые сертификаты для соединений Secure Sockets Layer (SSL)
Здесь приведена информация о том, как приложения могут с помощью цифровых сертификатов устанавливать защищенные соединения.

Применение цифровых сертификатов для идентификации пользователей
Здесь приведена информация о том, как с помощью цифровых сертификатов можно усовершенствовать процедуру идентификации пользователей, запрашивающих ресурсы сервера iSeries.

Применение цифровых сертификатов в соединениях виртуальной частной сети (VPN)
Здесь приведена информация о применении цифровых сертификатов в настройке соединений VPN.

Цифровые сертификаты подписи объектов
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

Применение цифровых сертификатов для проверки подписей объектов
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно убедиться в подлинности объектов путем проверки их цифровых подписей.

Требования для установки DCM

Диспетчер цифровых сертификатов (DCM) - это бесплатная программа iSeries, позволяющая централизованно управлять цифровыми сертификатами для приложений. Для успешной работы с DCM необходимо выполнить следующие действия:

- Установить лицензионную программу Cryptographic Access Provider (5722–AC3). Эта программа шифрования определяет максимальную длину ключа шифрования в соответствии с законодательством, регулирующим экспорт и импорт. Этот продукт необходимо установить перед созданием сертификатов.
- Установить компонент 34 операционной системы OS/400. Это DCM с интерфейсом браузера.

- Установить IBM HTTP Server для iSeries (5722–DG1) и запустить экземпляр сервера *ADMIN.
- Убедиться, что в системе настроен TCP, что позволяет работать с DCM с помощью Web-браузера и экземпляра *ADMIN сервера HTTP Server.

Примечание: Для создания сертификатов необходимо установить все перечисленные продукты. Если хотя бы один из необходимых продуктов не будет установлен, то будет выдано сообщение о необходимости установить недостающий компонент.

Типы цифровых сертификатов

Существует несколько классификаций цифровых сертификатов. Они отражают способ применения сертификатов. Диспетчер цифровых сертификатов (DCM) позволяет управлять следующими типами сертификатов:

Сертификаты сертификатных компаний (CA)
Сертификат сертификатной компании - это удостоверение, подтверждающее подлинность CA. Сертификат содержит идентификационную информацию о компании и общий ключ. С помощью общего ключа сертификатной компании другие пользователи могут проверить подлинность выдаваемых и подписываемых ей сертификатов. Сертификат CA может быть подписан другой сертификатной компанией, например VeriSign, или этой же сертификатной компанией, если она является независимой. Все сертификатные компании, создаваемые с помощью Диспетчера цифровых сертификатов, являются независимыми. С помощью общего ключа сертификатной компании другие пользователи могут проверить подлинность выдаваемых и подписываемых ей сертификатов. Для применения сертификата в соединениях SSL, подписания объектов или проверки подписей объектов у вас должна быть копия сертификата сертификатной компании, выдавшей сертификат.

Сертификаты клиентов и серверов
Сертификат клиента или сервера - это удостоверение, идентифицирующее применяющее его приложение клиента или сервера. Сертификаты клиента и сервера содержат идентификационную информацию об организации, которой принадлежит приложение, например, отличительное имя системы. Кроме того, сертификат содержит общий ключ системы. Сертификат обязателен, если сервер устанавливает защищенные соединения SSL. Приложение, поддерживающее цифровые сертификаты, идентифицирует сервер по сертификату во время подключения. На основе этой идентификации приложение устанавливает сеанс SSL между клиентом и сервером. Управление сертификатами этого типа может осуществляться только в хранилище сертификатов *SYSTEM.

Сертификаты подписи объектов
Сертификат подписи объектов - это сертификат, с помощью которого к объектам добавляются цифровые подписи. Подпись объекта позволяет проверить его целостность, а также определить источник его происхождения или принадлежность. С помощью сертификатов можно подписывать различные объекты, включая большинство объектов интегрированной файловой системы (IFS) и объекты *CMD. Полный список объектов, к которым могут быть добавлены цифровые подписи, приведен в разделе Подписание объектов и проверка подписей. Для проверки подписи, созданной с помощью личного ключа сертификата подписи объекта, у получателя объекта должны быть копия соответствующего сертификата проверки подписей. Управление сертификатами этого типа может осуществляться только в хранилище сертификатов *OBJECTSIGNING.

Сертификаты проверки подписей
Сертификат проверки подписей - это копия сертификата подписи объекта, но без личного ключа. Общий ключ сертификата проверки подписей предназначен для проверки цифровых подписей, созданных с помощью сертификата подписи объекта. Проверка подписи позволяет идентифицировать источник объекта, а также определить, не изменялся ли объект с момента его подписания. Управление сертификатами этого типа может осуществляться только в хранилище сертификатов *SIGNATUREVERIFICATION.

Сертификаты пользователей
Сертификат пользователя - это удостоверение, идентифицирующее личность своего владельца. Многие современные приложения поддерживают идентификацию пользователей с помощью сертификатов вместо имен пользователей и паролей. Диспетчер цифровых сертификатов (DCM) автоматически связывает сертификаты пользователей, выданные частной сертификатной компанией, с пользовательскими профайлами iSeries. Кроме того, DCM позволяет связать с пользовательским профайлом iSeries сертификат пользователя, выданный другой сертификатной компанией.

Диспетчер цифровых сертификатов (DCM) распределяет сертификаты по типам и размещает их вместе с соответствующими личными ключами в хранилище сертификатов.

Примечание: Если на сервере iSeries установлен шифровальный сопроцессор IBM 4758 PCI, то вы можете задать дополнительные опции хранения личных ключей для сертификатов (кроме сертификатов подписи объектов, которые, как известно, не содержат личных ключей). В частности, личные ключи можно хранить в самом сопроцессоре. Кроме того, сопроцессор позволяет зашифровать личный ключ и хранить его в специальном файле ключей, а не в хранилище сертификатов. В то же время, сертификаты пользователей и их личные ключи хранятся в системах пользователей: либо в браузере, либо в файле, предназначенном для применения другими клиентскими приложениями.

Сравнение общих и частных сертификатов

Если вы решили применять сертификаты, то сначала вы должны выбрать тип сертификатной компании. Возможны следующие варианты получения сертификатов:
- Приобретение сертификатов у общественной сертификатной компании (CA) Internet.
- Создание собственной сертификатной компании и выдача частных сертификатов локальным пользователям с ее помощью.
- Применение и сертификатов общественной CA, и сертификатов частной CA.

Выбор конкретного варианта зависит от нескольких факторов, наиболее важным из которых является среда, в которой будут применяться сертификаты. Ниже приведены советы по выбору наилучшего решения.

Применение общих сертификатов

Общественные сертификатные компании Internet выдают сертификаты любым пользователям за определенную плату. Для получения сертификата у общественной CA необходимо предоставить ей некоторую идентификационную информацию. Объем этой информации зависит от идентификационной стратегии данной сертификатной компании. Перед тем как остановить свой выбор на той или иной сертификатной компании, необходимо оценить, насколько ее идентификационная стратегия отвечает требованиям к защите вашей системы. С появлением стандартов Инфраструктуры общих ключей X.509 (PKIX) некоторые общественные сертификатные компании ужесточили свои требования к идентификационной информации. Хотя получение сертификатов от таких сертификатных компаний более трудоемко, эти сертификаты обеспечивают более надежную защиту доступа к приложениям. Диспетчер цифровых сертификатов (DCM) позволяет применять сертификаты, полученные от сертификатных компаний PKIX.

Оцените также затраты на получение сертификатов у общественной сертификатной компании. Если сертификаты требуются для ограниченного числа пользователей и приложений, то издержки, возможно, не будут играть решающей роли. Однако этот фактор становится существенным при наличии большого числа *частных* пользователей, применяющих сертификаты для идентификации клиента. В этом случае необходимо также учитывать административные издержки и расходы на настройку приложений, поскольку последние должны будут принимать только определенный набор сертификатов, выданных общественной сертификатной компанией.

Применение сертификатов, полученных от общественных сертификатных компаний, позволяет сэкономить время и ресурсы, так как многие серверные, клиентские и пользовательские приложения автоматически распознают широко известные общественные сертификатные компания. Кроме того, другие компании и пользователи могут больше доверять сертификатам, выданным общеизвестной сертификатной компанией, чем тем, что созданы частной сертификатной компанией.

Применение частных сертификатов

Локальная CA предназначена для выдачи сертификатов ограниченному кругу пользователей, например сотрудникам данной фирмы. Создав собственную CA, вы сможете выдавать сертификаты только тем пользователям, которым вы доверяете. Это обеспечивает более высокий уровень защиты, поскольку позволяет установить более строгий контроль за доступом к ресурсам. Недостаток локальной CA заключается в том, что для ее создания требуется значительное время и ресурсы. Однако задача существенно облегчается, если воспользоваться Диспетчером цифровых сертификатов (DCM).

Если с помощью локальной сертификатной компании пользователям выдаются сертификаты для идентификации клиентов, то вы должны решить, следует ли связывать сертификаты пользователей с пользовательскими профайлами iSeries. Если сертификаты необходимо связать с пользовательскими профайлами iSeries, то пользователи должны получать сертификаты от локальной сертификатной компании с помощью DCM. Кроме того, начиная с версии V5R2 можно с помощью API выдавать сертификаты пользователям других систем, не имеющим пользовательских профайлов iSeries.

Примечание: Независимо от типа CA, выбранной для получения сертификатов, системный администратор должен определить, сертификаты каких CA будет разрешено принимать системе. Если в браузере есть копия сертификата хорошо известной CA, то такую CA можно считать надежной. Однако если сертификат CA отсутствует в хранилище сертификатов *SYSTEM, то сервер не будет принимать сертификаты пользователей и клиентов, выданные этой CA. Для того чтобы принимать сертификаты пользователей, выданные определенной CA, необходимо получить копию сертификата этой CA. Копия должна быть передана в правильном формате и сохранена в хранилище сертификатов DCM.

Приведенные сценарии работы с сертификатами помогут вам выбрать наилучший вариант получения сертификатов.

Связанные задачи

Информация о выполнении следующих задач с помощью Диспетчера цифровых сертификатов поможет вам реализовать свой план, после того как вы выбрали способ применения и получения сертификатов:

- Раздел Создание и управление частной сертификатной компанией содержит описания задач по созданию сертификатов с помощью частной сертификатной компании.
- Раздел Управление сертификатами, полученными от общественной сертификатной компании содержит описания задач по работе с сертификатами, полученными от известной общественной сертификатной компании, включая сертификатные компании PKIX.
- Раздел Применение локальной сертификатной компании на других серверах iSeries содержит описания задач по применению сертификатов, созданных частной сертификатной компанией, в нескольких системах.

Применение цифровых сертификатов в защищенных соединениях SSL

Цифровые сертификаты позволяют настроить применение защищенных соединений Secure Sockets Layer (SSL) в приложениях. При настройке соединения SSL сервер предоставляет копию своего сертификата клиенту, запросившему соединение, для проверки. Применение соединения SSL позволяет:

- Идентифицировать сервер в системе клиента или конечного пользователя.
- Обеспечить шифрование данных, передаваемых через соединение.

Ниже описана процедура взаимодействия клиента и сервера в защищенном сеансе:

1. Приложение сервера отправляет сертификат приложению клиента (пользователя) для идентификации.
2. Приложение клиента проверяет подлинность сертификата сервера с помощью копии сертификата сертификатной компании, выдавшей сертификат сервера. (Приложению клиента необходимо доступ к локальной копии сертификата соответствующей сертификатной компании).
3. Приложения клиента и сервера согласовывают симметричный ключ для шифрования передаваемых данных.
4. Кроме того, перед тем как предоставить клиенту доступ к запрашиваемым ресурсам, сервер может потребовать от него идентификационную информацию. Приложения, поддерживающие применение сертификатов для идентификации пользователей, в качестве такой информации могут предоставить цифровой сертификат.

Во время согласования симметричного ключа в сеансе SSL применяется асимметричный (общий) ключ. Затем в течение всего сеанса SSL для шифрования и расшифровки данных приложения применяется симметричный ключ. Это означает, что в разных сеансах применяются разные ключи, срок действия которых автоматически истекает через определенное время. Даже если ключ какого-либо сеанса будет перехвачен и расшифрован, его нельзя будет использовать для определения последующих ключей.

Применение цифровых сертификатов для идентификации пользователей

Как правило, доступ к ресурсам из приложения или системы предоставляется на основе имени пользователя и пароля. Применение цифровых сертификатов вместо имен и паролей, обычно используемых для идентификации удаленного сервера или пользователя, еще больше повышает защищенность системы. С помощью Диспетчера цифровых сертификатов (DCM) вы можете связать сертификат пользователя с его пользовательским профайлом iSeries. В этом случае у сертификата будут те же права доступа, что и у связанного с ним пользовательского профайла. Начиная с версии V5R2, можно выдавать сертификаты частной локальной сертификатной компании пользователям других систем с помощью API. Эти API позволяют выдавать частные сертификаты пользователям, для которых вы не хотите создавать пользовательские профайлы iSeries.

Цифровой сертификат выступает в роли удостоверения личности своего владельца. Его можно сравнить с паспортом. И сертификат, и паспорт содержат данные о владельце, уникальный идентификационный номер, а также название организации, подтверждающей подлинность документа. В случае сертификата, в роли такой организации выступает сертификатная компания - уполномоченная третья сторона, которая выдает сертификат и выступает гарантом его подлинности.

В целях идентификации в сертификате применяется пара ключей - общий и личный. Сертификатная компания, выдающая сертификат, добавляет к сертификату эти ключи вместе с прочей информацией о владельце сертификата.

В настоящее время достаточно большое число приложений поддерживают применение сертификатов для идентификации клиентов в соединениях SSL. В текущей версии поддержку идентификации клиентов с помощью сертификатов обеспечивают следующие приложения iSeries:

- Сервер Telnet
- IBM HTTP Server (стандартный и на основе Apache)
- Сервер Служб каталогов (LDAP)
- Централизованное управление
- Client Access Express (включая Навигатор iSeries)
- Сервер FTP

В будущем список приложений, поддерживающих идентификацию клиентов с помощью сертификатов, может быть пополнен; информация о поддержке данной функции в конкретных приложениях приведена в соответствующей документации.

Сертификаты являются более надежными средствами идентификации пользователей по нескольким причинам:

- Пользователь может забыть свой пароль. По этой причине, пользователи часто записывают свои ИД пользователя и пароли, чтобы не забыть их. Однако в этом случае ИД и пароли могут быть обнаружены другими пользователями. Напротив, сертификаты хранятся в файле или другом электронном носителе, и обращение к сертификату и его предъявление для идентификации выполняется клиентским приложением (а не пользователем). Это уменьшает вероятность передачи сертификата незарегистрированному пользователю, если у последнего нет доступа к системе. Кроме того, сертификаты могут быть установлены на смарт-карты в качестве дополнительной меры защиты от несанкционированного доступа.
- Сертификат содержит личный ключ, который никогда не передается вместе с сертификатом. Этот ключ применяется системой для шифрования и расшифровки данных. Соответствующий общий ключ позволяет другим пользователям проверить подлинность отправителя объекта, подписанного личным ключом.

- Во многих системах длина пароля ограничена 8 символами, что делает систему уязвимой к атакам путем угадывания пароля. Длина шифровальных ключей сертификата составляет сотни символов. Ключ такой длины, содержащий к тому же случайный набор символов, подобрать намного сложнее, чем пароль.
- В отличие от паролей, цифровые сертификаты могут обеспечивать секретность и целостность данных. Применение сертификатов и соответствующих ключей позволяет:
  - Обеспечить целостность данных.
  - Гарантировать, что запрошенное действие было действительно выполнено. Такое свойство называется контролируемостью.
  - Защищенные соединения Secure Sockets Layer (SSL) с шифрованием данных обеспечивают секретность передаваемой информации.

Дополнительная информация о настройке применения сертификатов для идентификации клиентов в соединениях SSL в приложениях сервера iSeries приведена в разделе Защита приложений с помощью SSL.

Применение цифровых сертификатов в соединениях VPN

С помощью цифровых сертификатов можно устанавливать соединения виртуальной частной сети (VPN) iSeries. Обе конечных системы динамического соединения VPN должны иметь возможность идентифицировать друг друга перед активизацией соединения. Идентификация партнера выполняется серверами Обмена ключами Internet (IKE) в каждой из конечных систем. После успешной идентификации серверы IKE согласовывают методы шифрования и алгоритмы защиты соединений VPN.

В версиях до V5R1 серверы IKE могли выполнять идентификацию только с помощью заранее переданного ключа. Такой способ идентификации менее надежен, так как ключ должен быть вручную передан администратору другой конечной системы соединения VPN. Следовательно, существует вероятность перехвата ключа во время его передачи.

Для идентификации конечных систем можно применять цифровые сертификаты, что исключает возможность перехвата ключа. При установлении защищенного соединения сервер IKE идентифицирует конечную систему по ее сертификату.

Управлять сертификатами, с помощью которых сервер IKE устанавливает динамическое соединение VPN, можно с помощью Диспетчера цифровых сертификатов (DCM). Сначала необходимо решить, будет ли сервер IKE применять общие или личные сертификаты.

В некоторых реализациях VPN требуется, чтобы помимо отличительного имени сертификат содержал альтернативную информацию об имени субъекта, такую как имя домена или электронный адрес. Эту альтернативную информацию можно задать, когда вы выдаете сертификат с помощью частной сертификатной компании в DCM. Наличие альтернативной информации гарантирует совместимость данного соединения VPN iSeries с другими реализациями VPN.

Дополнительная информация по применению сертификатов в соединениях VPN приведена в следующих источниках:

- Если вы никогда прежде не работали с сертификатами с помощью DCM, ознакомьтесь со следующими разделами:
  - Раздел Создание и управление частной локальной сертификатной компанией содержит информацию о создании частных сертификатов для приложений с помощью DCM.

– Раздел Управление сертификатами, полученными от общественной сертификатной компании содержит информацию о работе с сертификатами, полученными от общественной сертификатной компании (CA), с помощью DCM.

- Если вы уже работаете с сертификатами, предназначенными для других приложений, с помощью DCM, то информация следующих разделов поможет вам настроить применение данного сертификата в приложении и определить, какие сертификаты принимает и идентифицирует данное приложение:
  – Раздел Управление присвоением сертификата приложению содержит информацию о том, как с помощью DCM связать существующий сертификат с приложением, например с сервером IKE.
  – Раздел Определение списка уполномоченных сертификатных компаний для приложения содержит информацию о том, как задать сертификатные компании, сертификаты которых приложение должно принимать при идентификации клиента (или VPN).

Цифровые сертификаты подписи объектов

Начиная с версии V5R1 операционная система OS/400 поддерживает подписание объектов с помощью цифровых сертификатов. Добавление цифровой подписи к объекту позволяет контролировать целостность его содержимого и подлинность его источника. Поддержка цифровых подписей повышает эффективность традиционных средств контроля за доступом к объектам iSeries. Обычные средства не позволяют защитить объект от несанкционированного изменения во время его передачи по сети Internet или другой незащищенной сети, а также при его хранении в системе, отличной от iSeries. Кроме того, обычные средства часто не позволяют определить, была ли нарушена целостность объекта. Добавление цифровых подписей к объектам позволяет обнаружить внесение изменений в подписанные объекты.

Подписание объекта заключается в выполнении специальной математической функции, которая на основе содержимого объекта и личного ключа сертификата генерирует определенный код - цифровую подпись. Этот код и добавляется к объекту. Подпись защищает данные от несанкционированного изменения. Содержимое самого объекта не шифруется цифровой подписью; однако шифруется сама подпись для защиты от изменения. Пользователь, желающий убедиться в целостности содержимого объекта и подлинности его источника, может с помощью общего ключа сертификата проверить цифровую подпись. Если подпись не совпадает, то объект, возможно, был изменен. В этом случае получателю следует воздержаться от применения объекта и обратиться к лицу, подписавшему объект, чтобы получить другую копию.

Если вы, в соответствии с требованиями к защите и стратегиями защиты, решили применять цифровые подписи, то вы должны выбрать между общими сертификатами и частными сертификатами. Если вы собираетесь распространять объекты среди широкого круга пользователей, то для подписания объектов рекомендуется применять сертификаты общеизвестной сертификатной компании (CA). Это позволяет внешним пользователям легко и без дополнительных затрат проверять подписи распространяемых вами объектов. Если же вы планируете распространять объекты в рамках своей организации, то вы можете с помощью Диспетчера цифровых сертификатов (DCM) создать собственную локальную сертификатную компанию для подписания объектов. Применение локальной сертификатной компании (CA) позволяет сэкономить на приобретении сертификатов у общеизвестной CA.

Подпись на объекте представляет систему, подписавшую объект, а не конкретного пользователя в этой системе (хотя для применения сертификатов подписи объектов пользователь должен обладать определенными правами доступа). Управлять сертификатами, с помощью которых подписываются объекты и проверяются цифровые подписи, вы можете с помощью Диспетчера цифровых сертификатов (DCM). DCM также позволяет подписывать объекты и проверять подписи объектов.

Применение цифровых сертификатов для проверки подписей объектов

Начиная с версии V5R1, сервер iSeries поддерживает применение сертификатов для проверки цифровых подписей объектов. Пользователь, желающий убедиться в целостности содержимого подписанного объекта и подлинности его источника, может с помощью общего ключа сертификата проверить цифровую подпись. Если подпись не совпадает, то объект, возможно, был изменен. В этом случае получателю следует воздержаться от применения объекта и обратиться к лицу, подписавшему объект, чтобы получить другую копию.

Подпись на объекте представляет систему, подписавшую объект, а не определенного пользователя в этой системе. Для проверки подписей объектов необходимо определить список уполномоченных сертификатных компаний и надежных сертификатов. Выбрав сертификатную компанию в качестве уполномоченной, вы можете дополнительно указать, будут ли приниматься объекты с подписями, созданными с помощью сертификатов, выданных этой сертификатной компанией. Если сертификатная компания отсутствует в списке уполномоченных, то объекты с подписями, созданными с помощью сертификатов, выданных этой сертификатной компанией, приниматься не будут.

Системное значение Проверять восстанавливаемые объекты (QVFYOBJRST)

Если вы решили применять проверку цифровых подписей, то одной из важнейших задач становится определение степени важности подписей объектов, восстанавливаемых в системе. Для этого служит системное значение QVFYOBJRST. По умолчанию это значение разрешает восстанавливать только неподписанные объекты и подписанные объекты с действительными подписями. Система считает подписанными только те объекты, подписи которых добавлены с помощью надежных сертификатов; другие подписи система игнорирует и считает такие объекты неподписанными.

Системное значение QVFYOBJRST может задавать различные режимы: от игнорирования любых подписей до проверки подписей всех восстанавливаемых объектов. Это системное значение действительно лишь для исполняемых объектов системы, но не для файлов сохранения и файлов IFS. Дополнительная информация о применении этого и других системных значений приведена в разделе Information Center Программа поиска системных значений.

Реализовать выбранную стратегию работы с сертификатами и сертификатными компаниями, а также управлять сертификатами, с помощью которых проверяются цифровые подписи, вы можете с помощью Диспетчера цифровых сертификатов (DCM). DCM также позволяет подписывать объекты и проверять подписи объектов.

Глава 7. Настройка DCM

Диспетчер цифровых сертификатов (DCM) обеспечивает управление цифровыми сертификатами для приложений и пользователей с помощью пользовательского интерфейса на основе браузера. Пользовательский интерфейс состоит из двух главных окон: окна навигации и окна задач.

Окно навигации предназначено для выбора задач по управлению сертификатами или применяющими их приложениями. Некоторые задачи вынесены непосредственно в главное окно навигации, но большинство задач в окне навигации находятся внутри разделов - категорий. Например, **Управление сертификатами** - это категория задач, в которую входят различные пошаговые задачи, такие как Просмотр сертификата, Обновление сертификата, Импорт сертификата и т.д. Категории в окне навигации отмечены стрелками слева от названия. При выборе категории появляется полный список ее задач.

Все задачи в окне навигации, кроме задач категории **Быстрый доступ**, являются пошаговыми, т.е. состоят из нескольких этапов, на каждом из которых предоставляется необходимая информация. Категория Быстрый доступ содержит набор функций управления сертификатами и приложениями, с помощью которых опытные пользователи DCM могут быстро выполнить необходимые задачи.

Набор задач, доступных в окне навигации, зависит от выбранного хранилища сертификатов. Кроме того, число категорий и содержащихся в них задач зависит от прав доступа, заданных в профайле пользователя iSeries. Все задачи по управлению сертификатной компанией и применяемыми приложениями сертификатами, а также другие задачи на уровне системы доступны только системным администраторам iSeries. Для просмотра и выполнения таких задач у системного администратора должны быть специальные права доступа *SECADM и *ALLOBJ. Пользователи без специальных прав доступа могут работать только со своими сертификатами.

Информация, необходимая для работы с цифровыми сертификатами с помощью DCM, приведена в следующих разделах:

Запуск DCM
Содержит информацию о запуске функции Диспетчер цифровых сертификатов сервера iSeries.

Первая настройка сертификатов
Здесь указано, какие действия необходимо выполнить перед началом работы с цифровыми сертификатами с помощью DCM. Здесь же приведена информация о работе с сертификатами общественных сертификатных компаний Internet (CA) и создании частной локальной сертификатной компании и выдаче сертификатов с ее помощью.

Дополнительная информация об усовершенствовании защиты системы и сети в среде Internet с помощью цифровых сертификатов приведена на Web-сайте VeriSign. Этот Web-сайт содержит большую библиотеку по темам, связанным с цифровыми сертификатами и защите информации в сети Internet. Ссылка на библиотеку VeriSign:

VeriSign Help Desk .

Запуск Диспетчера цифровых сертификатов

Прежде чем вы сможете работать с функциями Диспетчера цифровых сертификатов (DCM), вы должны его запустить. Для запуска DCM выполните следующие действия:

1. Установите компонент 34 продукта 5722 SS1. Это Диспетчер цифровых сертификатов (DCM).

   Установите продукт 5722 DG1. Это IBM HTTP Server для iSeries.

   Установите продукт 5722 AC3. Это программа шифрования, с помощью которой DCM V5R2 генерирует пару ключей - личный и общий - для каждого сертификата, шифрует файлы экспортированных сертификатов и расшифровывает файлы импортированных сертификатов.
2. С помощью Навигатора iSeries запустите экземпляр *ADMIN сервера HTTP:
   a. Запустите Навигатор **iSeries**.
   b. Щелкните дважды на сервере iSeries в главном окне иерархического списка.
   c. Дважды щелкните на **Сеть**.
   d. Дважды щелкните на **Серверы**.
   e. Дважды щелкните на **TCP/IP**.
   f. Дважды щелкните на **Управление HTTP**.
   g. Нажмите кнопку **Запустить**.
3. Запустите Web-браузер.
4. Загрузите в окно браузера страницу задач iSeries, введя следующий URL: http://*имя-системы*:2001.
5. В списке продуктов на странице задач iSeries выберите **Диспетчер цифровых сертификатов** для работы с функцией DCM.

Если вы переходите к новой версии DCM, то на этой странице будут приведены инструкции по обновлению системы.

Первая настройка сертификатов

В левой части окна Диспетчера цифровых сертификатов (DCM) расположено окно навигации. Это окно позволяет выбирать различные задачи по управлению сертификатами и применяющими их приложениями. Набор доступных задач зависит от выбранного хранилища сертификатов (если оно есть) и прав доступа профайла пользователя. Большинство задач доступны только при наличии специальных прав доступа *ALLOBJ и *SECADM.

При первом запуске Диспетчера цифровых сертификатов (DCM) хранилища сертификатов еще не созданы (кроме случая перехода от предыдущей версии DCM). По этой причине, в окне навигации будут показаны только следующие задачи (при наличии у пользователя необходимых прав доступа):

- Управление сертификатами пользователей.
- Создание хранилища сертификатов.
- Создание сертификатной компании (CA). (Примечание: После создания частной сертификатной компании путем выполнения этой задачи последняя будет удалена из списка.)
- Управление определениями CRL.
- Управление определениями запросов PKIX.

Даже если в системе уже созданы хранилища сертификатов (например, так будет в случае перехода от предыдущей версии DCM), в окне навигации DCM будет показано ограниченное число задач или категорий задач. Для работы с большинством задач по управлению сертификатами и приложениями необходимо сначала выбрать

соответствующее хранилище сертификатов. Для того чтобы открыть нужное хранилище сертификатов, нажмите в окне навигации кнопку **Выбрать хранилище сертификатов**.

В окне навигации DCM также предусмотрена кнопка **Защищенное соединение**. Эта кнопка позволяет открыть дополнительное окно браузера для установления защищенного соединения Secure Sockets Layer (SSL). Для этого необходимо сначала настроить IBM HTTP Server для iSeries для работы с SSL в защищенном режиме. После этого нужно запустить сервер HTTP в защищенном режиме. Если защищенный сервер HTTP не настроен и не запущен, то будет выдано сообщение об ошибке и браузер не запустит защищенный сеанс.

Начало работы

Перед тем, как начать непосредственное применение сертификатов для обеспечения защиты информации, необходимо выбрать способ их получения. Существует две основных стратегии работы с DCM, различающиеся в зависимости от того, будут ли применяться общие или частные сертификаты:

Создание и управление локальной сертификатной компанией для выдачи сертификатов приложениям.

Управление сертификатами общественной сертификатной компании Internet для применения их приложениями.

Создание и управление локальной сертификатной компанией (CA)

Эта информация предназначена для тех, кто решил создавать сертификаты с помощью собственной локальной сертификатной компании (CA). Диспетчер цифровых сертификатов (DCM) позволяет создать частную локальную сертификатную компанию для выдачи сертификатов. DCM предоставит пошаговые инструкции по созданию сертификатной компании и выдаче сертификатов приложениям. Пошаговые инструкции помогут подготовить все необходимое для настройки применения SSL в приложениях, подписания объектов и проверки подписей с помощью цифровых сертификатов.

Примечание: Если сертификаты будут применяться IBM HTTP Server для iSeries, то перед тем, как начать работу с сертификатами с помощью DCM, необходимо создать и настроить Web-сервер. После того как вы настроите сервер для работы с SSL, для него будет создан ИД приложения. Запишите этот ИД, чтобы указать в DCM, какой сертификат данное приложение будет использовать для сеансов SSL.

Не перезапускайте сервер, пока не назначите ему сертификат в DCM. Если вы перезапустите экземпляр Web-сервера *ADMIN до того, как с ним будет связан сертификат, то сервер не будет запущен, и вы уже не сможете связать сертификат с сервером с помощью DCM.

Для создания локальной CA с помощью DCM выполните следующие действия:
1. Запустите DCM.
2. В окне навигации DCM выберите **Создать сертификатную компанию (CA)**. Будет показано несколько форм. Эти формы содержат инструкции по созданию локальной сертификатной компании и выполнению других задач, необходимых для применения цифровых сертификатов в соединениях SSL, подписания объектов и проверки подписей.

Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.

3. Заполните все необходимые формы. В процессе настройки локальной сертификатной компании (CA) путем заполнения этих форм вы должны выполнить следующие задачи:
   a. Выбрать способ хранения личного ключа сертификата локальной CA. (Этот шаг выполняется только в том случае, если на сервере iSeries установлен шифровальный сопроцессор IBM 4758–023 PCI. В противном случае сертификат и его личный ключ будут помещены в хранилище сертификатов локальной сертификатной компании (CA).)
   b. Предоставить идентификационную информацию для локальной CA.
   c. Установить сертификат локальной CA на PC или в браузере, чтобы соответствующая программа могла распознавать эту локальную сертификатную компанию и проверять выдаваемые ей сертификаты.
   d. Выбрать информацию о полномочиях локальной CA.
   e. Создать с помощью новой локальной сертификатной компании сертификат клиента или сервера, с помощью которого приложения будут устанавливать соединения SSL. (Если на сервере iSeries установлен шифровальный сопроцессор IBM 4758–023 PCI, этот шаг позволяет выбрать способ хранения личного ключа сертификата клиента или сервера. Если сопроцессор не установлен, то DCM автоматически поместит сертификат вместе с его личным ключом в хранилище сертификатов *SYSTEM. Эта подзадача включает также создание хранилища сертификатов *SYSTEM.)
   f. Выбрать приложения, которые будут с помощью сертификата клиента или сервера устанавливать соединение SSL.

      Примечание: Если вы ранее создали с помощью DCM хранилище сертификатов *SYSTEM для управления сертификатами для SSL, полученными от общественной сертификатной компании Internet, то этот или предыдущий шаг выполнять не нужно.
   g. Создать с помощью новой локальной сертификатной компании сертификат подписи объектов, с помощью которого приложения будут подписывать объекты. Эта подзадача включает создание хранилища сертификатов *OBJECTSIGNING, предназначенного для управления сертификатами подписи объектов.
   h. Выбрать приложения, которые будут с помощью сертификата добавлять к объектам цифровые подписи.

      Примечание: Если вы ранее создали с помощью DCM хранилище сертификатов *OBJECTSIGNING для управления сертификатами подписи объектов, полученными от общественной сертификатной компании, то этот или предыдущий шаг выполнять не нужно.
   i. Выбрать приложения, которые будут принимать сертификаты локальной сертификатной компании.

После выполнения пошаговой задачи у вас будет все необходимое для настройки приложений для работы с SSL.

После настройки приложений каждый пользователь, работающий с приложениями через соединение SSL, должен с помощью DCM получить копию сертификата локальной сертификатной компании. Это необходимо для того, чтобы клиентское программное обеспечение пользователя могло в ходе согласований SSL проверить подлинность сертификата сервера. DCM позволяет скопировать сертификат локальной сертификатной компании в файл или загрузить его в браузер. Способ

хранения сертификата локальной CA зависит от клиентского программного обеспечения, с помощью которого пользователи устанавливают соединение SSL с приложением.

Кроме того, локальная сертификатная компания позволяет выдавать сертификаты приложениям в других системах iSeries в сети.

Дополнительная информация о работе с сертификатами пользователей с помощью DCM и о том, как пользователи могут получить сертификат локальной сертификатной компании (CA) для проверки выдаваемых этой CA сертификатов, приведена в следующих разделах:

Управление пользовательскими сертификатами
Здесь приведена информация о том, каким образом пользователи могут с помощью DCM получить сертификаты или связать существующие сертификаты со своими пользовательскими профайлами iSeries.

Выдача сертификатов пользователям других систем с помощью API
Здесь приведена информация о том, как с помощью локальной сертификатной компании можно выдавать частные сертификаты пользователям, не связывая эти сертификаты с пользовательскими профайлами iSeries.

Получение копии сертификата частной сертификатной компании
Здесь приведена информация о получении копии сертификата частной сертификатной компании и его установке на персональном компьютере с целью идентификации выданных этой сертификатной компанией сертификатов серверов.

Управление пользовательскими сертификатами

Диспетчер цифровых сертификатов (DCM) позволяет пользователям системы управлять сертификатами, необходимыми для установления соединений SSL.

При работе с внешними и внутренними серверами через соединение SSL у пользователей должна быть копия сертификата CA, выдавшей сертификат сервера. Эта копия необходима программному обеспечению клиента для проверки подлинности сертификата сервера при установлении соединения. Если сервер применяет сертификат общественной CA, то программное обеспечение пользователей обычно уже содержит копию этого сертификата. В этом случае для установления сеанса SSL никаких дополнительных действий ни от администратора DCM, ни от пользователей не требуется. Однако при работе с сертификатом локальной CA пользователи должны получить копию этого сертификата перед установлением сеанса SSL с сервером.

Кроме того, если приложение сервера поддерживает и требует идентификацию клиентов посредством сертификатов, то пользователи должны представить необходимый сертификат, чтобы получить доступ к ресурсам сервера. В зависимости от требований защиты пользователи могут предъявлять сертификаты, выданные общей сертификатной компанией Internet или локальной сертификатной компанией. Если приложение сервера предоставляет доступ к ресурсам внутренним пользователям с пользовательскими профайлами iSeries, то с помощью DCM вы можете внести сертификаты в эти профайлы. В этом случае при предъявлении сертификатов пользователи будут наделены теми же правами доступа, что и их профайлы.

Диспетчер цифровых сертификатов (DCM) позволяет управлять сертификатами, связанными с пользовательскими профайлами iSeries. При наличии специальных прав доступа *SECADM и *ALLOBJ пользователь может управлять сертификатами, связанными со своим профайлом и профайлами других пользователей. Если открытых хранилищ сертификатов нет или открыто хранилище сертификатов

локальной сертификатной компании (CA), доступ к задачам управления сертификатами, связанными с пользовательскими профайлами, обеспечивает категория **Управление пользовательскими сертификатами** в окне навигации. Если открыто другое хранилище сертификатов, задачи управления пользовательскими сертификатами включены в задачи категории **Управление сертификатами**.

Пользователи, не обладающие специальными правами доступа *SECADM и *ALLOBJ, могут управлять только своими сертификатами. В категории **Управление пользовательскими сертификатами** собраны задачи, позволяющие таким пользователям просмотреть сертификат, связанный с их пользовательским профайлом, удалить сертификат из своего пользовательского профайла, а также связать со своим пользовательским профайлом сертификат, полученный от другой CA. Независимо от наличия специальных прав доступа, пользователи могут получить сертификат от локальной сертификатной компании, выбрав в главном окне навигации задачу **Создать сертификат**.

Дополнительная информация о создании и управлении пользовательскими сертификатами с помощью DCM приведена в следующих разделах:

Создание пользовательского сертификата
Здесь приведена информация о том, как с помощью локальной сертификатной компании пользователи могут создать сертификаты для идентификации клиента.

Присвоение пользовательского сертификата
Здесь приведена информация о том, как пользователь может связать сертификат со своим пользовательским профайлом. Это может быть сертификат, полученный от частной локальной сертификатной компании из другой системы или от общеизвестной сертификатной компании, действующей в сети Internet. Это может быть только сертификат надежной сертификатной компании. Он не должен быть связан с другим профайлом пользователя.

Создание пользовательского сертификата: Если вы планируете применять цифровые сертификаты для идентификации пользователей, то у всех пользователей должны быть сертификаты. Эти сертификаты могут быть выданы частной локальной сертификатной компанией, управляемой с помощью Диспетчера цифровых сертификатов. Каждый пользователь должен получить сертификат, выполнив задачу **Создать сертификат** в Диспетчере цифровых сертификатов. Для получения сертификата от локальной сертификатной компании необходимо, чтобы стратегия сертификатной компании позволяла ей выдавать пользовательские сертификаты.

Для получения сертификата от локальной сертификатной компании выполните следующие действия:
1. Запустите DCM.
2. В окне навигации выберите **Создать сертификат**.
3. Выберите тип сертификата **Пользовательский сертификат**. Будет показана форма для ввода информации о сертификате.
4. Заполните форму и нажмите кнопку **Продолжить**.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
5. На этом этапе DCM с помощью браузера создает общий и личный ключи для сертификата. Появится окно браузера с инструкциями по выполнению этой задачи. Выполните описанные действия. После того, как браузер создаст ключи, будет показано подтверждающее сообщение о создании сертификата.

6. Установите новый сертификат в программном обеспечении браузера. Появится окно браузера с инструкциями по выполнению этой задачи. Выполните описанные действия.
7. Нажмите кнопку **OK** для завершения задачи.

Диспетчер цифровых сертификатов автоматически свяжет сертификат с вашим пользовательским профайлом iSeries.

Для того чтобы сертификат другой сертификатной компании, предъявляемый пользователем для идентификации клиента, предоставлял пользователю те же права доступа, что и его пользовательский профайл, пользователь должен связать сертификат со своим пользовательским профайлом с помощью DCM.

Присвоение пользовательского сертификата: Если вы планируете применять цифровые сертификаты для идентификации пользователей, то у всех пользователей должны быть сертификаты. Если сертификаты выдаются общественной CA Internet, то пользователи могут связать их со своими профайлами с помощью Диспетчера цифровых сертификатов. В этом случае пользователи смогут работать с своими сертификатами с помощью DCM.

Для выполнения задачи **Присвоить пользовательский сертификат** необходимо установить защищенное соединение с сервером HTTP, посредством которого вы работаете с Диспетчером цифровых сертификатов. Защищенность соединения определяется по номеру порта в URL, с помощью которого был вызван DCM. Если соединение установлено через порт `2001`, применяемый по умолчанию для работы с DCM, то оно не защищено. Кроме того, перед запуском защищенного сеанса необходимо настроить поддержку SSL на сервере HTTP.

При запуске этой задачи появится новое окно браузера. Если защищенный сеанс не начат, то Диспетчер цифровых сертификатов предложит запустить его нажатием кнопки **Присвоить пользовательский сертификат**. После этого DCM начнет согласование Secure Sockets Layer (SSL) с браузером.

В ходе этого согласования браузер может предложить вам определить, следует ли считать надежной сертификатную компанию, выдавшую сертификат сервера HTTP. Кроме того, браузер может запросить вас о том, следует ли принимать сам сертификат сервера.

После того как (с вашего разрешения) браузер сочтет CA надежной и примет сертификат сервера, вам необходимо будет предъявить сертификат для идентификации клиента. Вам может быть предоставлена возможность выбрать сертификат для идентификации, если это указано в конфигурации браузера. Если браузер предъявит сертификат от надежной (уполномоченной) сертификатной компании, Диспетчер цифровых сертификатов покажет информацию о сертификате в отдельном окне. Если приемлемый сертификат не будет предъявлен, сервер может запросить имя пользователя и пароль для идентификации.

После запуска защищенного сеанса DCM попытается получить сертификат от браузера, чтобы связать его с вашим пользовательским профайлом. В случае, если DCM удастся получить один или несколько сертификатов, вы сможете просмотреть информацию о них и выбрать сертификат, который будет связан с вашим пользовательским профайлом.

Если DCM не показывает информацию из сертификата, то это означает, что ему не удалось найти сертификат, который может быть связан с вашим пользовательским профайлом. Одна из возможных причин этого - неполадки с пользовательскими

сертификатами. Например, сертификат полученный от браузера, может быть уже связан с вашим пользовательским профайлом.

Если сертификаты выдаются пользователям локальной сертификатной компанией, то вместо вышеуказанной процедуры пользователи должны создать пользовательский сертификат.

Выдача сертификатов пользователям других систем с помощью API

В версии V5R2 добавлено два новых API, позволяющих выдавать сертификаты пользователям систем, отличных от iSeries. В предыдущих выпусках при выдаче пользователям сертификатов с помощью локальной сертификатной компании (CA) эти сертификаты автоматически связывались с их пользовательскими профайлами iSeries. Таким образом, для того чтобы пользователь мог применять для идентификации клиента сертификат, выданный локальной сертификатной компанией, для этого пользователя необходимо было создать пользовательский профайл iSeries. Кроме того, для создания необходимого сертификата каждому пользователю приходилось применять Диспетчер цифровых сертификатов (DCM). Это означало, что каждому пользователю был необходим пользовательский профайл на сервере iSeries, на котором установлен DCM, а также действительные данные для входа на этот сервер iSeries.

Связывание сертификата с пользовательским профайлом дает определенные преимущества, особенно для внутренних пользователей. Однако все вышеупомянутые ограничения и требования усложняли применение локальной сертификатной компании для выдачи сертификатов большому числу пользователей, особенно в случае, если для них не нужно было создавать пользовательские профайлы iSeries. Если бы вы решили не предоставлять пользовательские профайлы этим пользователям, им пришлось бы покупать сертификаты у общеизвестной CA.

Два новых API позволяют создавать сертификаты пользователей, подписанные локальной сертификатной компанией, для любых имен пользователей. Эти сертификаты не связываются с пользовательскими профайлами. Для пользователя не нужно создавать профайл на сервере iSeries, на котором установлен DCM, и создавать сертификат с помощью DCM.

Эти API предназначены для двух наиболее распространенных разновидностей Web-браузеров и позволяют с помощью Net.Data создать программу для выдачи сертификатов пользователям. Такая программа должно обладать необходимым графическим пользовательским интерфейсом и вызывать API для подписания сертификата с помощью локальной сертификатной компании.

Дополнительная информация об этих API приведена на следующих страницах:
- API запроса на создание и подписание сертификата пользователя (QYCUGSUC).
- API запроса на подписание сертификата пользователя (QYCUSUC).

Получение копии сертификата частной сертификатной компании

Когда вы отправляете запрос на сервер через соединение Secure Sockets Layer, сервер предъявляет вашей клиентской программе сертификат в качестве удостоверения личности. Клиентская программа должна проверить этот сертификат, прежде чем будет установлен сеанс. Для проверки сертификата у программы должен быть доступ к локальной копии сертификата сертификатной компании, выдавшей сертификат сервера. Если сервер предъявляет сертификат, полученный от общественной сертификатной компании Internet, то в вашем браузере или другом клиентском приложении уже должна быть копия сертификата этой сертификатной компании.

Если же сервер предъявляет сертификат, полученный от частной локальной сертификатной компании, то вы должны получить копию сертификата этой сертификатной компании с помощью Диспетчера цифровых сертификатов (DCM).

DCM позволяет скопировать сертификат локальной сертификатной компании как непосредственно в браузер, так и в файл для применения в других клиентских программах. Если защищенная передача данных применяется не только в браузере, но и в других приложениях, то необходимо скопировать сертификат и в браузер, и в файл. При этом сначала следует скопировать сертификат в браузер.

Если приложение сервера требует от вас предъявить сертификат, полученный от локальной сертификатной компании, то вы должны загрузить сертификат локальной сертификатной компании в браузер перед отправкой запроса на получение сертификата пользователя от локальной сертификатной компании.

Для того чтобы с помощью DCM получить копию сертификата локальной сертификатной компании, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации выберите **Установить сертификат локальной CA на PC**. Будет показана страница, позволяющая загрузить сертификат локальной сертификатной компании в браузер или сохранить его в файле.
3. Выберите способ получения сертификата локальной сертификатной компании.
   a. Выберите **Установить сертификат**, чтобы загрузить сертификат локальной сертификатной компании в браузер в качестве надежного базового сертификата. После этого браузер сможет устанавливать защищенные соединения с серверами, которые применяют сертификат, полученный от данной сертификатной компании. Браузер выдаст последовательность окон с инструкциями по установке сертификата.
   b. Выберите **Скопировать и вставить сертификат**. Будет показана страница, содержащая специально закодированную копию сертификата локальной сертификатной компании. Скопируйте текст, показанный на странице, в буфер обмена. Затем вставьте его в файл, который применяется утилитой PC (например MKKF или IKEYMAN) для хранения сертификатов клиентских программ, установленных на PC. Для того чтобы приложения распознавали сертификат и применяли его для идентификации, необходимо настроить приложения таким образом, чтобы они применяли данный сертификат в качестве базового надежного сертификата. Соответствующие инструкции по настройке приведены в приложениях.
4. Нажмите кнопку **OK** для возврата к главному окну Диспетчера цифровых сертификатов.

Управление сертификатами, полученными от общественной сертификатной компании

Предположим, что после тщательного анализа требований к защите и выбранной стратегии защиты вы решили применять сертификаты, выдаваемые общественной сертификатной компанией (CA) Internet, такой как VeriSign. Допустим, вы являетесь владельцем коммерческого Web-сайта и хотите защитить определенные транзакции с помощью SSL. Так как Web-сайт является общедоступным, необходимо использовать сертификаты, распознаваемые большинством Web-браузеров.

Другой пример: вы разрабатываете приложения для внешних пользователей и собираетесь применять сертификат для подписи пакетов приложений. Получив пакет с такой подписью, заказчики будут уверены, что получили его именно от вашей компании и код программ не был изменен третьей стороной. Применение общих

сертификатов позволит заказчикам легко и без лишних расходов проверять подписи на пакетах. С помощью этого сертификата можно также проверять подписи пакетов перед их отправкой заказчикам.

В Диспетчере цифровых сертификатов (DCM) предусмотрены пошаговые процедуры управления общими сертификатами и применяющими их приложениями. Эти процедуры позволяют устанавливать соединения SSL, подписывать объекты и проверять подписи объектов с помощью сертификатов.

Управление общими сертификатами

Для того чтобы с сертификатами, полученными от общественной сертификатной компании Internet, можно было работать с помощью DCM, необходимо сначала создать хранилище сертификатов. Хранилище сертификатов - это специальный файл базы данных, в котором Диспетчер цифровых сертификатов (DCM) хранит цифровые сертификаты и связанные с ними личные ключи. DCM позволяет создавать несколько типов хранилищ сертификатов (в зависимости от типа хранимых сертификатов) и управлять ими.

Тип хранилища сертификатов, которое необходимо создать, и последующие задачи по управлению сертификатами и применяющими их приложениями зависят от того, как вы планируете использовать сертификаты. Информация по созданию хранилищ сертификатов с помощью DCM и управлению общими сертификатами, применяемыми приложениями, приведена в следующих разделах:

- Управление общими сертификатами Internet для сеансов SSL.
- Управление общими сертификатами Internet для подписания объектов.
- Управление сертификатами Internet для проверки подписей объектов.

DCM также обеспечивает управление сертификатами, полученными от сертификатной компании Инфраструктуры общих ключей X.509 (PKIX).

Управление общими сертификатами Internet для сеансов SSL

Диспетчер цифровых сертификатов (DCM) позволяет управлять общими сертификатами Internet с целью обеспечить защиту SSL в сеансах приложений. Если вы не управляете собственной локальной сертификатной компанией с помощью DCM, то сначала вы должны создать хранилище сертификатов для управления общими сертификатами, предназначенными для сеансов SSL. Это должно быть хранилище сертификатов *SYSTEM. Когда вы создаете хранилище сертификатов, DCM предлагает вам ввести информацию, которую необходимо предоставить общественной сертификатной компании для получения сертификата.

Для настройки с помощью DCM общих сертификатов Internet таким образом, чтобы приложения могли устанавливать сеансы SSL, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать хранилище сертификатов**, чтобы запустить пошаговую задачу и заполнить несколько форм. Выполните показанные инструкции по созданию хранилища сертификатов и сертификата, с помощью которых приложения смогут устанавливать сеансы SSL.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Выберите хранилище сертификатов ***SYSTEM** и нажмите **Продолжить**.

4. Выберите **Да**, чтобы создать сертификат вместе с хранилищем сертификатов *SYSTEM, и нажмите **Продолжить**.
5. Выберите **VeriSign или другая сертификатная компания Internet** в качестве сертификатной компании, которая подпишет новый сертификат, и нажмите **Продолжить**. Появится форма, в которой следует указать идентифицирующую информацию о новом сертификате.

   Примечание: Если в системе iSeries установлен шифровальный сопроцессор IBM 4758–023 PCI, то DCM предложит вам выбрать место хранения личного ключа для сертификата. Если сопроцессор не установлен, то DCM автоматически поместит личный ключ в хранилище сертификатов *SYSTEM. Дополнительная информация о способах хранения личного ключа приведена в электронной справке в DCM.
6. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения. Она содержит данные о сертификате, которые необходимо предоставить общественной сертификатной компании для получения сертификата. Эти данные называются данными Запроса на подписание сертификата (CSR) и содержат общий ключ и другую информацию, указанную вами для нового сертификата.
7. Аккуратно скопируйте и вставьте данные CSR в форму запроса сертификата или в отдельный файл, необходимый для получения сертификата от общей сертификатной компании. Необходимо скопировать все данные CSR, включая строки Begin и End New Certificate Request. После завершения работы с этой страницей данные будут потеряны и не смогут быть восстановлены. Отправьте форму запроса или файл в выбранную сертификатную компанию.

   Примечание: Для завершения процедуры необходимо дождаться возвращения подписанного сертификата сертификатной компанией.

   Примечание: Если сертификаты будут применяться HTTP Server для iSeries, то перед тем, как вы начнете работу с подписанным сертификатом с помощью DCM, необходимо создать и настроить Web-сервер. После того как вы настроите сервер для работы с SSL, для него будет создан ИД приложения. Запишите этот ИД, чтобы указать в DCM, какой сертификат данное приложение будет использовать для сеансов SSL.

   Не перезапускайте сервер, пока не назначите ему сертификат в DCM. Если вы перезапустите экземпляр Web-сервера *ADMIN до того, как с ним будет связан сертификат, то сервер не будет запущен, и вы уже не сможете связать сертификат с сервером с помощью DCM.
8. После получения подписанного сертификата от общественной сертификатной компании запустите DCM.
9. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
10. На странице Хранилище сертификатов и пароль пароля укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
11. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
12. В списке задач выберите **Импортировать сертификат**, чтобы начать импортирование подписанного сертификата в хранилище сертификатов

*SYSTEM. По окончании импортирования вы сможете указать приложения, которые будут применять этот сертификат для сеансов SSL.

13. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
14. В списке задач выберите **Обновить присвоение сертификата** для просмотра списка приложений с поддержкой SSL, с которыми может быть связан сертификат.
15. Выберите приложение из списка и нажмите кнопку **Обновить присвоение сертификата**.
16. Выберите импортированный сертификат и нажмите **Присвоить новый сертификат**. Будет показано сообщение с подтверждением присвоения сертификата приложению.

    Примечание: Некоторый приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. Для того чтобы такое приложение идентифицировало сертификаты перед предоставлением доступа к ресурсам, необходимо задать список уполномоченных сертификатных компаний для приложения. Тогда приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения пошаговой задачи у вас будет все необходимое для настройки приложений для работы с SSL. Для работы с приложениями в сеансе SSL у пользователей должна быть копия сертификата той сертификатной компании, которая выдала сертификат сервера. Если сертификат сервера получен от известной сертификатной компании Internet, то клиентское программное обеспечение пользователя может уже содержать необходимую копию сертификата CA. Получить необходимый сертификат пользователи могут на Web-сайте соответствующей сертификатной компании, следуя приведенным на Web-сайте инструкциям.

Управление общими сертификатами Internet для подписания объектов

Диспетчер цифровых сертификатов (DCM) позволяет добавлять цифровые подписи к объектам с помощью общих сертификатов Internet. Если вы не управляете собственной локальной сертификатной компанией с помощью DCM, то сначала необходимо создать хранилище сертификатов для управления общими сертификатами, предназначенными для подписания объектов. Это должно быть хранилище сертификатов *OBJECTSIGNING. Когда вы создаете хранилище сертификатов, DCM предлагает вам ввести информацию, которую необходимо предоставить общественной сертификатной компании Internet для получения сертификата.

Кроме того, для подписания объектов с помощью сертификата необходимо задать ИД приложения. Этот ИД приложения определяет права доступа, необходимые для подписания объектов с помощью определенного сертификата, и обеспечивает дополнительный по сравнению с DCM уровень управления доступом. По умолчанию ИД приложения требует прав доступа *ALLOBJ. Однако это значение можно изменить с помощью Навигатора iSeries.

Для настройки с помощью DCM общих сертификатов Internet таким образом, чтобы приложения могли подписывать объекты, выполните следующие действия:

1. Запустите DCM.

2. В окне навигации DCM выберите **Создать хранилище сертификатов**, чтобы запустить пошаговую задачу и заполнить несколько форм. Выполните показанные инструкции по созданию хранилища сертификатов и сертификата, с помощью которых приложения смогут добавлять подписи к объектам.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Выберите хранилище сертификатов ***OBJECTSIGNING** и нажмите **Продолжить**.
4. Выберите **Да**, чтобы создать сертификат вместе с хранилищем сертификатов, и нажмите **Продолжить**.
5. Выберите **VeriSign или другая сертификатная компания Internet** в качестве сертификатной компании, которая подпишет новый сертификат, и нажмите **Продолжить**. Появится форма, в которой следует указать идентифицирующую информацию о новом сертификате.
6. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения. Она содержит данные о сертификате, которые необходимо предоставить общественной сертификатной компании для получения сертификата. Эти данные называются данными Запроса на подписание сертификата (CSR) и содержат общий ключ и другую информацию, указанную вами для нового сертификата.
7. Аккуратно скопируйте и вставьте данные CSR в форму запроса сертификата или в отдельный файл, необходимый для получения сертификата от общей сертификатной компании. Необходимо скопировать все данные CSR, включая строки Begin и End New Certificate Request. После завершения работы с этой страницей данные будут потеряны и не смогут быть восстановлены. Отправьте форму запроса или файл в выбранную сертификатную компанию.

   Примечание: Для завершения процедуры необходимо дождаться возвращения подписанного сертификата сертификатной компанией.
8. После получения подписанного сертификата от общественной сертификатной компании запустите DCM.
9. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
10. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
11. В окне навигации выберите категорию **Управление сертификатами** для просмотра списка задач.
12. В списке задач выберите **Импортировать сертификат**, чтобы начать импортирование подписанного сертификата в хранилище сертификатов *OBJECTSIGNING. По окончании импортирования вы сможете создать определение приложения для подписания объектов с помощью сертификата.
13. После обновления информации в окне навигации выберите **Управление приложениями** для просмотра списка задач.
14. В списке задач выберите **Добавить приложение**, чтобы начать создание определения приложения, которое будет добавлять подписи к объектам с помощью сертификата.
15. Заполните форму определения приложения, которое будет подписывать объекты, и нажмите кнопку **Добавить**. Это определение описывает не само приложение, а тип объектов, которые будут подписываться с помощью определенного сертификата. Заполнить форму вам поможет контекстная справка.

16. Нажмите **OK** для подтверждения заданного определения и возврата к списку задач Управления приложениями.
17. В списке задач выберите **Обновить присвоение сертификата** и нажмите **Продолжить** для просмотра списка тех приложений, подписывающих объекты, с которыми может быть связан сертификат.
18. Выберите нужный ИД приложения из списка и нажмите кнопку **Обновить присвоение сертификата**.
19. Выберите импортированный сертификат и нажмите **Присвоить новый сертификат**.

После выполнения этих задач у вас будет все необходимое, чтобы начать подписывать объекты для обеспечения их целостности.

При распространении подписанных объектов их получатели должны проверить подпись с помощью DCM версии V5R1 или выше, чтобы убедиться в отсутствии изменений в данных и в подлинности отправителя. Для проверки подписи получатель должен обладать копией сертификата проверки подписи. Эту копию следует предоставлять в составе пакета подписанных объектов.

У получателя также должна быть копия сертификата сертификатной компании, выдавшей сертификат, с помощью которого был подписан объект. Если объекты были подписаны с помощью сертификата, полученного от известной сертификатной компании Internet, то версия DCM получателя должна уже содержать необходимую копию сертификата CA. Однако, если вы не уверены в том, что у получателя есть копия этого сертификата, то следует предоставить ее вместе с подписанными объектами. Например, такую копию следует предоставить в случае, если объекты были подписаны с помощью сертификата, выпущенного частной локальной сертификатной компанией. Для соответствия требованиям защиты следует предоставить сертификат CA в отдельном пакете или сделать его общедоступным.

Управление сертификатами проверки подписей объектов

Диспетчер цифровых сертификатов (DCM) позволяет управлять сертификатами проверки подписей, применяемыми для проверки цифровых подписей объектов. При подписании объекта подпись создается с помощью личного ключа сертификата. При отправке подписанного объекта необходимо приложить к пакету копию сертификата, подписавшего объект. Для этого следует с помощью DCM экспортировать сертификат подписи объекта (без личного ключа сертификата) в качестве сертификата проверки подписей. Например, вы можете экспортировать сертификат проверки подписей в файл и затем рассылать этот файл получателям подписанных объектов. Кроме того, для проверки созданных вами подписей вы можете экспортировать сертификат проверки подписей в хранилище сертификатов *SIGNATUREVERIFICATION.

Для проверки подписи объекта нужна копия сертификата, с помощью которого был подписан объект. С помощью общего ключа сертификата проверяется подпись, созданная с помощью соответствующего личного ключа. Поэтому перед проверкой подписи объекта необходимо получить копию сертификата подписи объекта от отправителя подписанного объекта.

Кроме того, у вас должна быть копия сертификата сертификатной компании, выдавшей сертификат, с помощью которого был подписан объект. Сертификат CA служит для проверки подлинности сертификата, подписавшего объект. DCM содержит копии сертификатов наиболее известных сертификатных компаний. Если же объект был подписан сертификатом, полученным от другой общественной или

частной локальной сертификатной компании, то для проверки подписи объекта необходимо получить копию сертификата этой компании.

Для проверки подписей объектов с помощью DCM необходимо сначала создать хранилище сертификатов *SIGNATUREVERIFICATION для управления нужными сертификатами проверки подписей. При создании этого хранилища сертификатов DCM автоматически заполняет его копиями сертификатов наиболее известных общественных сертификатных компаний.

Примечание: Если вы хотите проверять подписи объектов, которые вы создали с помощью своих собственных сертификатов подписи объектов, то вы должны создать хранилище сертификатов *SIGNATUREVERIFICATION и скопировать в него сертификаты из хранилища сертификатов *OBJECTSIGNING. Это необходимо сделать, даже если вы будете проверять подписи из хранилища сертификатов *OBJECTSIGNING.

Для работы с сертификатами проверки подписей с помощью DCM выполните следующие задачи:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать хранилище сертификатов**, чтобы запустить пошаговую задачу и заполнить несколько форм.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Выберите хранилище сертификатов ***SIGNATUREVERIFICATION** и нажмите **Продолжить**.

   Примечание: Если существует хранилище сертификатов *OBJECTSIGNING, то DCM попросит указать, следует ли копировать сертификаты подписания объектов в новое хранилище сертификатов в качестве сертификатов проверки подписей. Если вы будете проверять подписи с помощью своих собственных сертификатов подписи объектов, укажите **Да** и нажмите кнопку **Продолжить**. Для копирования сертификатов из хранилища сертификатов *OBJECTSIGNING нужно знать его пароль.
4. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Будет показана страница с подтверждением создания хранилища сертификатов. Теперь хранилище сертификатов готово для размещения сертификатов проверки подписей объектов.

   Примечание: Если вы создавали это хранилище только для проверки собственных подписей, подготовка на этом завершена. Все вновь создаваемые сертификаты подписания объектов необходимо будет экспортировать из хранилища сертификатов *OBJECTSIGNING в это хранилище сертификатов. В противном случае вы не сможете проверять подписи, созданные с помощью этих сертификатов.

   Примечание: Если вы создали это хранилище сертификатов с целью проверки подписей объектов, поступающих из других источников, то следует продолжить подготовку и импортировать нужные сертификаты.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.

6. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
7. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
8. В списке задач выберите **Импортировать сертификат**. Эта пошаговая задача позволяет импортировать необходимые сертификаты в хранилище сертификатов, так что вы сможете проверять подписи полученных объектов.
9. Выберите тип сертификата для импорта. Выберите **Проверка подписей**, чтобы импортировать сертификат, полученный вместе с подписанными объектами, и завершить задачу импорта.

   Примечание: Если в хранилище сертификатов нет копии сертификата сертификатной компании, выдавшей сертификат подписи объекта, то вы должны *сначала* импортировать этот сертификат CA. Попытка импортировать сертификат проверки подписей, не получив сертификат CA, может привести к ошибке.

Теперь все готово для проверки подписей объектов с помощью сертификатов.

Глава 8. Управление DCM

После настройки Диспетчера цифровых сертификатов (DCM) вам придется выполнять различные операции по управлению сертификатами. Информация о работе с DCM и управлении цифровыми сертификатами приведена в следующих разделах:

Выдача сертификатов для других систем iSeries с помощью локальной сертификатной компании
Здесь приведена информация о применении частной локальной сертификатной компании для выдачи сертификатов для других систем iSeries.

Управление приложениями в DCM
Этот раздел содержит информацию о работе с определениями приложений, поддерживающих SSL, и приложений, подписывающих объекты, с помощью DCM. Здесь приведены сведения о создании определений приложений и управлении присвоением сертификатов приложения. Здесь также приведена информация о создании списков уполномоченных сертификатных компаний, на основе которых приложения принимают сертификаты для идентификации клиентов.

Проверка сертификатов и приложений
Этот раздел содержит информацию о способах проверки подлинности сертификата перед тем, как он будет применен или принят приложением.

Присвоение сертификатов
Этот раздел содержит информацию о том, как можно связать сертификат с одним или несколькими приложениями для применения в защищенных функциях.

Управление определениями CRL Этот раздел содержит сведения о создании и применении Списка аннулированных сертификатов (CRL), с помощью которого приложения проверяют допустимость принимаемых сертификатов.

Хранение ключей сертификатов в Шифровальном сопроцессоре IBM 4758
Этот раздел содержит информацию об использовании установленного сопроцессора в качестве более надежного хранилища личных ключей сертификатов.

Управление расположением сертификатной компании PKIX
В этом разделе приведена информация об управлении сертификатами, полученными от общественной сертификатной компании Internet, выпускающей сертификаты в соответствии со стандартами Инфраструктуры общих ключей X.509 (PKIX), с помощью DCM.

Подписание объектов
Этот раздел содержит информацию об управлении сертификатами подписи объектов с помощью DCM.

Проверка подписей объектов
В этом разделе приведена информация о проверке подлинности цифровых подписей объектов с помощью DCM.

Выдача сертификатов другим системам iSeries с помощью локальной сертификатной компании

Предположим, что вы уже работаете с частной локальной сертификатной компанией (CA) в системе iSeries, подключенной к сети. Теперь вы хотите с помощью этой локальной CA обслуживать и другую систему iSeries в сети. Например, вы хотите с помощью этой локальной CA выдавать сертификаты клиента или сервера

приложениям в другой системе iSeries для работы с SSL. Или, вы хотите с помощью сертификатов, выдаваемых этой локальной CA, подписывать объекты, находящиеся на другом сервере iSeries.

Эти задачи позволяет выполнить Диспетчер цифровых сертификатов (DCM). Часть задач выполняется в системе iSeries, в которой расположена локальная сертификатная компания, а другая часть - в системе iSeries, в которой находятся приложения, которым нужно выдать сертификаты. Последняя называется целевой системой. Задачи, которые необходимо выполнить в целевой системе, зависят от ее выпуска.

Примечание: Задача существенно усложняется в случае, если в системе iSeries, в которой расположена локальная сертификатная компания, установлен продукт Cryptographic Access Provider с более высоким уровнем шифрования, нежели в целевой системе. (В версии V5R2 возможна только версия Cryptographic Access Provider 5722–AC3, выполняющая шифрование по самому сложному алгоритму. Однако в предыдущих версиях можно было установить другие версии Cryptographic Access Provider (5722–AC1 или 5722–AC2) с более низким уровнем шифрования.) При экспорте сертификата (вместе с его личным ключом) система шифрует файл сертификата в целях защиты. Если в системе с CA применяется более сложное шифрование, чем в целевой системе, то целевая система не сможет расшифровать импортируемый файл. Следовательно, файл не будет импортирован или сертификат будет непригоден для установления соединений SSL. Это произойдет, даже если размер ключа созданного сертификата будет соответствовать требованиям программы шифрования в целевой системе.

Локальная сертификатная компания позволяет выдавать внешним системам сертификаты для настройки соединений SSL и подписания объектов. Файлы, создаваемые DCM при выдаче сертификатов внешним системам iSeries с помощью локальной сертификатной компании, содержат копию сертификата локальной сертификатной компании, а также копии сертификатов многих общественных сертификатных компаний.

Задачи, которые необходимо выполнить в DCM, несколько различаются в зависимости от типа сертификатов, выдаваемых локальной сертификатной компанией, и выпуска (а также других параметров) целевой системы.

Выдача частных сертификатов другой системе iSeries V5R2 или V5R1

Для того чтобы локальная сертификатная компания выдавала сертификаты, предназначенные для применения во внешней системе iSeries V5R2 или V5R1, выполните следующие действия в системе, в которой находится локальная сертификатная компания:

1. Запустите DCM.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
2. В окне навигации выберите **Создать сертификат** для просмотра списка типов сертификатов, которые можно создать с помощью локальной сертификатной компании.

   Для выполнения этой задачи не обязательно открывать хранилище сертификатов. В приведенных ниже инструкциях считается, что вы либо работаете с хранилищем

сертификатов локальной сертификатной компании, либо не работаете ни с одним из хранилищ сертификатов. Для выполнения этих задач в системе должна существовать локальная сертификатная компания.

3. Выберите тип сертификата, который необходимо создать с помощью локальной сертификатной компании, и нажмите кнопку **Продолжить**, чтобы запустить пошаговую задачу и заполнить несколько форм. Выберите **сертификат сервера или клиента для внешней системы iSeries** (для соединений SSL) или **сертификат подписи объекта для внешней системы iSeries** (для применения во внешней системе).

   Примечание: При создании сертификата подписи объекта для внешней системы необходимо, чтобы в целевой системе была установлена OS/400 версии V5R1 или выше. В силу этого, в DCM в исходной системе не выдается приглашение выбрать формат для создаваемого сертификата подписи объекта.
4. При создании сертификата клиента или сервера выберите выпуск системы iSeries, для которой создается сертификат. Нажмите кнопку **Продолжить**, чтобы перейти к форме, позволяющей указать идентификационную информацию для сертификата.

   Примечание: Указанный выпуск определяет формат, в котором DCM создает сертификат. Объем и тип идентификационной информации в форме зависят от выбранного выпуска системы. Это обеспечивает совместимость файлов сертификата с системой iSeries, в которой будет применяться этот сертификат.
5. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения.

   Примечание: Если в целевой системе существует хранилище сертификатов *OBJECTSIGNING или *SYSTEM, убедитесь, что указанные метка и имя файла сертификата уникальны. Это гарантирует, что вы сможете импортировать сертификат в существующее хранилище сертификатов в целевой системе.

   Страница подтверждения содержит имена файлов, созданных DCM для экспорта в целевую систему. Эти файлы создаются с учетом указанного выпуска целевой системы. DCM автоматически дополняет к этим файлам копию сертификата локальной сертификатной компании.

   Примечание: DCM создает новый сертификат в своем собственном хранилище сертификатов и два файла для экспорта: файл хранилища сертификатов (с расширением `.KDB`) и файл запроса (с расширением `.RDB`).
6. Перенесите файл в целевую систему с помощью протокола передачи файлов (FTP) в двоичном режиме или другим способом.

Выдача частного сертификата для системы iSeries V4R4 или V4R5

Для того чтобы локальная сертификатная компания выдавала сертификаты, предназначенные для применения в системе iSeries V4R4 или V4R5, выполните следующие действия в системе, в которой находится локальная сертификатная компания V5R2:

1. Запустите DCM.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.

2. В окне навигации выберите **Создать сертификат** для просмотра списка типов сертификатов, которые можно создать с помощью локальной сертификатной компании.

   Для выполнения этой задачи не обязательно открывать хранилище сертификатов. В приведенных ниже инструкциях считается, что вы либо работаете с хранилищем сертификатов локальной сертификатной компании, либо не работаете ни с одним из хранилищ сертификатов. Для выполнения этих задач в системе должна существовать локальная сертификатная компания.
3. Выберите тип сертификата, который необходимо создать с помощью локальной сертификатной компании, и нажмите кнопку **Продолжить**, чтобы запустить пошаговую задачу и заполнить несколько форм.

   Примечание: Так как сертификат создается для системы iSeries V4R4 или V4R5, необходимо выбрать **сертификат сервера или клиента для внешней системы iSeries**. Целевые системы выпуска до V5R1 не поддерживают работу с сертификатами подписи объекта.
4. Выберите выпуск системы iSeries, для которой создается сертификат. Нажмите кнопку **Продолжить**, чтобы перейти к форме, позволяющей указать идентификационную информацию для сертификата.

   Примечание: Указанный выпуск определяет формат, в котором DCM создает сертификат. Объем и тип идентификационной информации в форме зависят от выбранного выпуска системы. Это обеспечивает совместимость файлов сертификата с системой iSeries, в которой будет применяться этот сертификат.
5. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения.

   Примечание: Если в целевой системе существует хранилище сертификатов *SYSTEM, убедитесь, что указанные метка и имя файла сертификата уникальны. Это гарантирует, что вы сможете импортировать сертификат в существующее хранилище сертификатов в целевой системе.

   Страница подтверждения содержит имена файлов, созданных DCM для экспорта в целевую систему. Эти файлы создаются с учетом указанного выпуска целевой системы. DCM автоматически дополняет к этим файлам копию сертификата локальной сертификатной компании.

   Примечание: DCM создает новый сертификат в своем собственном хранилище сертификатов и два файла для экспорта: файл хранилища сертификатов (с расширением `.KDB`) и файл запроса (с расширением `.RDB`).

Примечание: Если вы планируете применять сертификаты из этих файлов в существующем хранилище сертификатов *SYSTEM в целевой системе V4R4 или V4R5, то сертификат локальной сертификатной компании не может быть непосредственно импортирован из файлов `.KDB` и `.RDB`. Функция импортирования DCM не сможет распознать сертификат сертификатной компании в этом формате. Вместо этого, необходимо в исходной системе экспортировать в отдельный файл копию сертификата локальной сертификатной компании в формате, поддерживаемом функцией импортирования более ранних выпусков.

6. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.

7. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
8. В окне навигации выберите категорию **Управление сертификатами** для просмотра списка задач.
9. В списке задач выберите **Экспортировать сертификат**.
10. Выберите **Сертификатная компания (CA)** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**, чтобы просмотреть список сертификатов сертификатных компаний.
11. В списке сертификатов выберите сертификат локальной сертификатной компании (например `LOCAL_CERTIFICATE_AUTHORITY`). Нажмите кнопку **Экспорт**, чтобы перейти к форме, позволяющей выбрать целевой объект для сертификата сертификатной компании.
12. Выберите **Файл** и нажмите кнопку **Продолжить**.
13. Укажите полное имя файла, в который будет экспортирован сертификат, и нажмите кнопку **Продолжить**. Будет показана страница с подтверждением экспортирования файла.

    Примечание: Не забудьте дать файлу уникальное имя и расширение. Например, файлу можно присвоить имя `mycafile.exp`. В имени файла недопустимы следующие расширения: `.TXT`, `.KDB`, `.RDB` и `.KYR`. Применение одного из этих расширений может привести к возникновению ошибок при импортировании файла в целевую систему.
14. Перенесите созданные файлы хранилища сертификатов (`.KDB` и `.RDB`) в целевую систему V4R4 или V4R5 с помощью Протокола передачи файлов (FTP) в двоичном режиме, либо другим способом. Для передачи файла, содержащего экспортированный сертификат локальной сертификатной компании, воспользуйтесь режимом ASCII FTP.

Работа с экспортированными файлами в целевой системе

Вторую часть действий над экспортированными файлами необходимо выполнить с помощью DCM в целевой системе. Задачи, которые необходимо выполнить с помощью DCM, зависят от выпуска целевой системы и существующих в ней хранилищ сертификатов. Кроме того, они зависят от типа сертификата, созданного в исходной системе. Информация о выполнении операций над файлами сертификатов с помощью DCM в целевой системе приведена в следующих разделах:

- Применение частных сертификатов в соединениях SSL в целевой системе V5R2.
- Применение частных сертификатов в соединениях SSL в целевой системе V5R1.
- Применение частных сертификатов для подписания объектов в целевой системе V5R2 или V5R1.
- Применение частных сертификатов в соединениях SSL в целевой системе V4R5 или V4R4.

Применение частных сертификатов в соединениях SSL в целевой системе V5R2

Для управления сертификатами SSL в Диспетчере цифровых сертификатов (DCM) предназначено хранилище сертификатов *SYSTEM. Если DCM в целевой системе V5R2 никогда прежде не использовался для управления сертификатами SSL, то этого хранилища сертификатов в целевой системе нет. Задачи, которые необходимо выполнить, чтобы работать с экспортированными файлами хранилища сертификатов, созданными в системе с локальной сертификатной компанией (CA), зависят от того, существует ли хранилище сертификатов *SYSTEM в целевой системе. Если хранилище сертификатов *SYSTEM не существует, его можно создать

с помощью экспортированных файлов сертификатов. Если хранилище сертификатов *SYSTEM существует в целевой системе V5R2, экспортированные файлы сертификатов можно использовать двумя способами:

- Применять экспортированные файлы сертификатов в качестве Хранилища сертификатов другой системы.
- Импортировать файлы сертификатов в существующее хранилище сертификатов *SYSTEM.

Хранилище сертификатов *SYSTEM не существует

Если в целевой системе V5R2 нет хранилища сертификатов *SYSTEM, то в качестве этого хранилища сертификатов можно использовать экспортированные файлы. Выполните следующие действия, чтобы создать хранилище сертификатов *SYSTEM для работы с файлами сертификатов в целевой системе V5R2:

1. Убедитесь, что файлы хранилища сертификатов (два файла: один с расширением `.KDB`, а другой с расширением `.RDB`), созданные в системе с локальной сертификатной компанией, находятся в каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER`.
2. В каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER` , измените имена этих файлов на `DEFAULT.KDB` и `DEFAULT.RDB`. Таким образом вы создадите компоненты хранилища сертификатов *SYSTEM в целевой системе. Файлы хранилища сертификатов уже содержат копии сертификатов многих общественных сертификатных компаний. При создании файлов для экспорта копии этих сертификатов были записаны в них вместе с копией сертификата локальной сертификатной компании.

   Внимание: Если в целевой системе есть файлы `DEFAULT.KDB` и `DEFAULT.RDB` в каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER`, то это означает, что в ней уже создано хранилище сертификатов *SYSTEM. В этом случае экспортированные файлы переименовывать не следует. Замена существующих файлов может вызвать сбои при работе с DCM, экспортированным хранилищем сертификатов и содержимым этого хранилища. Однако вы должны убедиться, что экспортированные файлы носят уникальные имена, и применять их в качестве **Хранилища сертификатов другой системы**. Учтите, что в этом случае DCM не позволяет указать, какие приложения должны применять данный сертификат.
3. Запустите DCM. Теперь необходимо изменить пароль хранилища сертификатов *SYSTEM. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.
4. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
5. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R2, и нажмите кнопку **Продолжить**.
6. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов. Изменив пароль, вновь откройте хранилище сертификатов. Теперь вы можете указать, какие приложения будут применять данный сертификат в соединениях SSL.
7. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
8. На странице Хранилище сертификатов и пароль введите новый пароль и нажмите кнопку **Продолжить**.

9. После обновления информации в окне навигации выберите категорию **Управление сертификатами**, чтобы просмотреть список задач.
10. Выберите из списка задачу **Присвоить сертификат**, чтобы просмотреть список сертификатов в текущем хранилище сертификатов.
11. Выберите сертификат, созданный вами в *исходной* системе, и нажмите кнопку **Присвоить приложениям**, чтобы просмотреть список приложений с поддержкой SSL, которым может быть присвоен этот сертификат.
12. Выберите приложения, которые будут применять этот сертификат в сеансах SSL, и нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением присвоения сертификата приложениям.

    Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. У таких приложений должны быть возможность идентифицировать сертификаты перед предоставлением доступа к ресурсам. Следовательно, вы должны задать список уполномоченных сертификатных компаний для приложения. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения описанных действий приложения в целевой системе смогут применять сертификат, выданный локальной сертификатной компанией другой системы iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат локальной CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Хранилище сертификатов *SYSTEM существует — работа с файлами как с Хранилищем сертификатов другой системы

Если в целевой системе V5R2 уже есть хранилище сертификатов *SYSTEM, необходимо выбрать способ применения файлов сертификатов. Экспортированные файлы сертификатов могут быть использованы в качестве **Хранилища сертификатов другой системы**. Кроме того, частный сертификат с соответствующим сертификатом локальной CA может быть импортирован в существующее хранилище сертификатов *SYSTEM.

Хранилища сертификатов других систем являются дополнительными пользовательскими хранилищами сертификатов SSL. Они служат для управления сертификатами для пользовательских приложений с поддержкой SSL, не применяющих API DCM для регистрации ИД приложения в утилите DCM. Хранилища сертификатов других систем обеспечивают управление сертификатами, программируемый доступ к которым при настройке соединения SSL осуществляется в пользовательских приложениях с помощью API SSL_Init. При работе с этим API приложения применяют сертификат по умолчанию, а не указанный вами сертификат.

Приложения IBM iSeries (и приложения многих других разработчиков программного обеспечения) применяют только сертификаты из хранилища сертификатов *SYSTEM. Если экспортированные файлы применяются в качестве Хранилища сертификатов

другой системы, то DCM не позволяет указать, какие приложения должны применять данный сертификат для соединений SSL. Таким образом, стандартные приложения iSeries с поддержкой SSL невозможно настроить для работы с данным сертификатом. Для применения сертификата в приложениях iSeries необходимо импортировать сертификат из экспортированных файлов хранилища сертификатов в хранилище сертификатов *SYSTEM.

Для применения экспортированных файлов сертификатов в качестве Хранилища сертификатов другой системы выполните следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
3. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов (файл с расширением `.KDB`), экспортированного из исходной системы. Кроме того, укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R2, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.

   Изменив пароль, вновь откройте хранилище сертификатов. Теперь вы можете указать сертификат в этом хранилище сертификатов, который будет применяться по умолчанию.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов и новый пароль, затем нажмите кнопку **Продолжить**.
7. После обновления панели навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Задать сертификат по умолчанию**.

После того, как хранилище сертификатов другой системы было создано и настроено, приложения могут применять находящиеся в нем сертификаты для установления соединений SSL с помощью API SSL_Init.

Хранилище сертификатов *SYSTEM существует — работа с сертификатами в существующем хранилище сертификатов *SYSTEM

Сертификаты из экспортированных файлов хранилища сертификатов могут применяться в существующем хранилище сертификатов *SYSTEM в системе V5R2. Для этого необходимо импортировать сертификаты из файлов хранилища сертификатов в существующее хранилище сертификатов *SYSTEM. Однако эти сертификаты не могут быть непосредственно импортированы из файлов `.KDB` и `.RDB`, так как функция импорта DCM не поддерживает их формат. Для работы с экспортированными сертификатами в существующем хранилище сертификатов *SYSTEM необходимо открыть эти файлы как Хранилище сертификатов другой системы и экспортировать их в хранилище сертификатов *SYSTEM.

Для экспорта сертификатов из файлов хранилища сертификатов в хранилище сертификатов *SYSTEM выполните в целевой системе V5R2 следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
3. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов (файл с расширением `.KDB`), экспортированного из исходной системы. Кроме того, укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R2, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов. Если не изменить пароль и выбрать опцию Автоматических вход в систему, то при экспортировании сертификатов из этого хранилища в хранилище сертификатов *SYSTEM могут возникнуть ошибки.

   Изменив пароль, вновь откройте хранилище сертификатов.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов и новый пароль, затем нажмите кнопку **Продолжить**.
7. После обновления информации в окне навигации выберите категорию **Управление сертификатами**, чтобы просмотреть список задач, и выберите **Экспортировать сертификат**.
8. Выберите **Сертификатная компания (CA)** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.

   Примечание: Перед экспортом сертификата клиента или сервера необходимо экспортировать в хранилище сертификатов сертификат локальной CA. В противном случае во время экспорта сертификата сервера или клиента может произойти ошибка.
9. Выберите сертификат локальной CA для экспорта и нажмите кнопку **Экспорт**.
10. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.
11. Укажите `*SYSTEM` в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного экспортирования сертификатов, либо, в том случае, если сертификат не был экспортирован, - сообщение с информацией об ошибках.
12. После этого можно экспортировать сертификат клиента или сервера в хранилище сертификатов *SYSTEM. Выберите задачу **Экспортировать сертификат**.
13. Выберите **Сервер или клиент** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.
14. Выберите соответствующий сертификат сервера или клиента для экспорта и нажмите кнопку **Экспорт**.
15. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.
16. Укажите `*SYSTEM` в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного экспортирования сертификатов, либо, в том случае, если сертификат не был экспортирован, - сообщение с информацией об ошибках.

17. Теперь можно присвоить сертификат приложению для применения в сеансах SSL. Нажмите кнопку на панели навигации **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
18. На странице Хранилище сертификатов и пароль введите пароль для хранилища сертификатов *SYSTEM и нажмите кнопку **Продолжить**.
19. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
20. Выберите из списка задачу **Присвоить сертификат**, чтобы просмотреть список сертификатов в текущем хранилище сертификатов.
21. Выберите сертификат, созданный вами в *исходной* системе, и нажмите кнопку **Присвоить приложениям**, чтобы просмотреть список приложений с поддержкой SSL, которым может быть присвоен этот сертификат.
22. Выберите приложения, которые будут применять этот сертификат в сеансах SSL, и нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением присвоения сертификата приложениям.

Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. У таких приложений должны быть возможность идентифицировать сертификаты перед предоставлением доступа к ресурсам. Следовательно, вы должны задать список уполномоченных сертификатных компаний для приложения. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения описанных действий приложения в целевой системе смогут применять сертификат, выданный локальной сертификатной компанией другой системы iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат локальной CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Применение частных сертификатов в соединениях SSL в целевой системе V5R1

Для управления сертификатами SSL в Диспетчере цифровых сертификатов (DCM) предназначено хранилище сертификатов *SYSTEM. Если DCM в целевой системе V5R1 никогда прежде не использовался для управления сертификатами SSL, то этого хранилища сертификатов в целевой системе нет. Задачи, которые необходимо выполнить, чтобы работать с экспортированными файлами хранилища сертификатов, созданными в системе с локальной сертификатной компанией (CA), зависят от того, существует ли хранилище сертификатов *SYSTEM в целевой системе. Если хранилище сертификатов *SYSTEM не существует, его можно создать с помощью экспортированных файлов сертификатов. Если хранилище сертификатов *SYSTEM существует в целевой системе V5R1, экспортированные файлы сертификатов можно использовать двумя способами:

- Применять экспортированные файлы сертификатов в качестве Хранилища сертификатов другой системы.

- Импортировать файлы сертификатов в существующее хранилище сертификатов *SYSTEM.

Хранилище сертификатов *SYSTEM не существует

Если в целевой системе V5R1 нет хранилища сертификатов *SYSTEM, то в качестве этого хранилища сертификатов можно использовать экспортированные файлы. Для того чтобы работать с файлами сертификатов в целевой системе V5R1, выполните следующие действия:

1. Убедитесь, что файлы хранилища сертификатов (два файла: один с расширением `.KDB`, а другой с расширением `.RDB`), созданные в системе с локальной сертификатной компанией, находятся в каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER`.
2. В каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER` , измените имена этих файлов на `DEFAULT.KDB` и `DEFAULT.RDB`. Таким образом вы создадите компоненты хранилища сертификатов *SYSTEM в целевой системе. Файлы хранилища сертификатов уже содержат копии сертификатов многих общественных сертификатных компаний. При создании файлов для экспорта копии этих сертификатов были записаны в них вместе с копией сертификата локальной сертификатной компании.

   Внимание: Если в целевой системе есть файлы `DEFAULT.KDB` и `DEFAULT.RDB` в каталоге `/QIBM/USERDATA/ICSS/CERT/SERVER`, то это означает, что в ней уже создано хранилище сертификатов *SYSTEM. В этом случае экспортированные файлы переименовывать не следует. Замена существующих файлов может вызвать сбои при работе с DCM, экспортированным хранилищем сертификатов и содержимым этого хранилища. Однако вы должны убедиться, что экспортированные файлы носят уникальные имена, и применять их в качестве **Хранилища сертификатов другой системы**. Учтите, что в этом случае DCM не позволяет указать, какие приложения должны применять данный сертификат.
3. Запустите DCM. Теперь необходимо изменить пароль хранилища сертификатов *SYSTEM. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.
4. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
5. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R1, и нажмите кнопку **Продолжить**.
6. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов. Изменив пароль, вновь откройте хранилище сертификатов. Теперь вы можете указать, какие приложения будут применять данный сертификат в соединениях SSL.
7. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
8. На странице Хранилище сертификатов и пароль введите новый пароль и нажмите кнопку **Продолжить**.
9. После обновления информации в окне навигации выберите категорию **Управление приложениями**, чтобы просмотреть список задач.
10. В списке задач выберите **Обновить присвоение сертификата** для просмотра списка приложений с поддержкой SSL, с которыми может быть связан сертификат.

11. Выберите приложение из списка и нажмите кнопку **Обновить присвоение сертификата**.
12. Выберите сертификат, выданный локальной сертификатной компанией в *исходной* системе, и нажмите кнопку **Присвоить новый сертификат**. Будет показано сообщение с подтверждением присвоения сертификата приложению.

    Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. У таких приложений должны быть возможность идентифицировать сертификаты перед предоставлением доступа к ресурсам. Следовательно, вы должны задать список уполномоченных сертификатных компаний для приложения. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения описанных действий приложения в целевой системе смогут применять сертификат, выданный локальной сертификатной компанией другой системы iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Хранилище сертификатов *SYSTEM существует — работа с файлами как с Хранилищем сертификатов другой системы

Если в целевой системе V5R1 уже есть хранилище сертификатов *SYSTEM, необходимо выбрать способ применения файлов сертификатов. Экспортированные файлы сертификатов могут быть использованы в качестве **Хранилища сертификатов другой системы**. Кроме того, частный сертификат с соответствующим сертификатом локальной CA может быть импортирован в существующее хранилище сертификатов *SYSTEM.

Хранилища сертификатов других систем являются дополнительными пользовательскими хранилищами сертификатов SSL. Они служат для управления сертификатами для пользовательских приложений с поддержкой SSL, не применяющих API DCM для регистрации ИД приложения в утилите DCM. Хранилища сертификатов других систем обеспечивают управление сертификатами, программируемый доступ к которым при настройке соединения SSL осуществляется в пользовательских приложениях с помощью API SSL_Init. При работе с этим API приложения применяют сертификат по умолчанию, а не указанный вами сертификат.

Приложения IBM iSeries (и приложения многих других разработчиков программного обеспечения) применяют только сертификаты из хранилища сертификатов *SYSTEM. Если экспортированные файлы применяются в качестве хранилища сертификатов другой системы, DCM не позволяет указать, какие приложения должны применять данный сертификат для соединений SSL. Таким образом, стандартные приложения iSeries с поддержкой SSL невозможно настроить для работы с данным сертификатом.

Для применения сертификата в приложениях iSeries необходимо импортировать сертификат из экспортированных файлов хранилища сертификатов в хранилище сертификатов *SYSTEM.

Для применения экспортированных файлов сертификатов в качестве хранилища сертификатов другой системы выполните следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
3. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов (файл с расширением `.KDB`), экспортированного из исходной системы. Кроме того, укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R1, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.

   Изменив пароль, вновь откройте хранилище сертификатов. Теперь вы можете указать сертификат в этом хранилище сертификатов, который будет применяться по умолчанию.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов и новый пароль, затем нажмите кнопку **Продолжить**.
7. После обновления панели навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Задать сертификат по умолчанию**.

После того, как хранилище сертификатов другой системы было создано и настроено, приложения могут применять находящиеся в нем сертификаты для установления соединений SSL с помощью API SSL_Init.

Хранилище сертификатов *SYSTEM существует — работа с сертификатами в существующем хранилище сертификатов *SYSTEM

Сертификаты из экспортированных файлов хранилища сертификатов могут применяться в существующем хранилище сертификатов *SYSTEM в системе V5R1. Для этого необходимо импортировать сертификаты из файлов хранилища сертификатов в существующее хранилище сертификатов *SYSTEM. Однако эти сертификаты не могут быть непосредственно импортированы из файлов `.KDB` и `.RDB`, так как функция импорта DCM не поддерживает их формат. Для работы с экспортированными сертификатами в существующем хранилище сертификатов *SYSTEM необходимо открыть эти файлы как Хранилище сертификатов другой системы и экспортировать их в хранилище сертификатов *SYSTEM.

Примечание: Ниже описано, каким образом с помощью Хранилища сертификатов другой системы, расположенного в целевой системе, можно экспортировать сертификаты из первоначальных файлов хранилища сертификатов в хранилище сертификатов *SYSTEM. Эта процедура добавления сертификатов в хранилище сертификатов *SYSTEM

позволяет избежать возможных неполадок в случае, если в целевой системе применяется более простая программа шифрования (например 5722–AC2), чем в исходной.

Для экспорта сертификатов из файлов хранилища сертификатов в хранилище сертификатов *SYSTEM выполните в целевой системе V5R1 следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
3. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов (файл с расширением `.KDB`), экспортированного из исходной системы. Кроме того, укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы V5R1, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов. Если не изменить пароль и выбрать опцию Автоматических вход в систему, то при экспортировании сертификатов из этого хранилища в хранилище сертификатов *SYSTEM могут возникнуть ошибки.

   Изменив пароль, вновь откройте хранилище сертификатов.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов и новый пароль, затем нажмите кнопку **Продолжить**.
7. После обновления информации в окне навигации выберите категорию **Управление сертификатами**, чтобы просмотреть список задач, и выберите **Экспортировать сертификат**.
8. Выберите **Сертификатная компания (CA)** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.

   Примечание: Перед экспортом сертификата клиента или сервера необходимо экспортировать в хранилище сертификатов сертификат локальной CA. В противном случае во время экспорта сертификата сервера или клиента может произойти ошибка.
9. Выберите сертификат локальной CA для экспорта и нажмите кнопку **Экспорт**.
10. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.
11. Укажите `*SYSTEM` в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**.
12. После этого можно экспортировать сертификат клиента или сервера в хранилище сертификатов *SYSTEM. Выберите задачу **Экспортировать сертификат**.
13. Выберите **Сервер или клиент** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.
14. Выберите соответствующий сертификат сервера или клиента для экспорта и нажмите кнопку **Экспорт**.
15. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.

16. Укажите *SYSTEM в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного экспортирования сертификатов, либо, в том случае, если сертификат не был экспортирован, - сообщение с информацией об ошибках.
17. Теперь можно присвоить сертификат приложению для применения в сеансах SSL. Нажмите кнопку на панели навигации **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM**.
18. На странице Хранилище сертификатов и пароль введите пароль для хранилища сертификатов *SYSTEM и нажмите кнопку **Продолжить**.
19. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
20. В списке задач выберите **Обновить присвоение сертификата** для просмотра списка приложений с поддержкой SSL, с которыми может быть связан сертификат.
21. Выберите приложение из списка и нажмите кнопку **Обновить присвоение сертификата**.
22. Выберите сертификат, выданный локальной сертификатной компанией в *исходной* системе, и нажмите кнопку **Присвоить новый сертификат**. Будет показано сообщение с подтверждением присвоения сертификата приложению.

    Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. У таких приложений должны быть возможность идентифицировать сертификаты перед предоставлением доступа к ресурсам. Следовательно, вы должны задать список уполномоченных сертификатных компаний для приложения. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения описанных действий приложения в целевой системе смогут применять сертификат, выданный локальной сертификатной компанией другой системы iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Применение частных сертификатов для подписания объектов в целевой системе V5R2 или V5R1

Для управления сертификатами подписи объекта в Диспетчере цифровых сертификатов (DCM) предназначено хранилище сертификатов *OBJECTSIGNING. Если DCM в целевой системе никогда прежде не использовался для управления сертификатами подписи объекта, то этого хранилища сертификатов в целевой системе нет. Задачи, которые необходимо выполнить, чтобы работать с файлами хранилища сертификатов, созданными в системе с локальной сертификатной компанией (CA), зависят от того, существует ли хранилище сертификатов *OBJECTSIGNING в целевой системе. Если хранилище сертификатов *OBJECTSIGNING не существует, его можно создать с помощью экспортированных

файлов сертификатов. Если хранилище сертификатов *OBJECTSIGNING существует в целевой системе, необходимо импортировать в него экспортированные сертификаты.

Хранилище сертификатов *OBJECTSIGNING не существует

Задачи, которые необходимо выполнить, чтобы работать с файлами хранилища сертификатов, созданными в системе с локальной сертификатной компанией (CA), зависят от того, применялся ли когда-либо DCM в целевой системе для управления сертификатами подписи объекта.

Если в целевой системе V5R2 или V5R1, в которую были экспортированы файлы хранилища сертификатов, нет хранилища сертификатов *OBJECTSIGNING, то выполните следующие действия:

1. Убедитесь, что файлы хранилища сертификатов (два файла: один с расширением `.KDB`, а другой с расширением `.RDB`), созданные в системе с локальной сертификатной компанией, находятся в каталоге `/QIBM/USERDATA/ICSS/CERT/SIGNING`.
2. В каталоге `/QIBM/USERDATA/ICSS/CERT/SIGNING` измените имена этих файлов на `SGNOBJ.KDB` и `SGNOBJ.RDB`, если это необходимо. Таким образом вы создадите компоненты хранилища сертификатов *OBJECTSIGNING в целевой системе. Файлы хранилища сертификатов уже содержат копии сертификатов многих общественных сертификатных компаний. При создании файлов для экспорта копии этих сертификатов были записаны в них вместе с копией сертификата локальной сертификатной компании.

   Внимание: Если в каталоге `/QIBM/USERDATA/ICSS/CERT/SIGNING` целевой системы уже есть файлы `SGNOBJ.KDB` и `SGNOBJ.RDB`, то это означает, что в ней уже создано хранилище сертификатов *OBJECTSIGNING. В этом случае экспортированные файлы переименовывать не следует. Замена существующих файлов может вызвать сбои при работе с DCM, экспортированным хранилищем сертификатов и содержимым этого хранилища. Сертификаты из этих файлов могут быть перенесены в хранилище сертификатов *OBJECTSIGNING двумя способами. Эти сертификаты могут быть импортированы в простые файлы, а из них - импортированы в существующее хранилище сертификатов *OBJECTSIGNING. Кроме того, экспортированные файлы можно открыть в качестве хранилища сертификатов другой системы и экспортировать сертификаты непосредственно в хранилище сертификатов *OBJECTSIGNING, как это описано ниже. В обоих случаях сертификаты необходимо экспортировать в хранилище сертификатов *OBJECTSIGNING, если вы хотите управлять применяющими их приложениями.
3. Запустите DCM. Теперь необходимо изменить пароль хранилища сертификатов *OBJECTSIGNING. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.
4. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
5. На странице ввода пароля укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
6. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов. Изменив пароль, вновь откройте

хранилище сертификатов. Теперь вы можете создать определение приложения для подписания объектов с помощью сертификата.
7. Повторно открыв хранилище сертификатов, выберите в окне навигации категорию **Управление приложениями** для просмотра списка задач.
8. В списке задач выберите **Добавить приложение**, чтобы начать создание определения приложения, которое будет добавлять подписи к объектам с помощью сертификата.
9. Заполните форму определения приложения, которое будет подписывать объекты, и нажмите кнопку **Добавить**. Это определение описывает не само приложение, а тип объектов, которые будут подписываться с помощью определенного сертификата. Заполнить форму вам поможет контекстная справка.
10. Нажмите **OK** для подтверждения заданного определения и возврата к списку задач **Управления приложениями**.
11. В списке задач выберите **Обновить присвоение сертификата** для просмотра списка тех приложений, подписывающих объекты, с которыми может быть связан сертификат.
12. Выберите нужный ИД приложения из списка и нажмите кнопку **Обновить присвоение сертификата**.
13. Выберите сертификат, выданный локальной сертификатной компанией в исходной системе, и нажмите кнопку **Присвоить новый сертификат**.

После выполнения этих задач у вас будет все необходимое, чтобы начать подписывать объекты для обеспечения их целостности.

При распространении подписанных объектов их получатели должны проверить подпись объектов с помощью DCM версии V5R2 или V5R1, чтобы убедиться в отсутствии изменений в данных и в подлинности отправителя. Для проверки подписи получатель должен обладать копией сертификата проверки подписи. Эту копию следует предоставлять в составе пакета подписанных объектов.

У получателя также должна быть копия сертификата сертификатной компании, выдавшей сертификат, с помощью которого был подписан объект. Если объекты были подписаны с помощью сертификата, полученного от известной сертификатной компании Internet, то версия DCM получателя должна уже содержать необходимую копию сертификата CA. Однако при необходимости следует предоставить копию сертификата сертификатной компании в отдельном пакете вместе с подписанными объектами. Например, такую копию следует предоставить в случае, если объекты были подписаны с помощью сертификата, выпущенного локальной сертификатной компанией. Для соответствия требованиям защиты следует предоставить сертификат CA в отдельном пакете или сделать его общедоступным.

Хранилище сертификатов *OBJECTSIGNING существует

Сертификаты из экспортированных файлов хранилища сертификатов могут применяться в существующем хранилище сертификатов *OBJECTSIGNING в системе выпуска V5R2 или V5R1. Для этого необходимо импортировать сертификаты из файлов хранилища сертификатов в существующее хранилище сертификатов *OBJECTSIGNING. Однако эти сертификаты не могут быть непосредственно импортированы из файлов `.KDB` и `.RDB`, так как функция импорта DCM не поддерживает их формат. Для добавления сертификатов в существующее хранилище сертификатов *OBJECTSIGNING необходимо открыть экспортированные файлы в целевой системе V5R2 или V5R1 как Хранилище сертификатов другой системы. Затем из этого хранилища сертификаты можно экспортировать в хранилище сертификатов *OBJECTSIGNING. Из экспортированных файлов необходимо экспортировать копии самого сертификата добавления подписей к объектам и сертификата локальной CA.

Для экспорта сертификатов из файлов хранилища сертификатов в хранилище сертификатов *OBJECTSIGNING выполните в целевой системе V5R2 или V5R1 следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
3. На странице Хранилище сертификатов и пароль введите полные имена файлов хранилища сертификатов. Кроме того, введите пароль, заданный при создании сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление хранилищем сертификатов**, а затем в списке задач выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов. Если не изменить пароль и выбрать опцию Автоматических вход в систему, то при экспортировании сертификатов из этого хранилища в хранилище сертификатов *OBJECTSIGNING могут возникнуть ошибки.

   Изменив пароль, вновь откройте хранилище сертификатов.
5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. На странице Хранилище сертификатов и пароль введите полное имя файла хранилища сертификатов и новый пароль, затем нажмите кнопку **Продолжить**.
7. После обновления информации в окне навигации выберите категорию **Управление сертификатами**, чтобы просмотреть список задач, и выберите **Экспортировать сертификат**.
8. Выберите **Сертификатная компания (CA)** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.

   Примечание: Формулировка этой задачи подразумевает, что в Хранилище сертификатов другой системы экспортируются сертификаты клиента или сервера. Это обусловлено тем, что это хранилище сертификатов предназначено для применения в качестве вспомогательного хранилища сертификатов *SYSTEM. Тем не менее, экспорт из этого хранилища сертификатов - простейший способ перемещения сертификатов из экспортированных файлов в существующее хранилище сертификатов *OBJECTSIGNING.
9. Выберите сертификат локальной CA для экспорта и нажмите кнопку **Экспорт**.

   Примечание: Перед экспортом сертификата подписи объекта необходимо экспортировать в хранилище сертификатов сертификат локальной CA. В противном случае во время экспорта сертификата подписи объекта может произойти ошибка.
10. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.
11. Укажите `*OBJECTSIGNING` в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**.
12. Теперь можно экспортировать сертификат подписи объекта в хранилище сертификатов *OBJECTSIGNING. Выберите задачу **Экспортировать сертификат**.
13. Выберите **Сервер или клиент** в качестве типа экспортируемого сертификата и нажмите кнопку **Продолжить**.
14. Выберите соответствующий сертификат для экспорта и нажмите кнопку **Экспорт**.

15. Выберите **Хранилище сертификатов** в качестве целевого объекта для экспорта сертификата и нажмите кнопку **Продолжить**.
16. Укажите *OBJECTSIGNING в качестве целевого хранилища сертификатов и введите его пароль, затем нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного экспортирования сертификатов, либо, в том случае, если сертификат не был экспортирован, - сообщение с информацией об ошибках.

    Примечание: Для того чтобы подписывать объекты с помощью этого сертификата, необходимо связать сертификат с приложением, подписывающим объекты.

Применение частных сертификатов в соединениях SSL в целевой системе V4R5 или V4R4

Для управления сертификатами SSL в Диспетчере цифровых сертификатов (DCM) предназначено хранилище сертификатов *SYSTEM. Если DCM в целевой системе V4R5 или V4R4 никогда прежде не использовался для управления сертификатами SSL, то этого хранилища сертификатов в целевой системе нет. Экспортированные файлы хранилища сертификатов, созданные в исходной системе с локальной сертификатной компанией, содержат два сертификата. Это созданный вами сертификат клиента или сервера и сертификат подписавшей этот сертификат частной локальной CA.

Задачи, которые необходимо выполнить, чтобы работать с файлами хранилища сертификатов, зависят от того, существует ли хранилище сертификатов *SYSTEM в целевой системе. Если хранилище сертификатов *SYSTEM не существует, его можно создать с помощью экспортированных файлов сертификатов. Если хранилище сертификатов *SYSTEM существует в целевой системе, экспортированные файлы сертификатов можно использовать двумя способами:

- Применять экспортированные файлы сертификатов в качестве Хранилища сертификатов другой системы.
- Импортировать файлы сертификатов в существующее хранилище сертификатов *SYSTEM.

Хранилище сертификатов *SYSTEM не существует

Если в целевой системе V4R5 или V4R4, в которую были экспортированы файлы хранилища сертификатов, нет хранилища сертификатов *SYSTEM, выполните следующие действия:

1. Убедитесь, что файлы хранилища сертификатов (два файла: один с расширением .KDB, а другой с расширением .RDB), созданные в системе с локальной сертификатной компанией, находятся в каталоге /QIBM/USERDATA/ICSS/CERT/SERVER.
2. В каталоге /QIBM/USERDATA/ICSS/CERT/SERVER измените имена этих файлов на DEFAULT.KDB и DEFAULT.RDB. Таким образом вы создадите компоненты хранилища сертификатов *SYSTEM в целевой системе. Файлы хранилища сертификатов уже содержат копии сертификатов многих общественных сертификатных компаний. При создании файлов для экспорта копии этих сертификатов были записаны в них вместе с копией сертификата локальной сертификатной компании.

    Внимание: Если в целевой системе есть файлы DEFAULT.KDB и DEFAULT.RDB в каталоге /QIBM/USERDATA/ICSS/CERT/SERVER, то это означает, что в ней уже создано хранилище сертификатов *SYSTEM. В этом случае экспортированные файлы переименовывать не следует. Замена существующих файлов может вызвать сбои при работе с DCM,

экспортированным хранилищем сертификатов и содержимым этого хранилища. Однако вы должны убедиться, что экспортированные файлы носят уникальные имена, и применять их в качестве **Хранилища сертификатов другой системы**. Учтите, что в этом случае DCM не позволяет указать, какие приложения должны применять данный сертификат.

3. Запустите DCM. Теперь необходимо изменить пароль хранилища сертификатов *SYSTEM. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.
4. Убедитесь, что в окне навигации в поле выпадающего списка показано хранилище сертификатов *SYSTEM, и выберите **Сертификаты системы** для просмотра списка доступных задач. Появится окно **Хранилище сертификатов и пароль**.
5. В соответствующих полях укажите хранилище сертификатов `*SYSTEM` и пароль, заданный при создании файлов с помощью локальной сертификатной компании в исходной системе. Теперь вы можете изменить пароль хранилища сертификатов.
6. В списке задач в окне навигации выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов. Изменив пароль, вновь откройте хранилище сертификатов.
7. После того как вы откроете хранилище сертификатов *SYSTEM, выберите в списке задач **Работа с защищенными приложениями**. Появится страница, позволяющая связать сертификат с приложением.
8. Выберите в списке приложение, которое будет устанавливать соединения SSL с помощью экспортированного частного сертификата.
9. Нажмите **Работа с сертификатом системы** и выберите сертификат, выданный локальной сертификатной компанией в исходной системе.
10. Нажмите кнопку **Присвоить новый сертификат**, чтобы связать сертификат с выбранным приложением.

Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. При применении сертификатов для идентификации клиентов приложение предоставляет доступ к ресурсам только после получения правильного сертификата. Для идентификации клиентов с помощью сертификатов, выданных определенной сертификатной компанией, такое приложение должно быть настроено для работы с сертификатами данной сертификатной компании. На странице **Работа с сертификатными компаниями** убедитесь, что этот сертификат CA является уполномоченным в хранилище сертификатов. После этого на странице **Работа с защищенными приложениями** убедитесь, что приложения, применяющие этот сертификат, принимают сертификаты выдавшей его локальной сертификатной компании. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

После выполнения описанных действий приложения в целевой системе V4R5 или V4R4 смогут применять сертификат, выданный локальной сертификатной компанией другой системы V5R2 iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Хранилище сертификатов *SYSTEM существует — работа с файлами как с Хранилищем сертификатов другой системы

Если в целевой системе V4R5 или V4R4 уже есть хранилище сертификатов *SYSTEM, необходимо выбрать способ применения файлов сертификатов. Экспортированные файлы хранилища сертификатов содержат два сертификата: созданный вами сертификат клиента или сервера и сертификат подписавшей его частной локальной CA. Экспортированные файлы сертификатов могут быть использованы в качестве **Хранилища сертификатов другой системы**. Кроме того, частный сертификат с соответствующим сертификатом CA может быть импортирован в существующее хранилище сертификатов *SYSTEM.

Если экспортированные файлы применяются в качестве **Хранилища сертификатов другой системы**, то DCM не позволяет указать, какие приложения должны применять данный сертификат для соединений SSL. Тем не менее, сертификат в этом хранилище сертификатов может быть назначен в качестве сертификата по умолчанию. Хранилища сертификатов других систем обеспечивают управление сертификатами, программируемый доступ к которым при настройке соединения SSL осуществляется в пользовательских приложениях с помощью API SSL_Init. При работе с этим API приложения применяют сертификат по умолчанию, а не указанный вами сертификат.

Если в целевой системе V4R5 или V4R4, в которую были экспортированы файлы хранилища сертификатов, есть хранилище сертификатов *SYSTEM, выполните следующие действия:

1. Запустите DCM. Теперь необходимо изменить пароль экспортированного хранилища сертификатов. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.
2. Убедитесь, что в окне навигации в поле выпадающего списка показано хранилище сертификатов OTHER, и выберите **Сертификаты системы** для просмотра списка доступных задач. Появится окно **Хранилище сертификатов и пароль**.
3. В соответствующих полях введите полное имя файла хранилища сертификатов (с расширением `.KDB`), экспортированного из локальной сертификатной компании в исходной системе. Введите пароль, заданный при создании этих файлов в *исходной* системе. Теперь вы можете изменить пароль хранилища сертификатов.
4. В окне навигации в списке задач Сертификат системы выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов.

   Изменив пароль, вновь откройте хранилище сертификатов. Теперь вы можете указать сертификат в этом хранилище сертификатов, который будет применяться по умолчанию.
5. В окне навигации выберите **Работа с сертификатами**. Будет показана страница, позволяющая выполнить несколько задач по управлению сертификатами.
6. Выберите в списке сертификат, который следует применять по умолчанию для данного хранилища сертификатов, и нажмите кнопку **Применять по умолчанию**.

После того, как хранилище сертификатов другой системы было создано и настроено, приложения могут применять находящиеся в нем сертификаты для установления соединений SSL с помощью API SSL_Init.

Хранилище сертификатов *SYSTEM существует — импорт файлов в существующее хранилище сертификатов *SYSTEM

Для того чтобы импортировать сертификаты в хранилище сертификатов *SYSTEM в целевой системе V4R5 или V4R4, необходимо сначала экспортировать их из созданного вами хранилища сертификатов в другом формате. Затем можно импортировать сертификаты из созданных файлов в хранилище сертификатов *SYSTEM. Экспортированные файлы хранилища сертификатов содержат два сертификата: созданный вами сертификат клиента или сервера и сертификат подписавшей его частной локальной CA. В хранилище сертификатов *SYSTEM необходимо импортировать оба эти сертификата.

Примечание: Функции экспорта DCM для V4R5 и V4R4 уступают по своим возможностям соответствующим функциями в версии V5R2, поэтому при экспорте сертификата частной локальной сертификатной компании в целевую систему вы можете столкнуться с затруднениями. По этой причине, вместо экспортирования в целевую систему V4R4 или V4R5 следует в исходной системе V5R2 экспортировать *дополнительную* копию сертификата локальной сертификатной компании в отдельный файл. После этого можно вручную перенести файл с экспортированным сертификатом в целевую систему V4R4 или V4R5 и, следуя приведенным ниже инструкциям, импортировать сертификат локальной сертификатной компании в хранилище сертификатов *SYSTEM. Сертификат локальной сертификатной компании необходимо импортировать *до* созданного с ее помощью частного сертификата. В противном случае могут возникнуть ошибки, поскольку на момент экспортирования сертификат локальной CA будет отсутствовать в хранилище сертификатов.

Для экспорта сертификатов из файлов хранилища сертификатов выполните в целевой системе V4R4 или V4R5 следующие действия:

1. Запустите DCM.
2. Убедитесь, что в окне навигации в поле выпадающего списка показано хранилище сертификатов OTHER, и выберите **Сертификаты системы** для просмотра списка доступных задач. Появится окно **Хранилище сертификатов и пароль**.
3. Укажите пароль и полные имена экспортированных файлов хранилища сертификатов и нажмите кнопку **OK**. Теперь вы можете изменить пароль хранилища сертификатов.
4. В окне навигации в списке задач Сертификат системы выберите **Изменить пароль**. Заполните форму, чтобы изменить пароль хранилища сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**. Это позволит DCM сохранить новый пароль, так что вам станут доступны все функции DCM по управлению сертификатами для данного хранилища сертификатов. Если не изменить пароль и выбрать опцию Автоматических вход в систему, то при экспортировании сертификатов из этого хранилища могут возникнуть ошибки.

   Изменив пароль, вновь откройте хранилище сертификатов.
5. В окне навигации выберите **Работа с сертификатами** для просмотра списка сертификатов.

6. Выберите в списке частный сертификат и нажмите кнопку **Экспортировать**. Появится страница Экспорт сертификата.
7. Заполните форму Экспорт сертификата.

   Примечание: Не забудьте дать файлу уникальное имя и расширение. Например, файлу можно присвоить имя `myfile.exp`. В имени файла недопустимы следующие расширения: `.TXT`, `.KDB`, `.RDB` и `.KYR`. Их применение может привести к возникновению ошибок при импортировании сертификатов из файла. Выберите выпуск, соответствующий целевой системе, в которой будет применяться сертификат. От выбранного выпуска зависит формат экспортированного сертификата.
8. Нажмите кнопку **OK**. В верхней области страницы появится сообщение о том, что сертификат был экспортирован в указанный файл.

К этому моменту дополнительная копия сертификата локальной сертификатной компании должна быть создана в исходной системе V5R2 с помощью DCM и перенесена вручную в целевую систему V4R4 или V5R5. Кроме того, в целевой системе с помощью DCM должен быть экспортирован в файл частный сертификат клиента или сервера. Теперь все готово для импорта этих сертификатов в хранилище сертификатов *SYSTEM. Сертификат локальной сертификатной компании необходимо импортировать *до* созданного с ее помощью частного сертификата. В противном случае могут возникнуть ошибки, поскольку на момент экспортирования сертификат локальной CA будет отсутствовать в хранилище сертификатов.

Для того чтобы импортировать сертификаты из экспортированных файлов и указать приложения с поддержкой SSL, которые будут их применять, выполните в целевой системе V4R4 или V4R5 следующие действия:

1. Запустите DCM.
2. Убедитесь, что в окне навигации в поле выпадающего списка показано хранилище сертификатов *SYSTEM, и выберите **Сертификаты системы** для просмотра списка доступных задач. Появится окно **Хранилище сертификатов и пароль**.
3. Укажите хранилище сертификатов *SYSTEM, введите пароль и нажмите кнопку **Продолжить**.
4. Теперь необходимо импортировать сертификат локальной CA из файла, экспортированного из исходной системы V5R2. В окне навигации выберите **Получить сертификат сертификатной компании**. Появится соответствующая форма.
5. Заполните форму и нажмите кнопку **OK**. Появится страница подтверждения получения сертификата. При работе с хранилищем сертификатов *SYSTEM эта страница содержит список приложений, которые могут применять импортированный сертификат сертификатной компании.

   Примечание: Некоторые приложения с поддержкой SSL допускают идентификацию клиентов на основе сертификатов. При применении сертификатов для идентификации клиентов приложение предоставляет доступ к ресурсам только после получения правильного сертификата. Для идентификации клиентов с помощью сертификатов, выданных определенной сертификатной компанией, такое приложение должно быть настроено для работы с сертификатами данной сертификатной компании. Приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или

клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

6. Выберите приложения, которым будет разрешено принимать сертификаты, выданные этой сертификатной компанией, и нажмите кнопку **OK**. Появится страница Состояние защищенных приложений, позволяющая подтвердить выбор приложений.
7. Теперь вы можете импортировать сертификат сервера. В окне навигации выберите **Работа с сертификатами** для просмотра списка сертификатов.
8. Нажмите кнопку **Импортировать**. Появится страница Импорт сертификата.
9. Заполните форму Импорт сертификата и нажмите кнопку **OK** для возврата на страницу Работа с сертификатами. Обязательно введите имя файла, в котором находится экспортированный сертификат клиента или сервера, и укажите целевой выпуск, заданный ранее при экспорте сертификата. В верхней области окна появится сообщение о том, что сертификат был добавлен в текущее хранилище сертификатов. Импортированный сертификат должен появиться в списке сертификатов.
10. Теперь необходимо указать, какие приложения будут применять импортированный частный сертификат в соединениях SSL. В окне навигации выберите **Работа с защищенными приложениями**. Появится страница, позволяющая связать сертификат с приложениями.
11. Выберите приложение из списка и нажмите **Работа с сертификатом системы** для просмотра списка сертификатов, которые могут быть связаны с приложением для применения в соединениях SSL.
12. Выберите сертификат из списка и нажмите кнопку **Присвоить новый сертификат**, чтобы связать выбранный сертификат с указанным приложением. В верхней части страницы появится сообщение с подтверждением выбора сертификата.

После выполнения описанных действий приложения в целевой системе V4R4 или V4R5 смогут применять сертификат, выданный локальной сертификатной компанией другой системы iSeries. Для того чтобы в этих приложениях можно было применять протокол SSL, необходимо настроить поддержку SSL в приложениях.

Перед установлением соединения SSL с выбранным приложением пользователь должен с помощью DCM получить копию сертификата локальной CA из исходной системы. Для этого сертификат CA нужно скопировать в файл на компьютере пользователя или загрузить в браузер, в зависимости от требований приложения с поддержкой SSL.

Управление приложениями в DCM

Диспетчер цифровых сертификатов (DCM) позволяет выполнять различные задачи по управлению приложениями с поддержкой SSL и приложениями, подписывающими объекты. Например, вы можете указать, какие сертификаты будут применяться приложениями в сеансах SSL. Набор доступных задач по управлению приложениями зависит от выбранных приложения и хранилища сертификатов. Управлять приложениями можно только с помощью хранилищ сертификатов *SYSTEM и *OBJECTSIGNING.

Хотя большинство задач по управлению приложениями в DCM сравнительно просты, некоторые из них могут оказаться незнакомыми для вас. Дополнительная информация об этих задачах приведена в следующих разделах:

Раздел **Создание определения приложения** содержит информацию о типах приложений, для которых можно создать определения.

В разделе **Управление присвоением сертификатов** приведена информация о том, как можно присвоить или изменить сертификат, с помощью которого приложение устанавливает сеанс SSL или подписывает объекты.

Раздел **Определение списка уполномоченных сертификатных компаний** содержит информацию о том, когда вы можете и должны указывать сертификатные компании, чьи сертификаты будет проверять и принимать приложение.

Информация о других задачах DCM приведена в электронной справке.

Создание определения приложения

В DCM существует два типа определений приложений: определения серверных или клиентских приложений с поддержкой SSL и определения приложений, подписывающих объекты.

Для работы в DCM с определениями приложений с поддержкой SSL и их сертификатами приложение необходимо зарегистрировать в DCM с соответствующим определением приложения, после чего оно получит уникальный ИД. Разработчики приложений регистрируют приложения с поддержкой SSL с помощью API (QSYRGAP, QsyRegisterAppForCertUse), который автоматически создает ИД приложения в DCM. Все приложения IBM iSeries, поддерживающие SSL, зарегистрированы в DCM. Определения и ИД для тех приложений, которые вы создали или приобрели, также можно создать с помощью DCM. Для создания определения клиентского или серверного приложения SSL необходимо открыть хранилище сертификатов *SYSTEM.

Для подписания объектов с помощью сертификата необходимо прежде всего создать определение приложения для сертификата. В отличие от определения приложения с поддержкой SSL, определение приложения, подписывающего объекты, не описывает само приложение. Вместо этого определение приложения содержит информацию о типе или группе объектов, которые будут подписываться. Для создания определения приложения, подписывающего объекты, необходимо открыть хранилище сертификатов *OBJECTSIGNING.

Для создания определения приложения выполните следующие действия:

1. Запустите DCM.
2. Нажмите кнопку **Выбрать хранилище приложений** и выберите необходимое хранилище сертификатов. (Это может быть хранилище сертификатов *SYSTEM или *OBJECTSIGNING, в зависимости от типа создаваемого определения приложения.)

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
3. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
5. В списке задач выберите **Добавить приложение**. Будет показана форма определения приложения.

   Примечание: При работе с хранилищем сертификатов *SYSTEM Диспетчер цифровых сертификатов предложит вам указать, будет ли добавлено определение для приложения сервера или для приложения клиента.

6. Заполните форму и нажмите кнопку **Добавить**. Информация, которую можно указать в определении приложения, зависит от типа определяемого приложения. При создании определения приложения сервера можно указать, может ли приложение применять сертификаты для идентификации клиентов и будет ли оно требовать идентификации клиентов. Кроме того, можно указать, что при идентификации сертификатов приложение должно применять список уполномоченных сертификатных компаний.

Управление присвоением сертификатов приложениям

Для выполнения функций защиты, таких как установление сеансов Secure Sockets Layer (SSL) или добавление подписей к объектам, необходимо с помощью DCM присвоить приложению сертификат. Для того чтобы присвоить сертификат приложению или изменить назначенный сертификат, выполните следующие действия:

1. Запустите DCM.
2. Нажмите кнопку **Выбрать хранилище приложений** и выберите необходимое хранилище сертификатов. (Это может быть хранилище сертификатов *SYSTEM или *OBJECTSIGNING, в зависимости от типа приложения, которому нужно присвоить сертификат.)

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
3. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
5. Работая с хранилищем сертификатов *SYSTEM, выберите тип приложения для управления. (Выберите приложение типа **Сервер** или **Клиент**.)
6. В списке задач выберите **Обновить присвоение сертификата** для просмотра списка приложений, с которыми может быть связан сертификат.
7. Выберите приложение из списка и нажмите кнопку **Обновить присвоение сертификата**, чтобы просмотреть список сертификатов, которые могут быть присвоены приложению.
8. Выберите сертификат из списка и нажмите кнопку **Присвоить новый сертификат**. Будет показано сообщение с подтверждением присвоения сертификата приложению.

   Примечание: При присвоении сертификата приложению с поддержкой SSL, которое применяет сертификаты для идентификации клиентов, необходимо задать список уполномоченных сертификатных компаний для этого приложения. Тогда приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

Если приложение активно, то замена или удаление его сертификата не всегда вступает в силу немедленно. Например, сервер Client Access Express автоматически применяет все изменения, внесенные при работе с сертификатами. Однако для серверов Telnet и IBM HTTP Server for iSeries и некоторых других приложений внесенные изменения вступят в силу только после перезапуска.

Начиная с версии V5R2, задача Присвоить сертификат позволяет назначить сертификат сразу нескольким приложениям.

Определение списка уполномоченных сертификатных компаний для приложения

Приложения, поддерживающие применение сертификатов для идентификации клиентов во время сеансов Secure Sockets Layer (SSL), определяют, может ли сертификат быть принят в качестве удостоверения личности. Один из критериев идентификации сертификата основан на том, является ли сертификатная компания, выдавшая этот сертификат, уполномоченной.

При работе с Диспетчером цифровых сертификатов (DCM) вы можете указать, сертификаты каких сертификатных компаний будет принимать приложение при идентификации клиентов. Для этого предназначен список уполномоченных сертификатных компаний.

Для того чтобы вы могли определить список уполномоченных сертификатных компаний для приложения, должны быть выполнены несколько условий:

- Приложение должно поддерживать идентификацию клиентов с помощью сертификатов.
- В определении приложения должно быть указано, что приложение применяет список уполномоченных сертификатных компаний.

Если в определении приложения указано, что приложение применяет список уполномоченных сертификатных компаний, то для успешной идентификации клиентов с помощью сертификатов необходимо определить этот список. Тогда приложение будет принимать сертификаты только указанных вами уполномоченных сертификатных компаний. Если пользователь или клиент предъявит сертификат от сертификатной компании, отсутствующей в списке уполномоченных, то приложение не примет такой сертификат.

При внесении сертификатной компании в список уполномоченных сертификатных компаний для приложения она должна быть активизирована.

Для определения списка уполномоченных сертификатных компаний для приложения выполните следующие действия:

1. Запустите DCM.
2. Нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов *SYSTEM.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
3. На странице Хранилище сертификатов и пароль укажите пароль, заданный вами при создании хранилища сертификатов в исходной системе, и нажмите кнопку **Продолжить**.
4. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
5. В списке задач выберите **Определить список уполномоченных CA**.
6. Выберите тип приложения (сервер или клиент), для которого нужно определить список, и нажмите кнопку **Продолжить**.
7. Выберите приложение из списка и нажмите **Продолжить**, чтобы просмотреть список сертификатов сертификатных компаний, которые могут быть внесены в список.
8. Выберите сертификатные компании, сертификаты которых приложение должно принимать, и нажмите кнопку **OK**. Будет показано сообщение с подтверждением выбора сертификатных компаний.

Примечание: Вы можете либо выбрать отдельные сертификатные компании из списка, либо указать, что приложение должно принимать сертификаты от всех или ни от одной из перечисленных сертификатных компаний. Кроме того, перед добавлением в список сертификат сертификатной компании можно просмотреть и проверить.

Проверка сертификатов и приложений

Диспетчер цифровых сертификатов (DCM) позволяет проверять отдельные сертификаты и применяющие их приложения. Проверка приложения несколько отличается от проверки сертификата.

Проверка приложения

Проверка определения приложения с помощью DCM позволяет избежать неполадок, связанных с сертификатами, в работе приложения. Такие неполадки могут помешать приложению устанавливать соединения Secure Sockets Layer (SSL) или подписывать объекты.

Когда вы выполняете проверку приложения, Диспетчер цифровых сертификатов проверяет, во-первых, существование сертификата, связанного с приложением, и во-вторых, правильность этого сертификата. Кроме того, если приложение применяет список уполномоченных сертификатных компаний (CA), то DCM проверяет, содержит ли этот список хотя бы одну сертификатную компанию. Затем DCM проверяет правильность сертификатов CA в списке уполномоченных CA приложения. Наконец, если приложение применяет список аннулированных сертификатов (CRL) и определение CRL для сертификатной компании существует, то DCM проверяет этот CRL.

Проверка сертификата

Когда вы выполняете проверку сертификата, DCM проверяет несколько элементов, относящихся к сертификату, с целью убедиться в его подлинности и правильности. Проверка сертификата позволяет избежать неполадок в работе приложений, применяющих сертификат в защищенных соединениях или для подписания объектов.

DCM проверяет, не истек ли срок действия сертификата. Если для сертификатной компании, выдавшей сертификат, задано определение CRL, то DCM также проверяет, не внесен ли сертификат в список аннулированных сертификатов (CRL). Кроме того, DCM проверяет, находится ли сертификат CA, выдавшей сертификат, в текущем хранилище сертификатов и является ли данная CA доступной, а следовательно, уполномоченной. Если сертификат содержит личный ключ (как, например, сертификаты сервера и клиента или сертификат подписи объекта), то DCM также проверяет соответствие личного ключа общему. Это означает, что DCM зашифровывает данные общим ключом и проверяет, могут ли они быть расшифрованы личным ключом.

Присвоение сертификата приложениям

В версии V5R2 добавлена новая функция Диспетчера цифровых сертификатов (DCM), которая позволяет присвоить сертификат нескольким приложениям. Эта функция применима только к хранилищам сертификатов *SYSTEM и *OBJECTSIGNING.

Для присвоения сертификата одному или нескольким приложениям выполните следующие действия:

1. Запустите DCM.

   Примечание: Для просмотра информации о заполнении полей формы при работе с DCM нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM** или ***OBJECTSIGNING**.
3. Введите пароль хранилища сертификатов и нажмите кнопку **Продолжить**.
4. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
5. В списке задач выберите **Присвоить сертификат**, чтобы просмотреть список сертификатов в текущем хранилище.
6. Выберите сертификат из списка и нажмите кнопку **Присвоить приложениям**, чтобы просмотреть список определений приложений для текущего хранилища сертификатов.
7. Выберите необходимые приложения из списка и нажмите кнопку **Продолжить**. Будет показано сообщение с подтверждением успешного выполнения операции, либо, в случае возникновения неполадки, с информацией об ошибках.

Управление определениями CRL

Диспетчер цифровых сертификатов (DCM) позволяет задать для сертификатной компании определение Списка аннулированных сертификатов (CRL), применяемое в процессе проверки сертификатов. С помощью CRL Диспетчер цифровых сертификатов и приложения могут проверить, не был ли сертификат аннулирован сертификатной компанией. После создания определения CRL оно становится доступным для приложений, поддерживающих идентификацию клиентов с помощью сертификатов.

Применение CRL позволяет повысить надежность проверки сертификатов в приложениях, поддерживающих идентификацию клиентов с помощью сертификатов. Для того чтобы приложение применяло CRL, необходимо указать это в определении приложения DCM.

Проверка с помощью CRL

При проверке сертификата или приложения с помощью DCM определение CRL применяется по умолчанию. Если определение CRL не задано, то DCM не может выполнить проверку с помощью CRL. Однако DCM может попытаться проверить другую важную информацию о сертификате, например является ли подпись CA сертификата действительной и включена ли эта CA в список уполномоченных.

Создание определения CRL

Для создания определения CRL для какой-либо сертификатной компании выполните следующие действия:
1. Запустите DCM.
2. В окне навигации выберите категорию **Управление определениями CRL** для просмотра списка задач.
3. Выберите в списке задач **Добавить определение CRL**. Будет показана форма, позволяющая указать определение CRL и способ обращения к нему из DCM или приложения.
4. Заполните форму и нажмите кнопку **OK**. Необходимо задать уникальное имя для определения CRL, сервер LDAP, на котором находится CRL, и информацию о соединении с сервером LDAP.

Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.

Теперь необходимо связать определение CRL с конкретной CA.

5. В окне навигации выберите категорию **Управление сертификатами** для просмотра списка задач.
6. Выберите в списке задачу **Обновить назначенное определение CRL**, чтобы просмотреть список сертификатов CA.
7. Выберите из списка сертификат CA, с которым необходимо связать определение CRL, и нажмите кнопку **Обновить назначенное определение CRL**. Будет показан список определений CRL.
8. Выберите из списка определение CRL, чтобы связать его с указанной сертификатной компанией, и нажмите кнопку **Обновить связь**. В верхней части страницы будет показано сообщение, подтверждающее успешное выполнение операции.

После того, как вы создадите определение CRL для сертификатной компании, DCM или другие приложения смогут с его помощью выполнять проверку сертификатов. Однако сначала необходимо поместить определение CRL на сервер Служб каталогов. Кроме того, необходимо настроить сервер Служб каталогов и клиентские приложения для работы с SSL и связать сертификат с приложением в DCM.

Дополнительная информация о настройке сервера Служб каталогов (LDAP) iSeries и работе с ним приведена в следующих разделах Information Center:

- Службы каталогов (LDAP)
  Этот раздел содержит всю необходимую информацию о настройке сервера Служб каталогов (LDAP) iSeries и работе с ним.
- Применение защиты Secure Sockets Layer (SSL) на сервере Служб каталогов LDAP
  В этом разделе приведена информация о настройке сервера LDAP для работы с SSL.

Хранение ключей сертификатов в Шифровальном сопроцессоре IBM 4758

Если в системе iSeries установлен Шифровальный сопроцессор IBM 4758–023, то его можно использовать для повышения надежности хранения личного ключа сертификата. Сопроцессор позволяет хранить личные ключи сертификата сервера, клиента или локальной сертификатной компании (CA). Личный ключ сертификата пользователя должен находиться в системе пользователя и поэтому не может храниться в сопроцессоре. Кроме того, в текущей версии системы в сопроцессоре не допускается хранение личного ключа сертификата подписи объектов.

Существует два способа повышения надежности хранения личного ключа сертификата с помощью сопроцессора:

- Хранение личного ключа сертификата непосредственно в сопроцессоре.
- Шифрование личного ключа сертификата с помощью главного ключа для хранения в специальном файле ключей.

Опция хранения ключей сертификатов в сопроцессоре задается в ходе создания или обновления сертификата. Кроме того, если ранее вы выбрали эту опцию, то вы можете назначить другой сопроцессор для данного ключа.

Для применения функций сопроцессора при хранении личного ключа необходимо перед началом работы с Диспетчером цифровых сертификатов (DCM) убедиться, что

сопроцессор включен. В противном случае, в ходе создания или обновления сертификата DCM не покажет страницу, позволяющую выбрать опцию хранения.

При создании или обновлении сертификата сервера или клиента опция хранения личного ключа сертификата задается после выбора типа сертификатной компании, подписавшей данный сертификат. При создании или обновлении локальной сертификатной компании опция хранения личного ключа сертификата задается в начале процесса.

Хранение личного ключа сертификата непосредственно в сопроцессоре

Для повышения надежности защиты личный ключ сертификата может храниться непосредственно в Шифровальном сопроцессоре IBM 4758–023 PCI. Опция хранения ключей сертификатов в сопроцессоре задается в ходе создания или обновления сертификата.

Для того чтобы личный ключ сертификата хранился непосредственно в сопроцессоре, выполните следующие действия на странице **Выбрать место хранения ключа**:

1. Выберите способ хранения **Аппаратное**.
2. Нажмите кнопку **Продолжить**. Появится страница **Выбрать описание шифровального устройства**.
3. Выберите в списке устройство, в котором будет храниться личный ключ сертификата.
4. Нажмите кнопку **Продолжить**. Появится следующая страница выполняемой пошаговой задачи DCM, например страница идентификационной информации для создаваемого или обновляемого сертификата.

Шифрование личного ключа сертификата с помощью главного ключа

Для повышения надежности защиты личный ключ сертификата может быть зашифрован главным ключом Шифровального процессора IBM 4758–023 PCI и помещен в специальный файл ключей. Опция хранения ключей сертификатов в сопроцессоре задается в ходе создания или обновления сертификата.

Перед выбором этой опции необходимо с помощью Web-интерфейса настройки Шифровального процессора IBM 4758–023 PCI создать соответствующий файл хранения ключей. Кроме того, с помощью того же интерфейса необходимо связать файл хранения ключей с описанием нужного сопроцессора. Web-интерфейс настройки сопроцессора может быть вызван со страницы задач iSeries.

Если в системе установлено и включено несколько сопроцессоров, то личный ключ сертификата может храниться в нескольких устройствах. Для этого все сопроцессоры должны применять один и тот же главный ключ. Процесс распределения одного и того же главного ключа среди нескольких устройств называется *дублированием*. Хранение ключа на нескольких сопроцессорах позволяет управлять нагрузкой на соединения Secure Sockets Layer (SSL), что способствует повышению их пропускной способности.

Для того чтобы личный ключ сертификата был зашифрован главным ключом сопроцессора и хранился в специальном файле ключей, выполните следующие действия на странице **Выбрать место хранения ключа**:

1. Выберите способ хранения **Аппаратное шифрование**.
2. Нажмите кнопку **Продолжить**. Появится страница **Выбрать описание шифровального устройства**.

3. Выберите в списке устройство, с помощью которого будет зашифрован личный ключ сертификата.
4. Нажмите кнопку **Продолжить**. Если в системе установлено и включено несколько сопроцессоров, то появится страница **Выбрать описания дополнительных шифровальных устройств**.

   Примечание: Если в системе установлен только один сопроцессор, то появится следующая страница выполняемой пошаговой задачи DCM, например страница идентификационной информации для создаваемого или обновляемого сертификата.
5. Выберите в списке одно или несколько описаний устройств, на которых будет храниться личный ключ сертификата.

   Примечание: Выбранные описания устройств должны применять тот же главный ключ, что и устройство, выбранное на предыдущей странице. Убедиться в этом можно, выполнив задачу Проверка главного ключа в Web-интерфейсе настройки Шифровального сопроцессора 4758. Web-интерфейс настройки сопроцессора может быть вызван со страницы задач iSeries.
6. Нажмите кнопку **Продолжить**. Появится следующая страница выполняемой пошаговой задачи DCM, например страница идентификационной информации для создаваемого или обновляемого сертификата.

Управление расположением сертификатной компании PKIX

Сертификатная компания инфраструктуры общих ключей X.509 (PKIX) - это сертификатная компания, выдающая сертификаты на основе новейших стандартов Internet x.509 применения инфраструктуры общих ключей. Стандарты PKIX описаны в документе RFC 2560.

Сертификатная компания PKIX предъявляет повышенные требования к идентификации при выдаче сертификатов; обычно претендент должен предоставить удостоверение личности через регистрационную компанию (RA). После того, как претендент предоставит необходимое удостоверение личности, регистрационная компания заверяет его личность. Затем регистрационная компания или претендент, в зависимости от конкретной сертификатной компании, отправляют заверенное заявление в сертификатную компанию. По мере распространения этих стандартов число сертификатных компаний PKIX будет увеличиваться. Сертификатные компании PKIX рекомендуется применять в случае, если требуется ужесточить контроль за доступом к ресурсам приложений с поддержкой SSL. Сертификатную компанию PKIX для внешнего использования предоставляет, например, Lotus Domino.

Если вы решили применять сертификаты, выдаваемые сертификатной компанией PKIX, то вы можете воспользоваться Диспетчером цифровых сертификатов (DCM). DCM позволяет задать URL для сертификатной компании PKIX. После этого в Диспетчере цифровых сертификатов будет предусмотрена опция получения сертификатов от сертификатной компании PKIX.

Для того чтобы настроить DCM для работы с сертификатами, выдаваемыми сертификатной компанией PKIX, вы должны указать в DCM расположение сертификатной компании, выполнив следующие действия:
1. Запустите DCM.
2. В окне навигации выберите **Управление расположением PKIX**. Появится форма, позволяющая задать URL сертификатной компании PKIX или связанной с ней регистрационной компании.

3. Введите полный URL сертификатной компании PKIX, от которой необходимо получить сертификат, например `http://www.thawte.com`, и нажмите кнопку **Добавить**. После этого в Диспетчере цифровых сертификатов будет предусмотрена опция получения сертификатов от сертификатной компании PKIX.

После того как вы добавите расположение сертификатной компании PKIX, в задаче DCM **Создать сертификат** появится опция, позволяющая указать тип требуемой сертификатной компании.

Подписание объектов

Существует три способа подписания объектов. Подписать объект можно путем вызова API Подписать объект. Кроме того, подписать объект можно с помощью Диспетчера цифровых сертификатов (DCM). Наконец, начиная с версии V5R2 можно подписать объекты с помощью Централизованного управления Навигатора во время упаковки объектов для их рассылки в другие системы iSeries.

Сертификаты, которыми вы управляете с помощью DCM, позволяют подписывать любые объекты интегрированной файловой системы, кроме объектов в библиотеках. В файловой системе QSYS.LIB можно подписывать объекты только следующих типов: *PGM, *SRVPGM, *MODULE, *SQLPKG и *FILE (только файл сохранения). Начиная с версии V5R2, поддерживается добавление подписей к объектам типа *CMD (команды). Подписывать объекты, находящиеся на других серверах iSeries, нельзя.

Сертификаты, применяемые для подписания объектов, могут быть как приобретенными у общественной сертификатной компании Internet (CA), так и созданными в частной локальной сертификатной компании в DCM. Процедура подписания объекта в обоих случаях одинакова.

Требования для подписания объектов

Перед подписью объектов с помощью DCM (или API Подписать объект) убедитесь, что выполнены следующие условия:

- Должно быть создано хранилище сертификатов *OBJECTSIGNING - либо во время создания локальной CA, либо в процессе управления сертификатами подписи объектов, полученными от общественной CA Internet.
- В хранилище сертификатов *OBJECTSIGNING должен быть по крайней мере один сертификат, созданный с помощью локальной CA или полученный от общественной CA Internet.
- Должно быть создано определение приложения, которое будет подписывать объекты.
- Приложению, которое будет подписывать объекты, должен быть присвоен сертификат.

Подписание объектов с помощью DCM

Для подписания объектов с помощью DCM выполните следующие действия:

1. Запустите DCM.

   Примечание: Для просмотра информации о заполнении полей формы при работе с DCM нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
3. Введите пароль для хранилища сертификатов *OBJECTSIGNING и нажмите **Продолжить**.

4. После обновления информации в окне навигации выберите **Управление доступными объектами** для просмотра списка задач.
5. В списке задач выберите **Подписать объект**. Будет показан список определений приложений, позволяющих подписать объект.
6. Выберите приложение и нажмите кнопку **Подписать объект**. Будет показана форма, в которой необходимо указать расположение подписываемых объектов.

   Примечание: Если выбранному приложению не присвоен сертификат, то с его помощью нельзя подписать объект. Сначала необходимо с помощью задачи **Обновить присвоение сертификата** в категории **Управление приложениями** присвоить сертификат определению приложения.
7. В появившемся поле введите полное имя файла объекта или каталог объектов, которые нужно подписать, и нажмите кнопку **Продолжить**. Вы можете также ввести расположение каталога и нажать **Обзор**, чтобы просмотреть содержимое каталога и выбрать объекты, которые нужно подписать.

   Примечание: Во избежание ошибок полное имя объекта следует начинать с косой черты. Вместо некоторой части каталога можно указать символы подстановки. Это звездочка (*****), означающая ″любое число символов,″ и вопросительный знак (**?**), означающий ″любой символ.″ Например, для того чтобы подписать все объекты в каталоге, введите `/mydirectory/*`; для того чтобы подписать все программы в определенной библиотеке, введите `/QSYS.LIB/QGPL.LIB/*.PGM`. Символы подстановки разрешено применять только в последней части имени; например, имя `/mydirectory*/filename` недопустимо. Если вы хотите просмотреть содержимое каталога или библиотеки с помощью функции обзора, то введите имя с символом подстановки и нажмите кнопку **Обзор**.
8. Выберите необходимые опции подписания выбранных объектов и нажмите кнопку **Продолжить**.

   Примечание: Если вы выбрали опцию ожидания результатов, то результаты выполнения задания будут показаны в окне браузера. Результаты выполнения текущего задания записываются в конец файла результатов. Таким образом, файл может содержать результаты выполнения не только текущего, но и предыдущих заданий. Определить, какие строки относятся к текущему заданию, можно по полю даты. Дата записывается в формате ГГГГММДД. Первое поле в файле содержит либо ИД сообщения (если при обработке объекта произошла ошибка), либо дату (дату выполнения задания).
9. Укажите полное имя файла для записи результатов операции подписания объекта и нажмите кнопку **Продолжить**. Вы можете также ввести расположение каталога и нажать **Обзор**, чтобы просмотреть содержимое каталога и выбрать файл для записи результатов. Появится сообщение о том, что задание подписания объектов передано на выполнение. Результаты можно просмотреть в протоколе задания **QOBJSGNBAT**.

Проверка подписей объектов

Диспетчер цифровых сертификатов (DCM) позволяет проверить подлинность цифровых подписей объектов. Проверка подписи позволяет убедиться в том, что содержимое объекта не было изменено с того момента, как владелец объекта подписал его.

Требования для проверки подписи

Перед проверкой подписей объектов с помощью DCM следует убедиться, что выполнены следующие условия:

- Должно быть создано хранилище сертификатов *SIGNATUREVERIFICATION для управления сертификатами проверки подписей.

  Примечание: Проверка подписей объектов в той же системе, в которой они были подписаны, может быть выполнена с помощью хранилища сертификатов *OBJECTSIGNING. Процедура проверки подписи с помощью DCM не зависит от выбранного хранилища сертификатов. Однако даже при проверке подписей с помощью хранилища сертификатов *OBJECTSIGNING в системе должно существовать хранилище сертификатов *SIGNATUREVERIFICATION, содержащее копию сертификата, с помощью которого был подписан объект.
- Хранилище сертификатов *SIGNATUREVERIFICATION должно содержать копию сертификата, с помощью которого были подписаны объекты.
- Хранилище сертификатов *SIGNATUREVERIFICATION должно содержать копию сертификата CA, выдавшей сертификат, с помощью которого были подписаны объекты.

Проверка подписей объектов с помощью DCM

Для проверки подписей объектов с помощью DCM выполните следующие действия:

1. Запустите DCM.

   Примечание: Для просмотра информации о заполнении полей формы при работе с DCM нажмите кнопку с вопросительным знаком (**?**) в верхней части страницы. Появится контекстная справка.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.
3. Введите пароль для хранилища сертификатов *SIGNATUREVERIFICATION и нажмите **Продолжить**.
4. После обновления информации в окне навигации выберите **Управление доступными объектами** для просмотра списка задач.
5. В списке задач выберите **Проверить подпись объекта**, чтобы задать расположение проверяемых объектов.
6. В появившемся поле введите полное имя файла объекта или каталог объектов, подписи которых нужно проверить, и нажмите кнопку **Продолжить**. Вы можете также ввести расположение каталога и нажать **Обзор**, чтобы просмотреть содержимое каталога и выбрать объекты, подписи которых нужно проверить.

   Примечание: Вместо некоторой части полного имени можно указать символы подстановки. Это звездочка (*****), означающая ″любое число символов,″ и вопросительный знак (**?**), означающий ″любой символ.″ Например, для того чтобы проверить все объекты в каталоге, введите `/mydirectory/*`; для того чтобы проверить все программы в определенной библиотеке, введите `/QSYS.LIB/QGPL.LIB/*.PGM`. Символы подстановки разрешено применять только в последней части имени; например, имя `/mydirectory*/filename` недопустимо. Если вы хотите просмотреть содержимое каталога или библиотеки с помощью функции обзора, то введите имя с символом подстановки и нажмите кнопку **Обзор**.
7. Выберите необходимые опции проверки подписи выбранного объекта или объектов и нажмите кнопку **Продолжить**.

Примечание: Если вы выбрали опцию ожидания результатов, то результаты выполнения задания будут показаны в окне браузера. Результаты выполнения текущего задания записываются в конец файла результатов. Таким образом, файл может содержать результаты выполнения не только текущего, но и предыдущих заданий. Определить, какие строки относятся к текущему заданию, можно по полю даты. Дата записывается в формате ГГГГММДД. Первое поле в файле содержит либо ИД сообщения (если при обработке объекта произошла ошибка), либо дату (дату выполнения задания).

8. Укажите полное имя файла для записи результатов операции проверки подписи объекта и нажмите кнопку **Продолжить**. Вы можете также ввести расположение каталога и нажать **Обзор**, чтобы просмотреть содержимое каталога и выбрать файл для записи результатов. Появится сообщение о том, что задание проверки подписи передано на выполнение. Результаты можно просмотреть в протоколе задания **QOBJSGNBAT**.

Кроме того, DCM позволяет просмотреть информацию о сертификате, с помощью которого был подписан объект. Это позволяет перед началом работы с объектом убедиться, что он получен из надежного источника.

Глава 9. Устранение неполадок в DCM

Здесь описаны действия по устранению некоторых наиболее распространенных неполадок, которые могут возникнуть при работе с Диспетчером цифровых сертификатов (DCM).

Ниже приведена информация о неполадках и возможных способах их устранения:

Устранение общих неполадок и неполадок, связанных с паролями
Здесь приведена информация о наиболее распространенных неполадках пользовательского интерфейса DCM и возможных способах их устранения.

Устранение неполадок хранилищ сертификатов и баз данных ключей
Здесь приведена информация о наиболее распространенных неполадках хранилищ сертификатов и баз данных ключей и возможных способах их устранения.

Устранение неполадок браузера
Здесь приведена информация о наиболее распространенных неполадках, которые могут возникнуть при работе с DCM с помощью браузера, и возможных способах их устранения.

Устранение неполадок HTTP Server для iSeries
Здесь приведена информация о наиболее распространенных неполадках в работе сервера HTTP и возможных способах их устранения.

Исправление ошибок, возникших при переходе к другой версии
Здесь приведена информация о наиболее распространенных неполадках, которые могут возникнуть при переходе к другой версии DCM, и возможных способах их устранения.

Устранение неполадок, возникших при регистрации сертификата пользователя
Здесь приведена информация о наиболее распространенных неполадках, которые могут возникнуть при регистрации сертификата пользователя с помощью DCM, и возможных способах их устранения.

Устранение общих неполадок и неполадок, связанных с паролями

В приведенной ниже таблице описаны действия по устранению некоторых наиболее распространенных неполадок, связанных с паролями, и других неполадок общего характера, которые могут возникнуть при работе с Диспетчером цифровых сертификатов (DCM).

Неполадка	Исправление
Не найдена дополнительная справка по DCM.	Щелкните на значке справки "**?**" в DCM. Кроме того, вы можете найти дополнительную информацию в Information Center и на других Web-сайтах в Internet.
При попытке открыть хранилище сертификатов появляется сообщение об ошибке NET.DATA.	При выполнении задачи **Выбрать хранилище сертификатов** нажмите с помощью мыши кнопку **Продолжить** на экране вместо клавиши **Enter** на клавиатуре.
Пароль хранилищ сертификатов локальной сертификатной компании (CA) и *SYSTEM не действует.	Пароли нужно вводить с учетом регистра. Убедитесь, что установлен тот же режим Caps Lock, что и при определении пароля.

Неполадка	Исправление
Попытка сбросить пароль после выполнения задачи Выбрать хранилище сертификатов не удалась.	Функция сброса пароля действует, только если пароль был сохранен. DCM автоматически сохраняет пароль при создании хранилища сертификатов. Однако при изменении пароля Хранилища сертификатов другой системы необходимо выбрать опцию **Автоматический вход в систему**, для того чтобы DCM сохранил пароль.
	Кроме того, для автоматического сохранения пароля в DCM после перемещения хранилища сертификатов из одной системы в другую необходимо изменить пароль хранилища сертификатов. Для изменения пароля при открытии хранилища сертификатов после его перемещения в другую систему необходимо ввести его прежний пароль. До того, как вы откроете хранилище сертификатов с помощью прежнего пароля и измените пароль, опция сброса пароля будет недоступна. Если не изменить и не сохранить пароль, средства DCM и SSL не смогут автоматически восстановить пароль для различных функций. При перемещении хранилища сертификатов, которое будет применяться как Хранилище сертификатов другой системы, после изменения пароля необходимо выбрать опцию **Автоматический вход в систему**, чтобы DCM сохранил пароль для этого типа хранилища сертификатов.
	Проверьте значение атрибута ″Разрешить создание цифровых сертификатов″ опции Работа с защитой системы Системного инструментария (SST). Если для этого атрибута указано значение 2 (Нет), то пароль хранилища сертификатов нельзя сбросить. Для просмотра или изменения значения этого атрибута запустите команду STRSST и введите ИД пользователя и пароль сервисных средств. Затем выберите опцию ″Работа с защитой системы″. Скорее всего, ИД пользователя сервисных средств - QSECOFR.
Не найден сертификат CA, который нужно получить в системе iSeries.	Не все CA свободно выдают свои сертификаты. Если вам не удалось получить сертификат CA, обратитесь к своему VAR, чтобы он заключил особый или платный договор с CA.
Не найдено хранилище сертификатов *SYSTEM.	Полным именем файла хранилища сертификатов *SYSTEM должно быть `/qibm/userdata/icss/cert/server/default.kdb`. Если этот файл не существует, создайте его с помощью DCM. Воспользуйтесь задачей **Создать хранилище сертификатов**.
При работе с DCM возникла ошибка, сообщение о которой продолжает появляться и после ее исправления.	Очистите кэш браузера. Установите нулевой размер кэша и перезапустите браузер.
Сразу после выдачи сертификата серверу LDAP он не был показан в информации о защищенном приложении. Чаще всего эта ошибка возникает в случае, когда для запуска браузера Netscape Communications применяется Навигатор iSeries. В параметре кэша браузера для сравнения документа в кэше с документом в сети указано значение ″Один раз за сеанс.″	Измените значение параметра таким образом, чтобы документ в кэше сравнивался с документом в сети при каждой загрузке последнего.
При импорте с помощью DCM сертификата, подписанного глобальной CA, такой как Entrust, появилось сообщение о том, что срок действия сертификата не включает сегодняшний день или превосходит срок действия выдавшей его CA.	Срок действия сертификата задается в общем формате времени. Повторите операцию завтра. Убедитесь, что в системе iSeries правильно задана разница с временем UTC (`dspsysval qutcoffset`). Убедитесь, что в меню Сезонное время указана правильная разница во времени.

Неполадка	Исправление
При импорте сертификата Entrust возникла ошибка основного набора символов base 64.	Сертификат отправляется в специальном формате, например в формате PEM. Если функция копирования браузера работает неправильно, то вместе с сертификатом могут быть скопированы дополнительные символы, например пробелы в начале каждой строки. В этом случае в системе iSeries сертификат будет сохранен в неправильном формате. Некоторые Web-страницы автоматически исправляют эту неполадку. Некоторые ее игнорируют. Убедитесь, что формат копии сертификата совпадает с форматом его оригинала.
При переходе от DCM версии V4R3 сертификаты с истекшим сроком действия не обновляются.	Недействительные сертификаты системы не применяются, поэтому их нельзя сохранить в файле сертификатов *SYSTEM. Удалите или переименуйте старые файлы наборов ключей версии V4R3, проигнорируйте сообщение об ошибке преобразования или выполните операцию еще раз.
Не найден пример программы, которая добавляет сертификаты в контрольный список.	Пример программы еще не создан.

Устранение неполадок хранилищ сертификатов и баз данных ключей

В приведенных ниже таблицах описаны действия по устранению некоторых наиболее распространенных неполадок, которые могут возникнуть при работе с Диспетчером цифровых сертификатов (DCM).

Неполадка	Исправление
База данных ключей не найдена или недопустима.	Проверьте, правильно ли указаны имя файла и пароль. Убедитесь, что задано полное имя файла, начинающееся с косой черты.
База данных ключей не создана.	Убедитесь в отсутствии конфликтов имен файлов. Причиной такого конфликта могут служить файлы, которые явно не указаны в запросе.
Система не принимает текстовый файл CA, переданный в двоичном формате из другой системы. Текстовые файлы должны передаваться в формате ASCII.	Наборы ключей и базы данных ключей хранятся в двоичном формате, поэтому они отличаются от текстовых файлов CA. Текстовые файлы CA нужно передавать по FTP в текстовом режиме, а двоичные файлы, в том числе `.kdb`, `.kyr`, `.sth` и `.rdb`, - в двоичном режиме.
Не удалось изменить пароль базы данных ключей. Сертификат, хранящийся в базе данных ключей, больше не действителен.	Убедитесь, что пароль введен правильно. После этого удалите недействительные сертификаты из хранилища сертификатов и повторите операцию. Если в хранилище сертификатов находится сертификат с истекшим сроком действия, он больше не может применяться. В этом случае функция изменения пароля запретит смену пароля, а программа шифрования не обработает личные ключи недействительных сертификатов. Таким образом, пароль не будет изменен, и система отправит сообщение об ошибке хранилища сертификатов. Удалите недействительные сертификаты из хранилища сертификатов.

Неполадка	Исправление
Вы хотите применять сертификаты для идентификации пользователей Internet. Для этого вам необходимы контрольные списки, однако DCM не поддерживает их.	Разработчики приложений, применяющих контрольные списки, должны предоставлять контрольные списки вместе со своими приложениями. Кроме того, в приложении должна быть предусмотрена функция, идентифицирующая пользователя Internet и добавляющая его сертификат в контрольный список. Обратитесь к разделу Information Center, посвященному API QsyAddVldlCertificate. Информация о настройке применения контрольных списков в экземпляре защищенного сервера приведена в книге Webmaster's Guide.

Устранение неполадок браузера

В приведенной ниже таблице описаны действия по устранению некоторых наиболее распространенных неполадок браузеров, которые могут возникнуть при работе с Диспетчером цифровых сертификатов (DCM).

Неполадка	Исправление
Microsoft Internet Explorer не позволяет выбрать другой сертификат до тех пор, пока не будет запущен новый сеанс браузера.	Запустите новый сеанс Internet Explorer.
Internet Explorer показывает не все доступные сертификаты клиента и пользователя в своем списке. В нем содержатся только те сертификаты, выданные уполномоченной CA, которые может использовать защищенный сервер.	Сертификат CA должен быть помечен как надежный базовый сертификат не только в базе данных ключей, но и в списке сертификатов защищенного приложения. Убедитесь, что на PC вы вошли в систему под тем же именем, под которым сертификат пользователя был загружен в браузер. Получите другой сертификат пользователя от системы, к которой вы хотите подключиться. Системный администратор должен убедиться, что сертификатная компания, выдавшая сертификаты системы и пользователя, по-прежнему считается уполномоченной.
Сертификат CA был загружен в Internet Explorer 5. Однако не удалось открыть файл или найти диск, на котором был сохранен сертификат.	Это новая функция браузера. Такая ситуация возникает при работе с сертификатами, которым еще не присвоен статус надежных базовых сертификатов. Откройте или сохраните файл на PC.
Браузер отправил предупреждение о том, что имя системы не соответствует сертификату системы.	В некоторых браузерах применяются иные правила сравнения строчных и прописных букв в именах систем. Введите URL в том же регистре, в котором он задан в сертификате системы. Или, создайте сертификат системы, указав информацию в том регистре, который применяется большинством пользователей. Не изменяйте имя сервера и имя системы, если только вы не уверены в правильности своих действий. Кроме того, проверьте правильность настройки DNS.
При запуске Internet Explorer с HTTPS вместо HTTP появилось предупреждение о том, что будут применяться как защищенные, так и незащищенные соединения.	Выберите ответ Принять и проигнорировать предупреждение; в следующей версии Internet Explorer эта неполадка будет исправлена.
Netscape Communicator 4.04 для Windows при работе с польской кодовой страницей преобразует шестнадцатеричные значения A1 и B1 в B2 и 9A.	Это ошибка NLS браузера. Установите другую версию браузера, либо ту же версию, но для другой платформы (например Netscape Communicator 4.04 для AIX).

Неполадка	Исправление
Netscape Communicator 4.04 правильно отображает прописные символы NLS в сертификате пользователя, хранящемся в профайле пользователя, но неправильно отображает строчные символы.	Некоторые символы национального языка, которые было введены правильно, заменяются на другой символ при последующем просмотре. Например, Netscape Communicator 4.04 для Windows преобразует шестнадцатеричные значения A1 и B1 в значения B2 и 9A при работе с польской кодовой страницей.
В окне браузера конечного пользователя появилось сообщение о том, что сертификатная компания по-прежнему не является уполномоченной.	С помощью DCM измените **состояние CA** на ″доступна″, чтобы обозначить сертификатную компанию как уполномоченную.
Internet Explorer отклонил запрос на соединение HTTPS.	Это ошибка в программе браузера или в его конфигурации. Браузер отказался от подключения к серверу, сертификат которого подписан им самим или недействителен по какой-либо другой причине.
Браузер Netscape Communicator и другие продукты сервера применяют базовые сертификаты от различных компаний (VeriSign и других), чтобы воспользоваться преимуществами соединений SSL — в первую очередь, возможностью идентификации. Срок действия базовых сертификатов ограничен. Срок действия некоторых базовых сертификатов браузера Netscape и сервера истек между 25 и 31 декабря 1999 г. Если эта неполадка не была исправлена 14 декабря 1999 г. или ранее, то будет выдано сообщение об ошибке.	Более ранние версии браузера (Netscape Communicator версии 4.05 и ниже) содержат сертификаты, срок действия которых ограничен. Необходимо обновить браузер до текущей версии Netscape Communicator. Информация о базовых сертификатах браузера приведена на многих сайтах, например `http://home.netscape.com/security/` и `http://www.verisign.com/server/cus/rootcert/webmaster.html`. Браузер можно бесплатно загрузить с сайта `http://www.netcenter.com`.

Устранение неполадок HTTP Server для iSeries

В приведенной ниже таблице описаны действия по устранению некоторых наиболее распространенных неполадок HTTP Server для iSeries, которые могут возникнуть при работе с Диспетчером цифровых сертификатов (DCM).

Неполадка	Исправление
Не работает Защищенный протокол передачи гипертекстовой информации (HTTPS).	Убедитесь, что HTTP Server правильно настроен для работы с SSL. В V5R1 и более поздних версиях в файле конфигурации должен быть задан параметр **SSLAppName** с помощью графического пользовательского интерфейса HTTP Server. Кроме того, в конфигурации должен быть настроен виртуальный узел, применяющий порт SSL, с параметром **SSLEnable**. Также должны быть указаны два оператора ожидания для двух портов - SSL и не SSL. Кроме того, убедитесь, что экземпляр сервера создан, а его сертификат подписан.
Процесс регистрации экземпляра HTTP Server в списке защищенных приложений требует дополнительных пояснений.	В системе iSeries настройте конфигурацию сервера HTTP в его Web-интерфейсе. Сначала необходимо настроить виртуальный узел для применения SSL. Это можно сделать в меню Управление контекстом. Виртуальный узел должен применять порт SSL, указанный в директиве Listen. После этого необходимо включить SSL для настроенного виртуального узла в меню Общие параметры SSL. Все изменения необходимо сохранить в файле конфигурации. Учтите, что при регистрации экземпляра применяемый тип сертификатов не выбирается автоматически. С помощью DCM свяжите этот сертификат с приложением до перезапуска экземпляра сервера.

Неполадка	Исправление
Возникли затруднения при настройке контрольных списков и расширенной идентификации клиентов в HTTP Server.	Информация о настройке экземпляра сервера приведена в книге HTTP Server Webmaster's Guide. Эту информацию можно также найти в разделе Web-серверы справочной системы Information Center.
Netscape Communicator позволит выбрать другой сертификат только после истечения срока действия предыдущего, в соответствии с директивой конфигурации HTTP Server.	Вам не удалось зарегистрировать новый сертификат, так как браузер все еще применяет старый сертификат, для которого установлен продолжительный срок действия.
Не удалось загрузить сертификат X.509 для HTTP Server в окно браузера и обработать его с помощью API QsyAddVldlCertificate.	Для того чтобы сервер HTTP загружал переменную среды HTTPS_CLIENT_CERTIFICATE, необходимо указать **SSLEnable** и **SSLClientAuth ON**. Информация об этих API приведена в разделе API OS/400 справочной системы Information Center. Кроме того, рекомендуется просмотреть описание следующих контрольных списков и API, предназначенных для работы с сертификатами: • QsyListVldlCertificates и QSYLSTVC • QsyRemoveVldlCertificate и QRMVVC • QsyCheckVldlCertificate и QSYCHKVC • QsyParseCertificate и QSYPARSC, и т.д.
Не найден файл запроса, созданный при установке HTTP Server. С помощью этого файла система выбирает правильные файлы наборов ключей, заданные в директиве KEYFILE файлов конфигурации в каталоге сервера.	Дополнительная информация приведена в разделе Переход от предыдущей версии DCM. Для HTTP Server правильный файл - `/qibm/userdata/httpsvr/keyring/keymreq.crt`. Для сервера LDAP - `/qibm/userdata/os400/dirsrv/qdirsrv.crt`.
При запросе у HTTP Server списка сертификатов из контрольного списка, содержащего более 10000 элементов, возникает очень долгая пауза или тайм-аут.	Создайте пакетное задание, которое удаляет сертификаты по соответствующим критериям, например, недействительные сертификаты или сертификаты, выданные некоторой CA.
После обновления версии V4R3 до версии V5R2 и создания файла `/qibm/userdata/httpsvr/keyring/keymreq.crt` или `/qibm/usedata/os400/dirsrv/qdirsrv.crt` возникли ошибки при работе с хранилищем сертификатов. Автоматическое преобразование набора ключей в базу данных ключей не завершено.	Укажите старые файлы набора ключей в качестве хранилища сертификатов, удалите недействительные сертификаты из набора ключей и вызовите `qicss/qyepmgrt` для их преобразования. Если все необходимые сертификаты уже преобразованы, проигнорируйте или удалите файл `.crt`.
Сервер HTTP не запускается при заданном параметре **SSLEnable**, в протокол задания заносится сообщение об ошибке `HTP8351`. В протокол задания сервера *ADMIN при сбое сервера HTTP заносится сообщение об ошибке инициализации SSL с кодом `107`.	Ошибка `107` свидетельствует об истечении срока действия сертификата. Если вы попытались запустить экземпляр сервера *ADMIN, временно задайте параметр **SSLDisable**, чтобы вы смогли работать с сервером *ADMIN в DCM. С помощью DCM присвойте приложению другой сертификат, например QIBM_HTTP_SERVER_ADMIN в случае сервера *ADMIN.

Исправление ошибок, возникших при переходе к другой версии

Возможные ошибки и действий по их исправлению

Ниже описаны ошибки, которые могут возникнуть при переходе к другой версии:

/QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
Появление этого файла после установки компонента 34 и продукта 5722-DG1 означает, что продукт 5722-DG1 не преобразовал файл набора ключей. Вам потребуется преобразовать файл набора ключей в файл сертификатов *SYSTEM.

/QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT
Появление этого файла после успешной установки компонента 34 означает, что выполнить миграцию файла набора ключей для сервера LDAP не удалось.

Помимо описанных ошибок, при переходе к другой версии могут возникнуть и другие ошибки, о которых не будут выданы сообщения. Например, во время преобразования файлов наборов ключей в файл сертификатов *SYSTEM система может обнаружить конфликты с существующими пользовательскими файлами интегрированной файловой системы. В таком случае система не выполнит преобразование набора ключей. Несмотря на это, сообщение об ошибке отправлено не будет.

Иногда сообщение об ошибке отправляется уже после преобразования файла набора ключей с неполным сертификатом системы. Это может привести к ошибке при запуске экземпляра сервера *ADMIN IBM HTTP Server со значением ON параметра SSLMODE. Ниже перечислены возможные причины ошибки:

- Для преобразованного набора ключей был задан неверный сертификат по умолчанию.
- DCM прервал преобразование, так как в системе уже существует пользовательский файл с именем одного из целевых файлов преобразования.
- Во время преобразования возникла непредвиденная ошибка.

Вы можете запустить IBM HTTP Server, не присваивая параметру SSLMODE значение ON. Для этого перед запуском экземпляра сервера *ADMIN временно присвойте параметру SSLMODE значение OFF. Это позволит вам просмотреть файлы сертификатов с помощью DCM и исправить ошибку до завершения работы экземпляра сервера *ADMIN. После завершения работы экземпляра сервера *ADMIN присвойте параметру SSLMODE значение ON и вновь запустите экземпляр сервера *ADMIN для инициализации SSL.

После обновления компонента 34 могут возникать ошибки при работе с файлами сертификатов в DCM. Эти ошибки происходят в работе браузера. Ниже приведены примеры таких ошибок:

```
Ошибка базы данных
Ошибка при чтении из базы данных
Ошибка при записи в базу данных
Повреждение базы данных
Повреждение таблицы базы данных
```

Кроме того, в каталоге `/QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR` или `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR` системы может существовать файл `default.kdb`, который не является файлом сертификатов. В этом случае для создания новых сертификатов вам потребуется выполнить следующие действия в DCM:

Примечание: Если вы решили не преобразовывать файлы наборов ключей, а создать вместо этого новую CA и сертификат системы, то пропустите описанную ниже процедуру преобразования.

- Если вы собираетесь устанавливать сервер HTTP Server для iSeries (5722-DG1), то сделайте это сейчас, перед продолжением работы.

  Примечания:

  1. Программа установки компонента 34 продукта 5722–SS1 не будет обновлять версию, если компонент 34 уже установлен. Следовательно, эту задачу нельзя выполнить путем повторной установки компонента 34.
  2. Соответствующие файлы расположены в пользовательских каталогах, созданных с правами доступа PUBLIC *EXCLUDE. Убедитесь, что у вас есть права доступа к этим каталогам.

- Проверьте, существуют ли следующие файлы:
  - /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  - /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB

  Если да, то переименуйте их с помощью команды WRKLNK и создайте резервную копию.
- От имени пользователя с правами *ALLOBJ вызовите из командной строки программу QICSS/QYEPMGRT:

  ```
  CALL QICSS/QYEPMGRT
  ```

  В случае ее успешного выполнения убедитесь, что в системе нет следующих файлов:
  - /QIBM/USERDATA/HTTPSVR/KEYRING/KEYMREQ.CRT
  - /QIBM/USERDATA/OS400/DIRSRV/QDIRSRV.CRT

Обычно DCM создает резервную копию пользовательских данных, сохраненных в файлах, имена которых применяются DCM. Если следующие файлы не существуют:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KYR

а перечисленные ниже файлы существуют:

- /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
- /QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH

то система попытается переименовать их, добавив расширение .OLD Если и такие файлы уже есть в указанных каталогах, система не будет создавать резервную копию. Вместо этого она заменит существующие файлы .STH.

Другие ошибки

Если создать CA и сертификат системы по-прежнему не удается из-за конфликтов имен, то возможны следующие причины ошибок:

- **Различные конфликты имен файлов** – DCM пытается защитить пользовательские файлы в создаваемых каталогах, даже если их имена конфликтуют с именами служебных файлов DCM. Для того чтобы исправить эту ошибку, скопируйте все конфликтующие файлы в другой каталог и удалите их из исходного каталога с помощью DCM. Если эти файлы невозможно удалить средствами DCM, выполните эту операцию вручную. Запишите имена файлов, которые вы скопировали в другой каталог, а также имя этого каталога. Позднее вы сможете восстановить необходимые файлы. Для создания CA вам нужно переместить следующие файлы:

  ```
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.KDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.RDB
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STH .OLD
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.KYR
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POL
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.STHBAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.TEMP.STH
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TXT
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.BAK
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/CA.TMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLTMP
  /QIBM/USERDATA/ICSS/CERT/CERTAUTH/DEFAULT.POLBAK
  /QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CACRT
  ```

```
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CATMP
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CERTAUTH/CA.CABAK
/QIBM/USERDATA/ICSS/CERT/DOWNLOAD/CLIENT/*.USRCRT
```

После перемещения перечисленных ниже файлов нужно создать новый файл сертификатов *SYSTEM и сертификат системы:

```
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.RDB
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STH.OLD
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.STHBAK
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.TEMP.STH
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.TXT
/QIBM/USERDATA/ICSS/CERT/SERVER/SRV.SGN
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/SGN.BAK
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSRV.TMP
/QIBM/USERDATA/ICSS/CERT/SERVER/EXPSGN.TMP
```

- **Не выполнены предварительные требования** – Убедитесь, что в системе установлены все необходимые лицензионные программы (LPP).
- **Ошибка в программе** – Обратитесь в сервисное представительство.

Устранение неполадок, возникших при регистрации пользовательского сертификата

При выборе задачи **Присвоить пользовательский сертификат** появляется окно Диспетчера цифровых сертификатов (DCM), содержащее сертификат, регистрацию которого нужно подтвердить. Если окно с сертификатом не появилось, то возникла одна из следующих ошибок:

1. Браузер не предложил выбрать сертификат, который должен быть отправлен серверу. Возможно, это объясняется тем, что в кэше браузера сохранился старый сертификат, который применялся для доступа к другому серверу. Очистите кэш браузера и повторите операцию. Браузер должен выдать приглашение выбрать сертификат.
2. Выбранный сертификат уже зарегистрирован с помощью DCM.
3. У сертификатной компании, выдавшей сертификат, нет надежного базового сертификата. Это означает, что выбранный сертификат нельзя зарегистрировать. Выясните у системного администратора, правильно ли вы выбрали сертификатную компанию. Если CA выбрана верно, то системный администратор должен **импортировать** сертификат этой CA в хранилище сертификатов *SYSTEM. Если сертификат этой компании уже получен, то системный администратор должен выбрать задачу **Работа с сертификатами сертификатных компаний** и пометить сертификат этой CA как надежный базовый сертификат.
4. У вас нет ни одного сертификата, который можно зарегистрировать. Просмотрите список сертификатов пользователей с помощью браузера.
5. Для регистрации выбран неполный сертификат или сертификат с истекшим сроком действия. Обновите сертификат или обратитесь к CA, выдавшей сертификат.
6. IBM HTTP Server for iSeries настроен неправильно. Это не позволяет зарегистрировать сертификат, настроив соединение SSL и идентифицировав клиента с помощью экземпляра сервера *ADMIN. Если причина ошибки отлична от перечисленных выше, обратитесь к системному администратору и составьте отчет о неполадке.

Для того чтобы **присвоить пользовательский сертификат**, нужно установить соединение SSL с Диспетчером цифровых сертификатов. Если вы попытаетесь **присвоить пользовательский сертификат**, установив обычное соединение, то DCM отправит сообщение о том, что нужно установить соединение SSL. Нажав кнопку в окне сообщения, вы сможете подключиться к DCM с помощью SSL. Если в окне сообщения нет кнопки, обратитесь к системному администратору. Возможно, для включения поддержки SSL потребуется перезапустить Web-сервер.

Глава 10. Связанная информация о DCM

По мере роста популярности цифровых сертификатов увеличивается и количество источников информации о них. Ниже приведен небольшой список дополнительных источников информации о цифровых сертификатах и способах их применения для повышения надежности защиты информации iSeries:

- **Web-сайт VeriSign Help Desk**
  Этот Web-сайт содержит большую библиотеку по темам, связанным с цифровыми сертификатами и защите информации в сети Internet.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  В этом справочном руководстве фирмы IBM описаны усовершенствования функций защиты сети в версии V5R1. В книге освещено множество вопросов: функции подписания объектов в iSeries, Диспетчер цифровых сертификатов (DCM), поддержка Шифровального сопроцессора 4758 для SSL и др.
- **AS/400 Internet Security: Developing a Digital Certificate Infrastructure (SG24-5659)**
  Это руководство содержит информацию о работе с цифровыми сертификатами на сервере iSeries. Здесь приведены инструкции по настройке различных серверов и клиентов для работы с сертификатами. Кроме того, здесь приведена информация о применении API OS/400 для работы с цифровыми сертификатами в пользовательских приложениях, а также примеры программ.
- **RFC Index Search**
  Этот сайт представляет собой архив документов RFC, в котором возможен поиск. RFC описывает стандарты протоколов Internet, связанные с применением цифровых сертификатов, такие как SSL, PKIX и др.

Напечатано в Дании