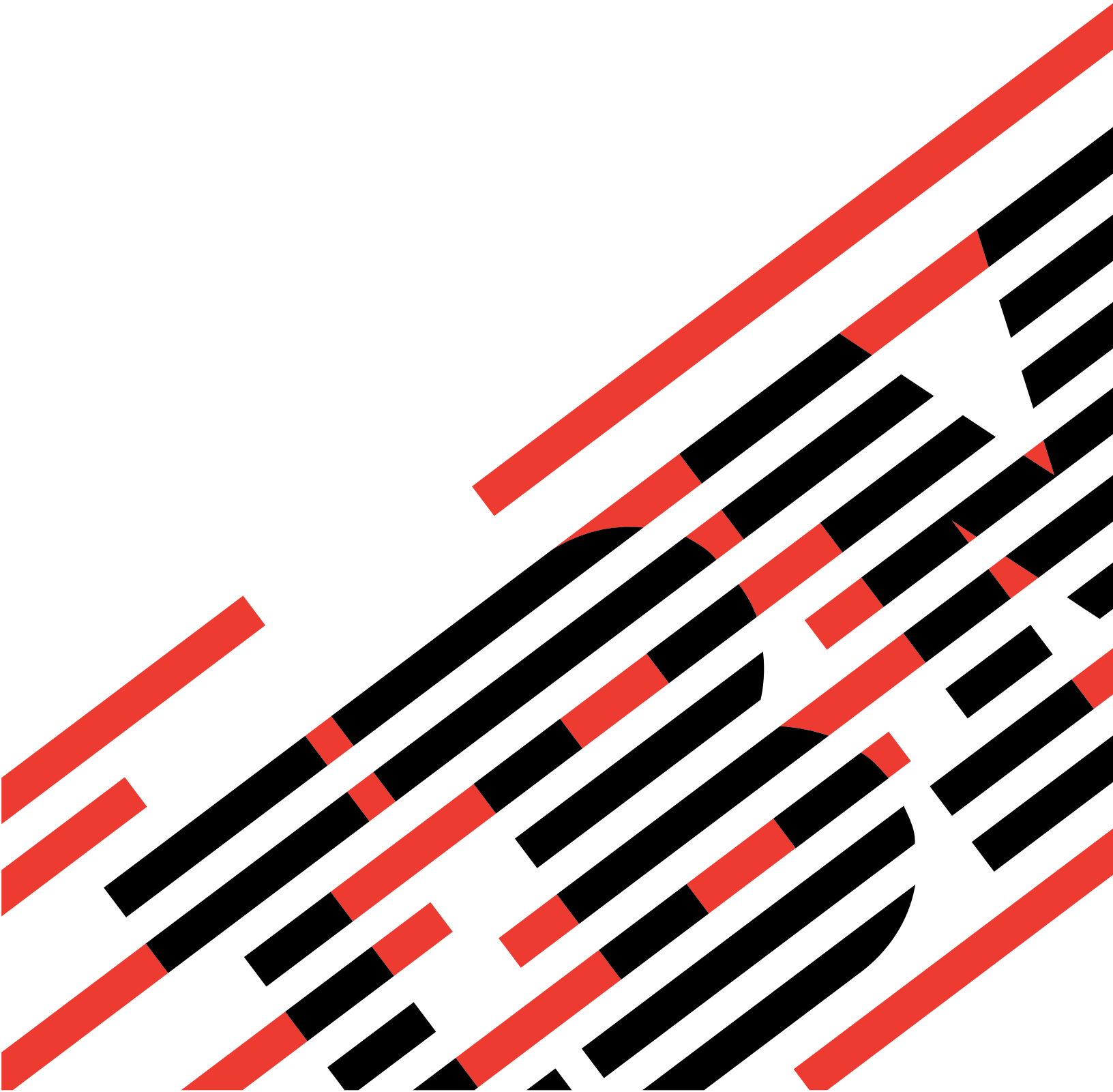
IBM Systems - iSeries

Диспетчер цифровых сертификатов безопасности

Версия 5, выпуск 4



IBM Systems - iSeries

Диспетчер цифровых сертификатов безопасности

Версия 5, выпуск 4

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 89.

Девятое издание (Февраль 2006 г.)

Данное издание относится к версии 5, выпуску 4, модификации 0 IBM i5/OS (код продукта 5722-SS1), а также ко всем последующим выпускам, если в новых изданиях не будет указано обратное. Данный выпуск работает не во всех системах с сокращенным набором команд (RISC) и не работает в системах с полным набором команд (CISC).

Содержание

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. Многие службы и приложения iSeries, такие как FTP, Telnet, HTTP Server и другие, поддерживают SSL для обеспечения конфиденциальности данных.

iSeries предоставляет широкую поддержку цифровых сертификатов, что позволяет 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, 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 выпуске V5R4

В этом разделе приведены изменения или дополнения, внесенные в этом выпуске.

Новая информация об обновлении сертификатов

В обновленном разделе приведено описание всех действий, из которых состоит процедура обновления существующих сертификатов, выданных локальными сертификатными компаниями, либо сертификатными компаниями Internet.

• “Обновление существующего сертификата” на стр. 55

Новая информация об импорте сертификатов

В этом разделе шаг за шагом объясняется процедура импорта сертификатов, которые находятся в файлах на сервере, либо в файлах в другой системе.

• “Импорт сертификата” на стр. 57

Расширения Списка аннулированных сертификатов (CRL) и информация о протоколе LDAP

Раздел обновлен, теперь в нем содержится информация об анонимном подключении к серверу LDAP для обработки CRL.

• “Управление определениями CRL” на стр. 72

- “Управление каталогом LDAP для пользовательских сертификатов” на стр. 75
- “Определения списка аннулированных сертификатов (CRL)” на стр. 6

Как получить информацию о новых возможностях и изменениях

Для того чтобы упростить поиск измененной технической информации, в данном документе применяются следующие обозначения:

- Рисунок  указывает на начало новой или измененной информации.
- Рисунок  указывающий на окончание новой или измененной информации.

Сведения о новых возможностях, появившихся в этом выпуске, приведены в разделе Информация для пользователей.

Файл PDF, доступный для печати

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

Для просмотра или загрузки этого раздела в формате PDF щелкните на ссылке Диспетчер цифровых сертификатов  (примерно 600 Кб или 116 страниц).

Сохранение файлов PDF

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

1. Щелкните правой кнопкой на файле PDF в окне браузера (т.е. на приведенной выше ссылке).
2. Если вы используете Internet Explorer, выберите пункт меню **Сохранить объект как...**. Если вы используете Netscape Communicator, выберите пункт меню **Сохранить ссылку как...**
3. Укажите каталог, в котором вы хотите сохранить документ.
4. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Acrobat Reader

Для просмотра и печати этих файлов PDF необходима программа Adobe Acrobat Reader. Копию программы можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Концепции DCM

В этом разделе более подробно рассмотрены цифровыми сертификаты и принципы их работы. Раздел содержит информацию о различных типах сертификатов и их роли в стратегии защиты.

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. Идентификационные данные, которые предоставляет цифровой сертификат, называют отличительными именем субъекта. Специальная уполномоченная организация, называемая сертификатной компанией (CA), выдает цифровые сертификаты пользователям и организациям. Полномочия CA служат гарантией подлинности сертификатов, которые она выдает.

Цифровой сертификат также содержит общий ключ, входящий в состав пары из общего и личного ключей. Множество функций защиты основаны на применении цифровых сертификатов и связанных пар ключей. С помощью цифровых сертификатов можно настраивать защищенные сеансы связи Secure Sockets Layer (SSL),

между пользователями и серверными приложениями. Можно обеспечить дополнительную защиту, настроив приложения SSL таким образом, чтобы для идентификации пользователей применялись не имя пользователя и пароль, а цифровой сертификат.

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

Расширения сертификатов

Расширения сертификата - это информационные поля, которые содержат дополнительные сведения о сертификате.

Расширения сертификата позволяют расширить возможности основного стандарта данных сертификата X.509. Часть полей расширения содержит дополнительные сведения об идентификации сертификата, а часть - дополнительные сведения о возможностях шифрования сертификата.

Не во всех сертификатах поля расширения служат для дополнения отличительного имени и хранения другой информации. Число и тип полей расширения в сертификатах разных сертификатных компаний (CA) могут существенно различаться.

Например, локальная сертификатная компания, которую можно создать с помощью диспетчера цифровых сертификатов (DCM), поддерживает только расширения Дополнительное имя субъекта. Эти расширения позволяют связывать сертификат с конкретным IP-адресом, доменным именем или с адресом электронной почты. Если такой сертификат применяется для идентификации конечной точки соединения VPN в системе iSeries, то необходимо указать данные в этих полях расширения.

Понятия, связанные с данным

“Отличительное имя” на стр. 4
Этот раздел содержит информацию об идентификационных характеристиках цифровых сертификатов.

Обновление сертификатов

Процесс обновления сертификата, применяемый Диспетчером цифровых сертификатов (DCM), зависит от типа сертификатной компании (CA), выдавшей сертификат.

Если обновленный сертификат подписан локальной CA, то DCM на основе предоставленной пользователем информации создает новый сертификат в текущем хранилище сертификатов и не удаляет предыдущий сертификат.

Если сертификат получен от общеизвестной сертификатной компании Internet, то обновить сертификат можно одним из двух способов: импортировать обновленный сертификат из файла, полученного от сертификатной компании, либо создать с помощью DCM новую пару из общего и личного ключа для сертификата. При обновлении сертификата в компании, выдавшей его, в DCM применяется первый способ.

Если вы решили создать новую пару ключей, то для обновления сертификата DCM применяет ту же процедуру, что и для создания сертификата. DCM создаст новую пару из личного и общего ключей для обновленного сертификата, и создаст запрос на подписание сертификата (CSR), который состоит из общего ключа и других сведений, содержащихся в сертификате. После этого с помощью CSR можно отправить запрос на получение нового сертификата в компанию VeriSign или любую другую CA. После получения подписанного сертификата можно с помощью DCM импортировать его в соответствующее хранилище сертификатов. После этого хранилище будет содержать обе копии сертификата - исходную и обновленную.

Если вы решили не создавать новую пару ключей, то DCM предложит вам последовательно выполнить операции по импорту обновленного подписанного сертификата из полученного от сертификатной компании файла в хранилище сертификатов. В этом случае предыдущая версия сертификата будет заменена на новую импортированную версию.

Отличительное имя

Этот раздел содержит информацию об идентификационных характеристиках цифровых сертификатов.

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 хранящуюся в сертификате идентификационную информацию. Отличительное имя входит в состав сертификата. Сертификат содержит как DN владельца или отправителя запроса на сертификат (DN субъекта), так и DN сертификатной компании, выдавшей сертификат (DN сертификатной компании). 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
- Населенный пункт или город
- Область или округ
- Страна или регион

При выдаче личных сертификатов с помощью DCM вы можете воспользоваться расширениями сертификата и включить в них данные DN:

- IP-адрес версии 4
- Полное имя домена
- Электронный адрес

Понятия, связанные с данным

“Расширения сертификатов” на стр. 3
Расширения сертификата - это информационные поля, которые содержат дополнительные сведения о сертификате.

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 i5/OS 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.

Понятия, связанные с данным

“Сертификатная компания (CA)” на стр. 6
Сертификатная компания (CA) - это центральный административный орган, уполномоченный выдавать цифровые сертификаты пользователям и серверам.

“Шифрование” на стр. 9
В этом разделе приведена информация о том, что такое шифрование и каким образом обеспечивается защита с помощью функций шифрования сертификатов.

“Общий и личный ключи”
С каждым сертификатом связана пара шифровальных ключей, состоящая из личного и общего ключей.

Общий и личный ключи

С каждым сертификатом связана пара шифровальных ключей, состоящая из личного и общего ключей.

Примечание: 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.

Понятия, связанные с данным

“Цифровые подписи” на стр. 4
Цифровая подпись в электронном документе или другом объекте аналогична обычной подписи в напечатанном документе и создается с помощью одного из видов шифрования.

“Сертификатная компания (CA)” на стр. 6
Сертификатная компания (CA) - это центральный административный орган, уполномоченный выдавать цифровые сертификаты пользователям и серверам.

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 цифровую подпись, указывающую на происхождение сертификата. С помощью общего ключа сертификатной компании другие пользователи могут проверить подлинность выдаваемых и подписываемых ей сертификатов.

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. Диспетчер цифровых сертификатов (DCM) позволяет применять сертификаты, полученные как от частных, так и общественных сертификатных компаний.

DCM позволяет также выдавать системам и пользователям сертификаты с помощью собственной локальной частной сертификатной компании. При выдаче локальной CA пользовательского сертификата DCM автоматически связывает сертификат с пользовательским профайлом системы iSeries или с идентификатором пользователя. Тип объекта, с которым DCM связывает сертификат, зависит о того, поддерживает ли текущая конфигурация DCM работу с функцией преобразования идентификаторов в рамках предприятия (EIM). 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. 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 локальную сертификатную компанию с помощью Диспетчера цифровых сертификатов, вы можете указать ее полномочия. В полномочиях локальной 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.

Понятия, связанные с данным

“Цифровые подписи” на стр. 4
Цифровая подпись в электронном документе или другом объекте аналогична обычной подписи в напечатанном документе и создается с помощью одного из видов шифрования.

“Общий и личный ключи” на стр. 5
С каждым сертификатом связана пара шифровальных ключей, состоящая из личного и общего ключей.

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 подключении к серверу LDAP нужно ввести DN и пароль, во избежание анонимного подключения. Анонимное подключение к серверу не обеспечивает уровень доступа, необходимый для работы с ″критическими″ атрибутами, такими как CRL. В этом случае в результате проверки сертификата Диспетчер цифровых сертификатов может выдать аннулированное состояние, поскольку он не может получить правильное состояние от CRL. Для анонимного доступа к серверу LDAP необходимо с помощью Web-инструмента администрирования сервера каталогов выбрать задачу ″Управление схемой″ и изменить класс защиты (который также называется ″классом доступа″) атрибутов **certificateRevocationList** и **authorityRevocationList** с ″critical″ до ″normal″.

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 .

Понятия, связанные с данным

“Проверка сертификатов и приложений” на стр. 70
Диспетчер цифровых сертификатов (DCM) позволяет проверять отдельные сертификаты и применяющие их приложения. Проверка приложения несколько отличается от проверки сертификата.

Задачи, связанные с данной

“Управление определениями CRL” на стр. 72
Диспетчер цифровых сертификатов (DCM) позволяет задать для сертификатной компании определение Списка аннулированных сертификатов (CRL), применяемое в процессе проверки сертификатов.

Хранилища сертификатов

Хранилище сертификатов - это специальный файл базы данных, в котором Диспетчер цифровых сертификатов (DCM) хранит цифровые сертификаты.

В хранилище сертификатов хранятся личные ключи сертификатов, если только для этого не был выбран шифровальный сопроцессор IBM. DCM позволяет создавать несколько типов хранилищ сертификатов и управлять ими. Кроме того, в DCM паролями защищены хранилища сертификатов, а также каталоги интегрированной файловой системы и файлы, образующие 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 в системе установлен шифровальный сопроцессор IBM, то вы можете воспользоваться дополнительными возможностями хранения личных ключей сертификатов (за исключением сертификатов подписания объектов). 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.

Понятия, связанные с данным

“Типы цифровых сертификатов” на стр. 29
В этом разделе описаны различные типы цифровых сертификатов и работа с ними в Диспетчере цифровых сертификатов (DCM).

Шифрование

В этом разделе приведена информация о том, что такое шифрование и каким образом обеспечивается защита с помощью функций шифрования сертификатов.

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.

Понятия, связанные с данным

“Цифровые подписи” на стр. 4
Цифровая подпись в электронном документе или другом объекте аналогична обычной подписи в напечатанном документе и создается с помощью одного из видов шифрования.

“Secure Sockets Layer (SSL)” на стр. 10
Протокол Secure Sockets Layer (SSL), разработанный фирмой Netscape, является стандартным средством шифрования данных в соединениях между клиентом и сервером.

Шифровальные сопроцессоры IBM для iSeries

Шифровальный сопроцессор содержит проверенные функции шифрования, обеспечивающие конфиденциальность и целостность данных при разработке защищенных приложений электронного бизнеса.

Шифровальный сопроцессор IBM для iSeries значительно расширяет возможности шифрования системы. Если в системе установлен и включен шифровальный сопроцессор, то он предоставляет дополнительное защищенное хранилище для личных ключей сертификатов.

С помощью шифровального сопроцессора можно сохранить личный ключ сертификата сервера и клиента, а также сертификата локальной сертификатной компании (CA). Личный ключ сертификата пользователя должен находиться в системе пользователя и поэтому он не может храниться в сопроцессоре. Кроме того, в текущей версии системы в сопроцессоре не допускается хранение личного ключа сертификата подписи объектов.

Личный ключ сертификата можно хранить непосредственно в шифровальном сопроцессоре, либо зашифровать ключ с помощью главного ключа сопроцессора и хранить его 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.

Понятия, связанные с данным

“Хранение ключей сертификатов в шифровальном сопроцессоре IBM” на стр. 73
В этом разделе приведена информация об использовании установленного сопроцессора в качестве более надежного хранилища личных ключей сертификатов.

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.

Понятия, связанные с данным

“Шифрование” на стр. 9
В этом разделе приведена информация о том, что такое шифрование и каким образом обеспечивается защита с помощью функций шифрования сертификатов.

“Типы цифровых сертификатов” на стр. 29
В этом разделе описаны различные типы цифровых сертификатов и работа с ними в Диспетчере цифровых сертификатов (DCM).

Определения приложений

В этом разделе приведена информация об определениях приложений DCM и применении этих определений для настройки SSL и подписания объектов.

С помощью Диспетчера цифровых сертификатов (DCM) можно управлять двумя типами определений приложений:

- Определения клиентских или серверных приложений, применяющих соединения SSL.
- Определения приложений подписания объектов, применяющих подписи для обеспечения целостности объектов.

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) для автоматического создания 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.

Понятия, связанные с данным

“Управление приложениями в DCM” на стр. 67
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.

Задачи, связанные с данной

“Создание определения приложения” на стр. 67
В этом разделе описаны два различных типа приложений, для работы с которыми можно создавать их определения.

Проверка

В DCM предусмотрены задачи, позволяющие проверять свойства сертификатов и приложений.

Проверка сертификатов

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).

Если Упрощенный протокол доступа к каталогам (LDAP) настроен на применение CRL, то Диспетчер цифровых сертификатов проверяет CRL при проверке сертификата для того, чтобы убедиться, что сертификат не указан в CRL. Однако для того чтобы обеспечить точность проверки CRL, сервер каталогов (сервер LDAP), настроенный с преобразованием LDAP, должен содержать соответствующий CRL. В противном случае, сертификат может не пройти проверку. Для того чтобы сертификат не был признан аннулированным, необходимо ввести DN привязки и пароль. Кроме того, если DN и пароль не указаны при настройке преобразования LDAP, то будет выполняться анонимное подключение к серверу LDAP. Анонимное подключение к серверу LDAP не обеспечивает права доступа, достаточные для работы с ″критическими″ атрибутами, а CRL - это ″критический″ атрибут. В этом случае в результате проверки сертификата Диспетчер цифровых сертификатов может выдать аннулированное состояние, поскольку он не может получить правильное состояние от CRL. Для анонимного доступа к серверу LDAP необходимо с помощью Web-инструмента администрирования сервера каталогов выбрать задачу ″Управление схемой″ и изменить класс защиты (который также называется ″классом доступа″) атрибутов **certificateRevocationList** и **authorityRevocationList** с ″critical″ до ″normal″.

DCM также проверяет, находится ли сертификат CA для сертификатной компании в текущем хранилище сертификатов, и является ли сертификат CA надежным. 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.

Проверка приложения

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 приложения позволяет устранить потенциальные неполадки приложений при работе с сертификатами. Такие неполадки могут помешать приложению устанавливать соединения Secure Sockets Layer (SSL) или подписывать объекты.

Понятия, связанные с данным

“Проверка сертификатов и приложений” на стр. 70
Диспетчер цифровых сертификатов (DCM) позволяет проверять отдельные сертификаты и применяющие их приложения. Проверка приложения несколько отличается от проверки сертификата.

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.

Диспетчер цифровых сертификатов и функция поддержки цифровых сертификатов iSeries позволяют существенно повысить уровень защиты системы за счет применения 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. Кроме того, в зависимости от конфигурации DCM, с его помощью можно связать сертификат пользователя с его пользовательским профайлом iSeries или с идентификатором EIM. 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 соединений. Каждый из сценариев, кроме того, содержит описание всех предварительных требований к системе и программному обеспечению, а также необходимых действий по настройке.

Информация, связанная с данной

Сценарии подписи объектов

Сценарий: Внешняя идентификация 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.

Задача:

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 идентификации пользователей приложений, 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 конфиденциальной информации, с которой работает данное приложение, можно обеспечить с помощью цифровых сертификатов. Сертификаты позволяют защитить передачу важных данных с помощью SSL. 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. Кроме того, вы планируете и далее выполнять идентификацию пользователей как с помощью сертификатов, так и с помощью имен пользователей и паролей, поскольку SSL обеспечивает защиту конфиденциальных данных при их передаче.

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, размещая в сети Internet Web-сайт или приложение 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 финансовой информации, предоставляемой ее приложением внешним пользователям с правами доступа. Кроме того, компания собирается ввести более защищенный метод идентификации пользователей приложения.

Цели этого сценария следующие:

- Внутренний Web-сайт персонала компании должен применять протокол SSL для защиты предоставляемых 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, если сертификат недоступен, то действительные имя пользователя и пароль.

Подробности

На следующей схеме представлена конфигурация сети для данного сценария:

На рисунке представлена следующая информация об этом сценарии:

Общий сервер компании – iSeries A

- iSeriesA - это сервер, на котором работает приложение расчета страховых премий.
- На сервере iSeries A выполняется i5/OS версия 5 выпуск 4 (V5R4).
- На сервере iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 системы i5/OS) и IBM HTTP Server for i5/OS (5722–DG1).
- На сервере iSeries A размещено приложение расчета премий, которое:
  - Требует применения SSL.
  - Применяет для создания соединений SSL сертификат, полученный от общеизвестной сертификатной компании (CA).
  - Требует идентификации клиентов по имени пользователя и паролю.
- Сервер iSeries A предоставляет свой сертификат для создания соединений SSL, когда клиентские системы B и C обращаются к приложению расчета премий.
- После создания сеанса SSL сервер iSeries A просит клиентские системы B и C предоставить правильные имя пользователя и пароль для доступа к приложению расчета премий.

Клиентские системы агентов – клиент B и клиентC

- 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.
- Клиенты B и C обращаются к приложению расчета премий на сервере iSeries A, который представляет свой сертификат программному обеспечению клиентов для идентификации и создания соединения SSL.

- Клиентское программное обеспечение в системах B и C принимает в качестве средства идентификации для создания сеанса SSL сертификат сервера iSeries A.
- После создания сеанса SSL сервер iSeries A запрашивает у клиентских систем B и C имя пользователя и пароль для доступа к приложению расчета премий.

Предварительные требования и допущения

Этот сценарий зависит от выполнения следующих предварительных требований и допущений:

- Предложение расчета премий на сервере iSeries A - это стандартное приложение, которое можно настроить для работы с SSL. Большинство приложений, включая многие приложения сервера iSeries, поддерживают SSL. Действия по настройке SSL различаются в зависимости от конкретного приложения. В связи с этим сценарий не содержит инструкций по настройке SSL в приложении расчета ставок. В этом сценарии приведены инструкции по настройке и управлению сертификатами, которые необходимы для всех приложений, применяющих протокол SSL.
- 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.
- Сервер iSeries A соответствует требованиям к установке и применению Диспетчера цифровых сертификатов (DCM)
- Ранее DCM на сервере iSeries A не настраивался и не применялся.
- У пользователя, выполняющего задачи этого сценария с помощью DCM, есть специальные права доступа *SECADM и *ALLOBJ.
- На сервере iSeries A не установлен шифровальный сопроцессор IBM.

Задачи настройки

Задачи, связанные с данной

“Запуск Диспетчера цифровых сертификатов” на стр. 40
Содержит информацию о запуске функции Диспетчер цифровых сертификатов (DCM) в системе сервере.

Заполните формы планирования

В приведенных ниже формах планирования показана информация, которую необходимо собрать, и решения, которые необходимо принять для реализации предлагаемого способа применения цифровых сертификатов. Для успешной реализации необходимо, чтобы на все вопросы о предварительных требованиях был дан ответ Да, а также чтобы была собрана вся необходимая информация.

Таблица 1. Форма предварительных требований

Форма предварительных требований	**Ответы**
Работаете ли вы с системой i5/OS V5R42 (5722-SS1)?	Да
Установлен ли компонент 34 системы i5/OS?	Да
Установлен ли в системе сервер IBM HTTP Server for i5/OS (5722–DG1) и запущен ли административный экземпляр сервера?	Да
Позволяет ли конфигурация TCP обращаться к DCM с помощью Web-браузера и административного сервера HTTP?	Да
Есть ли у вас специальные права доступа *SECADM и *ALLOBJ?	Да

Для выполнения задач настройки и реализации рассматриваемого сценария необходима следующая информация о применяемых цифровых сертификатах:

Таблица 2. Форма параметров сертификатов

Форма планирования для сервера iSeries A	**Ответы**
Будете ли вы использовать локальную сертификатную компанию или применять сертификаты общественной CA?	Применять сертификаты общественной CA
Находятся ли на сервере iSeries A приложения, для которых необходимо включить поддержку SSL?	Да
Какое полное имя будет использоваться при создании запроса на подписание сертификата (CSR) с помощью DCM? • **Размер ключа**: определяет уровень ключей шифрования сертификата. • **Метка сертификата**: служит идентификатором сертификата с уникальным набором параметров. • **Общее имя**: идентифицирует владельца сертификата, например, человека, объект или приложение; входит в полное имя (DN) субъекта сертификата. • **Отдел организации**: организационное подразделение или часть приложения, применяющего данный сертификат. • **Название организации**: название компании или ее подразделения, в котором применяется приложение, использующее данный сертификат. • **Город**: город или район, в котором расположена организация. • **Область или район**: область или край, в котором будет применяться данный сертификат. • **Страна или регион**: двухсимвольный идентификатор страны или региона, в котором применяется данный сертификат.	**Длина ключа**: 1024**Метка сертификата**: Myco_public_cert**Общее имя**: myco_rate_server@myco.com**Подразделение**: Rate dept**Организация**: организация**Адрес или город**: любой-город**Область или район**: Любые**Страна или регион**: ZZ
Каков в DCM ИД приложения, которое необходимо настроить для работы с SSL?	mcyo_agent_rate_app
Будет ли в приложениях с поддержкой SSL выполняться идентификация клиентов с помощью сертификатов? Если да, то какие сертификатные компании необходимо добавить в список уполномоченных CA приложения?	Нет

Создайте запрос на сертификат клиента или сервера

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, полное имя 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.

   Примечание: После завершения работы с этой страницей данные будут потеряны и не смогут быть восстановлены.
8. После завершения работы с этой страницей данные будут потеряны и не смогут быть восстановлены.
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.

Настройка поддержки SSL в приложении

Получив подписанный сертификат от общественной сертификатной компании (CA), вы можете продолжить настройку поддержки протокола Secure Sockets Layer (SSL) в приложении. Поддержку SSL необходимо настроить до начала работы с подписанным сертификатом. Некоторые приложения, например, HTTP Server для iSeries, создают уникальный ИД приложения и регистрируют ИД в Диспетчере цифровых сертификатов (DCM) при настройке SSL. 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. Дополнительная информация о настройке SSL для различных приложений IBM приведена в разделе Secure Sockets Layer (SSL) в iSeries Information Center.

После завершения настройки SSL для приложения можно создать для этого приложения подписанный общий сертификат, который можно будет применять в сеансах связи SSL.

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. Когда на экране появится страница **Хранилище сертификатов и пароль**, укажите пароль хранилища сертификатов, заданный при его создании, 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 импорт 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.

Запуск приложения в режиме SSL

После импорта 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.

Для того чтобы идентификация клиентов выполнялась с помощью сертификатов, создайте список уполномоченных CA для приложения.

(Необязательно): Создайте список уполномоченных CA для приложения, которое их требует.

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, но это приложение должно поддерживать идентификацию с помощью сертификатов, когда они будут применяться. 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. Когда на экране появится страница **Хранилище сертификатов и пароль**, укажите пароль хранилища сертификатов, заданный при его создании, 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 один или несколько сертификатов 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: Внутренняя идентификация с помощью сертификатов

В этом сценарии показано, когда и как следует применять сертификаты для защиты и ограничения доступа внутренних пользователей к ресурсам и приложениям или приложениям на внутренних серверах.

Задача

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 отвечаете за администрирование этого Web-сайта, размещенного на сервере IBM HTTP Server for i5/OS (на основе Apache).

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. Кроме того, ограничение доступа к данным компании выполняется с помощью традиционных средств, таких как имя пользователя и пароль. Поскольку пользователи работают с частной и конфиденциальной информацией, 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 пользователей 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.
  - У пользователей уже есть пользовательские профайлы iSeries, позволяющие управлять их доступом к приложениям и данным.
  - 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 реализовать более надежный метод идентификации пользователей 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 следующей схеме представлена конфигурация сети для данного сценария:

На рисунке представлена следующая информация об этом сценарии:

Общий сервер компании – iSeries A

- iSeriesA - это сервер, на котором работает приложение расчета страховых премий.
- На сервере iSeries A выполняется i5/OS версия 5 выпуск 4 (V5R4).
- На сервере iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 системы i5/OS) и IBM HTTP Server for i5/OS (5722–DG1).
- На сервере iSeries A размещено приложение расчета премий, которое:
  - Требует применения SSL.
  - Применяет для создания соединений SSL сертификат, полученный от общеизвестной сертификатной компании (CA).
  - Требует идентификации клиентов по имени пользователя и паролю.
- Сервер iSeries A предоставляет свой сертификат для создания соединений SSL, когда клиентские системы B и C обращаются к приложению расчета премий.
- После создания сеанса SSL сервер iSeries A просит клиентские системы B и C предоставить правильные имя пользователя и пароль для доступа к приложению расчета премий.

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.
- Клиенты B и C обращаются к приложению расчета премий на сервере iSeries A, который представляет свой сертификат программному обеспечению клиентов для идентификации и создания соединения SSL.
- Клиентское программное обеспечение в системах B и C принимает в качестве средства идентификации для создания сеанса SSL сертификат сервера iSeries A.
- После создания сеанса SSL сервер iSeries A запрашивает у клиентских систем B и C имя пользователя и пароль для доступа к приложению расчета премий.

Предварительные требования и допущения

Этот сценарий зависит от выполнения следующих предварительных требований и допущений:

- Приложение отдела кадров сервера iSeries A выполняется на сервере IBM HTTP Server for i5/OS (на основе Apache). Сценарий не содержит инструкций по настройке SSL в на сервере HTTP. В этом сценарии приведены инструкции по настройке и управлению сертификатами, которые необходимы для всех приложений, применяющих протокол SSL.
- 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.
- На сервере HTTP отдела кадров на сервере iSeries A уже применятся идентификация с помощью паролей.
- Сервер iSeries A соответствует требованиям к установке и применению Диспетчера цифровых сертификатов (DCM).
- Ранее DCM на сервере iSeries A не настраивался и не применялся.
- У пользователя, выполняющего задачи этого сценария с помощью DCM, есть специальные права доступа *SECADM и *ALLOBJ.
- На сервере iSeries A не установлен шифровальный сопроцессор IBM.

Задачи настройки

Заполните формы планирования

В приведенных ниже формах планирования показана информация, которую необходимо собрать, и решения, которые необходимо принять для реализации предлагаемого способа применения цифровых сертификатов. Для успешной реализации необходимо, чтобы на все вопросы о предварительных требованиях был дан ответ Да, а также чтобы была собрана вся необходимая информация.

Таблица 3. Форма предварительных требований

Форма предварительных требований	**Ответы**
Работаете ли вы с системой i5/OS V5R4 (5722-SS1)?	Да
Установлен ли компонент 34 системы i5/OS?	Да
Установлен ли в системе сервер IBM HTTP Server for i5/OS (5722–DG1) и запущен ли административный экземпляр сервера?	Да
Позволяет ли конфигурация TCP обращаться к DCM с помощью Web-браузера и административного сервера HTTP?	Да
Есть ли у вас специальные права доступа *SECADM и *ALLOBJ?	Да

Для выполнения задач настройки и реализации рассматриваемого сценария необходима следующая информация о применяемых цифровых сертификатах:

Таблица 4. Форма параметров сертификатов

Форма планирования для сервера iSeries A	**Ответы**
Будете ли вы использовать локальную сертификатную компанию или применять сертификаты общественной CA?	Локальная CA для выдачи сертификатов
Находятся ли на сервере iSeries A приложения, для которых необходимо включить поддержку SSL?	Да

Таблица 4. Форма параметров сертификатов (продолжение)

Форма планирования для сервера iSeries A	**Ответы**
Какое отличительное имя будет использоваться при создании локальной сертификатной компании? • **Размер ключа**: определяет уровень ключей шифрования сертификата. • **Имя сертификатной компании (CA)**: служит для идентификации CA и является именем сертификата CA и отличительным именем выдающей организации для сертификатов данной CA. • **Отдел организации**: организационное подразделение или часть приложения, применяющего данный сертификат. • **Название организации**: название компании или ее подразделения, в котором применяется приложение, использующее данный сертификат. • **Город**: город или район, в котором расположена организация. • **Область или район**: область или край, в котором будет применяться данный сертификат. • **Страна или регион**: двухсимвольный идентификатор страны или региона, в котором применяется данный сертификат. • **Период действия сертификатной компании**: срок, в течение которого действительны сертификаты сертификатной компании.	**Длина ключа**: 1024**Сертификатная компания**: Myco_CA@myco.com**Подразделение**: Rate dept**Организация**: myco**Адрес или город**: Любой-город**Область или район**: Любые**Страна или регион**: ZZ**Срок годности сертификатной компании**: 1095
Нужно ли в стратегии локальной сертификатной компании разрешить выдачу пользовательских сертификатов для идентификации клиентов?	Да
Какое отличительное имя будет использоваться при создании сертификата сервера локальной сертификатной компании? • **Размер ключа**: определяет уровень ключей шифрования сертификата. • **Метка сертификата**: служит идентификатором сертификата с уникальным набором параметров. • **Общее имя**: идентифицирует владельца сертификата, например, человека, объект или приложение; входит в полное имя (DN) субъекта сертификата. • **Отдел организации**: организационное подразделение или часть приложения, применяющего данный сертификат. • **Название организации**: название компании или ее подразделения, в котором применяется приложение, использующее данный сертификат. • **Город**: город или район, в котором расположена организация. • **Область или район**: область или край, в котором будет применяться данный сертификат. • **Страна или регион**: двухсимвольный идентификатор страны или региона, в котором применяется данный сертификат.	**Длина ключа**: 1024**Метка сертификата**: Myco_public_cert**Общее имя**: myco_rate_server@myco.com**Подразделение**: Rate dept**Организация**: организация**Адрес или город**: любой-город**Область или район**: Любые**Страна или регион**: ZZ
Каков в DCM ИД приложения, которое необходимо настроить для работы с SSL?	mcyo_agent_rate_app

Таблица 4. Форма параметров сертификатов (продолжение)

Форма планирования для сервера iSeries A	Ответы
Будет ли в приложениях с поддержкой SSL выполняться идентификация клиентов с помощью сертификатов? Если да, то какие сертификатные компании необходимо добавить в список уполномоченных CA приложения?	ДаMyco_CA@myco.com

Настройка поддержки SSL на сервере HTTP отдела кадров

Для настройки SSL на сервере HTTP отдела кадров (на основе Apache), установленном на сервере iSeries A, необходимо выполнить набор задач, который зависит от текущей конфигурации вашего сервера.

Для настройки SSL на сервере выполните следующие действия:

1. Запустите интерфейс администрирования сервера HTTP.
2. Для работы с нужным сервером HTTP выберите вкладки **Управление —> Все серверы —> Все серверы HTTP**. Будет показан список всех настроенных серверов HTTP.
3. Выберите нужный сервер из списка и нажмите **Параметры управления**.
4. В окне навигации выберите **Защита**.
5. Выберите вкладку **Идентификация SSL с помощью сертификатов**.
6. В поле **SSL** укажите значение Включено.
7. В поле **Имя приложения сертификата сервера** укажите ИД приложения для данного экземпляра сервера.Это имя можно также выбрать из списка. ИД приложения можно задать в форме QIBM_HTTP_SERVER_[имя_сервера], например, QIBM_HTTP_SERVER_MYCOTEST.**Примечание:** Запишите этот ИД приложения.Его необходимо будет еще раз указать в DCM.

Дополнительная информация обо всех параметрах настройки SSL на сервере HTTP приведена в разделе HTTP Server для iSeries справочной системы, в частности, в примере Сценарий: Применение SSL для защиты сервера HTTP (на основе Apache) компании JKL. В этом сценарии, относящемся к серверу HTTP, приведены инструкции по созданию виртуального хоста и настройки на нем поддержки SSL, в том числе:

1. Настройка виртуального хоста на основе имен.
2. Настройка директивы обработки для виртуального хоста.
3. Настройка каталогов виртуального хоста.
4. Настройка простой идентификации с помощью паролей.
5. Включение SSL для виртуального хоста

Дополнительная информация о настойке текущей и будущих версий сервера iSeries приведена в разделе HTTP Server для iSeries.

После завершения настройки SSL на сервере HTTP можно с помощью DCM настроить поддержку сертификатов, необходимую для идентификации клиентов и соединений SSL.

Создание и управление локальной сертификатной компанией (CA)

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: Убедитесь в том, что ИД приложения сервера HTTP отдела кадров, например, `QIBM_HTTP_SERVER_MYCOTEST`, выбран в качестве одного из приложений, принимающего сертификаты локальной CA.

После завершения настройки сертификата, необходимой для применения SSL в приложениях Web-сервера, можно настроить на Web-сервере идентификацию пользователей с помощью сертификатов.

Настройка идентификации клиентов на Web-сервере отдела кадров

В процессе настройки идентификации с помощью сертификатов на сервере HTTP необходимо задать общие параметры идентификации сервера HTTP. Это можно сделать с помощью той же формы защиты, в которой задаются параметры SSL на сервере.

Для настройки идентификации клиентов на сервере с помощью сертификатов выполните следующие действия:

1. Запустите интерфейс администрирования сервера HTTP.
2. Откройте в браузере страницу задач i5/OS, введя следующий URL: http://имя_системы:2001.
3. Выберите **Web-администрация IBM дляi5/OS**.
4. Для работы с нужным сервером HTTP выберите вкладки **Управление → Все серверы → Все серверы HTTP**. Будет показан список всех настроенных серверов HTTP.
5. Выберите нужный сервер из списка и нажмите **Параметры управления**.
6. В окне навигации выберите **Защита**.
7. Выберите вкладку **Идентификация**.
8. Выберите значение **Применить клиентский профайл i5/OS**.
9. В поле **Область или имя идентификации** укажите имя области идентификации.
10. Установите значение Включено в поле **Обработка запросов на основе прав доступа клиента** и нажмите **Применить**.
11. Выберите вкладку **Управление доступом**.
12. Выберите значение **Все идентифицированные пользователи (указавшие правильное имя и пароль)** и нажмите кнопку **Применить**.
13. Выберите вкладку **Идентификация SSL с помощью сертификатов**.
14. Убедитесь, что в поле **SSL** выбрано значение Включено.
15. Убедитесь, что в поле **Имя сертификата приложения сервера** задано правильное значение, например, QIBM_HTTP_SERVER_MYCOTEST.
16. Выберите значение **Принимать доступные клиентские сертификаты перед созданием соединения**.Нажмите кнопку **OK**.

Дополнительная информация обо всех параметрах настройки SSL на сервере HTTP приведена в разделе HTTP Server для iSeries справочной системы, в частности, в примере Сценарий: Применение SSL для защиты сервера HTTP (на основе Apache) компании JKL. В этом сценарии описаны все действия, необходимые для создания виртуального хоста и настройки на нем поддержки SSL.

После завершения настройки идентификации клиентов можно перезапустить сервер HTTP в режиме SSL, обеспечивающем надежную защиту данных приложения отдела кадров.

Запуск Web-сервера 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 (на основе Apache) выполните следующие действия:

1. В iSeries Navigator разверните вашу систему.
2. Разверните **Сеть → Серверы → TCP/IP → Управление HTTP** .
3. Нажмите кнопку **Запустить** для запуска интерфейса администрирования сервера HTTP.
4. Выберите вкладку **Управление**, чтобы просмотреть список всех настроенных серверов HTTP.
5. Выберите нужный сервер из списка и нажмите кнопку **Остановить**, если сервер запущен.
6. Нажмите кнопку **Запустить**, чтобы перезапустить сервер. Дополнительная информация о параметрах запуска приведена в электронной справке.

Для того чтобы пользователи могли работать с Web-приложением отдела кадров, им необходимо установить в браузере копию сертификата локальной сертификатной компании.

Информация, связанная с данной

Обзор Information Center по серверу HTTP

Оповестите пользователей о том, что в браузере необходимо установить копию сертификата локальной CA

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 Web-серверами, которые применяют сертификат, полученный от данной сертификатной компании. Браузер выдаст последовательность окон с инструкциями по установке сертификата.
4. Нажмите кнопку **OK** для возврата к главному окну Диспетчера цифровых сертификатов.

Теперь, поскольку пользователи могут работать с Web-сервером отдела кадров в режиме SSL, им необходим соответствующий сертификат для идентификации на сервере. Следовательно, им необходимо получить пользовательский сертификат локальной сертификатной компании.

Предложение пользователям получить сертификаты 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.

После выполнения этих задач обращаться к данным Web-сервера отдела кадров смогут только пользователи с действительными сертификатами и соответствующими правами доступа, а все данные, передаваемые во время сеансов связи, будут защищены с помощью протокола SSL.

Планирование работы с DCM

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

Перечитайте этот раздел, чтобы убедиться, что вы обеспечили все опции, необходимые для установки Диспетчера цифровых сертификатов (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 компонент 34 операционной системы i5/OS. Это DCM с интерфейсом браузера.
- Установить IBM HTTP Server for i5/OS (5722–DG1) и запустить административный экземпляр сервера.
- Убедиться, что в системе настроен протокол TCP, что позволяет работать с DCM с помощью Web-браузера и административного экземпляра 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.

Особенности резервного копирования и восстановления данных DCM

В этом разделе приведена информация о резервном копировании и восстановлении важных данных DCM.

Пароли для базы данных зашифрованных ключей, служащие для работы с хранилищами сертификатов Диспетчера цифровых сертификатов (DCM), хранятся (*спрятаны*) в специальном файле защиты в системе. При создании хранилища сертификатов с помощью DCM последний автоматически сохраняет пароль в этом файле. Тем не менее, в некоторых случаях необходимо вручную проверять, был ли сохранен пароль.

В качестве примера можно привести создание с помощью DCM сертификата для другой системы **iSeries** в случае, когда файлы сертификатов применяются в новой системе для создания нового хранилища сертификатов. В этом случае необходимо открыть новое хранилище сертификатов и с помощью задачи **Изменить пароль** изменить пароль хранилища сертификатов в целевой системе, что обеспечит надежное сохранение нового пароля в DCM. Если в качестве хранилища сертификатов выбрано значение Хранилище сертификатов в другой системе, то необходимо также указать, что после смены пароля нужно применять

опция **Автоматический вход в систему**. Дополнительная информация о создании сертификатов для других систем iSeries с помощью DCM приведена в разделе Создание сертификатов для других систем iSeries с помощью локальной сертификатной компании (CA).

Кроме того, при изменении и сбросе пароля хранилища сертификатов в другой системе необходимо указать опцию **Автоматический вход в систему**.

Для создания резервных копий всех важных данных DCM выполните следующие действия:

- С помощью команды сохранения (SAV) сохраните все файлы `.KDB` и `.RDB`.Каждое хранилище сертификатов DCM состоит из двух файлов, первый из которых имеет расширение `.KDB` , а второй - `.RDB`.
- С помощью команд сохранения системы (SAVSYS) и данных защиты (SAVSECDTA) сохраните файл защиты паролей, который содержит основные пароли базы данных для доступа к хранилищу сертификатов. Восстановить файл защиты паролей DCM можно с помощью команды восстановления пользовательских профайлов (RSTUSRPRF), указав значение `*ALL` для параметра пользовательских профайлов (USRPRF).

Кроме того, необходимо помнить, что при применении команды SAVSECDTA текущие пароли хранилища сертификатов могут отличаться от паролей в сохраненном файле защиты паролей DCM. Если пароль хранилища сертификатов изменяется после операции SAVSECDTA, но до восстановления данных, сохраненных с помощью этой операции, то текущий пароль хранилища сертификатов будет отличаться от восстановленного.

Для того чтобы избежать такой ситуации, необходимо с помощью задачи **Изменить пароль** (в разделе **Управление хранилищем сертификатов** в окне навигации) DCM изменить пароли хранилища сертификатов после восстановления данных с помощью команды SAVSECDTA. Это позволит вновь синхронизировать пароли.Обратите внимание на то, что в этой ситуации не рекомендуется пользоваться кнопкой **Сбросить пароль**, которая появляется на экране при выборе открываемого хранилища сертификатов.При попытке сброса пароля DCM попытается получить пароль, сохраненный в файле защиты. Если этот пароль отличается от текущего, то при сбросе пароля произойдет ошибка. Если пароли хранилища сертификатов изменяются редко, то при каждом изменении можно с помощью команды SAVSECDTA сохранять текущий пароль в файле защиты, благодаря чему резервная копия всегда будет содержать правильный пароль.

Задачи, связанные с данной

“Выдача сертификатов для других систем iSeries с помощью локальной сертификатной компании” на стр. 58

Ознакомьтесь с этой информацией о применении частной локальной сертификатной компании для выдачи сертификатов для других систем iSeries.

Типы цифровых сертификатов

В этом разделе описаны различные типы цифровых сертификатов и работа с ними в Диспетчере цифровых сертификатов (DCM).

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. Локальная CA, которая была создана с помощью Диспетчера цифровых сертификатов (DCM), и управление которой осуществляется с помощью DCM, является независимым объектом. 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 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 в соответствии с классификацией.

Примечание: Если в системе установлен шифровальный сопроцессор IBM, то вы можете воспользоваться дополнительными возможностями хранения личных ключей сертификатов (за исключением сертификатов подписания объектов). В частности, личные ключи можно хранить в памяти сопроцессора. 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.

Понятия, связанные с данным

“Secure Sockets Layer (SSL)” на стр. 10
Протокол Secure Sockets Layer (SSL), разработанный фирмой Netscape, является стандартным средством шифрования данных в соединениях между клиентом и сервером.

“Хранилища сертификатов” на стр. 7
Хранилище сертификатов - это специальный файл базы данных, в котором Диспетчер цифровых сертификатов (DCM) хранит цифровые сертификаты.

Сравнение общих и частных сертификатов

В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

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.Как только вы решили, какой тип сертификатной компании будет выдавать сертификаты, нужно выбрать тип реализации сертификатов, которые лучше всего соответствует вашим требованиям к безопасности. Возможны следующие варианты получения сертификатов:

- Приобретение сертификатов у общественной сертификатной компании (CA) Internet.
- Создание собственной локальной сертификатной компании и выдача частных сертификатов локальным пользователям с ее помощью.
- Применение как сертификатов общественной CA, так и сертификатов частной локальной 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 локальной сертификатной компанией.

Применение частных сертификатов

Локальная CA предназначена для выдачи сертификатов ограниченному кругу пользователей, например сотрудникам данной фирмы. Создав собственную локальную 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).

При выдаче пользователям сертификатов локальной CA для идентификации в клиентских системах и приложениях необходимо определить хранилище пользовательских сертификатов. Когда пользователи получают сертификаты локальной CA с помощью DCM, эти сертификаты по умолчанию хранятся вместе с пользовательскими профайлами. Тем не менее, настроив соответствующим образом DCM и EIM, можно использовать в качестве хранилища сертификатов каталог простого протокола доступа к каталогам (LDAP). Если вы не хотите связывать сертификаты с пользовательскими профайлами и хранить их вместе, то вы сможете выдавать сертификаты пользователям других систем с помощью API.

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. Администратор задает уровень надежности сертификатов CA в соответствующем хранилище DCM, которое содержит копии сертификатов большинства известных общественных CA. Однако если сертификат CA отсутствует в хранилище сертификатов, то для того чтобы сервер принимал сертификаты пользователей и клиентов, выданные этой CA, необходимо получить и импортировать копию сертификата этой компании. Сертификат CA должен находиться в файле правильного формата и его необходимо добавить 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 частных сертификатов с помощью локальной 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.

Понятия, связанные с данным

“Управление сертификатами, полученными от общественной сертификатной компании” на стр. 49
В этом разделе описано управление сертификатами, полученными от сертификатной компании из Internet путем создания хранилища сертификатов.

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

“Первая настройка сертификатов” на стр. 40
В этом разделе приведена информация о работе с сертификатами общественных сертификатных компаний Internet (CA) и создании частной локальной сертификатной компании и выдаче сертификатов с ее помощью.

“Цифровые сертификаты подписи объектов” на стр. 37
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

Задачи, связанные с данной

“Цифровые сертификаты и технология преобразования идентификаторов в рамках предприятия (EIM)” на стр. 35
Совместное использование EIM и DCM позволяет применять сертификат в качестве источника данных

для операции преобразования EIM, которая преобразует сертификаты в целевой идентификатор пользователя, связанный с тем же идентификатором EIM.

“Создание пользовательского сертификата” на стр. 44
В этом разделе приведена информация о том, как с помощью локальной сертификатной компании пользователи могут создать сертификаты для идентификации клиента.

“Создание и управление локальной сертификатной компанией (CA)” на стр. 41
В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

“Выдача сертификатов для других систем iSeries с помощью локальной сертификатной компании” на стр. 58
Ознакомьтесь с этой информацией о применении частной локальной сертификатной компании для выдачи сертификатов для других систем iSeries.

Ссылки, связанные с данной

“Выдача сертификатов пользователям других систем с помощью API” на стр. 47
В этом разделе приведена информация о том, как с помощью локальной сертификатной компании можно выдавать частные сертификаты пользователям, не связывая эти сертификаты с пользовательскими профайлами iSeries.

Применение цифровых сертификатов в защищенных соединениях SSL

Здесь приведена информация о том, как приложения могут с помощью цифровых сертификатов устанавливать защищенные соединения.

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.

Понятия, связанные с данным

“Применение цифровых сертификатов для идентификации пользователей” на стр. 34
В этом разделе приведена информация о том, как с помощью цифровых сертификатов можно усовершенствовать процедуру идентификации пользователей, запрашивающих ресурсы сервера iSeries.

Применение цифровых сертификатов для идентификации пользователей

В этом разделе приведена информация о том, как с помощью цифровых сертификатов можно усовершенствовать процедуру идентификации пользователей, запрашивающих ресурсы сервера iSeries.

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 или другим идентификатором пользователя iSeries. В этом случае у сертификата будут те же права доступа, что и у связанного с ним пользовательского профайла. Кроме того, 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 или другие пользовательские идентификаторы.

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 предоставляют следующие приложения iSeries:

- Сервер Telnet
- IBM HTTP Server for i5/OS (на основе Apache)
- Сервер каталогов IBM Directory Server
- iSeries Access for Windows (включая Навигатор iSeries Navigator)
- 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 идентификации клиентов с помощью сертификатов во время сеансов SSL в серверных приложениях iSeries приведена в разделе Secure Sockets Layer (SSL) справочной системы iSeries Information Center.

Понятия, связанные с данным

“Применение цифровых сертификатов в защищенных соединениях SSL” на стр. 33
Здесь приведена информация о том, как приложения могут с помощью цифровых сертификатов устанавливать защищенные соединения.

Ссылки, связанные с данной

“Выдача сертификатов пользователям других систем с помощью API” на стр. 47
В этом разделе приведена информация о том, как с помощью локальной сертификатной компании можно выдавать частные сертификаты пользователям, не связывая эти сертификаты с пользовательскими профайлами iSeries.

Цифровые сертификаты и технология преобразования идентификаторов в рамках предприятия (EIM)

Совместное использование EIM и DCM позволяет применять сертификат в качестве источника данных для операции преобразования EIM, которая преобразует сертификаты в целевой идентификатор пользователя, связанный с тем же идентификатором EIM.

EIM - это технология 

, позволяющая администраторам корпоративных сетей управлять идентификаторами пользователей, в том числе пользовательскими профайлами и сертификатами. Чаще всего в роли идентификатора пользователя выступают имя пользователя и пароль; идентификатором также может служить сертификат. Для некоторых приложений предпочтительной формой идентификации пользователей является сертификат, а не имя пользователя и пароль.

EIM позволяет создавать связи между разными идентификаторами одного и того же пользователя, благодаря чему пользователь может однократно выполнить идентификацию и работать с любыми приложениями, поддерживающими другие типы идентификации. Для этого в EIM создаются связи между различными идентификаторами пользователей. Идентификаторами могут служить разные объекты, в том числе пользовательские сертификаты. Вы можете создавать отдельные связи между идентификатором EIM и другими объектами, идентифицирующими пользователя. Можно также создать связи стратегий, определяющие соответствие между группами пользовательских идентификаторов и одним целевым идентификатором. Идентификаторами могут служить разные объекты, в том числе пользовательские сертификаты. При создании этих связей пользовательские сертификаты можно связать с соответствующими идентификаторами EIM, что позволит упростить идентификацию с помощью сертификатов.

Для применения данной функции управления пользовательскими сертификатами EIM перед настройкой DCM необходимо выполнить следующие задачи настройки EIM:

1. Настройте EIM с помощью мастера **Настройка EIM** в программе **Навигатор iSeries**.
2. Для каждого пользователя EIM необходимо создать идентификатор EIM.
3. Создайте целевую связь между каждым идентификатором EIM и пользовательским профайлом в локальном реестре пользователей i5/OS. После этого все сертификаты, которые пользователь присвоит или создаст с помощью DCM, будут связываться с его пользовательским профайлом. В качестве имени локального реестра пользователей **i5/OS** укажите имя определения реестра EIM, заданное с помощью мастера **Настройка EIM**.

После настройки EIM необходимо с помощью задачи **Управление каталогом LDAP** изменить конфигурацию DCM, выбрав в качестве хранилища пользовательских сертификатов каталог простого протокола доступа к каталогам (LDAP), а не пользовательский профайл.При настройке совместной работы EIM и DCM задачи **Создать сертификат** для пользовательских сертификатов и **Присвоить пользовательский сертификат** служат для подготовки сертификатов к работе с EIM, а не для присвоения сертификатов пользовательскому профайлу. DCM хранит сертификат в настроенном каталоге LDAP и создает исходные связи для соответствующих идентификаторов EIM с помощью отличительного имени (DN) сертификата. Это позволяет операционным системам и приложениям использовать сертификат в качестве источника данных для операции преобразования EIM, которая преобразует сертификаты в целевой идентификатор пользователя, связанный с тем же идентификатором EIM.

Кроме того, при настройке совместной работы EIM и DCM с помощью DCM можно проверить срок действия пользовательского сертификата не только на уровне системы, но и на уровне предприятия.

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

Задачи, связанные с данной

“Управление пользовательскими сертификатами с помощью сроков действия” на стр. 46
Диспетчер цифровых сертификатов (DCM) содержит функции управления сроками действия сертификатов, позволяющие проверять даты окончания срока действия пользовательских сертификатов в локальной системе iSeries. Эти функции можно использовать совместно с технологией Преобразование идентификаторов в рамках предприятия (EIM), что позволит администраторам проверять даты окончания срока действия пользовательских сертификатов на уровне предприятия.

“Управление каталогом LDAP для пользовательских сертификатов” на стр. 75
В этом разделе приведена информация о настройке DCM для хранения пользовательских сертификатов в каталоге LDAP. Такая конфигурация позволяет службе преобразования идентификаторов в рамках предприятия (EIM) работать с пользовательскими сертификатами.

Информация, связанная с данной

Раздел EIM Information Center

Применение цифровых сертификатов в соединениях VPN

Здесь приведена информация о применении цифровых сертификатов в настройке соединений VPN.

С помощью цифровых сертификатов можно устанавливать соединения виртуальной частной сети 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.

Один из способов идентификации серверов IKE основан на применении подготовленного общего ключа. Тем не менее, этот способ отличается пониженным уровнем защиты, поскольку этот ключ нужно передать из рук в руки администратору другой конечной точки 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 частные 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 при выдаче сертификата с помощью локальной сертификатной компании в DCM. Наличие альтернативной информации гарантирует совместимость данного соединения VPN 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).

Информация, связанная с данной

Настройка соединения 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.

IBM i5/OS поддерживает добавление цифровых подписей к объектам с помощью сертификатов. Добавление цифровой подписи к объекту позволяет контролировать целостность его содержимого и подлинность его источника. Поддержка цифровых подписей повышает эффективность традиционных для iSeries средств контроля за доступом к объектам. 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 либо общие, либо частные сертификаты. 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, можно с помощью Диспетчера цифровых сертификатов (DCM). Кроме того, подписывать объекты и проверять цифровые подписи можно с помощью Диспетчера цифровых сертификатов (DCM).

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

“Применение цифровых сертификатов проверки подписей объектов”
В этом разделе приведены сведения о том, как с помощью цифровых сертификатов можно убедиться в подлинности объектов путем проверки их цифровых подписей.

Задачи, связанные с данной

“Проверка подписей объектов” на стр. 78
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.

“Управление общими сертификатами Internet для подписания объектов” на стр. 52
Диспетчер цифровых сертификатов (DCM) позволяет добавлять цифровые подписи к объектам с помощью общих сертификатов Internet.

“Управление сертификатами проверки подписей объектов” на стр. 54
Диспетчер цифровых сертификатов (DCM) позволяет управлять сертификатами проверки подписей, применяемыми для проверки цифровых подписей объектов.

Применение цифровых сертификатов проверки подписей объектов

В этом разделе приведены сведения о том, как с помощью цифровых сертификатов можно убедиться в подлинности объектов путем проверки их цифровых подписей.

IBM i5/OS поддерживает проверку цифровых подписей объектов с помощью сертификатов. 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 интегрированной файловой системы. Дополнительная информация об этом и других системных значениях приведена в разделе Поиск системных значений в iSeries Information Center.

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). Кроме того, подписывать объекты и проверять цифровые подписи можно с помощью Диспетчера цифровых сертификатов (DCM).

Понятия, связанные с данным

“Цифровые сертификаты подписи объектов” на стр. 37
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

Информация, связанная с данной

Поиск системных значений

Настройка DCM

Здесь содержится информация о действиях по настройке, которые необходимо выполнить для управления сертификатами и их ключами с помощью 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 i5/OS. 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:

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. Эта библиотека приведена в разделе VeriSign Help Desk .

Запуск Диспетчера цифровых сертификатов

Содержит информацию о запуске функции Диспетчер цифровых сертификатов (DCM) в системе сервере.

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).
2. Установите продукт 5722 DG1. Это IBM HTTP Server for i5/OS.
3. С помощью iSeries Navigator запустите административный экземпляр сервера HTTP:
   a. Запустите **iSeries Navigator** .
   b. Щелкните дважды на значке своей системы в главном окне иерархического списка.
   c. Разверните **Сеть > Серверы > TCP/IP**.
   d. Дважды щелкните на **Управление HTTP**.
   e. Нажмите кнопку **Запустить**.
4. Запустите Web-браузер.
5. Откройте в браузере страницу задач iSeries, введя следующий URL: http://*имя_системы*:2001.
6. Для того чтобы начать работу с DCM, в списке продуктов на странице задач iSeries выберите **Диспетчер цифровых сертификатов**.

Понятия, связанные с данным

“Сценарий: Внешняя идентификация с помощью сертификатов” на стр. 12
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.

Первая настройка сертификатов

В этом разделе приведена информация о работе с сертификатами общественных сертификатных компаний Internet (CA) и создании частной локальной сертификатной компании и выдаче сертификатов с ее помощью.

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. Для проверки подписей объектов с помощью DCM у пользовательского профайла должны быть специальные права доступа *AUDIT.

При первом запуске Диспетчера цифровых сертификатов (DCM) хранилища сертификатов еще не созданы. В связи с этим при первом запуске DCM в панели навигации будут показаны только перечисленные ниже задачи и только при наличии у вас необходимых специальных прав доступа:

- Управление сертификатами пользователей.
- Создание хранилища сертификатов.
- Создание сертификатной компании (CA). (Примечание: После создания частной сертификатной компании эта задача будет удалена из списка.)
- Управление определениями CRL.
- Управление каталогом LDAP.
- Управление определениями запросов PKIX.

- Возврат к разделу Задачи iSeries.

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. Показанные задачи и категории зависят от открытого хранилища сертификатов (если оно есть) и от специальных прав доступа пользовательского профайла.

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 for i5/OS 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.

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

Создание и управление локальной сертификатной компанией (CA)

В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

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 сервером IBM HTTP Server for i5/OS, 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 (?) 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. Выбрать способ хранения личного ключа сертификата локальной CA. (Этот шаг выполняется только в том случае, если на сервере IBM установлен шифровальный сопроцессор. 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 полномочия локальной CA.
   e. С помощью новой локальной сертификатной компании создать сертификат клиента или сервера, с помощью которого приложения будут устанавливать соединения SSL. (Если на сервере IBM установлен шифровальный сопроцессор, 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. 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.
   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 согласования SSL проверить идентификационные данные 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:

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

“Управление пользовательскими сертификатами”
Диспетчер цифровых сертификатов (DCM) позволяет получать сертификаты с помощью SSL или связывать существующие сертификаты с их пользовательскими профайлами iSeries.

Задачи, связанные с данной

“Выдача сертификатов для других систем iSeries с помощью локальной сертификатной компании” на стр. 58
Ознакомьтесь с этой информацией о применении частной локальной сертификатной компании для выдачи сертификатов для других систем iSeries.

“Получение копии сертификата частной сертификатной компании” на стр. 48
В этом разделе приведена информация о получении копии сертификата частной сертификатной компании и его установке на персональном компьютере с целью идентификации выданных этой сертификатной компанией сертификатов серверов.

Ссылки, связанные с данной

“Выдача сертификатов пользователям других систем с помощью API” на стр. 47
В этом разделе приведена информация о том, как с помощью локальной сертификатной компании можно выдавать частные сертификаты пользователям, не связывая эти сертификаты с пользовательскими профайлами iSeries.

Управление пользовательскими сертификатами:

Диспетчер цифровых сертификатов (DCM) позволяет получать сертификаты с помощью SSL или связывать существующие сертификаты с их пользовательскими профайлами iSeries.

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:

Задачи, связанные с данной

“Создание и управление локальной сертификатной компанией (CA)” на стр. 41
В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

“Получение копии сертификата частной сертификатной компании” на стр. 48
В этом разделе приведена информация о получении копии сертификата частной сертификатной компании и его установке на персональном компьютере с целью идентификации выданных этой сертификатной компанией сертификатов серверов.

Создание пользовательского сертификата:

В этом разделе приведена информация о том, как с помощью локальной сертификатной компании пользователи могут создать сертификаты для идентификации клиента.

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 (**?**)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.

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.

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

Задачи, связанные с данной

“Присвоение пользовательского сертификата”
Можно связать принадлежащий вам сертификат с пользовательским профайлом i5/OS или с идентификатором пользователя. Это может быть сертификат, полученный от частной локальной сертификатной компании из другой системы или от общеизвестной сертификатной компании, действующей в сети Internet. Для того чтобы идентификатору пользователя можно было присвоить сертификат, выдающая его CA должна являться уполномоченной CA на сервере, и сертификат не должен быть связан с пользовательским профайлом или с другим идентификатором пользователя в системе.

“Получение копии сертификата частной сертификатной компании” на стр. 48
В этом разделе приведена информация о получении копии сертификата частной сертификатной компании и его установке на персональном компьютере с целью идентификации выданных этой сертификатной компанией сертификатов серверов.

Присвоение пользовательского сертификата:

Можно связать принадлежащий вам сертификат с пользовательским профайлом i5/OS или с идентификатором пользователя. Это может быть сертификат, полученный от частной локальной сертификатной компании из другой системы или от общеизвестной сертификатной компании, действующей в сети Internet. Для того чтобы идентификатору пользователя можно было присвоить сертификат, выдающая его CA должна являться уполномоченной CA на сервере, и сертификат не должен быть связан с пользовательским профайлом или с другим идентификатором пользователя в системе.

У некоторых пользователей могут быть сертификаты общественных сертификатных компаний (CA) или локальных CA других систем iSeries. Системный администратор должен сделать такие сертификаты доступными для Диспетчера цифровых сертификатов (DCM). В этом случае пользователи смогут работать со своими сертификатами с помощью DCM. С помощью задачи **Присвоить пользовательский сертификат** пользователь может создать связь DCM для сертификата, полученного от общественной CA.

В случае, когда пользователь присваивает сертификат общественной CA, DCM может обрабатывать такой сертификат двумя способами:

- Хранение сертификата в локальной системе iSeries вместе с пользовательским профайлом пользователя. Если для DCM не определен каталог LDAP, то с помощью задачи **Присвоить пользовательский сертификат** пользователь может присвоить сертификат общественной CA пользовательскому профайлу i5/OS. В этом случае сертификат можно использовать для идентификации клиентов в приложениях системы, поддерживающих такой алгоритм идентификации.
- Хранение сертификата в каталоге LDAP и его применение с технологией преобразования данных в рамках предприятия (EIM). Если в системе iSeries определен каталог LDAP и конфигурация системы поддерживает EIM, то с помощью задачи **Присвоить пользовательский сертификат** пользователь может сохранить копию сертификата общественной CA в указанном каталоге LDAP. Кроме того, DCM создает для сертификата исходную связь EIM. Такой способ хранения сертификата позволяет администратору EIM применять сертификат в качестве допустимого идентификатора пользователя, поддерживаемого EIM.

  Примечание: Для того чтобы пользователь мог присвоить идентификатору EIM сертификат, необходимо правильно настроить EIM для этого пользователя. Для этого необходимо создать идентификатор пользователя EIM и создать целевую связь между этим идентификатором

EIM и пользовательским профайлом. В противном случае DCM не сможет создать для сертификата соответствующую исходную связь с идентификатором EIM.

Для работы с задачей **Присвоить пользовательский сертификат** необходимо:

1. Защищенное соединение с сервером HTTP, с помощью которого выполняется обращение к DCM.

   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 выборе этой задачи на экране появляется новое окно браузера. Если защищенный сеанс не начат, то Диспетчер цифровых сертификатов предложит запустить его с помощью 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.
2. Предоставить 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.
3. Наличие в браузере сертификата, не присвоенного идентификатору пользователя, запустившего задачу. (Либо, если DCM работает с EIM, в браузере у пользователя должен быть сертификат, не хранящийся в каталоге LDAP для DCM.)

   После запуска защищенного сеанса DCM попытается получить сертификат от браузера, чтобы связать его с вашим ИД пользователя. 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 ИД пользователя. Это может быть связано с одной из неполадок пользовательского сертификата. Например, сертификат полученный от браузера, может быть уже связан с вашим ИД пользователя.

   Задачи, связанные с данной

   “Создание пользовательского сертификата” на стр. 44
   В этом разделе приведена информация о том, как с помощью локальной сертификатной компании пользователи могут создать сертификаты для идентификации клиента.

   “Устранение неполадок, возникших при регистрации пользовательского сертификата” на стр. 85

   Информация, связанная с данной

   Обзор EIM Information Center

Управление пользовательскими сертификатами с помощью сроков действия:

Диспетчер цифровых сертификатов (DCM) содержит функции управления сроками действия сертификатов, позволяющие проверять даты окончания срока действия пользовательских сертификатов в локальной системе iSeries. Эти функции можно использовать совместно с технологией Преобразование идентификаторов в рамках предприятия (EIM), что позволит администраторам проверять даты окончания срока действия пользовательских сертификатов на уровне предприятия.

Для работы с функциями управления пользовательскими сертификатами с помощью сроков действия на уровне предприятия необходимо настроить в сети предприятия функцию EIM, которая должна содержать информацию о преобразовании для пользовательских сертификатов. Для проверки срока действия пользовательских сертификатов, не связанных с вашим пользовательским профайлом необходимы специальные права доступа *ALLOBJ и *SECADM.

Просмотр сертификатов с помощью DCM в зависимости от срока действия позволяет быстро и просто определить сертификаты, срок действия которых близок к завершению, и своевременно обновить такие сертификаты.

Для просмотра и управления сертификатами с помощью сроков действия выполните следующие операции:

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 выберите категорию **Управление сертификатами пользователей** для просмотра списка задач.

   Примечание: Если вы уже работаете с хранилищем сертификатов, выберите **Управление сертификатами** для просмотра списка задач, после этого выберите пункты **Проверить сроки действия** и **Пользователь**.

3. Если у вашего пользовательского профайла есть специальные права доступа *ALLOBJ и *SECADM, то вы можете задать способ выбора сертификатов для просмотра и управления с помощью сроков действия. (Если у вашего профайла нет этих специальных прав доступа, то DCM предложит вам указать диапазон дат окончания срока действия, как описано ниже.) Вы можете выбрать любую из следующих опций:
   - **Пользовательский профайл** - для просмотра и управления пользовательскими сертификатами, присвоенными определенному пользовательскому профайлу i5/OS. Задайте **Имя пользовательского профайла** и нажмите кнопку **Продолжить**.

     Примечание: Задать имя, отличающееся от имени вашего пользовательского профайла, можно только в том случае, если у вас есть специальные права доступа *ALLOBJ и *SECADM.
   - **Все пользовательские сертификаты** - для просмотра и управления пользовательскими сертификатами для всех идентификаторов пользователей.

4. В поле **Диапазон сроков окончания действия (1-365)** укажите срок окончания действия сертификатов для просмотра и нажмите **Продолжить**.В окне DCM будут показаны все сертификаты пользовательского профайла, срок действия которых истекает в течение указанного количества дней. В окне DCM будут также показаны все пользовательские сертификаты, срок действия которых уже истек.
5. Выберите пользовательский сертификат, с которым нужно выполнить какую-либо операцию. Вы можете как просмотреть подробные сведения о сертификате, так и удалить данные о сертификате из связанного пользовательского профайла.
6. После окончания работы с сертификатами нажмите кнопку **Отмена** для завершения работы с задачей.

Задачи, связанные с данной

“Цифровые сертификаты и технология преобразования идентификаторов в рамках предприятия (EIM)” на стр. 35
Совместное использование EIM и DCM позволяет применять сертификат в качестве источника данных для операции преобразования EIM, которая преобразует сертификаты в целевой идентификатор пользователя, связанный с тем же идентификатором EIM.

Информация, связанная с данной

Обзор EIM Information Center

Выдача сертификатов пользователям других систем с помощью API:

В этом разделе приведена информация о том, как с помощью локальной сертификатной компании можно выдавать частные сертификаты пользователям, не связывая эти сертификаты с пользовательскими профайлами iSeries.

Начиная с i5/OS 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).

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

“Применение цифровых сертификатов для идентификации пользователей” на стр. 34
В этом разделе приведена информация о том, как с помощью цифровых сертификатов можно усовершенствовать процедуру идентификации пользователей, запрашивающих ресурсы сервера iSeries.

Задачи, связанные с данной

“Создание и управление локальной сертификатной компанией (CA)” на стр. 41
В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

Получение копии сертификата частной сертификатной компании:

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

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.

Понятия, связанные с данным

“Управление пользовательскими сертификатами” на стр. 43
Диспетчер цифровых сертификатов (DCM) позволяет получать сертификаты с помощью SSL или связывать существующие сертификаты с их пользовательскими профайлами iSeries.

Задачи, связанные с данной

“Создание и управление локальной сертификатной компанией (CA)” на стр. 41
В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

“Создание пользовательского сертификата” на стр. 44
В этом разделе приведена информация о том, как с помощью локальной сертификатной компании пользователи могут создать сертификаты для идентификации клиента.

Управление сертификатами, полученными от общественной сертификатной компании

В этом разделе описано управление сертификатами, полученными от сертификатной компании из Internet путем создания хранилища сертификатов.

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, поддерживаемые 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.

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

Информация по созданию хранилищ сертификатов с помощью DCM и управлению общими сертификатами, применяемыми приложениями, приведена в следующих разделах:

Понятия, связанные с данным

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

Задачи, связанные с данной

“Управление расположением сертификатной компании PKIX” на стр. 74
Сертификатная компания инфраструктуры общих ключей X.509 (PKIX) - это сертификатная компания, выдающая сертификаты на основе новейших стандартов Internet X.509 применения инфраструктуры общих ключей.

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 (**?**)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.

   Примечание: Если в системе установлен шифровальный сопроцессор IBM то DCM предложит вам выбрать способ 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.

   Если вы планируете применять в системе сертификаты с сервером HTTP Server, то перед началом работы 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 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 импорт подписанного сертификата в хранилище сертификатов *SYSTEM.По окончании импорта 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: Некоторые 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.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 программы iSeries Navigator.

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 пункт **Создать хранилище сертификатов**. Будет запущен мастер пошагового выполнения задачи, который предложит вам 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 (**?**)в верхней части 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 импорт подписанного сертификата в хранилище сертификатов *OBJECTSIGNING.По окончании импорта 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 OS/400 V5R1 или более поздней версии DCM, 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.

Понятия, связанные с данным

“Цифровые сертификаты подписи объектов” на стр. 37
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

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 пункт **Создать хранилище сертификатов**. Будет запущен мастер пошагового выполнения задачи, который предложит вам заполнить несколько форм.

   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 ***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. 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.

Понятия, связанные с данным

“Цифровые сертификаты подписи объектов” на стр. 37
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

Задачи, связанные с данной

“Проверка подписей объектов” на стр. 78
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.

Обновление существующего сертификата

Процесс обновления сертификата, применяемый Диспетчером цифровых сертификатов (DCM), зависит от типа сертификатной компании (CA), выдавшей сертификат.

Сертификат можно обновить с помощью локальной сертификатной компании, либо с помощью сертификатной компании Internet.

Обновление сертификата, полученного от локальной сертификатной компании

Если обновленный сертификат подписан локальной CA, то DCM на основе предоставленной пользователем информации создает новый сертификат в текущем хранилище сертификатов и не удаляет предыдущий сертификат.

Для обновления сертификата от локальной сертификатной компании выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов, где находится сертификат, который нужно обновить.
2. В окне навигации выберите **Управление сертификатами**.
3. В окне навигации выберите **Обновить сертификат**.
4. Выберите сертификат, который нужно обновить, и нажмите **Обновить**.
5. Выберите **Локальная сертификатная компания (CA)** и нажмите **Продолжить**.
6. Заполните форму идентификации сертификата. Необходимо изменить поле этикетки **Новый сертификат**, другие поля могут остаться без изменений.
7. Выберите приложения, для которых необходим обновленный сертификат и нажмите **Продолжить**, чтобы завершить обновлениесертификата.

   Примечание: Не нужно выбирать приложение, использующее сертификат.

Обновление сертификата, полученного от сертификатной компании в Internet

Если сертификат получен от общеизвестной сертификатной компании Internet, то обновить сертификат можно двумя различными способами.

Можно обновить сертификат напрямую от сертификатной компании Internet, затем импортировать обновленный сертификат из полученного файла. Кроме того, можно с помощью DCM создать новую пару из личного и общего ключей, а также запрос на подписание сертификата (CSR), и отправить эту информацию в сертификатную компанию Internet для получения нового сертификата. Тогда при получении этого сертификата от компании можно завершить процедуру обновления.

Импорт и обновление сертификата, полученного непосредственно от сертификатной компании Internet:

Для того чтобы импортировать и обновить сертификат, полученный непосредственно от сертификатной компании Internet, выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов, где находится сертификат, который нужно обновить.

   Примечание: Нажмите ″?″ в любой панели, если у вас возникли вопросы о дальнейших действиях.
2. В окне навигации выберите **Управление сертификатами**.
3. В окне навигации нажмите **Обновить сертификат**.
4. Выберите сертификат, который нужно обновить, и нажмите **Обновить**.
5. Выберите **VeriSign** или другая **Сертификатная компания Internet** и нажмите **Продолжить**.
6. Выберите **Нет - Импортировать обновленный подписанный сертификат из файла**.
7. Для импорта сертификата выполните пошаговую задачу. Если вы решили обновить сертификат непосредственно у сертификатной компании, выдавшей его, то эта компания возвращает обновленный сертификат в файле. При импорте сертификата убедитесь, что указан правильный полный путь к файлу, в котором сертификат хранится на сервере. Файл, который содержит обновленный сертификат, может храниться в любом каталоге интегрированной файловой системы (IFS).
8. Нажмите кнопку **OK** для завершения задачи.

Обновление сертификата путем создания новой пары из личного и общего ключей, а также запроса на подписание сертификата.:

Для обновления сертификата у сертификатной компании Internet путем создания пары из личного и общего ключей, а также запроса на подписание сертификата, выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов, где находится сертификат, который нужно обновить.

   Примечание: Нажмите ″?″ в любой панели, если у вас возникли вопросы о дальнейших действиях.
2. В окне навигации выберите **Управление сертификатами**.
3. В окне навигации нажмите **Обновить сертификат**
4. Выберите сертификат, который нужно обновить, и нажмите **Обновить**.
5. Выберите **VeriSign** или другая **Сертификатная компания Internet** и нажмите **Продолжить**.
6. Нажмите **Да - Создать для этого сертификата новую пару ключей и нажать кнопку Продолжить**.
7. Заполните форму идентификации сертификата. Необходимо изменить поле этикетки Новый сертификат, другие поля могут остаться без изменений. Примечание: Нажмите ″?″ в любой панели, если у вас возникли вопросы о дальнейших действиях.
8. Нажмите кнопку **OK** для завершения задачи.

Импорт сертификата

В этом разделе приведена информация об импорте сертификатов, найденных в файлах на сервере, с помощью Диспетчера цифровых сертификатов (DCM).

Кроме того, сертификат можно импортировать с другого сервера, а не создавать сертификат заново на текущем сервере. Например, на сервере iSeries A при создании сертификата для розничного Web-приложения, инициирующего соединения SSL, применялась локальная сертификатная компания. Ваша организация за последнее время выросла, и вы установили новый сервер iSeries (iSeries B) для хранения большей части экземпляров этого занятого розничного приложения. Необходимо, чтобы все экземпляры розничного приложения применяли один и тот же сертификат для идентификации и установки SSL-соединений. Следовательно, можно импортировать одновременно сертификат локальной сертификатной компании и сертификат сервера с сервера iSeries A на сервер iSeries B, а не применять локальную сертификатную компанию на сервере iSeries A для создания нового, другого сертификата для сервера iSeries B.

Для того чтобы импортировать сертификат с помощью Диспетчера цифровых сертификатов, выполните следующие действия:

1. В левой панели навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов, в которое нужно импортировать сертификат. Хранилище сертификатов, в которое нужно импортировать сертификат, должно содержать сертификаты того же типа, что и сертификаты, экспортированные из другой системы. Например, вы импортируете сертификат сервера (тип), затем импортируете его в хранилище сертификатов, которое содержит сертификаты серверов, такие как *SYSTEM, либо Хранилище других сертификатов.
2. В окне навигации выберите **Управление сертификатами**.
3. В окне навигации выберите **Импортировать сертификат**.
4. Выберите тип сертификата для импорта и нажмите **Продолжить**. Тип импортируемого сертификата должен совпадать с типом экспортированного сертификата. Например, если вы экспортировали сертификат сервера, то для импорта нужно выбрать также сертификат сервера.

   Примечание: Когда Диспетчер цифровых сертификатов экспортирует сертификат в формате pkcs12, то сертификатная компания, выдавшая сертификат, включается в цепочку экспортированного сертификата и, следовательно, автоматически импортируется в хранилище, когда Диспетчер цифровых сертификатов импортирует сам сертификат. Тем не менее, если сертификат не экспортируется в формате pkcs12 и в том хранилище, куда он импортируется, нет сертификатной компании, то необходимо импортировать в хранилище компанию, выдавшую сертификат, до того, как импортировать сам сертификат.

5. Для импорта сертификата выполните пошаговую задачу. При импорте сертификата убедитесь, что правильно указан полный путь к файлу, в котором сертификат хранится на сервере.

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.

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

Ознакомьтесь с этой информацией о применении частной локальной сертификатной компании для выдачи сертификатов для других систем iSeries.

Предположим, что вы уже работаете с частной локальной сертификатной компанией (CA) на сервере, подключенном к сети. Теперь вы хотите с помощью этой локальной CA обслуживать и другой сервер в сети. Например, вы хотите с помощью этой локальной CA выдавать сертификаты клиента или сервера приложениям на другом сервере для работы с SSL. Или, вы хотите с помощью сертификатов, выдаваемых этой локальной CA, подписывать объекты, находящиеся на другом сервере.

Эти задачи позволяет выполнить Диспетчер цифровых сертификатов (DCM). Часть задач выполняется на сервере, где расположена локальная сертификатная компания, а другая часть - на сервере, где 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 на сервере, где расположена локальная сертификатная компания, установлен продукт Cryptographic Access Provider с более высоким уровнем шифрования, нежели в целевой системе. В системах OS/400 V5R2 и OS/400 V5R3 применятся только самый мощный из существующих продуктов такого класса - 5722–AC3. 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 (с частным ключом) система защищает файлы с помощью шифрования. 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 серверам 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 частного сертификата для другого сервера iSeries

Для того чтобы локальная сертификатная компания выдавала сертификаты, предназначенные для применения на другом сервере, выполните следующие действия на сервере, на котором находится локальная сертификатная компания:

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

   Примечание: 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. 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 тип сертификата, который необходимо создать с помощью локальной сертификатной компании, и нажмите кнопку **Продолжить**, чтобы запустить пошаговую задачу и заполнить несколько форм.
4. Выберите **сертификат сервера или клиента для другой системыiSeries** (для соединений SSL), или **сертификат подписи объекта для другой системыiSeries** (для применения в другой 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, DCM в исходной системе не предлагает выбрать формат для создаваемого сертификата подписи объекта.
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.

   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.

Понятия, связанные с данным

“Особенности резервного копирования и восстановления данных DCM” на стр. 28
В этом разделе приведена информация о резервном копировании и восстановлении важных данных DCM.

“Сравнение общих и частных сертификатов” на стр. 31
В этом разделе приведена информация, которая поможет вам выбрать наиболее подходящий тип цифровых сертификатов (общих или частных).

Задачи, связанные с данной

“Создание и управление локальной сертификатной компанией (CA)” на стр. 41
В этом разделе объясняется процедура создания и работы с локальной сертификатной компанией, выдающей частные сертификаты для приложений.

Применение общих сертификатов в SSL

Для управления сертификатами SSL в Диспетчере цифровых сертификатов (DCM) предназначено хранилище сертификатов *SYSTEM. Если DCM в целевой системе 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 в целевой системе нет хранилища сертификатов *SYSTEM, то можно использовать экспортированные файлы в качестве хранилища сертификатов другой системы, либо импортировать экспортированные файлы в существующее хранилище сертификатов *SYSTEM.

Хранилище сертификатов *SYSTEM не существует:

Если в целевой системе нет хранилища сертификатов *SYSTEM, то в качестве этого хранилища сертификатов можно использовать экспортированные файлы. Для того чтобы создать хранилище сертификатов *SYSTEM и использовать файлы хранилища в целевой системе, 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. Когда на экране появится страница Хранилище сертификатов и пароль, укажите пароль, заданный вами в *исходной* системе при создании сертификата для целевой системы 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. Когда на экране появится страница **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 другого сервера. 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 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.

Другие хранилища сертификатов 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. 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.

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, 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. Когда на экране появится страница **Хранилище сертификатов и пароль**, введите полное имя файла хранилища сертификатов, новый пароль и 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. 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 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, 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. Изменив пароль, вновь откройте хранилище сертификатов.

   Примечание: При изменении пароля хранилища сертификатов необходимо выбрать опцию **Автоматический вход в систему**.Это позволит DCM сохранить новый пароль, после чего 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.

5. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите **Хранилище сертификатов другой системы**.
6. Когда на экране появится страница **Хранилище сертификатов и пароль**, введите полное имя файла хранилища сертификатов, новый пароль и 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 экспорта 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 экспорта 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 другого сервера. 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 для подписи объектов в целевой системе

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, в которую были экспортированы файлы хранилища сертификатов, нет хранилища сертификатов *OBJECTSIGNING, 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. Если хранилище сертификатов *OBJECTSIGNING существует, необходимо поместить в него сертификаты другим способом.
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 с помощью DCM, 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. 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.Добавить сертификаты в существующее хранилище сертификатов *OBJECTSIGNING можно, открыв экспортированные файлы в целевой системе 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 непосредственно в хранилище сертификатов *OBJECTSIGNING выполните в целевой системе 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, после чего 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 экспорта 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.

Управление приложениями в 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.

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:

Понятия, связанные с данным

“Определения приложений” на стр. 10
В этом разделе приведена информация об определениях приложений DCM и применении этих определений для настройки SSL и подписания объектов.

Создание определения приложения

В этом разделе описаны два различных типа приложений, для работы с которыми можно создавать их определения.

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.

   Понятия, связанные с данным

   “Определения приложений” на стр. 10
   В этом разделе приведена информация об определениях приложений DCM и применении этих определений для настройки SSL и подписания объектов.

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.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, на серверах iSeries Access for Windows все изменения, связанные с сертификатами, вступят в силу автоматически. Однако для серверов Telnet и IBM HTTP Server for i5/OS и некоторых других приложений внесенные изменения вступят в силу только после перезапуска.

В OS/400 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 на основе 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. 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.

Управление пользовательскими сертификатами с помощью сроков действия

Диспетчер цифровых сертификатов (DCM) содержит функции управления сроками действия сертификатов, позволяющие администраторам управлять пользовательскими сертификатами, сертификатами серверов и клиентов, а также сертификатами подписания объектов в локальной системе. При этом для управления сертификатами применяются сведения о сроках действия этих сертификатов.

Примечание: Если настроить DCM для работы с EIM, то можно таким образом управлять пользовательскими сертификатами через дату истечения срока действия на всем предприятии.

Просмотр сертификатов в DCM с упорядочением по сроку действия позволяет быстро и просто определить сертификаты, срок действия которых близок к завершению, и своевременно обновить такие сертификаты.

Примечание: Поскольку с помощью сертификата проверки подписи можно проверять подписи объектов даже после окончания срока его действия, DCM не позволяет проверять срок действия таких сертификатов.

Для просмотра сертификатов серверов и клиентов, а также сертификатов подписи объектов с помощью сроков действия выполните следующие операции:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM** или ***OBJECTSIGNING**.

   Примечание: Для просмотра информации о заполнении полей формы при работе с DCM нажмите кнопку с вопросительным знаком (**?**)в верхней части страницы. Появится контекстная справка.
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 **Проверить срок действия**.
6. Выберите тип сертификата для проверки. Если вы работаете с хранилищем сертификатов *SYSTEM, выберите **Сервер или клиент**; если вы работаете с хранилищем сертификатов *OBJECTSIGNING, выберите **Подпись объектов**.
7. В поле **Диапазон сроков окончания действия (1-365)** укажите срок окончания действия сертификатов для просмотра и нажмите **Продолжить**.В окне DCM будут показаны все сертификаты, срок действия которых должен закончиться в течение указанного количества дней. В окне DCM будут также показаны все сертификаты, срок действия которых уже истек.
8. Выберите нужный тип сертификата. Вы можете просмотреть подробные сведения о сертификате, удалить сертификат или обновить его.
9. После окончания работы с сертификатами нажмите кнопку **Отмена** для завершения работы с задачей.

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.

Понятия, связанные с данным

“Определения списка аннулированных сертификатов (CRL)” на стр. 6
Список аннулированных сертификатов (CRL) - это файл, содержащий список всех недопустимых и аннулированных сертификатов определенной сертификатной компании (CA).

“Проверка” на стр. 11
В DCM предусмотрены задачи, позволяющие проверять свойства сертификатов и приложений.

Присвоение сертификата приложениям

Диспетчер цифровых сертификатов (DCM) 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.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SYSTEM** или ***OBJECTSIGNING**.

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

   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 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. 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.

Примечание: Для того чтобы анонимно связать сервер LDAP для обработки CRL, необходимо с помощью Web-инструмента администрирования для сервера каталогов выбрать задачу ″Схема управления″ и изменить класс защиты (который также называется ″классом доступа″) атрибутов certificateRevocationList и authorityRevocationList с ″critical″ до ″normal″, а также оставить пустыми поля **Определенное имя для входа в систему** и **Пароль**.

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 приложениями в DCM.

Понятия, связанные с данным

“Определения списка аннулированных сертификатов (CRL)” на стр. 6
Список аннулированных сертификатов (CRL) - это файл, содержащий список всех недопустимых и аннулированных сертификатов определенной сертификатной компании (CA).

Информация, связанная с данной

Сервер каталогов IBM для iSeries (LDAP)

Применение SSL на сервере LDAP

Хранение ключей сертификатов в шифровальном сопроцессоре IBM

В этом разделе приведена информация об использовании установленного сопроцессора в качестве более надежного хранилища личных ключей сертификатов.

Если в системе установлен шифровальный сопроцессор IBM, то его можно использовать для 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.

Понятия, связанные с данным

“Шифровальные сопроцессоры IBM для iSeries” на стр. 9
Шифровальный сопроцессор содержит проверенные функции шифрования, обеспечивающие конфиденциальность и целостность данных при разработке защищенных приложений электронного бизнеса.

Хранение личного ключа сертификата непосредственно в сопроцессоре

Для повышения надежности защиты личный ключ сертификата может храниться непосредственно в шифровальном сопроцессоре IBM. 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 можно зашифровать с помощью главного ключа шифровального сопроцессора IBM и хранить его в специальном файле 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 сопроцессора IBM создать соответствующий файл хранения ключей. Кроме того, с помощью того же интерфейса необходимо связать файл хранения ключей с описанием нужного сопроцессора. К Web-интерфейсу настройки сопроцессора можно обратиться 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. К Web-интерфейсу настройки сопроцессора можно обратиться 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.

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.

Примечание: Стандарты PKIX описаны в документе RFC 2560.

Понятия, связанные с данным

“Управление сертификатами, полученными от общественной сертификатной компании” на стр. 49
В этом разделе описано управление сертификатами, полученными от сертификатной компании из Internet путем создания хранилища сертификатов.

Управление каталогом LDAP для пользовательских сертификатов

В этом разделе приведена информация о настройке DCM для хранения пользовательских сертификатов в каталоге LDAP. Такая конфигурация позволяет службе преобразования идентификаторов в рамках предприятия (EIM) работать с пользовательскими сертификатами.

По умолчанию Диспетчер цифровых сертификатов (DCM) хранит пользовательские сертификаты, выданные локальной сертификатной компанией, в пользовательских профайлах i5/OS. Тем не менее, можно настроить Диспетчер цифровых сертификатов (DCM) и функцию преобразования идентификаторов в рамках предприятия (EIM) таким образом, что при выдаче пользовательских сертификатов локальной сертификатной компанией общедоступная копия сертификата будет сохраняться в каталоге LDAP. Совместное применение EIM и DCM позволяет хранить пользовательские сертификаты в каталоге LDAP, благодаря чему значительно расширяются возможности применения сертификатов при работе с приложениями. Кроме того такая конфигурация позволяет с помощью EIM управлять пользовательскими сертификатами так же, как и другими идентификаторами пользователей на предприятии.

Примечание: Для того чтобы пользователь мог сохранить в каталоге LDAP сертификат другой CA, ему необходимо выполнить задачу **Присвоение пользовательского сертификата**.

EIM - это технология @server , позволяющая администраторам корпоративных сетей управлять идентификаторами пользователей, в том числе пользовательскими профайлами и сертификатами i5/OS. Для того чтобы управлять пользовательскими сертификатами с помощью EIM, перед выполнением задач настройки DCM необходимо выполнить следующие задачи настройки EIM:

1. Настройте EIM с помощью мастера **Настройка EIM** в программе iSeries Navigator.
2. Создайте домене EIM реестр X.509 для применения с соответствиями сертификатов
3. Выберите опцию меню Свойства для настройки папки в домене EIM и введите имя реестра X.509.
4. Для каждого пользователя EIM необходимо создать идентификатор EIM.
5. Создайте целевую связь между каждым идентификатором EIM и пользовательским профайлом в локальном реестре пользователей i5/OS. В качестве имени локального реестра пользователей i5/OS укажите имя определения реестра EIM, заданное с помощью мастера **Настройка EIM**.

Примечание: Дополнительная информация о настройке EIM приведена в разделе EIM.

После выполнения всех задач настройки EIM необходимо завершить создание совместной конфигурации EIM и DCM, выполнив следующие задачи:

1. В DCM с помощью задачи **Управление каталогом LDAP** задать каталог LDAP, в котором DCM будет хранить пользовательские сертификаты, выданные локальной CA.Каталог LDAP может располагаться не в локальной системе iSeries и не на сервере LDAP, с которым работает EIM. При настройке в DCM каталога LDAP Диспетчер цифровых сертификатов хранит все пользовательские сертификаты, выданные локальной CA, в заданном каталоге LDAP. Кроме того, сертификаты, обработанные с помощью задачи **Присвоить пользовательский сертификат**, DCM также хранит в каталоге LDAP, а не в пользовательском профайле.
2. Запустите команду **Преобразовать пользовательские сертификаты** (CVTUSRCERT).Эта команда копирует существующие пользовательские сертификаты в соответствующий каталог LDAP. Следует помнить, что команда копирует только сертификаты пользователей, для профайлов которых создана целевая связь с идентификаторами EIM. После этого команда создает исходную связь между каждым сертификатом и соответствующим ему идентификатором EIM. Имя идентификатора пользователя для исходной связи определяется с помощью полного имени (DN) субъекта сертификата, DN сертификатной компании, а также объединения этих имен и общего ключа сертификата.

Примечание: Для того чтобы анонимно связать сервер LDAP для обработки CRL, необходимо с помощью Web-инструмента администрирования для сервера каталогов выбрать задачу ″Схема управления″ и изменить класс защиты (который также называется ″классом доступа″) атрибутов certificateRevocationList и authorityRevocationList с ″critical″ до ″normal″, а также оставить пустыми поля **Определенное имя для входа в систему** и **Пароль**.

Задачи, связанные с данной

“Цифровые сертификаты и технология преобразования идентификаторов в рамках предприятия (EIM)” на стр. 35
Совместное использование EIM и DCM позволяет применять сертификат в качестве источника данных для операции преобразования EIM, которая преобразует сертификаты в целевой идентификатор пользователя, связанный с тем же идентификатором EIM.

Подписание объектов

В этом разделе приведена информация об управлении сертификатами подписи объектов с помощью DCM.

Существует три способа подписания объектов. Подписать объект можно путем вызова API Подписать объект.Кроме того, подписать объект можно с помощью Диспетчера цифровых сертификатов (DCM).Начиная с версии OS/400 V5R2, при создании пакета для отправки в другие системы можно воспользоваться функцией подписания объектов Централизованного управления программы iSeries Navigator.

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 OS/400 версии V5R2, поддерживается добавление подписей к объектам типа *CMD (команды). Подписывать объекты, находящиеся в других системах, 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. Запуск DCM
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.

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

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

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.

Понятия, связанные с данным

“Цифровые сертификаты подписи объектов” на стр. 37
Здесь приведены сведения о том, как с помощью цифровых сертификатов можно обеспечить подлинность и целостность объектов путем создания и проверки их цифровых подписей.

Задачи, связанные с данной

“Управление сертификатами проверки подписей объектов” на стр. 54
Диспетчер цифровых сертификатов (DCM) позволяет управлять сертификатами проверки подписей, применяемыми для проверки цифровых подписей объектов.

Устранение неполадок DCM

В этом разделе приведены инструкции по устранению неполадок при работе с DCM.

При работе с Диспетчером цифровых сертификатов (DCM) и сертификатами могут возникнуть ошибки, не позволяющие выполнить необходимые действия и решить стоящие перед пользователем задачи. Большинство из часто встречающихся неполадок можно отнести к одной из следующих категорий:

Устранение общих неполадок и неполадок 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. Дополнительную информацию можно также найти в Information Center и на Web-сайтах IBM.
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.
Появится сообщение об ошибке, в котором говорится, что при попытке открыть хранилище сертификатов было обнаружено, что срок действия пароля закончился.	Необходимо изменить пароль хранилища сертификатов. Для того чтобы изменить пароль, нажмите кнопку **OK**.

Неполадка	Исправление
При работе с задачей **Выбор хранилища сертификатов** не был сброшен пароль.	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** в меню Системный инструментарий (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. После этого выберите команду **Работа с защитой системы**.Скорее всего, ИД пользователя сервисных средств - QSECOFR.
Не найден сертификат CA, который нужно получить в системе.	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 Navigator. В соответствии с параметрами кэша браузер сравнивает документ в кэше с документом в сети **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 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 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.

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.

Неполадка	Исправление

Не удалось создать базу данных ключей, либо не удалось выполнить задачу Создать локальную CA.	Убедитесь в отсутствии конфликтов имен файлов. Причиной такого конфликта могут служить файлы, которые явно не указаны в запросе. DCM пытается защитить пользовательские данные в создаваемых каталогах даже в том случае, если защита файлов не позволяет DCM создавать другие необходимые файлы.
	
	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. После перемещения следующих файлов необходимо создать новую локальную CA:
	`/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`

	В системе может быть не установлена необходимая лицензионная программа (LPP), которая требуется для работы DCM. Просмотрите список Предварительных требований для DCM и убедитесь в том, что все необходимые лицензионные программы правильно установлены.

Неполадка	Исправление
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.
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.Дополнительная информация о настройке контрольного списка на защищенном экземпляре сервера HTTP приведена в документации к продукту Сервер HTTP дляiSeries.

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.

Неполадка	Исправление
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 шестнадцатиричные 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).
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 шестнадцатиричные значения A1 и B1 в значения B2 и 9A при работе с польской кодовой страницей.
В окне браузера 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/` and `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

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 необходимо с помощью графического пользовательского интерфейса HTTP Server задать параметр **SSLAppName**. Кроме того, файл конфигурации должен содержать данные для виртуального хоста с портом SSL для которого параметру **SSL** присвоено значение **Enabled**.Кроме того, файл должен содержать две директивы **Listen** для двух разных портов, с поддержкой SSL и без поддержки SSL.Их можно задать на странице **Общие параметры**.Кроме того, убедитесь, что экземпляр сервера создан, а его сертификат подписан.

Неполадка	Исправление
Процесс регистрации экземпляра HTTP Server в списке защищенных приложений требует дополнительных пояснений.	В системе откройте интерфейс администрирования сервера HTTP и настройте конфигурацию сервера HTTP. Сначала необходимо определить виртуальный хост с поддержкой SSL. После этого необходимо указать, что этот хост применяет порт SSL, заданный в директиве **Listen** (на странице **Общие параметры**.После этого на странице **Идентификация SSL с помощью сертификатов** в разделе **Защита** необходимо включить SSL для виртуального хоста, настроенного на предыдущем шаге.Все изменения необходимо сохранить в файле конфигурации. Обратите внимание на то, что при регистрации экземпляра не будут автоматически определены типы сертификатов, с которыми этот экземпляр будет работать. С помощью DCM свяжите этот сертификат с приложением до перезапуска экземпляра сервера.
Возникли затруднения при настройке контрольных списков и расширенной идентификации клиентов в HTTP Server.	Информация о параметрах настройки экземпляра приведена в документации по серверу HTTP Server для iSeries.
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**. Информацию об этих API можно найти в разделе Поиск API в системе 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.
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.
Сервер HTTP не запускается, параметру **SSL** присвоено значение **Enabled** и в протокол задания заносится сообщение об ошибке HTP8351. В протокол задания сервера HTTP при сбое сервера HTTP заносится сообщение об ошибке инициализации SSL с кодом 107.	Ошибка 107 свидетельствует об истечении срока действия сертификата.С помощью DCM присвойте приложению другой сертификат, например QIBM_HTTP_SERVER_ADMIN. Если сбой возникает при запуске сервера *ADMIN, то временно присвойте параметру **SSL** значение Disabled, что позволит обратиться к DCM с помощью этого сервера. После этого с помощью DCM присвойте приложению QIBM_HTTP_SERVER_ADMIN другой сертификат и попробуйте снова присвоить **SSL** значение **Enabled**.

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 показать приглашение для выбора сертификата.
2. Это может также быть вызвано такой конфигурацией сервера, при которой список выбора не показывается и браузер содержит только один сертификат сертификатной компании (CA), относящейся к уполномоченным сертификатным компаниям сервера. Проверьте настройку браузера и при необходимости измените ее. После этого браузер предложит вам выбрать сертификат. Если вы не можете представить сертификат уполномоченной CA сервера, то присвоить сертификат нельзя. Обратитесь к администратору DCM.
3. Выбранный сертификат уже зарегистрирован с помощью DCM.
4. Сертификатная компания, выдавшая сертификат, не является уполномоченной для данной системы или приложения. 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.Кроме того, администратор может устранить неполадку, сделав сертификатную компанию уполномоченной с помощью задачи **Задать состояние CA**.
5. У вас нет ни одного сертификата, который можно зарегистрировать. Просмотрите список сертификатов пользователей с помощью браузера.
6. Для регистрации выбран неполный сертификат или сертификат с истекшим сроком действия. Обновите сертификат или обратитесь к CA, выдавшей сертификат.
7. IBM HTTP Server for i5/OS настроен неправильно. Это не позволяет зарегистрировать сертификат путем настройки соединения SSL и идентификации клиента с помощью административного экземпляра сервера. 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.

Задачи, связанные с данной

“Присвоение пользовательского сертификата” на стр. 45
Можно связать принадлежащий вам сертификат с пользовательским профайлом i5/OS или с идентификатором пользователя. Это может быть сертификат, полученный от частной локальной сертификатной компании из другой системы или от общеизвестной сертификатной компании, действующей в сети Internet. Для того чтобы идентификатору пользователя можно было присвоить сертификат, выдающая его CA должна являться уполномоченной CA на сервере, и сертификат не должен быть связан с пользовательским профайлом или с другим идентификатором пользователя в системе.

Связанная информация о DCM

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

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 в системе:

- **Web-сайт VeriSign Help Desk** Этот Web-сайт содержит большую библиотеку по темам, связанным с цифровыми сертификатами и защите информации в сети Internet.

- **Защита проводных сетей IBM eServer iSeries: Расширения Диспетчера цифровых сертификатов OS/400 V5R1 и шифрования SG24-6168** В этом руководстве IBM подробно описаны расширения сетевой безопасности для OS/400 V5R1. В книге освещено множество вопросов: функции подписания объектов iSeries, Диспетчер цифровых сертификатов (DCM), поддержка Шифровального сопроцессора 4758 для SSL и др.
- **Internet-защитаAS/400: Разработка инфраструктуры цифровых сертификатов (SG24-5659)** В этом руководстве описана работа 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.
- **Поиск по индексу RFC** 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.

Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Лицензионного соглашения на машинный код IBM или любого другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Все указанные цены являются текущими розничными ценами, рекомендуемыми IBM, и могут быть изменены без предварительного уведомления. Реальные цены могут отличаться от указанных.

Данный документ содержит примеры данных и отчетов, применяемых в повседневных бизнес-операциях. Для более наглядной демонстрации возможностей продукта эти примеры содержат имена людей, названия компаний и продуктов. Все имена и названия являются вымышленными и любые совпадения с реально существующими именами и адресами являются случайными.

ЛИЦЕНЗИЯ НА ПРОДУКТЫ, ЗАЩИЩЕННЫЕ АВТОРСКИМ ПРАВОМ:

В этой публикации приведены примеры программ, иллюстрирующие технологии программирования на различных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для той операционной системы, для которой были созданы эти примеры. Примеры не были тщательно и всесторонне протестированы. По этой причине IBM не может гарантировать их надежность, удобство их обслуживания и отсутствие в них ошибок.

Каждая полная или частичная копия примеров программ, а также любых продуктов, созданных на их основе, должна содержать следующую информацию об авторских правах:

© (имя вашей компании) (год). Части этого кода были созданы на основе примеров программ IBM Corp. . © Copyright IBM Corp. _год или годы_. Все права защищены.

При просмотре данного документа в электронном виде фотографии и цветные иллюстрации могут не отображаться.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

| AIX
| AS/400
| Domino
| eServer
| i5/OS
| IBM
| iSeries
| Lotus
| Net.Data
| OS/400

Microsoft, Windows, и эмблема Windows являются товарными знаками Microsoft Corporation в США и/или других странах.

Названия других компаний продуктов и услуг могут быть товарными или служебными знаками других компаний.

Условия и постановления

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать эти публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в случае, если, по мнению IBM, использование этих публикаций может нанести ущерб интересам IBM или если IBM установит, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Данные публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии соблюдения прав, коммерческой ценности или применения для каких-либо конкретных целей.

Напечатано в Дании