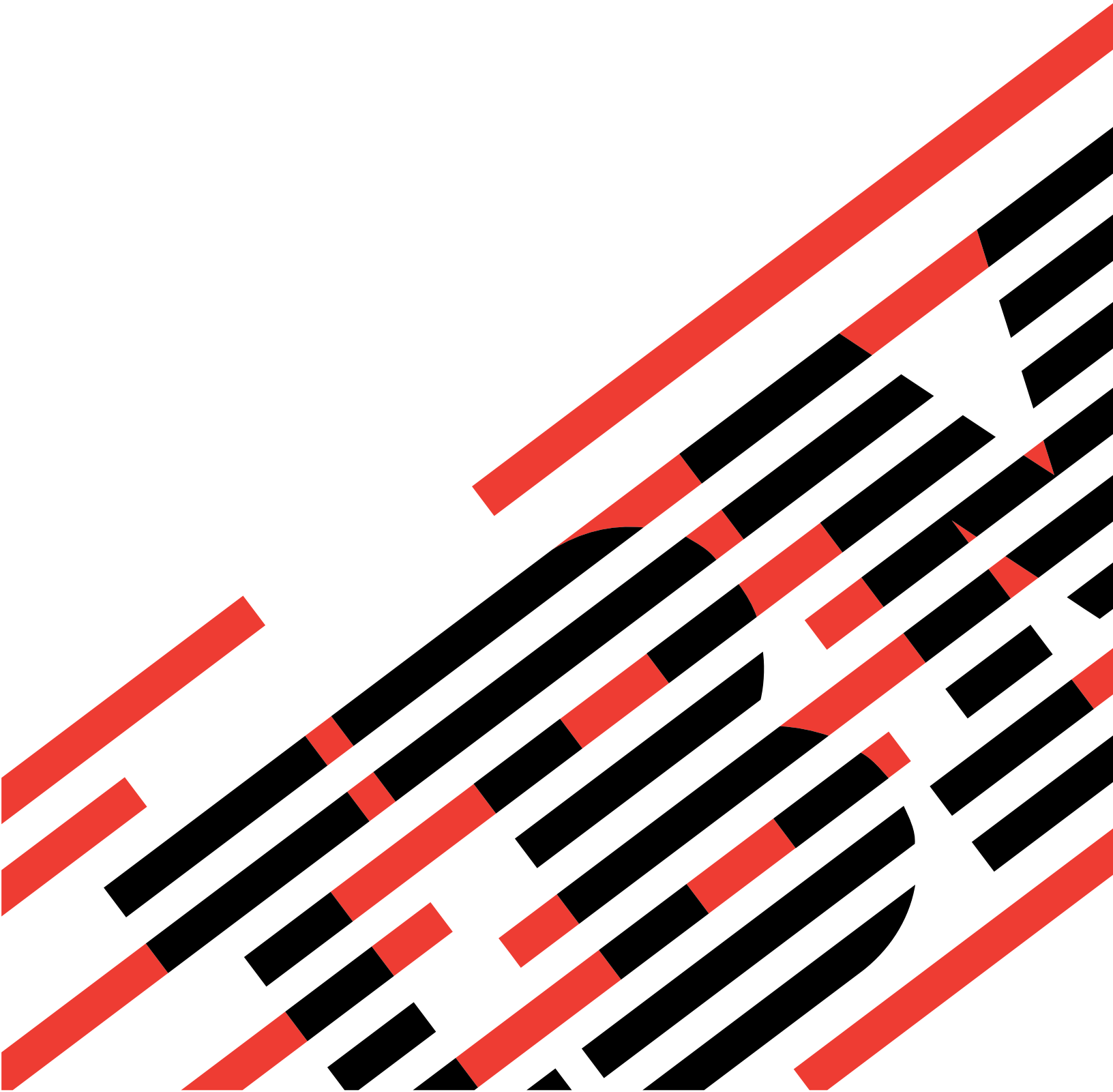
IBM

eserver

iSeries

Создание и проверка подписей объектов



IBM

@server

iSeries

Создание и проверка подписей объектов

Содержание

Создание и проверка подписей объектов

Создание и проверка подписей объектов - это способы защиты, позволяющие проверить целостность различных объектов сервера iSeries. Для создания подписи объекта применяется личный ключ цифрового сертификата, а для проверки этой подписи - соответствующий общий ключ сертификата. Цифровая подпись гарантирует целостность объекта в момент его подписания. Она применяется как для идентификации, так и для проверки прав доступа. Ее нельзя подделать. Подпись позволяет проверить источник объекта и то, что объект не был изменен. Добавление подписи к объекту позволяет идентифицировать источник объекта и дает возможность проверить целостность объекта. При проверке подписи объекта можно узнать, было ли содержимое объекта изменено с момента подписания объекта. Кроме того, можно узнать, кем была создана подпись, и таким образом определить степень надежности источника объекта.

Для создания подписей объектов iSeries и проверки подписей применяются следующие средства:

- API - для создания подписей объектов и проверки подписей в программах.
- Диспетчер цифровых сертификатов - для создания, просмотра и проверки подписей объектов.
- Функция Централизованное управление программы Навигатор iSeries - для создания подписей объектов при рассылке пакетов в другие системы.
- Команды CL, например, Проверить целостность объекта (CHKOBJITG), - для проверки подписей.

Дополнительная информация об этих средствах работы с подписями и сведения о том, как с помощью подписей объектов можно повысить надежность текущей стратегии защиты, приведены в следующих разделах:

Новое в выпуске V5R2
В этом разделе приведена информация о новых средствах создания и проверки подписей объектов iSeries, а также об изменениях, внесенных в документацию по этому выпуску.

Как напечатать этот раздел
Содержит информацию о том, как напечатать весь раздел в виде файла PDF.

Сценарии создания подписей объектов
Описание типичных сценариев создания и проверки подписей объектов iSeries. В каждом сценарии перечислены задачи по настройке, которые необходимо выполнить для реализации сценария.

Основная информация о подписях объектов
Содержит справочную информацию о цифровых подписях, их создании и проверке.

Предварительные требования для создания и проверки подписей объектов
Содержит информацию о требованиях к конфигурации, а также о планировании создания и проверки подписей объектов.

Работа с подписанными объектами
Содержит информацию о командах и системных значениях iSeries, предназначенных для работы с подписанными объектами. Кроме того, содержит сведения о том, как наличие объектов с подписью влияет на резервное копирование и восстановление данных.

Устранение неполадок при создании и проверке подписей объектов
Содержит инструкции по устранению ошибок, которые могут возникнуть при создании и проверке подписей объектов.

Дополнительная информация о подписях объектов и их проверке
Содержит ссылки на другие источники информации о подписях объектов и проверке подписей.

Новое в выпуске V5R2

Функции создания и проверки подписей объектов iSeries впервые появились в выпуске V5R1. В выпуске V5R2 были добавлены новые и усовершенствованы старые функции.

К числу таких функций относятся:

- **Функция создания подписей объектов приложения Централизованное управление программы Навигатор iSeries**
  В этом выпуске в приложение Централизованное управление включен мастер Определение продукта, позволяющий подписывать объекты в пакетах, рассылаемых конечным системам iSeries.
- **Создание подписей для объектов команд (*CMD)**
  В этом выпуске разрешено создавать подписи для объектов команд (*CMD). Можно подписать как весь объект *CMD, так и его отдельные компоненты.
- **Новые API для создания и проверки подписей**
  Для применения расширенных функций создания и проверки подписей, предусмотренных в этом выпуске OS/400, разработано три новых API:
  - API Подписать буфер (QYDOSGNB, QydoSignBuffer)
    Этот API позволяет локальной системе создать цифровую подпись для буфера, подтверждающую его надежность. Созданная подпись возвращается программе, вызвавшей API. Например, с помощью этого API можно подписать фрагмент файла XML и сохранить подпись в другом фрагменте этого файла. Кроме того, можно считать в буфер записи из файла базы данных и подписать эти записи.
  - Проверить буфер (QYDOVFYB, QydoVerifyBuffer)
    Этот API позволяет локальной системе проверить цифровую подпись, ранее созданную для буфера.
  - API Добавить сертификат для проверки (QYDOADDV, QydoAddVerifier)
    Этот API добавляет сертификат в хранилище сертификатов *SIGNATUREVERIFICATION системы. Добавленный сертификат может применяться для проверки подписей объектов, созданных с помощью этого сертификата. Проверка подписи позволяет удостовериться в целостности объекта, т.е. убедиться, что объект не был изменен с момента создания подписи. Если хранилище сертификатов не существует, API создает хранилище и добавляет в него сертификат.

    Примечание: По соображениям защиты с помощью этого API в хранилище сертификатов *SIGNATUREVERIFICATION нельзя добавить сертификат Сертификатной компании (CA). После добавления сертификата CA в хранилище сертификатов система считает эту CA уполномоченной компанией по выдаче сертификатов. Другими словами, сертификаты, выданные этой CA, считаются надежными. Указанное ограничение введено для того, чтобы нельзя было создать программу выхода из процедуры установки, которая добавляет сертификат CA в хранилище сертификатов с помощью этого API. Сертификаты CA следует добавлять в хранилище сертификатов с помощью Диспетчера цифровых сертификатов. Это дает возможность назначить администратора, который будет самостоятельно определять, какие CA можно считать надежными. В этом случае в систему можно будет импортировать только те сертификаты, которые администратор явно указал как надежные.

    Если вы не хотите, чтобы этот API применялся без вашего ведома для добавления сертификата подписи объекта в хранилище сертификатов *SIGNATUREVERIFICATION, рекомендуется запретить доступ к этому API в системе. Для этого необходимо запретить изменение системных значений, связанных с защитой, с помощью Системного инструментария (SST).

Ранее информация о подписях объектов iSeries и их проверке содержалась в разделе Управление цифровыми сертификатами справочной системы Information Center. Теперь появились новые способы создания и проверки подписей объектов. В связи с этим был создан отдельный раздел Information Center, содержащий полную информацию об этих возможностях. Этот раздел содержит подробные сведения о работе с подписями объектов, в том числе сценарии их применения.

Новая информация включает:

- Сценарии, с помощью которых можно выбрать оптимальный способ применения подписей объектов в стратегии защиты.
- Новые разделы с описанием команд и системных значений, предназначенных для управления объектами с подписями.
- Новые разделы, содержащие описание процедур планирования и прочую информацию о принципах работы с подписями.

Более подробная информация о дополнениях и изменениях, внесенных в этот выпуск, приведена в документе Информация для пользователей  .

Как напечатать этот раздел

Для просмотра или загрузки документа в формате PDF щелкните на ссылке Создание и проверка подписей объектов  (размер файла 350 Кб, около 44 страниц).

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

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

Для просмотра и печати документа в формате PDF применяется программа Adobe Acrobat Reader. Ее можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Сценарии создания подписей объектов

На сервере iSeries предусмотрено несколько способов создания и проверки подписей объектов. Выберите нужный способ, исходя из требуемого уровня защиты и преследуемых целей. В некоторых случаях подписи объектов служат только для проверки целостности этих объектов. В других случаях требуется подписывать объекты, которые рассылаются другим системам. Подпись объекта позволяет другим пользователям идентифицировать отправителя объекта и проверить целостность объекта.

На выбор способа создания и проверки подписей могут повлиять многие факторы. В приведенных ниже сценариях описаны наиболее стандартные ситуации, в которых применяются функции создания и проверки подписей объектов. Каждый сценарий содержит список предварительных требований и список задач, которые необходимо выполнить для реализации сценария. Ознакомьтесь с этими сценариями, для того чтобы лучше понять назначение функций работы с подписями объектов iSeries.

Сценарий: Создание и проверка подписей объектов с помощью Диспетчера цифровых сертификатов
В этом сценарии рассматривается пример фирмы, которой требуется создать подписи для

незащищенных объектов приложений на корпоративном Web-сервере. Такие подписи позволят быстро определить, были ли внесены несанкционированные изменения в объекты. С учетом поставленных целей и требований к защите в качестве основного способа создания и проверки подписей объектов был выбран Диспетчер цифровых сертификатов (DCM).

Сценарий: Создание и проверка подписей объектов с помощью API
В этом сценарии рассматривается пример фирмы, занимающейся разработкой прикладных программ, которой необходимо программным образом создавать подписи для защиты собственных приложений. С помощью подписи заказчики смогут убедиться, что приложение действительно создано этой фирмой и не содержит несанкционированных изменений. С учетом поставленных целей и требований к защите в качестве способа создания и проверки подписей объектов были выбраны API Подписать объект и API Добавить сертификат для проверки.

Сценарий: Создание подписей объектов с помощью Централизованного управления
В этом сценарии рассматривается пример фирмы, которая планирует подписывать объекты, объединяемые в пакеты для последующей рассылки на серверы iSeries. Для подписания объектов и создания пакетов, рассылаемых другим серверам iSeries, в данном сценарии применяется функция Централизованное управление программы Навигатор iSeries.

Сценарий: Создание и проверка подписей объектов с помощью DCM

Описание

Занимая должность администратора систем iSeries в фирме MyCo., Inc, вы отвечаете за управление двумя серверами iSeries этой фирмы. Один из этих серверов iSeries содержит Web-сайт фирмы. Второй, рабочий сервер iSeries, применяется для создания содержимого Web-сайта. Созданные файлы и объекты программ после тестирования передаются на внешний Web-сервер.

Внешний Web-сервер фирмы содержит Web-сайт с информацией о фирме. На этом Web-сайте заказчики могут заполнять различные формы для регистрации продуктов и получения информации о продуктах и их изменениях, центре рассылки продуктов и т.д. Вам необходимо защитить программы cgi-bin, служащие для создания этих форм, так как они могут быть изменены. У вас должна быть возможность проверять целостность объектов программ и своевременно узнавать о несанкционированном изменении этих объектов. Для достижения поставленной цели было решено создать цифровые подписи для этих объектов.

После изучения возможностей, предусмотренных в OS/400 для работы с подписями объектов, вы узнали, что существует несколько способов создания и проверки подписей объектов. Поскольку вы отвечаете за небольшое число серверов iSeries, и вам не требуется часто создавать подписи объектов, для работы с цифровыми подписями был выбран Диспетчер цифровых сертификатов (DCM). Кроме того, вы решили создать локальную сертификатную компанию (CA), чтобы применять собственные сертификаты для создания подписей объектов. Использование сертификатов, выданных локальной CA, сокращает расходы по реализации этого способа защиты, так как в этом случае не требуется приобретать сертификат у глобальной CA.

В этом примере рассмотрена настройка и использование подписей объектов в небольшом числе систем iSeries.

Достоинства сценария

У этого сценария есть следующие достоинства:

- Создание подписей для незащищенных объектов позволяет проверять их целостность и легко определять, были ли эти объекты изменены с момента их подписания. В будущем это позволит значительно сократить время, затрачиваемое на устранение неполадок приложений и системы.
- Графический интерфейс (GUI) приложения DCM позволяет быстро создавать и проверять подписи объектов.
- Применение DCM для создания и проверки подписей объектов значительно сокращает время, которое требуется для работы с подписями объектов.
- Создание подписей объектов с помощью сертификата, выданного локальной сертификатной компанией (CA), значительно сокращает расходы по реализации этого сценария.

Цели

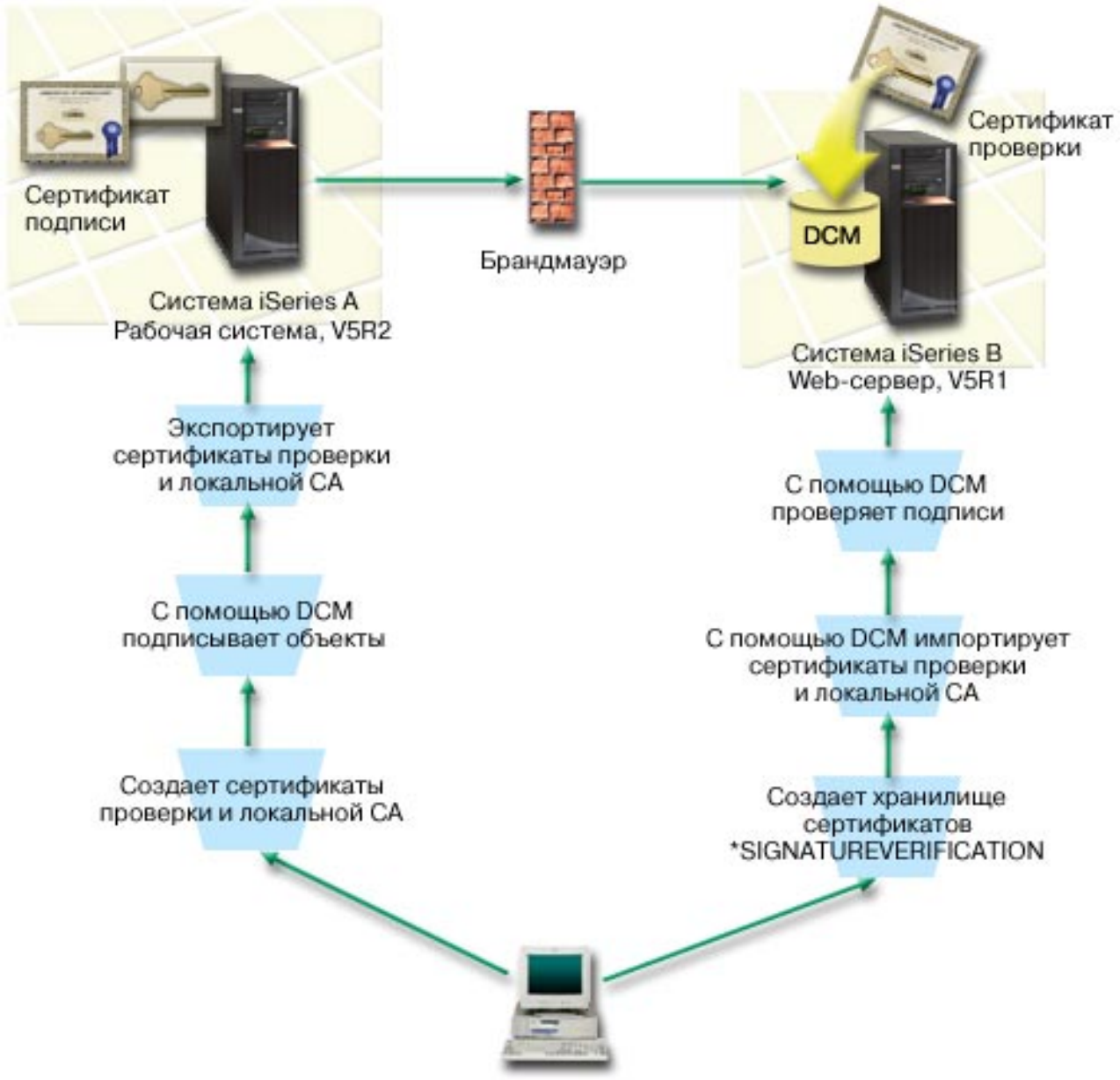
В этом сценарии требуется создать цифровые подписи для незащищенных объектов, расположенных на внешнем сервере iSeries фирмы, например, для программ cgi-bin, служащих для создания форм. Занимая должность системного администратора в фирме MyCo, Inc., вы решили создавать и проверять подписи объектов с помощью Диспетчера цифровых сертификатов (DCM).

В этом сценарии преследуются следующие цели:

- Приложения и другие незащищенные объекты, расположенные на Web-сервере фирмы (iSeries B), должны быть подписаны с помощью сертификата, выданного локальной CA. Такая CA выбрана для сокращения стоимости реализации сценария.
- У системных администраторов и других уполномоченных пользователей должна быть возможность быстро проверить цифровые подписи на сервере iSeries, чтобы идентифицировать источник и проверить подлинность подписанных объектов. Для этого в хранилище сертификатов *SIGNATUREVERIFICATION каждого сервера iSeries необходимо скопировать сертификат проверки подписи фирмы и сертификат локальной сертификатной компании (CA).
- Путем проверки подписей приложений и других объектов фирмы администраторы iSeries могут определять, изменялось ли содержимое объектов с момента их подписания.
- Администратор системы должен создавать подписи объектов с помощью DCM. Он и другие пользователи должны иметь возможность проверять подписи объектов с помощью DCM.

Дополнительные сведения

На следующем рисунке показан процесс создания и проверки подписей объектов в данном сценарии:



На рисунке показаны следующие системы, рассмотренные в данном сценарии:

iSeries A

- В системе iSeries A установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- iSeries A - это внутренний рабочий сервер фирмы, на котором разрабатываются приложения для внешнего Web-сервера iSeries (iSeries B).
- В системе iSeries A установлен продукт Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- В системе iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 OS/400) и IBM HTTP Server (5722–DG1).
- iSeries A выполняет функции локальной сертификатной компании (CA). В этой системе хранится сертификат, служащий для создания подписей объектов.

- В системе iSeries A создаются подписи для внешних объектов и приложений фирмы с помощью DCM.
- В системе iSeries A предусмотрена возможность проверки подписей.

iSeries B

- В системе iSeries B установлена операционная система OS/400 версии 5, выпуска 1 (V5R1).
- iSeries B - это внешний Web-сервер фирмы, не защищенный брандмауэром.
- В системе iSeries B установлен продукт Cryptographic Access Provider 128-bit (5722–AC3).
- В системе iSeries B установлены и настроены Диспетчер цифровых сертификатов (компонент 34 OS/400) и IBM HTTP Server (5722–DG1).
- iSeries B не выполняет функции локальной CA и не применяется для создания подписей объектов.
- В системе iSeries B настроена функция проверки подписей. Для этого в DCM создано хранилище сертификатов *SIGNATUREVERIFICATION, в которое импортирован сертификат проверки подписей и сертификат локальной CA.
- Для проверки подписей объектов применяется DCM.

Предварительные требования

Для реализации этого сценария должны быть выполнены следующие требования:

1. На всех серверах iSeries должны быть выполнены требования к установке и применению Диспетчера цифровых сертификатов (DCM).
2. Приложение DCM ранее не настраивалось и не применялось ни на одном сервере iSeries.
3. На всех серверах iSeries установлена последняя версия программы Cryptographic Access Provider 128-bit (5722-AC3).
4. На всех серверах iSeries системному значению Проверять подписи объектов при восстановлении (QVFYOBJRST) присвоено значение по умолчанию (3). Это значение разрешает серверу проверять подписи объектов при восстановлении.
5. Профайлу администратора iSeries A должны быть предоставлены специальные права доступа *ALLOBJ, для того чтобы администратор мог подписывать объекты, либо у этого профайла должны быть права на работу с приложением, применяемым для подписания объектов.
6. У администратора системы или другого пользователя, отвечающего за создание хранилищ сертификатов в DCM, должны быть специальные права доступа *SECADM и *ALLOBJ.
7. Во всех остальных системах iSeries администратору системы и другим пользователям должны быть предоставлены специальные права доступа *AUDIT, необходимые для проверки подписей объектов.

Задачи

Для реализации этого сценария необходимо выполнить две группы задач. К первой из них относятся задачи по настройке системы iSeries A в качестве локальной сертификатной компании (CA), а также задачи по настройке функций создания и проверки подписей объектов. Ко второй группе относятся задачи по настройке системы iSeries B для проверки подписей объектов, созданных в системе iSeries A.

Задачи по настройке iSeries A

Выполните перечисленные задачи в системе iSeries A для настройки локальной CA и создания и проверки подписей объектов:

1. Установите все необходимые продукты iSeries, указанные в предварительных требованиях.

2. С помощью Диспетчера цифровых сертификатов (DCM) создайте локальную сертификатную компанию (CA) для выдачи сертификата, который будет применяться для создания подписей объектов.
3. С помощью DCM создайте определение приложения.
4. С помощью DCM назначьте сертификат определению приложения, предназначенного для создания подписей объектов.
5. С помощью DCM подпишите объекты программ cgi-bin.
6. С помощью DCM экспортируйте сертификаты, которые необходимы другим системам для проверки подписей объектов. Нужно экспортировать в файл копию сертификата локальной CA, а также копию сертификата подписи объекта в качестве сертификата проверки подписи.
7. Отправьте файлы с сертификатами на внешний сервер iSeries фирмы (iSeries B). Это даст возможность проверять подписи, созданные в системе iSeries A.

Задачи по настройке iSeries B

Если вы планируете восстановить подписанные объекты, переданные на внешний Web-сервер (iSeries B), то перед передачей этих объектов в iSeries B необходимо настроить функцию проверки подписей. Проверка подписей выполняется при восстановлении подписанных объектов на внешнем Web-сервере.

Для настройки функции проверки подписей объектов в этом сценарии необходимо выполнить следующие задачи в системе iSeries B:

8. С помощью Диспетчера цифровых сертификатов (DCM) создайте хранилище сертификатов *SIGNATUREVERIFICATION.
9. С помощью DCM импортируйте сертификат локальной CA и сертификат проверки подписей.
10. С помощью DCM проверьте подписи переданных объектов.

Сведения о настройке

Для создания подписей объектов с помощью Диспетчера цифровых сертификатов необходимо выполнить следующие действия по настройке.

Шаг 1: Выполните все предварительные требования

Перед выполнением задач по настройке для реализации данного сценария необходимо установить все необходимые продукты iSeries, перечисленные в предварительных требованиях.

Шаг 2: Создайте локальную сертификатную компанию для получения сертификата подписи объекта

При создании локальной сертификатной компании (CA) с помощью Диспетчера цифровых сертификатов (DCM) необходимо заполнить ряд форм. Эти формы позволят вам создать CA и выполнить другие задачи, необходимые для применения цифровых сертификатов в SSL, а также при создании и проверке подписей объектов. Хотя в этом сценарии не требуется настраивать сертификаты для SSL, для создания подписей в системе необходимо заполнить все формы.

Для создания локальной CA с помощью DCM и работы с ней выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать сертификатную компанию (CA)**. Будет показано несколько форм.

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

3. Заполните все необходимые формы. После этого выполните следующие действия:
   a. Укажите идентификационную информацию для локальной CA.
   b. Установите сертификат локальной CA в браузере, чтобы программы распознавали эту сертификатную компанию и принимали сертификаты, выданные локальной CA.
   c. Задайте стратегию для локальной CA.
   d. С помощью локальной CA создайте сертификат клиента или сервера, с помощью которого приложения будут устанавливать соединения SSL.

      Примечание: Хотя в этом сценарии такой сертификат не применяется, его необходимо создать для того, чтобы локальная CA могла выдать сертификат подписи объекта. Если вы не создадите такой сертификат, вам потребуется по отдельности создать сертификат подписи объекта и его хранилище *OBJECTSIGNING.
   e. Выберите приложения, которые будут с помощью сертификата клиента или сервера устанавливать соединение SSL.

      Примечание: В этом сценарии не нужно выбирать никакие приложения. Нажмите кнопку **Продолжить** для перехода к следующей форме.
   f. С помощью локальной CA создайте сертификат подписи объекта, который будет применяться приложениями для создания цифровых подписей объектов. При этом будет создано хранилище сертификатов *OBJECTSIGNING. Это хранилище применяется для работы с сертификатами подписи объекта.
   g. Выберите приложения, которые будут принимать сертификаты локальной CA.

      Примечание: В этом сценарии не нужно выбирать никакие приложения. Нажмите кнопку **Продолжить** для завершения задачи.

После создания сертификата локальной CA и сертификата подписи объекта необходимо определить приложение, которое будет применяться для создания подписей объектов с помощью сертификата.

Шаг 3: Создайте определение приложения для подписания объектов

После создания сертификата подписи объекта воспользуйтесь Диспетчером цифровых сертификатов (DCM) для определения приложения, которое будет применяться для создания подписей объектов. Определение приложения не обязательно должно быть связано с реальным приложением. Оно содержит информацию о типе или группе объектов, которые вы планируете подписывать. Определение необходимо для того, чтобы с сертификатом можно было связать ИД приложения.

Для создания определения приложения, служащего для подписания объектов, выполните следующие действия с помощью DCM:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
2. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании хранилища сертификатов, и нажмите кнопку **Продолжить**.
3. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
4. В списке задач выберите **Добавить приложение**. Будет показана форма определения приложения.
5. Заполните форму и нажмите кнопку **Добавить**.

Теперь необходимо связать созданное приложение с сертификатом подписи объекта.

Шаг 4: Назначьте сертификат определению приложения, служащего для подписания объектов

Для того чтобы связать сертификат с определением приложения, предназначенного для создания подписей объектов, выполните следующие действия:

1. В окне навигации DCM выберите категорию **Управление сертификатами** для просмотра списка задач.
2. В списке задач выберите **Назначить сертификат**. Появится список сертификатов из текущего хранилища сертификатов.
3. Выберите сертификат в списке и нажмите кнопку **Назначить приложениям**. Появится список определений приложений, связанных с текущим хранилищем сертификатов.
4. Выберите одно или несколько приложений в списке и нажмите кнопку **Продолжить**. Появится сообщение, запрашивающее подтверждение назначения сертификата, либо сообщение с информацией об ошибке.

После выполнения этой задачи вы можете подписать объекты программ, которые будут применяться внешним Web-сервером фирмы (iSeries B), с помощью DCM.

Шаг 5: Подпишите объекты программ

Для того чтобы с помощью DCM подписать объекты программ, которые будут применяться на внешнем Web-сервере фирмы (iSeries B), выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
2. Введите пароль для хранилища сертификатов *OBJECTSIGNING и нажмите **Продолжить**.
3. После обновления информации в окне навигации выберите **Управление доступными объектами** для просмотра списка задач.
4. В списке задач выберите **Подписать объект**. Будет показан список определений приложений, позволяющих подписать объект.
5. Выберите приложение, которое было определено на предыдущем этапе, и нажмите кнопку **Подписать объект**. Появится окно, в котором можно задать расположение объектов, которые необходимо подписать.
6. Введите полное имя файла объекта или имя каталога объектов, которые нужно подписать, и нажмите кнопку **Продолжить**. При необходимости введите имя каталога и нажмите кнопку **Обзор** для выбора объектов в списке содержимого каталога.

   Примечание: Во избежание ошибок полное имя объекта следует начинать с косой черты. Для того чтобы выбрать часть объектов каталога, можно указать символы подстановки. К таким символам относится звездочка (*****), заменяющая *любое число символов*, и знак вопроса (**?**), заменяющий *один 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 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. Строки, относящиеся к текущему заданию, можно определить 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 подписания объектов и нажмите кнопку **Продолжить**. Для того чтобы выбрать файл для записи результатов в списке содержимого каталога, введите имя каталога и нажмите кнопку **Обзор**. Появится сообщение о том, что задание подписания объектов передано на выполнение. Результаты можно просмотреть в протоколе задания **QOBJSGNBAT**.

Для того чтобы вы или другие пользователи могли проверять подписи, экспортируйте необходимые сертификаты в файл и передайте этот файл в систему iSeries B. Перед передачей подписанных объектов программ в iSeries B необходимо выполнить все задачи по настройке функции проверки подписей в iSeries B. Подписи проверяются при восстановлении подписанных объектов в iSeries B.

Шаг 6: Экспортируйте сертификаты, необходимые для проверки подписей в iSeries B

Для обеспечения целостности объектов с помощью цифровых подписей необходимо, чтобы у пользователей была возможность проверять цифровые подписи. Для проверки подписей объектов в той системе, в которой были созданы подписи (iSeries A), создайте с помощью DCM хранилище сертификатов *SIGNATUREVERIFICATION. В этом хранилище должна находиться копия сертификата подписи объекта и копия сертификата CA, выдавшей сертификат подписи объекта.

Для того чтобы другие пользователи могли проверять подпись объекта, им необходимо предоставить копию сертификата, с помощью которого была создана эта подпись. Если сертификат был выдан локальной сертификатной компанией (CA), то этим пользователям также необходимо предоставить сертификат локальной CA.

Для проверки подписей с помощью DCM в той системе, в которой эти подписи были созданы (в данном сценарии - в iSeries A), выполните следующие действия:

1. В окне навигации выберите опцию **Создать хранилище сертификатов** и выберите для создания хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. Нажмите кнопку **Да**, для того чтобы существующие сертификаты подписей объектов были скопированы в новое хранилище в качестве сертификатов проверки подписей.
3. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Теперь вы можете проверить подписи объектов с помощью DCM в той системе, в которой эти подписи были созданы.

Для того чтобы экспортировать копию сертификата локальной CA, а также копию сертификата подписи объекта в качестве сертификата проверки подписи в другие системы (iSeries B), выполните следующие действия:

1. В окне навигации выберите категорию **Управление сертификатами**, а затем выберите задачу **Экспортировать сертификат**.
2. Выберите **сертификатную компанию (CA)** и нажмите кнопку **Продолжить**. Появится список сертификатов CA, которые можно экспортировать.
3. Выберите в списке сертификат локальной CA и нажмите кнопку **Экспортировать**.
4. Укажите в качестве целевого расположения **Файл** и нажмите кнопку **Продолжить**.
5. Укажите полное имя файла для экспорта сертификата локальной CA и нажмите кнопку **Продолжить**.
6. Нажмите кнопку **OK**, чтобы закрыть окно подтверждения экспорта. Теперь можно экспортировать копию сертификата подписи объекта.
7. Снова выберите задачу **Экспортировать сертификат**.
8. Выберите опцию **Подписи объектов** . Появится список сертификатов подписей объектов, которые можно экспортировать.
9. Выберите сертификат подписи объекта в списке и нажмите кнопку **Экспортировать**.
10. Выберите опцию **Файл, сертификат проверки подписи** и нажмите кнопку **Продолжить**.

11. Укажите полное имя файла для экспорта сертификата подписи объекта и нажмите кнопку **Продолжить**.

Теперь файлы с сертификатами можно передать в конечные системы iSeries для проверки подписей.

Шаг 7: Передайте файлы сертификатов на внешний сервер iSeries B

Перед проверкой подписей объектов необходимо передать файлы сертификатов, созданные в iSeries A, на сервер iSeries B - внешний Web-сервер фирмы. Файлы сертификатов можно передать несколькими способами. Например, для этого можно воспользоваться FTP или функцией рассылки пакетов Централизованного управления.

Шаг 8: Задачи проверки подписей - Создайте хранилище сертификатов *SIGNATUREVERIFICATION

Для проверки подписей объектов в iSeries B (на внешнем Web-сервере фирмы) необходимо, чтобы в хранилище сертификатов *SIGNATUREVERIFICATION сервера iSeries B была копия сертификата проверки подписей. Поскольку для создания подписей объектов применялся сертификат, выданный локальной CA, в этом хранилище сертификатов также должна находиться копия сертификата локальной CA.

Для создания хранилища сертификатов *SIGNATUREVERIFICATION выполните следующие действия:

1. Запустите DCM.
2. В окне навигации Диспетчера цифровых сертификатов (DCM) выберите опцию **Создать хранилище сертификатов**, а затем выберите для создания хранилище ***SIGNATUREVERIFICATION**.

   Примечание: Для просмотра информации о заполнении полей формы при работе с DCM нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Теперь вы можете импортировать в хранилище сертификаты, необходимые для проверки подписей объектов.

Шаг 9: Задачи проверки подписей - Импортируйте сертификаты

Для проверки подписи объекта необходимо, чтобы в хранилище сертификатов *SIGNATUREVERIFICATION была копия сертификата проверки подписи. Если сертификат подписи является частным, то в хранилище также должна быть копия сертификата локальной сертификатной компании, выдавшей сертификат подписи. В данном сценарии оба сертификата были экспортированы в файл и переданы в конечные системы iSeries.

Для того чтобы импортировать эти сертификаты в хранилище *SIGNATUREVERIFICATION, выполните следующие действия:

1. В окне навигации DCM выберите задачу **Выбрать хранилище сертификатов**. После этого выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании хранилища сертификатов, и нажмите кнопку **Продолжить**.
3. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
4. В списке задач выберите **Импортировать сертификат**.
5. Выберите в качестве типа сертификата значение **Сертификатная компания (CA)** и нажмите кнопку **Продолжить**.

Примечание: Сертификат локальной CA нужно импортировать до частного сертификата подписи. В противном случае вам не удастся импортировать сертификат подписи.

6. Укажите полное имя файла, содержащего сертификат CA, и нажмите кнопку **Продолжить**. Появится сообщение о завершении импорта или сообщение с информацией об ошибке.
7. Снова выберите задачу **Импортировать сертификат**.
8. Выберите в качестве типа импортируемого сертификата **Проверка подписи** и нажмите кнопку **Продолжить**.
9. Укажите полное имя файла, содержащего сертификат проверки подписи, и нажмите кнопку **Продолжить**. Появится сообщение о завершении импорта или сообщение с информацией об ошибке.

Теперь с помощью DCM системы iSeries B можно проверить подписи объектов, созданные на основе соответствующего сертификата в iSeries A.

Шаг 10: Задачи проверки подписи - Проверьте подпись объектов программ

Для проверки подписи переданных объектов программ с помощью DCM выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. Введите пароль для хранилища сертификатов *SIGNATUREVERIFICATION и нажмите **Продолжить**.
3. После обновления информации в окне навигации выберите **Управление доступными объектами** для просмотра списка задач.
4. В списке задач выберите **Проверить подпись объекта**, чтобы задать расположение проверяемых объектов.
5. В появившемся поле введите полное имя файла объекта или имя каталога объектов, подписи которых нужно проверить, и нажмите кнопку **Продолжить**. При необходимости можно ввести имя каталога и нажать кнопку **Обзор**, чтобы просмотреть содержимое каталога и выбрать объекты, подписи которых нужно проверить.

   Примечание: Для того чтобы выбрать часть объектов каталога, можно указать символы подстановки. К таким символам относится звездочка (*****), заменяющая *любое число символов*, и знак вопроса (**?**), заменяющий *один 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**.
6. Выберите необходимые опции проверки подписи 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. Строки, относящиеся к текущему заданию, можно определить 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).
7. Укажите полное имя файла для записи результатов операции проверки подписи объекта и нажмите кнопку **Продолжить**. Вы можете также ввести имя 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**.

Сценарий: Создание и проверка подписей объектов с помощью API

Описание

Ваша фирма (MyCo, Inc.) является деловым партнером iSeries и занимается разработкой приложений для заказчиков. Занимая должность разработчика программного обеспечения в этой фирме, вы отвечаете за создание пакетов приложений для их последующей рассылки заказчикам. В настоящий момент для создания пакетов приложений применяется специальная программа. Заказчики могут получить приложение на компакт-диске (CD-ROM) или загрузить его с Web-сайта.

Вы периодически знакомитесь с новостями, связанными с компьютерными технологиями, в том числе с новостями из области средств защиты. Вам известно о том, что заказчики хотят иметь полную информацию об источнике и содержимом программ, которые они получают и загружают. Иногда заказчики загружают продукты из ненадежных источников, думая, что это надежные и проверенные источники. Это приводит к тому, что заказчик устанавливает не тот продукт, который ему был нужен. Установленный продукт может оказаться вредоносной программой или программой, которая изменяет конфигурацию или повреждает данные системы.

Хотя заказчики iSeries редко сталкиваются с такими проблемами, вы хотите дать им возможность проверять, что полученные приложения действительно созданы вашей фирмой. Кроме того, вы хотите дать возможность заказчикам проверять целостность приложений. В этом случае перед установкой приложения заказчик сможет проверить, что приложение не было изменено.

Для достижения поставленных целей вы решили использовать функции для работы с подписями объектов, предусмотренные в OS/400. Создание цифровых подписей для приложений позволит заказчикам проверять, что источником полученного или загруженного приложения действительно является ваша фирма. Поскольку для создания пакетов приложений применяется специальная программа, вы решили добавлять подписи с помощью API во время создания пакетов. Кроме того, для создания подписей объектов вы решили использовать глобальный сертификат, для того чтобы заказчикам не нужно было выполнять никаких специальных действий для проверки подписи при установке продукта.

Во время создания пакета приложений в него будет добавляться цифровой сертификат, применявшийся для создания подписи объекта. В этом случае заказчик сможет проверить подпись полученного приложения с помощью общего ключа этого сертификата. При этом он сможет идентифицировать источник приложения и проверить, что содержимое объектов приложения не было изменено с момента их подписания.

В этом примере рассмотрен программный способ создания подписей для приложений, предназначенных для других пользователей.

Достоинства сценария

У этого сценария есть следующие достоинства:

- Применение API для программной упаковки и подписи объектов позволяет экономить время, необходимое для реализации данного способа защиты.
- Создание подписи для пакета объектов позволяет проще определить, были ли объекты изменены после их подписания. В будущем это позволит значительно сократить время, которое потребуется заказчикам для устранения некоторых неполадок приложений.

- Создание подписей с помощью сертификата, выданного глобальной сертификатной компанией (CA), позволяет использовать в программе выхода из процедуры установки продукта API Добавить сертификат для проверки. Этот API добавляет глобальный сертификат, применявшийся для создания подписи приложения, в систему заказчика. Таким образом, заказчику не потребуется выполнять никаких специальных действий для проверки подписи.

Цели

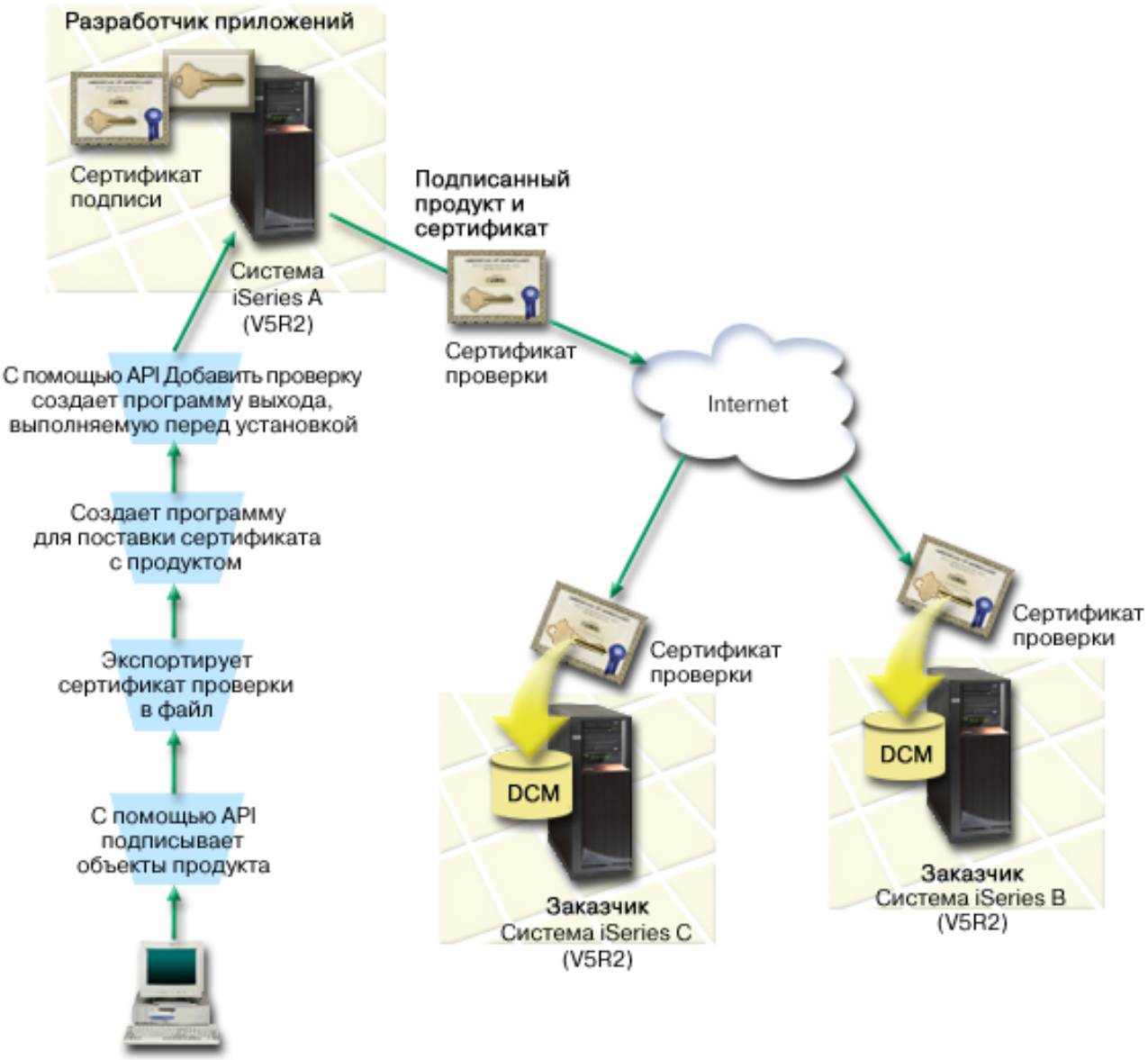
В данном сценарии фирма MyCo, Inc. планирует программным образом подписывать собственные приложения, которые объединяются в пакеты и рассылаются заказчикам. Являясь разработчиком приложений в фирме MyCo, Inc., вы отвечаете за создание пакетов приложений для их последующей рассылки заказчикам. Пакеты приложений создаются с помощью специальной программы. Для создания подписей приложений планируется применять API iSeries, для того чтобы заказчики iSeries могли программным образом проверить подпись при установке продукта.

В этом сценарии преследуются следующие цели:

- Разработчик приложений фирмы должен создавать подписи объектов в программе, формирующей пакеты приложений, с помощью API Подписать объект.
- Приложения фирмы должны быть подписаны с помощью глобального сертификата, для того чтобы во время установки приложения заказчику не нужно было выполнять никаких специальных действий для проверки подписи.
- У фирмы должна быть возможность применять API iSeries, для того чтобы программным образом добавлять необходимый сертификат проверки подписи в хранилище сертификатов *SIGNATUREVERIFICATION сервера iSeries заказчика. Если это хранилище не существует на сервере iSeries заказчика, оно должно быть создано во время установки продукта.
- У заказчиков должна быть возможность быстро проверить цифровую подпись приложения фирмы после установки продукта. Это даст возможность заказчику идентифицировать источник подписанного приложения и определить, было ли приложение изменено с момента его подписания.

Дополнительные сведения

На следующем рисунке показан процесс создания и проверки подписей объектов в данном сценарии:



На рисунке показаны следующие системы, рассмотренные в данном сценарии:

Центральная система (iSeries A)

- В системе iSeries A установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- В iSeries A установлена программа создания пакетов продуктов.
- В системе iSeries A установлен продукт Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- В системе iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 OS/400) и IBM HTTP Server (5722–DG1).
- В iSeries A создаются подписи для всех объектов приложений фирмы. Для создания подписей объектов, предназначенных для последующей рассылки заказчикам, в iSeries A выполняются следующие задачи:
  1. С помощью API создаются подписи для приложений фирмы.
  2. С помощью DCM сертификат проверки подписи экспортируется в файл, для того чтобы заказчики могли проверить подписи объектов.

3. Создается программа для добавления сертификата проверки подписи в подписанное приложение.
4. Создается программа выхода, вызываемая перед установкой продукта, в которой используется API Добавить сертификат для проверки. Этот API позволяет добавить сертификат проверки подписи в хранилище сертификатов *SIGNATUREVERIFICATION на сервере iSeries заказчика (iSeries B и C) во время установки продукта.

Серверы заказчиков (iSeries B и C)

- В системе iSeries B установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- В системе iSeries C установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- В системах iSeries B и C установлен и настроен Диспетчер цифровых сертификатов (компонент 34) и IBM HTTP Server (5722–DG1).
- Пользователи систем iSeries B и C приобрели приложение и загрузили его с Web-сайта фирмы, разработавшей это приложение (этой фирме принадлежит система iSeries A).
- Во время установки продукта в системах iSeries B и C было создано хранилище сертификатов *SIGNATUREVERIFICATION. При этом в системы был скопирован сертификат проверки подписи фирмы MyCo.

Предварительные требования

Для реализации этого сценария должны быть выполнены следующие требования:

1. На всех серверах iSeries должны быть выполнены требования к установке и применению Диспетчера цифровых сертификатов (DCM).

   Примечание: Для серверов заказчиков (в данном сценарии - серверов iSeries B и C) это требование не является обязательным. Если во время установки продукта требуется создать хранилище сертификатов *SIGNATUREVERIFICATION, API Добавить сертификат для проверки создает его с паролем по умолчанию. Для ограничения доступа к этому хранилищу сертификатов заказчику потребуется изменить пароль с помощью DCM.
2. Приложение DCM ранее не настраивалось и не применялось ни на одном сервере iSeries.
3. На всех серверах iSeries установлена последняя версия программы Cryptographic Access Provider 128-bit (5722-AC3).
4. На всех серверах iSeries системному значению Проверять подписи объектов при восстановлении (QVFYOBJRST) присвоено значение по умолчанию (3). Это значение разрешает серверу проверять подписи объектов при их восстановлении.
5. У администратора сети iSeries A должны быть специальные права доступа *ALLOBJ, для того чтобы он мог подписывать объекты, либо у него должны быть права на работу с приложением, применяемым для подписания объектов.
6. У администратора системы и других пользователей (в том числе программ), отвечающих за создание хранилищ сертификатов в DCM, должны быть специальные права доступа *SECADM и *ALLOBJ.
7. На всех остальных серверах iSeries администратору системы и другим пользователям, планирующим проверять подписи объектов, должны быть предоставлены специальные права доступа *AUDIT.

Задачи

Для создания подписей объектов в соответствии с данным сценарием выполните следующие задачи в системе iSeries A:

1. Установите и настройте все необходимые продукты iSeries, перечисленные в предварительных требованиях.
2. С помощью DCM создайте запрос для получения сертификата подписи объекта от глобальной сертификатной компании (CA).
3. С помощью DCM создайте определение приложения, предназначенного для создания подписей объектов.
4. С помощью DCM импортируйте сертификат подписи объекта и назначьте его определению приложения, предназначенного для создания подписей объектов.
5. С помощью DCM экспортируйте сертификат подписи объекта в качестве сертификата проверки подписи, для того чтобы заказчики могли с его помощью проверить подписи объектов приложения.
6. Измените программу создания пакетов приложений таким образом, чтобы перед рассылкой пакета заказчикам в продукт добавлялся файл сертификата проверки подписи, а приложение подписывалось с помощью API Подписать объект.
7. Создайте программу выхода, запускаемую перед установкой, которая вызывает API Добавить сертификат для проверки в ходе установки продукта. С помощью этой программы выхода во время установки продукта на сервере iSeries заказчика можно создать хранилище сертификатов *SIGNATUREVERIFICATION и добавить в него сертификат проверки подписей.
8. Проинструктируйте заказчиков, что они должны запустить DCM и сбросить пароль по умолчанию, установленный для хранилища сертификатов *SIGNATUREVERIFICATION на их сервере iSeries.

Сведения о настройке

Для создания подписей объектов с помощью API OS/400 необходимо выполнить следующие действия.

Шаг 1: Выполните все предварительные требования

Перед выполнением задач по настройке для реализации данного сценария необходимо установить и настроить все продукты iSeries, перечисленные в предварительных требованиях.

Шаг 2: С помощью DCM получите сертификат у глобальной CA

В этом сценарии предполагается, что Диспетчер цифровых сертификатов (DCM) ранее не применялся для создания сертификатов и работы с ними. В связи с этим перед созданием сертификата подписи объекта необходимо создать хранилище сертификатов *OBJECTSIGNING. После создания этого хранилища сертификатов вы сможете выполнять любые задачи по созданию сертификатов подписи объекта и управления ими. Для получения сертификата у глобальной сертификатной компании (CA) необходимо создать в DCM идентификационную информацию, а также общий и личный ключ, и передать эти сведения глобальной CA.

Для создания запроса на получение сертификата подписи объекта, который требуется передать глобальной CA, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите опцию **Создать хранилище сертификатов**. Эта опция позволяет выполнить пошаговую процедуру, заполнив несколько форм. Выполните приведенные инструкции по созданию хранилища сертификатов и сертификата, с помощью которых приложения смогут добавлять подписи к объектам.

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

4. Выберите значение **Да**, чтобы создать сертификат вместе с хранилищем сертификатов *OBJECTSIGNING, и нажмите кнопку **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 идентификационную информацию для нового сертификата.
6. Заполните форму и нажмите кнопку **Продолжить**. Будет показана страница подтверждения. Она содержит данные о сертификате, которые необходимо предоставить глобальной сертификатной компании для получения сертификата. Эти данные называются данными Запроса на подписание сертификата (CSR). Они 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 глобальной сертификатной компании. Необходимо скопировать все данные CSR, включая строки Begin и End New Certificate Request. После завершения работы с этой страницей данные будут потеряны. Их нельзя будет восстановить.
8. Отправьте форму запроса или файл в выбранную сертификатную компанию.
9. Подождите, пока CA вернет подписанный сертификат, а затем перейдите к следующему шагу задачи.

Шаг 3: Создайте определение приложения для подписания объектов

После того как вы отправите запрос глобальной CA для получения сертификата, создайте в DCM определение приложения, служащего для подписания объектов. Определение приложения не обязательно должно быть связано с реальным приложением. Оно содержит информацию о типе или группе объектов, которые вы планируете подписывать. Определение необходимо для того, чтобы с сертификатом можно было связать ИД приложения.

Для создания определения приложения, служащего для подписания объектов, с помощью DCM выполните следующие действия:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
2. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании хранилища сертификатов, и нажмите кнопку **Продолжить**.
3. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
4. В списке задач выберите **Добавить приложение**. Будет показана форма определения приложения.
5. Заполните форму и нажмите кнопку **Добавить**.

После получения подписанного сертификата от CA вы можете назначить этот сертификат созданному приложению.

Шаг 4: Импортируйте подписанный глобальный сертификат и назначьте его приложению для подписания объектов

Для того чтобы импортировать сертификат и назначить его приложению, служащему для создания подписей, выполните следующие действия:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
3. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании 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 опцию **Импортировать сертификат**, чтобы начать импорт подписанного сертификата в хранилище сертификатов.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
6. Выберите в списке задач **Управление сертификатами** опцию **Назначить сертификат**. Появится список сертификатов из текущего хранилища сертификатов.
7. Выберите сертификат в списке и нажмите кнопку **Назначить приложениям**. Появится список определений приложений, связанных с текущим хранилищем сертификатов.
8. Выберите приложение в списке и нажмите кнопку **Продолжить**. Появится сообщение с подтверждением или сообщение об ошибке.

После выполнения этой задачи можно подписать приложения и другие объекты с помощью API OS/400. Для того чтобы обеспечить возможность проверки подписей, необходимо экспортировать сертификаты в файл и передать их серверам iSeries, на которых будет установлено подписанное приложение. После этого серверам iSeries заказчиков необходимо предоставить возможность проверить подпись приложения во время его установки с помощью переданного сертификата. Для настройки функции проверки подписей во время установки приложения можно вызвать API Добавить сертификат для проверки. Например, вы можете создать программу выхода, запускаемую перед установкой, которая вызывает API Добавить сертификат для проверки на сервере iSeries заказчика.

Шаг 5: Экспортируйте сертификаты для проверки подписей на других серверах iSeries

Для обеспечения целостности объектов с помощью цифровых подписей необходимо, чтобы у пользователей была возможность проверять цифровые подписи. Для проверки подписей объектов в той системе, в которой были созданы эти подписи, необходимо создать хранилище сертификатов *SIGNATUREVERIFICATION с помощью DCM. В этом хранилище должна находиться копия сертификата подписи объекта и копия сертификата CA, выдавшей сертификат подписи объекта.

Для того чтобы другие пользователи могли проверять подпись объекта, им необходимо предоставить копию сертификата, с помощью которого была создана эта подпись. Если сертификат был выдан локальной сертификатной компанией (CA), то этим пользователям также необходимо предоставить сертификат локальной CA.

Для проверки подписей с помощью DCM в той системе, в которой эти подписи были созданы (в данном сценарии - в iSeries A), выполните следующие действия:

1. В окне навигации выберите опцию **Создать хранилище сертификатов** и выберите для создания хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. Нажмите кнопку **Да**, для того чтобы существующие сертификаты подписей объектов были скопированы в новое хранилище в качестве сертификатов проверки подписей.
3. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Теперь вы можете проверить подписи объектов с помощью DCM в той системе, в которой эти подписи были созданы.

Для того чтобы экспортировать копию сертификата подписи объекта в качестве сертификата проверки подписей с помощью DCM, выполните следующие действия:

1. В окне навигации выберите категорию **Управление сертификатами**, а затем выберите задачу **Экспортировать сертификат**.
2. Выберите опцию **Подписи объектов** . Появится список сертификатов подписей объектов, которые можно экспортировать.

3. Выберите сертификат подписи объекта в списке и нажмите кнопку **Экспортировать**.
4. Выберите опцию **Файл, сертификат проверки подписи** и нажмите кнопку **Продолжить**.
5. Укажите полное имя файла для экспорта сертификата подписи объекта и нажмите кнопку **Продолжить**.

Теперь вы можете добавить этот файл в установочный пакет приложения. Путем вызова API Добавить сертификат для проверки из программы установки этот сертификат можно добавить в хранилище сертификатов *SIGNATUREVERIFICATION системы заказчика. Если это хранилище не существует, оно будет создано API. В результате программа установки продукта сможет проверить подписи объектов приложения во время их восстановления на сервере iSeries заказчика.

Шаг 6: Добавьте API iSeries для создания подписи приложения в программу, формирующую пакет приложения

После добавления файла с сертификатом проверки подписи в пакет приложения можно добавить API Подписать объект в существующую программу создания пакетов приложений, предназначенных для рассылки заказчикам. Этот API создаст подписи для библиотек продукта.

Для того чтобы лучше понять, каким образом следует использовать API Подписать объект в программе, создающей пакеты приложений, ознакомьтесь с приведенным ниже фрагментом программы. Этот пример, написанный на языке C, не является полноценной программой, создающей подписи и формирующей пакет программ. Он содержит лишь фрагмент кода программы, в котором вызывается API Подписать объект. Вы можете использовать этот фрагмент в собственной программе, изменив его соответствующим образом. По соображениям защиты специалисты фирмы IBM рекомендуют изменить значения по умолчанию, использованные в этом примере.

Примечание: IBM предоставляет вам неисключительную лицензию на использование всех примеров кода программ, на основе которых можно разработать аналогичные функции. Все фрагменты коды приведены фирмой IBM только в качестве примера. Эти примеры не прошли тщательного и всестороннего тестирования. В связи с этим, фирма IBM не гарантирует и не подразумевает, что эти программы правильно работают и не содержат ошибок. Все приведенные здесь программы предоставляются на условиях ″КАК ЕСТЬ″ без каких-либо гарантий. В том числе, фирма IBM отказывается от предоставления неявных гарантий соблюдения авторских прав, коммерческой ценности или пригодности для какой-либо цели.

Измените этот фрагмент кода, демонстрирующий применение API Подписать объект, и добавьте его в свою программу создания пакетов продуктов. Данной программе передается два параметра: имя библиотеки, которую нужно подписать, и ИД приложения, служащего для создания подписей объектов. В ИД приложения учитывается регистр символов, а в имени библиотеки - нет. В вашей программе этот фрагмент кода может вызываться несколько раз для подписания различных библиотек, входящих в состав продукта.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Применение API Подписать объект для подписания библиотек         */
/*                                                                  */
/* API создаст цифровые подписи для всех объектов из библиотеки     */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Ниже вашему вниманию предлагается исходный код программы.       */
/* Этот пример программы не был тщательно и всесторонне            */
/* протестирован. В связи с этим, фирма IBM не гарантирует          */
/* и не подразумевает, что эта программа правильно работает и      */
/* не содержит ошибок. Все приведенные здесь программы              */
```

```
/* предоставляются "КАК ЕСТЬ". ФИРМА IBM ОТКАЗЫВАЕТСЯ ОТ            */
/* ПРЕДОСТАВЛЕНИЯ НЕЯВНЫХ ГАРАНТИЙ КОММЕРЧЕСКОЙ ЦЕННОСТИ И          */
/* ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. Предложения фирмы IBM по        */
/* обслуживанию программ не относятся к этим программам и файлам.   */
/*                                                                   */
/*                                                                   */
/*                                                                   */
/* Параметры:                                                        */
/*                                                                   */
/*  char *   имя библиотеки, которую нужно подписать                 */
/*  char *   имя ИД приложения                                       */
/*                                                                   */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* параметры:

       char * библиотека, в которой нужно подписать объекты,
       char * идентификатор приложения, создающего подпись

     */

    int         lib_length, applid_length, path_length, multiobj_length;
    Qus_EC_t    error_code;
    char        libname[11];
    char        path_name[256];

    Qydo_Multi_Objects_T * multi_objects = NULL;
    multiobj_length = 0;
    error_code.Bytes_Provided = 0;    /* в случае ошибки возвращается код исключительной ситуации */


    /* ------------------------------------ */
    /* создание пути к заданной библиотеке  */
    /* ------------------------------------ */
    memset(libname, '\00', 11); /* инициализация имени библиотеки */
    for(lib_length = 0;
        ((*(argv[1] + lib_length) != ' ') &&
         (*(argv[1] + lib_length) != '\00'));
        lib_length++);
    memcpy(argv[1], libname, lib_length); /* копирование имени библиотеки */

    /* создание параметра пути для вызова API */
    sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
    path_length = strlen(path_name);

    /* ---------------------------- */
    /* подсчет длины ИД приложения */
    /* ---------------------------- */
    for(applid_length = 0;
        ((*(argv[2] + applid_length) != ' ') &&
         (*(argv[2] + applid_length) != '\00'));
        applid_length++);

    /* ------------------------------- */
    /* создание подписей для всех объектов библиотеки */
    /* ------------------------------- */
    QYDOSGNO  (path_name,             /* путь к объекту  */
               &path_length,          /* длина пути  */
               "OBJN0100",            /* имя формата  */
               argv[2],               /* ИД приложения */
```

```
                &applid_length,        /* длина ИД приложения  */
                "1",                   /* замена дубликата подписи */
                multi_objects,         /* способ обработки нескольких
                                             объектов */
                &multiobj_length,      /* размер применяемой структуры
                                           нескольких объектов
                                          (0=не применять такую структуру)*/
                &error_code);          /* код ошибки */


        return 0;

}
```

Шаг 7: Создайте программу выхода из процедуры установки, вызывающую API Добавить сертификат для проверки

Создав программу для подписания приложений, можно добавить в программу установки API Добавить сертификат для проверки. После этого продукт будет готов к рассылке. Например, API может вызываться в программе выхода, которая запускается до установки. В этом случае сертификат будет добавлен в хранилище сертификатов до того, как начнется восстановление подписанных объектов приложения. В результате программа установки сможет проверить подписи объектов приложения во время их восстановления на сервере iSeries заказчика.

Примечание: По соображениям защиты с помощью этого API в хранилище сертификатов *SIGNATUREVERIFICATION нельзя добавить сертификат Сертификатной компании (CA). После добавления сертификата CA в хранилище сертификатов система считает эту CA уполномоченной компанией по выдаче сертификатов. Другими словами, сертификаты, выданные этой CA, считаются надежными. Указанное ограничение введено для того, чтобы нельзя было создать программу выхода из процедуры установки, которая добавляет сертификат CA в хранилище сертификатов с помощью этого API. Сертификаты CA следует добавлять в хранилище сертификатов с помощью Диспетчера цифровых сертификатов. Это дает возможность назначить администратора, который будет самостоятельно определять, какие CA можно считать надежными. В этом случае в систему можно будет импортировать только те сертификаты, которые администратор явно указал как надежные.

Если вы не хотите, чтобы этот API применялся без вашего ведома для добавления сертификата подписи объекта в хранилище сертификатов *SIGNATUREVERIFICATION, рекомендуется запретить доступ к этому API в системе. Для этого необходимо запретить изменение системных значений, связанных с защитой, с помощью Системного инструментария (SST).

Для того чтобы лучше понять, каким образом следует использовать API Добавить сертификат для проверки в программе установки приложения, ознакомьтесь с приведенным ниже примером программы выхода, вызываемой перед установкой. Этот пример, написанный на языке C, не является полноценной программой выхода. Он содержит лишь фрагмент кода программы, в котором вызывается API Добавить сертификат для проверки. Вы можете использовать этот фрагмент в собственной программе, изменив его соответствующим образом. По соображениям защиты специалисты фирмы IBM рекомендуют изменить значения по умолчанию, использованные в этом примере.

Примечание: IBM предоставляет вам неисключительную лицензию на использование всех примеров кода программ, на основе которых можно разработать аналогичные функции. Все фрагменты коды приведены фирмой IBM только в качестве примера. Эти примеры не прошли тщательного и всестороннего тестирования. В связи с этим, фирма IBM не гарантирует и не подразумевает, что эти программы правильно работают и не

содержат ошибок. Все приведенные здесь программы предоставляются на условиях ″КАК ЕСТЬ″ без каких-либо гарантий. В том числе, фирма IBM отказывается от предоставления неявных гарантий соблюдения авторских прав, коммерческой ценности или пригодности для какой-либо цели.

Измените этот фрагмент кода, демонстрирующий применение API Добавить сертификат для проверки, и включите его в свою программу выхода, вызываемую перед установкой, для добавления необходимого сертификата проверки подписей на сервер iSeries заказчика.

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Добавление сертификата из указанного файла IFS в хранилище       */
/* *SIGNATUREVERIFICATION с помощью API Добавить сертификат         */
/*                                                                  */
/* API создаст хранилище сертификатов, если оно не существует.      */
/* В этом случае для него будет задан пароль по умолчанию,          */
/* который при первой возможности нужно изменить с помощью DCM.     */
/* Предупредите об этом пользователей системы, которые будут        */
/* работать с этой программой.                                      */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Ниже вашему вниманию предлагается исходный код программы.        */
/* Этот пример программы не был тщательно и всесторонне             */
/* протестирован. В связи с этим, фирма IBM не гарантирует          */
/* и не подразумевает, что эта программа правильно работает и       */
/* не содержит ошибок. Все приведенные здесь программы              */
/* предоставляются "КАК ЕСТЬ". ФИРМА IBM ОТКАЗЫВАЕТСЯ ОТ            */
/* ПРЕДОСТАВЛЕНИЯ НЕЯВНЫХ ГАРАНТИЙ КОММЕРЧЕСКОЙ ЦЕННОСТИ И          */
/* ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. Предложения фирмы IBM по        */
/* обслуживанию программ не относятся к этим программам и файлам.   */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* Параметры:                                                       */
/*                                                                  */
/*  char *   имя файла IFS, содержащего сертификат                  */
/*  char *   метка сертификата                                      */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */

#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

    int         pathname_length, cert_label_length;
    Qus_EC_t    error_code;
    char      * pathname = argv[1];
    char      * certlabel = argv[2];

    /* определение длины имени */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* определение длины метки сертификата */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
```

```
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;    /* в случае ошибки возвращается код исключительной ситуации */

    QydoAddVerifier (pathname,         /* имя файла с сертификатом */
                     &pathname_length, /* длина имени      */
                     "OBJN0100",       /* имя формата           */
                     certlabel,        /* метка сертификата      */
                     &cert_label_length, /* длина метки сертификата    */
                     &error_code);     /* код ошибки                */

    return 0;
}
```

После выполнения описанных задач вы можете создать пакет приложения и разослать его заказчикам. При установке приложения будут проверены подписи его объектов. Позднее заказчики могут проверить подписи объектов приложения с помощью Диспетчера цифровых сертификатов (DCM). Таким образом они могут убедиться, что приложение создано надежным источником, и его содержимое не было изменено с момента создания подписи.

Примечание: Программа установки создаст в системе заказчика хранилище сертификатов *SIGNATUREVERIFICATION, если его еще нет. Посоветуйте заказчикам при первой возможности изменить пароль этого хранилища сертификатов с помощью DCM, чтобы защитить его от несанкционированного доступа.

Шаг 8: Попросите заказчиков сбросить пароль по умолчанию, заданный для хранилища сертификатов *SIGNATUREVERIFICATION

Во время установки продукта на сервере iSeries заказчика вызывается API Добавить сертификат для проверки, который создает хранилище сертификатов *SIGNATUREVERIFICATION, если его еще нет. Для созданного хранилища сертификатов задается пароль по умолчанию. Порекомендуйте своим заказчикам сбросить этот пароль с помощью DCM, чтобы защитить хранилище сертификатов от несанкционированного доступа.

Для этого попросите заказчиков выполнить следующую последовательность действий:

1. Запустите DCM.
2. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.
3. На странице Хранилище сертификатов и пароль нажмите кнопку **Сбросить пароль**. Появится страница Сбросить пароль хранилища сертификатов.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
4. Укажите новый пароль хранилища сертификатов, повторите его ввод, выберите срок действия пароля и нажмите кнопку **Продолжить**.

Сценарий: Создание подписей объектов с помощью Централизованного управления

Описание

Ваша фирма (MyCo, Inc.) разрабатывает приложения, которые рассылаются различным серверам iSeries, принадлежащим этой фирме. Занимая должность администратора сети, вы отвечаете за

установку и обновление этих приложений на всех серверах iSeries фирмы. Для создания и рассылки пакетов приложений, а также для выполнения других административных задач вы применяете функцию Централизованное управление программы Навигатор. Значительное время вам приходится затрачивать на обнаружение и исправление ошибок приложений, связанных с несанкционированным изменением объектов этих приложений. В связи с этим, вы приняли решение обеспечить целостность этих объектов путем создания цифровых подписей.

После изучения возможностей, предусмотренных в OS/400 для работы с подписями объектов, вы узнали, что в выпуске V5R2 функция Централизованное управление позволяет подписывать объекты при создании и рассылке пакетов. Следовательно, с помощью Централизованного управления вы можете просто и эффективно решить поставленную задачу. Для создания подписей объектов вы решили применять сертификат, выданный локальной сертификатной компанией (CA). Для этой цели в системе потребуется создать локальную CA. Использование сертификатов, выданных локальной CA, сокращает расходы по реализации этого способа защиты, так как в этом случае не требуется приобретать сертификат у глобальной CA.

В этом примере рассмотрена настройка и использование подписей объектов приложений, которые рассылаются нескольким корпоративным серверам iSeries.

Достоинства сценария

У этого сценария есть следующие достоинства:

- Применение Централизованного управления для формирования пакетов и создания подписей объектов сокращает время, необходимое для рассылки подписанных объектов корпоративным серверам iSeries.
- Для создания подписей объектов не требуется выполнять отдельную процедуру, так как они создаются с помощью Централизованного управления во время формирования пакета.
- Создание подписи для пакета объектов позволяет проще определить, были ли объекты изменены после их подписания. В будущем это позволит значительно сократить время, которое потребуется для устранения некоторых ошибок приложений.
- Создание подписей объектов с помощью сертификата, выданного локальной сертификатной компанией (CA), значительно сокращает расходы по реализации этого сценария.

Цели

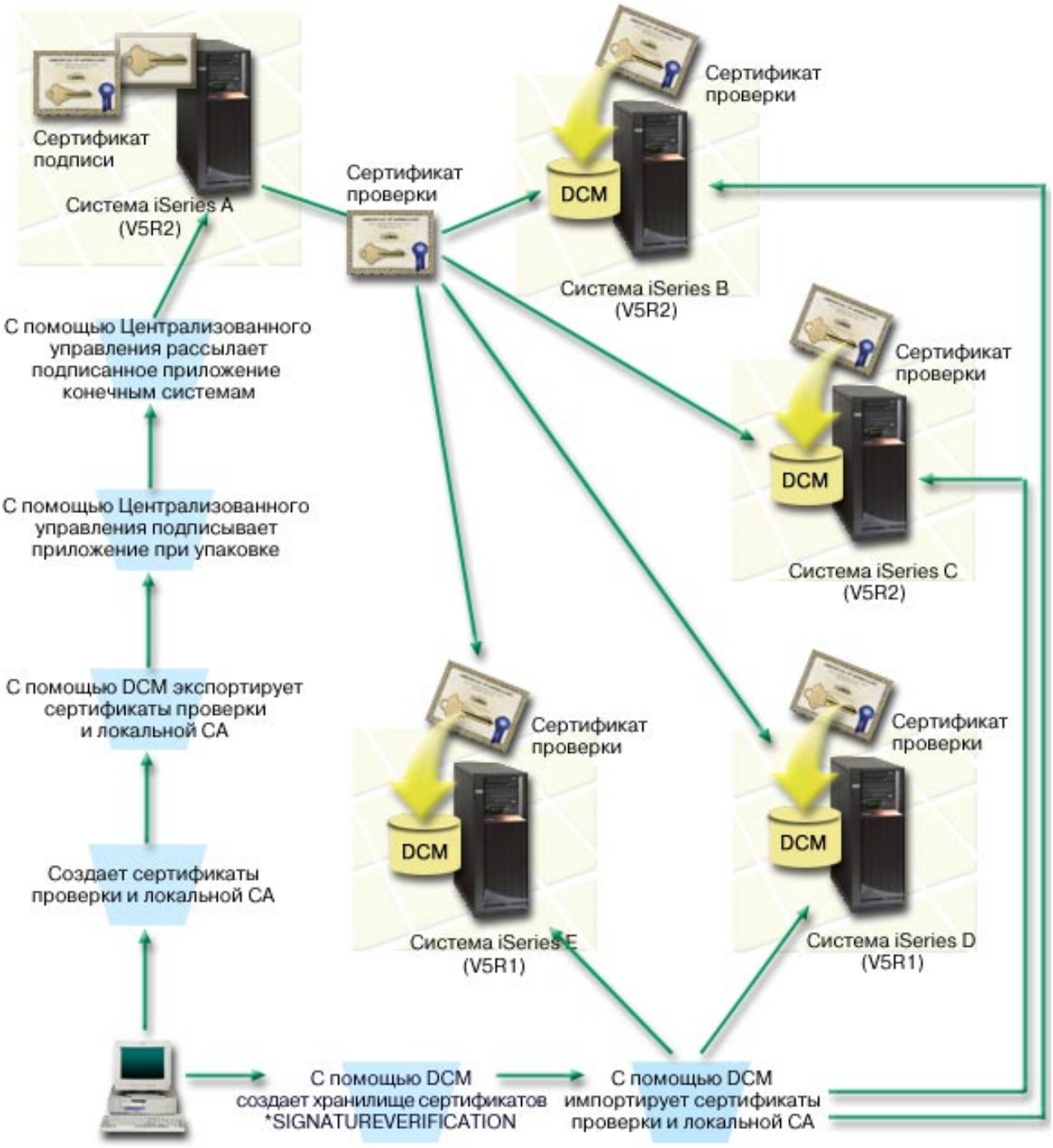
В этом сценарии фирма MyCo, Inc. планирует создавать цифровые подписи для приложений, которые требуется разослать нескольким корпоративным серверам iSeries. В качестве администратора сети фирмы MyCo, Inc. вы уже применяете функцию Централизованное управление для выполнения ряда административных задач в iSeries. Вы планируете воспользоваться возможностями этой функции для создания подписей приложений, которые требуется разослать другим серверам iSeries.

В этом сценарии преследуются следующие цели:

- Приложения фирмы должны быть подписаны с помощью сертификата, выданного локальной CA. Такой сертификат выбран для сокращения расходов по реализации этого сценария.
- У системных администраторов и других уполномоченных пользователей должна быть возможность быстро проверить цифровые подписи на всех серверах iSeries, чтобы идентифицировать источник и проверить подлинность подписанных объектов. Для этого в хранилище сертификатов *SIGNATUREVERIFICATION каждого сервера iSeries необходимо скопировать сертификат проверки подписи фирмы и сертификат локальной сертификатной компании (CA).
- Путем проверки подписей приложений фирмы администраторы систем iSeries и другие пользователи могут убедиться, что объекты не были изменены с момента создания подписи.
- Пакеты приложений должны создаваться, подписываться и рассылаться другим серверам iSeries с помощью функции Централизованное управление.

Дополнительные сведения

На следующем рисунке показан процесс создания и проверки подписей объектов в данном сценарии:



На рисунке показаны следующие системы, рассмотренные в данном сценарии:

Центральная система (iSeries A)

- В системе iSeries A установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).

- iSeries A играет роль центральной системы, на которой запущена функция Централизованное управление, применяемая для создания и рассылки пакетов приложений, а также для выполнения других задач.
- В системе iSeries A установлен продукт Cryptographic Access Provider 128-bit for iSeries (5722–AC3).
- В системе iSeries A установлены и настроены Диспетчер цифровых сертификатов (компонент 34 OS/400) и IBM HTTP Server (5722–DG1).
- iSeries A выполняет функции локальной сертификатной компании (CA). В этой системе хранится сертификат, служащий для создания подписей объектов.
- iSeries A применяется для создания подписей объектов приложений. Для создания подписей объектов, предназначенных для последующей рассылки, в iSeries A выполняются следующие задачи:
  1. С помощью DCM создается локальная CA, которая выдает сертификат подписи объекта.
  2. С помощью DCM копия сертификата локальной CA и копия сертификата проверки подписи экспортируется в файл, для того чтобы конечные системы (iSeries B, C, D и E) могли проверять подписи объектов.
  3. С помощью Централизованного управления создаются подписи объектов приложений, а приложения и файл с сертификатом проверки подписи включаются в пакет.
  4. С помощью Централизованного управления подписанные приложения и файлы сертификатов рассылаются конечным системам.

Конечные системы (iSeries B, C, D и E)

- В системах iSeries B и C установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- В системах iSeries D и E установлена операционная система OS/400 версии 5, выпуска 1 (V5R1).
- В системах iSeries B, C, D и E установлен и настроен Диспетчер цифровых сертификатов (компонент 34) и IBM HTTP Server (5722–DG1).
- Вместе с подписанным приложением, отправленным из центральной системы (iSeries A), системы iSeries B, C, D и E получат копию сертификата проверки подписи и копию сертификата локальной CA.
- С помощью DCM будет создано хранилище сертификатов *SIGNATUREVERIFICATION, в которое будет импортирован сертификат локальной CA и сертификат проверки подписи.

Предварительные требования

Для реализации этого сценария должны быть выполнены следующие требования:

1. На всех серверах iSeries должны быть выполнены требования к установке и применению Диспетчера цифровых сертификатов (DCM).
2. Приложение DCM ранее не настраивалось и не применялось ни на одном сервере iSeries.
3. В iSeries A должны быть выполнены требования, предъявляемые к установке и применению программы Навигатор и функции Централизованное управление.
4. Во всех конечных системах iSeries должен быть запущен сервер Централизованного управления.
5. На всех серверах iSeries установлена последняя версия программы Cryptographic Access Provider 128-bit (5722-AC3).
6. На всех серверах iSeries системному значению Проверять подписи объектов при восстановлении (QVFYOBJRST) присвоено значение по умолчанию (3). Это значение разрешает серверу проверять подписи объектов при восстановлении.
7. У администратора сети iSeries A должны быть специальные права доступа *ALLOBJ, для того чтобы он мог подписывать объекты, либо у него должны быть права на работу с приложением, применяемым для подписания объектов.
8. У администратора сети или любого другого пользователя, отвечающего за создание хранилища сертификатов в DCM, должны быть специальные права доступа *SECADM и *ALLOBJ.

9. На всех остальных серверах iSeries администратору системы и другим пользователям, планирующим проверять подписи объектов, должны быть предоставлены специальные права доступа *AUDIT.

Задачи

Для реализации этого сценария необходимо выполнить две группы задач. К первой из них относятся задачи по настройке функции Централизованное управление в системе iSeries A для создания подписей приложений и рассылки пакетов приложений. Ко второй группе относятся задачи по настройке функции проверки подписей приложений на других серверах iSeries.

Задачи создания подписей объектов

Для создания подписей объектов в соответствии с данным сценарием выполните в системе iSeries A следующие задачи:

1. Установите и настройте все необходимые продукты iSeries, перечисленные в предварительных требованиях.
2. С помощью Диспетчера цифровых сертификатов (DCM) создайте локальную сертификатную компанию (CA) для получения сертификата подписи объекта.
3. С помощью DCM создайте определение приложения.
4. С помощью DCM назначьте сертификат определению приложения, предназначенного для создания подписей объектов.
5. С помощью DCM экспортируйте сертификаты, которые необходимы другим системам для проверки подписей объектов. Нужно экспортировать в файл копию сертификата локальной CA, а также копию сертификата подписи объекта в качестве сертификата проверки подписи.
6. Передайте файлы сертификатов во все конечные системы iSeries, в которых планируется проверять подписи приложений.
7. С помощью Централизованного управления подпишите объекты приложений.

Задачи проверки подписей

Перечисленные задачи по настройке функции проверки подписей необходимо выполнить во всех конечных системах iSeries. Только после этого в конечные системы можно будет передать подписанные объекты приложений с помощью Централизованного управления. Проверка подписей выполняется при восстановлении подписанных объектов в конечных системах.

Для проверки подписей объектов в соответствии с данным сценарием в каждой конечной системе iSeries необходимо выполнить следующие действия:

8. С помощью Диспетчера цифровых сертификатов (DCM) создайте хранилище сертификатов *SIGNATUREVERIFICATION.
9. С помощью DCM импортируйте сертификат локальной CA и сертификат проверки подписей.

Сведения о настройке

Для создания подписей объектов с помощью Централизованного управления выполните следующие действия.

Шаг 1: Выполните все предварительные требования

Перед выполнением задач по настройке для реализации данного сценария необходимо установить и настроить все продукты iSeries, перечисленные в предварительных требованиях.

Шаг 2: Создайте локальную сертификатную компанию для получения сертификата, предназначенного для подписания объектов

При создании локальной сертификатной компании (CA) с помощью Диспетчера цифровых сертификатов (DCM) необходимо заполнить ряд форм. Эти формы позволят вам создать CA и выполнить другие задачи, необходимые для применения цифровых сертификатов в SSL, а также при создании и проверке подписей объектов. Хотя в этом сценарии не требуется настраивать сертификаты для SSL, для создания подписей в системе необходимо заполнить все формы.

Для создания локальной CA с помощью DCM и работы с ней выполните следующие действия:

1. Запустите DCM.
2. В окне навигации DCM выберите **Создать сертификатную компанию (CA)**. Будет показано несколько форм.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Заполните все необходимые формы. После этого выполните следующие действия:
   a. Укажите идентификационную информацию для локальной CA.
   b. Установите сертификат локальной CA в браузере, чтобы программы распознавали эту сертификатную компанию и принимали сертификаты, выданные локальной CA.
   c. Задайте стратегию для локальной CA.
   d. С помощью локальной CA создайте сертификат клиента или сервера, с помощью которого приложения будут устанавливать соединения SSL.

      Примечание: Хотя в этом сценарии такой сертификат не применяется, его необходимо создать для того, чтобы локальная CA могла выдать сертификат подписи объекта. Если вы не создадите такой сертификат, вам потребуется по отдельности создать сертификат подписи объекта и его хранилище *OBJECTSIGNING.
   e. Выберите приложения, которые будут с помощью сертификата клиента или сервера устанавливать соединение SSL.

      Примечание: В этом сценарии не нужно выбирать никакие приложения. Нажмите кнопку **Продолжить** для перехода к следующей форме.
   f. С помощью локальной CA создайте сертификат для подписания объектов, который будет применяться приложениями для создания цифровых подписей объектов. При этом будет создано хранилище сертификатов *OBJECTSIGNING. Это хранилище применяется для работы с сертификатами подписей объектов.
   g. Выберите приложения, которые будут принимать сертификаты локальной CA.

      Примечание: В этом сценарии не нужно выбирать никакие приложения. Нажмите кнопку **Продолжить** для завершения задачи.

После создания сертификата локальной CA и сертификата подписи объекта необходимо определить приложение, которое будет применяться для создания подписей объектов с помощью сертификата.

Шаг 3: Создайте определение приложения для подписания объектов

После создания сертификата подписи объекта воспользуйтесь Диспетчером цифровых сертификатов (DCM) для определения приложения, которое будет применяться для создания подписей объектов. Определение приложения не обязательно должно быть связано с реальным приложением. Оно содержит информацию о типе или группе объектов, которые вы планируете подписывать. Определение необходимо для того, чтобы с сертификатом можно было связать ИД приложения.

Для создания определения приложения, служащего для подписания объектов, выполните следующие действия с помощью DCM:

1. В окне навигации нажмите кнопку **Выбрать хранилище сертификатов** и выберите хранилище сертификатов ***OBJECTSIGNING**.
2. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании хранилища сертификатов, и нажмите кнопку **Продолжить**.
3. В окне навигации выберите категорию **Управление приложениями** для просмотра списка задач.
4. В списке задач выберите **Добавить приложение**. Будет показана форма определения приложения.
5. Заполните форму и нажмите кнопку **Добавить**.

Теперь необходимо связать созданное приложение с сертификатом для подписания объектов.

Шаг 4: Назначьте сертификат определению приложения, предназначенного для создания подписей объектов

Для того чтобы связать сертификат с определением приложения, предназначенного для создания подписей объектов, выполните следующие действия:

1. В окне навигации DCM выберите категорию **Управление сертификатами** для просмотра списка задач.
2. В списке задач выберите **Назначить сертификат**. Появится список сертификатов из текущего хранилища сертификатов.
3. Выберите сертификат в списке и нажмите кнопку **Назначить приложениям**. Появится список определений приложений, связанных с текущим хранилищем сертификатов.
4. Выберите одно или несколько приложений в списке и нажмите кнопку **Продолжить**. Появится сообщение, запрашивающее подтверждение назначения сертификата, либо сообщение с информацией об ошибке.

После выполнения этой задачи вы можете создать подписи объектов с помощью Централизованного управления во время формирования и рассылки пакетов. Для того чтобы обеспечить возможность проверки подписей, необходимо экспортировать необходимые сертификаты в файл и передать их во все конечные системы iSeries. Перед передачей подписанных объектов приложений в конечные системы iSeries с помощью функции Централизованное управление в этих системах необходимо выполнить все задачи по настройке проверки подписей. Проверка подписей выполняется при восстановлении подписанных объектов в конечных системах.

Шаг 5: Экспортируйте сертификаты проверки подписей в другие системы iSeries

Для обеспечения целостности объектов с помощью цифровых подписей необходимо, чтобы у пользователей была возможность проверять цифровые подписи. Для проверки подписей объектов в той системе, в которой были созданы эти подписи, необходимо создать хранилище сертификатов *SIGNATUREVERIFICATION с помощью DCM. В этом хранилище должна находиться копия сертификата подписи объекта и копия сертификата CA, выдавшей сертификат подписи объекта.

Для того чтобы другие пользователи могли проверять подпись объекта, им необходимо предоставить копию сертификата, с помощью которого была создана эта подпись. Если сертификат был выдан локальной сертификатной компанией (CA), то этим пользователям также необходимо предоставить сертификат локальной CA.

Для проверки подписей с помощью DCM в той системе, в которой эти подписи были созданы (в данном сценарии - в iSeries A), выполните следующие действия:

1. В окне навигации выберите опцию **Создать хранилище сертификатов** и выберите для создания хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. Нажмите кнопку **Да**, для того чтобы существующие сертификаты подписей объектов были скопированы в новое хранилище в качестве сертификатов проверки подписей.
3. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Теперь вы можете проверить подписи объектов с помощью DCM в той системе, в которой эти подписи были созданы.

Для того чтобы экспортировать копию сертификата локальной CA, а также копию сертификата подписи объекта в качестве сертификата проверки подписи в другие системы, выполните следующие действия:

1. В окне навигации выберите категорию **Управление сертификатами**, а затем выберите задачу **Экспортировать сертификат**.
2. Выберите **сертификатную компанию (CA)** и нажмите кнопку **Продолжить**. Появится список сертификатов CA, которые можно экспортировать.
3. Выберите в списке сертификат локальной CA и нажмите кнопку **Экспортировать**.
4. Укажите в качестве целевого расположения **Файл** и нажмите кнопку **Продолжить**.
5. Укажите полное имя файла для экспорта сертификата локальной CA и нажмите кнопку **Продолжить**.
6. Нажмите кнопку **OK**, чтобы закрыть окно подтверждения экспорта. Теперь можно экспортировать копию сертификата подписи объекта.
7. Снова выберите задачу **Экспортировать сертификат**.
8. Выберите опцию **Подписи объектов** . Появится список сертификатов подписей объектов, которые можно экспортировать.
9. Выберите сертификат подписи объекта в списке и нажмите кнопку **Экспортировать**.
10. Выберите опцию **Файл, сертификат проверки подписи** и нажмите кнопку **Продолжить**.
11. Укажите полное имя файла для экспорта сертификата подписи объекта и нажмите кнопку **Продолжить**.

Теперь файлы с сертификатами можно передать в конечные системы iSeries для проверки подписей.

Шаг 6: Передайте файлы сертификатов в конечные системы iSeries

Передайте в конечные системы iSeries файлы сертификатов, созданные в iSeries A, а затем настройте эти системы для проверки подписей объектов. Файлы сертификатов можно передать несколькими способами. Например, для этого можно воспользоваться FTP или функцией рассылки пакетов Централизованного управления.

Шаг 7: Подпишите объекты с помощью Централизованного управления

В Централизованном управлении подписи объектов создаются при рассылке пакетов программ. Перед передачей подписанных объектов приложений в конечные системы iSeries с помощью Централизованного управления, в этих системах необходимо выполнить все задачи по настройке проверки подписей. Проверка подписей выполняется при восстановлении подписанных объектов в конечных системах.

Для создания подписи приложения, которое планируется разослать в конечные системы iSeries, выполните следующие действия:

1. С помощью Централизованного управления выполните процедуру создания и рассылки пакета программ.

2. Когда при работе с мастером **Определение продукта** появится панель **Идентификация**, нажмите кнопку **Дополнительно**. Появится панель **Дополнительные параметры идентификации**.
3. В поле **Цифровая подпись** введите ИД приложения, определение которого было создано ранее, и нажмите кнопку **OK**.
4. Завершив работу с мастером, продолжите выполнять процедуру создания и рассылки пакета программ с помощью Централизованного управления.

Шаг 8: Задачи проверки подписей - Создайте хранилище сертификатов *SIGNATUREVERIFICATION в конечных системах iSeries

Для проверки подписей объектов в конечных системах iSeries необходимо, чтобы в хранилище сертификатов *SIGNATUREVERIFICATION этих систем была копия сертификата проверки подписи. Если объекты были подписаны с помощью локального сертификата, то в хранилище также должна быть копия сертификата локальной CA.

Для создания хранилища сертификатов *SIGNATUREVERIFICATION выполните следующие действия:

1. Запустите DCM.
2. В окне навигации Диспетчера цифровых сертификатов (DCM) выберите опцию **Создать хранилище сертификатов**, а затем выберите для создания хранилище ***SIGNATUREVERIFICATION**.

   Примечание: Для просмотра информации о заполнении полей формы при выполнении этой задачи нажмите кнопку с вопросительным знаком (**?**) вверху страницы. Появится контекстная справка.
3. Укажите пароль для нового хранилища сертификатов и нажмите кнопку **Продолжить**, чтобы создать хранилище сертификатов. Теперь вы можете импортировать в хранилище сертификаты, необходимые для проверки подписей объектов.

Шаг 9: Задачи проверки подписей - Импортируйте сертификаты

Для проверки подписи объекта необходимо, чтобы в хранилище сертификатов *SIGNATUREVERIFICATION была копия сертификата проверки подписи. Если сертификат подписи является частным, то в хранилище также должна быть копия сертификата локальной сертификатной компании, выдавшей сертификат подписи. В данном сценарии оба сертификата были экспортированы в файл и переданы в конечные системы iSeries.

Для того чтобы импортировать эти сертификаты в хранилище *SIGNATUREVERIFICATION, выполните следующие действия:

1. В окне навигации DCM выберите задачу **Выбрать хранилище сертификатов**. После этого выберите хранилище сертификатов ***SIGNATUREVERIFICATION**.
2. На странице Хранилище сертификатов и пароль введите пароль, заданный при создании хранилища сертификатов, и нажмите кнопку **Продолжить**.
3. После обновления информации в окне навигации выберите **Управление сертификатами** для просмотра списка задач.
4. В списке задач выберите **Импортировать сертификат**.
5. Выберите в качестве типа сертификата значение **Сертификатная компания (CA)** и нажмите кнопку **Продолжить**.

   Примечание: Сертификат локальной CA нужно импортировать до локального сертификата подписи. В противном случае вам не удастся импортировать сертификат подписи.

6. Укажите полное имя файла, содержащего сертификат CA, и нажмите кнопку **Продолжить**. Появится сообщение о завершении импорта или сообщение с информацией об ошибке.
7. Снова выберите задачу **Импортировать сертификат**.
8. Выберите в качестве типа импортируемого сертификата **Проверка подписи** и нажмите кнопку **Продолжить**.
9. Укажите полное имя файла, содержащего сертификат проверки подписи, и нажмите кнопку **Продолжить**. Появится сообщение о завершении импорта или сообщение с информацией об ошибке.

Теперь при восстановлении объектов в системе iSeries можно проверить подписи этих объектов, созданные с помощью соответствующего сертификата подписи объекта.

Основная информация о подписях объектов

Перед началом работы с функциями создания и проверки подписей объектов iSeries ознакомьтесь со следующими основными понятиями:

Цифровые подписи
Информация о том, что такое цифровые подписи и какую защиту они обеспечивают.

Объекты, допускающие создание подписи
Список объектов iSeries, которые можно подписать, и перечень опций создания подписи для объектов команд (*CMD).

Процесс создания подписи объекта
Описание процесса создания подписи объекта и параметров, с помощью которых вы можете управлять этим процессом.

Процесс проверки подписи
Описание процесса проверки подписи и параметров, с помощью которых вы можете управлять этим процессом.

Цифровые подписи

В OS/400 предусмотрена возможность ″подписывать″ объекты цифровой подписью. Цифровая подпись объекта аналогична обычной подписи в напечатанном документе и создается с помощью одного из видов шифрования. Она подтверждает подлинность источника объекта и позволяет проверить 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.

Применение цифровых подписей повышает эффективность традиционных средств контроля за доступом к объектам сервера iSeries. Обычные средства не позволяют защитить объект от несанкционированного изменения во время его передачи по сети Internet или другой незащищенной сети. Цифровая подпись позволяет проверить, было ли изменено содержимое объекта во время его передачи, поэтому вы можете легко определить, следует ли использовать такой объект.

Цифровая подпись - это определенный код, который генерируется математической функцией путем обработки содержимого объекта. 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 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 (хотя для применения сертификатов подписи объектов пользователь должен обладать определенными правами доступа).

Если для реализации стратегии защиты было решено применять цифровые подписи, вы должны выбрать между глобальными и локальными сертификатами. Если вы собираетесь распространять объекты среди широкого круга пользователей, то для создания подписей 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 с помощью Диспетчера цифровых сертификатов (DCM) можно создать собственную сертификатную компанию, что позволит вам выдавать собственные сертификаты для подписания объектов. Это позволит вам сэкономить за счет того, что не потребуется приобретать сертификаты у глобальной CA.

Типы цифровых подписей

В выпусках V5R2 и старше разрешено создавать подписи для объектов команд (*CMD). Для таких объектов существуют подписи двух типов: подписи основной части объекта и подписи всего объекта.

- **Подпись всего объекта**
  Такой тип подписи защищает весь объект, за исключением нескольких несущественных байт.
- **Подпись основной части объекта**
  Такой тип подписи защищает только те байты объекта *CMD, которые содержат важную информацию. Подпись не распространяется на ту часть объекта, которая изменяется чаще всего. Такой тип подписи позволяет вносить некоторые изменения в команду, не нарушая цифровую подпись. В различных объектах *CMD подпись защищает разные байты объекта. Например, значения параметров по умолчанию остаются незащищенными. Ниже перечислены примеры операций, выполнение которых не нарушает подпись основной части объекта:
  - Изменение значений параметров команды по умолчанию.
  - Добавление программы проверки правильности данных в команду, не содержащую такой программы.
  - Изменение значения параметра Где разрешено запускать.
  - Изменение значения параметра Ограничить число пользователей.

Дополнительная информация об объектах iSeries, для которых можно создать цифровую подпись, а также о фрагментах объекта *CMD, защищаемых подписью основной части объекта, приведена в разделе Объекты, допускающие создание подписи.

Объекты, допускающие создание подписи

Цифровую подпись можно создавать для объектов OS/400 различных типов. При этом не важно, какой способ создания подписи вы выберете. Можно создать подпись для любого объекта (*STMF), хранящегося в интегрированной файловой системе, за исключением объектов из библиотек. Если с объектом связана программа на Java, подпись будет создана и для этой программы. В файловой системе QSYS.LIB разрешено создавать подписи для следующих объектов: программ (*PGM), служебных программ (*SRVPGM), модулей (*MODULE), пакетов SQL (*SQLPKG), объектов *FILE (только файлы сохранения) и команд (*CMD).

Подпись можно создать только для того объекта, который расположен в локальной системе. Например, если вы работаете с сервером Windows 2000, установленным на плате Integrated xSeries Server for iSeries, то в состав интегрированной файловой системы будет входить файловая система QNTC. Каталоги этой файловой системы не считаются локальными, так как они содержат файлы, принадлежащие операционной системе Windows 2000. Кроме того, нельзя создавать подписи для пустых объектов и объектов, скомпилированных для выпуска младше V5R1.

Подписи объектов команд (*CMD)

Для объекта *CMD можно создать подпись одного из двух типов. Вы можете подписать весь объект или только основную часть этого объекта. Если вы решите создать подпись для всего объекта, она будет распространяться на весь объект за исключением нескольких несущественных байт. В частности, такая подпись защищает основную часть объекта.

Подпись основной части объекта защищает только те байты, которые содержат наиболее важную информацию. При этом часто изменяемые фрагменты объекта остаются незащищенными. Незащищенные байты выбираются в зависимости от типа объекта *CMD, однако в их число может входить режим, в котором допустимо применение объекта, и параметр, задающий область применения объекта. Подписи основной части объекта не защищают значения параметров по умолчанию. Такой тип подписи позволяет вносить некоторые изменения в команду, не нарушая цифровую подпись. Ниже перечислены примеры таких изменений:

- Изменение значений параметров команды по умолчанию.
- Добавление программы проверки правильности данных в команду, не содержащую такой программы.
- Изменение значения параметра Где разрешено запускать.
- Изменение значения параметра Ограничить число пользователей.

В приведенной ниже таблице указано, какие байты относятся к основной части объекта *CMD и защищаются цифровой подписью.

Фрагменты объектов *CMD, защищаемые подписью основной части объекта

Фрагмент объекта	**Включается ли в основную часть объекта, защищенную подписью**
Значения параметров команды по умолчанию, изменяемые командой CHGCMDDFT	Не включается
Имя и библиотека программы для обработки команды	Всегда включается
Имя и библиотека исходного файла REXX	Включается, если этот параметр задан для команды на момент ее подписания
Исходный элемент REXX	Включается, если этот параметр задан для команды на момент ее подписания
Среда выполнения и библиотека команды REXX	Включается, если этот параметр задан для команды на момент ее подписания
Имя, библиотека и код программы выхода REXX	Включается, если этот параметр задан для команды на момент ее подписания
Имя и библиотека программы проверки правильности данных	Включается, если этот параметр задан для команды на момент ее подписания
Режим, в котором разрешено применение	Не включается
Область применения	Не включается
Ограничить число пользователей	Не включается
Книжная полка справки	Включается, если этот параметр задан для команды на момент ее подписания
Группа панелей и библиотека справки	Включается, если этот параметр задан для команды на момент ее подписания
Идентификатор справки	Включается, если этот параметр задан для команды на момент ее подписания

Фрагмент объекта	Включается ли в основную часть объекта, защищенную подписью
Индекс поиска справки и библиотека	Включается, если этот параметр задан для команды на момент ее подписания
Текущая библиотека	Включается, если этот параметр задан для команды на момент ее подписания
Библиотека продукта	Включается, если этот параметр задан для команды на момент ее подписания
Имя и библиотека программы переопределения приглашения	Включается, если этот параметр задан для команды на момент ее подписания
Описание	Не защищается ни подписью основной части объекта, ни подписью всего объекта, так как не содержится в объекте
Подключить графический интерфейс (GUI)	Не включается

Процесс создания подписи объекта

При создании подписи объекта можно задать следующие параметры.

- **Обработка ошибок**
  Способ обработки ошибок, который должен применяться приложением при создании подписей для нескольких объектов. При возникновении ошибки приложение может прекращать процесс создания подписей или переходить к созданию подписи для другого объекта.
- **Дубликат подписи объекта**
  Вы можете указать, какое действие должно выполнять приложение при повторном создании подписи для объекта. Приложение может либо оставить старую подпись, либо заменить старую подпись на новую.
- **Объекты в подкаталогах**
  Вы можете указать, каким образом приложение должно обрабатывать объекты в подкаталогах. Оно может создавать подписи для всех объектов, в том числе объектов подкаталогов, либо только для объектов основного каталога.
- **Область действия подписи объекта**
  При создании подписи для объекта *CMD можно указать, для какой части объекта создается подпись: для всего объекта или только для основной части объекта.

Процесс проверки подписей

Можно задать следующие параметры проверки подписи объекта:

- **Обработка ошибок**
  Способ обработки ошибок, который должен применяться приложением при проверке подписей для нескольких объектов. При возникновении ошибки приложение может прекращать процесс проверки подписей или переходить к проверке подписи следующего объекта.
- **Объекты в подкаталогах**
  Вы можете указать, каким образом приложение должно обрабатывать объекты в подкаталогах. Оно может проверять подписи всех объектов, в том числе объектов подкаталогов, либо только подписи объектов основного каталога.
- **Проверка подписи всего объекта и подписи основной части объекта**
  Существуют определенные правила, по которым выполняется проверка подписей всего объекта и основной части объекта. Эти правила перечислены ниже:
  - Если объекта не подписан, программа проверки указывает это в отчете и переходит к проверке следующего объекта.
  - Если объект подписан уполномоченной организацией (IBM), то эта подпись должна быть правильной. В противном случае проверка завершится неудачно. Если подпись верна, выполнение проверки продолжается. Подпись - это зашифрованный результат применения

математической функции к содержимому объекта. Подпись считается верной, если содержимое объекта во время проверки совпадает с содержимым объекта на момент создания подписи.

- Если для всего объекта созданы надежные подписи (подписи, основанные на сертификате из хранилища *SIGNATUREVERIFICATION), то по крайней мере одна из этих подписей должна быть верной. В противном случае проверка завершится неудачно. Если верна хотя бы одна из подписей, заданных для всего объекта, то выполнение проверки продолжается.
- Если для основной части объекта созданы надежные подписи, то по крайней мере одна из них должна соответствовать сертификату из хранилища *SIGNATUREVERIFICATION. В противном случае проверка завершится неудачно. Если хотя бы одна из подписей основной части объекта будет верна, проверка продолжится.

Предварительные требования к созданию и проверке подписей объектов

Функции создания и проверки подписей объектов OS/400 предоставляют дополнительные возможности для управления объектами на сервере iSeries. Для применения этих функций должны быть выполнены некоторые требования.

Предварительные требования к созданию подписей объектов

Существует несколько способов создания подписей объектов, применяемых в различных случаях:

- С помощью Диспетчера цифровых сертификатов (DCM).
- Путем создания программы, вызывающей API Подписать объект API.
- С помощью функции Централизованное управление программы Навигатор iSeries. Эта функция позволяет подписывать объекты во время создания пакетов для их последующей рассылки конечным системам iSeries.

Вы можете выбрать любой из способов создания подписей объектов. Перед применением выбранного способа необходимо убедиться, что выполнены следующие требования:

- Предварительные требования к установке и применению Диспетчера цифровых сертификатов (DCM).
  - С помощью DCM должно быть создано хранилище сертификатов *OBJECTSIGNING. Оно создается во время создания локальной сертификатной компании (CA) или во время работы с сертификатом подписи объекта, полученным от глобальной CA.
  - Хранилище сертификатов *OBJECTSIGNING должно содержать хотя бы один сертификат. Он может быть выдан локальной CA или получен от глобальной CA.
  - С помощью DCM должно быть создано хотя бы одно определение приложения, служащего для подписания объектов.
  - С помощью DCM определению приложения, служащего для подписания объектов, должен быть назначен сертификат.
- Профайлу пользователя iSeries, отвечающего за создание подписей объектов, должны быть предоставлены специальные права доступа *ALLOBJ. Профайлу пользователя iSeries, отвечающего за создание хранилища сертификатов *SIGNATUREVERIFICATION, должны быть предоставлены специальные права доступа *SECADM и *ALLOBJ.

Предварительные требования к проверке подписей

Существует несколько способов проверки подписей объектов:

- С помощью Диспетчера цифровых сертификатов (DCM).
- С помощью специальной программы, вызывающей API Проверить объект (QYDOVFYO).

- С помощью одной из команд, например, команды Проверить целостность объекта (CHKOBJITG).

Вы можете выбрать любой из способов проверки подписей объектов. Перед применением выбранного способа необходимо убедиться, что выполнены следующие требования:

- Должны быть выполнены предварительные требования к установке и применению Диспетчера цифровых сертификатов (DCM).
- Должно быть создано хранилище сертификатов *SIGNATUREVERIFICATION. Хранилище можно создать двумя способами. Во-первых, хранилище можно создать с помощью Диспетчера цифровых сертификатов (DCM) для работы с сертификатами проверки подписи. Кроме того, если для создания подписей объектов применялся глобальный сертификат, то хранилище сертификатов можно создать с помощью специальной программы, вызывающей API Добавить сертификат для проверки (QYDOADDV).

  Примечание: API Добавить сертификат для проверки создает хранилище сертификатов с паролем по умолчанию. Вам необходимо изменить этот пароль с помощью DCM, для того чтобы предотвратить несанкционированный доступ к хранилищу сертификатов.
- Хранилище сертификатов *SIGNATUREVERIFICATION должно содержать копию сертификата, с помощью которого были подписаны объекты. Сертификат можно добавить в хранилище двумя способами. Во-первых, вы можете экспортировать сертификат в файл с помощью DCM системы, предназначенной для создания подписей, а затем импортировать этот сертификат в хранилище *SIGNATUREVERIFICATION с помощью DCM системы, предназначенной для проверки подписей. Если для создания подписей объектов применяется глобальный сертификат, его можно добавить в хранилище сертификатов системы, предназначенной для проверки подписей, путем создания программы, вызывающей API Добавить сертификат для проверки.
- Хранилище сертификатов *SIGNATUREVERIFICATION должно содержать копию сертификата CA, выдавшей сертификат, с помощью которого были подписаны объекты. Если для создания подписей объектов применяется глобальный сертификат, то копия сертификата CA уже должна находиться в хранилище сертификатов системы, предназначенной для проверки подписей. Если применяется сертификат, выданный локальной CA, то добавьте копию сертификата этой CA в хранилище сертификатов целевой системы с помощью DCM.

  Примечание: По соображениям защиты сертификат сертификатной компании (CA) нельзя добавить в хранилище сертификатов *SIGNATUREVERIFICATION с помощью API Добавить сертификат для проверки. После добавления сертификата CA в хранилище сертификатов система считает эту CA уполномоченной компанией по выдаче сертификатов. Другими словами, сертификаты, выданные этой CA, считаются надежными. Указанное ограничение введено для того, чтобы нельзя было создать программу выхода из процедуры установки, которая добавляет сертификат CA в хранилище сертификатов с помощью этого API. Сертификаты CA следует добавлять в хранилище сертификатов с помощью Диспетчера цифровых сертификатов. Это дает возможность назначить администратора, который будет самостоятельно определять, какие CA можно считать надежными. В этом случае в систему можно будет импортировать только те сертификаты, которые администратор явно указал как надежные.

  Если для создания подписей объектов применяется сертификат, выданный локальной CA, то экспортируйте копию сертификата CA в файл на том сервере iSeries, на котором создана локальная CA. После этого импортируйте сертификат локальной CA в хранилище сертификатов *SIGNATUREVERIFICATION с помощью DCM сервера iSeries, предназначенного для проверки подписей. Во избежание ошибки это необходимо сделать до того, как будет вызван API Добавить сертификат для проверки, которые добавляет сертификат проверки подписей. В связи с этим при работе с сертификатом, выданным локальной CA, проще всего импортировать в хранилище сертификатов как сертификат CA, так и сертификат проверки подписи.

Если вы не хотите, чтобы этот API применялся без вашего ведома для добавления сертификата подписи объекта в хранилище сертификатов *SIGNATUREVERIFICATION, рекомендуется запретить доступ к этому API в системе. Для этого необходимо запретить изменение системных значений, связанных с защитой, с помощью Системного инструментария (SST).

- Профайлу пользователя iSeries, отвечающего за проверку подписей объектов, должны быть предоставлены специальные права доступа *AUDIT. Профайлу пользователя iSeries, отвечающего за создание хранилища сертификатов *SIGNATUREVERIFICATION или изменения пароля этого хранилища, должны быть предоставлены специальные права доступа *SECADM и *ALLOBJ.

Работа с подписанными объектами

Начиная с выпуска V5R1, фирма IBM создает цифровые подписи для всех лицензионных программ и PTF OS/400. Подпись позволяет проверить, что программа или PTF действительно получен от IBM, а в системные объекты не были внесены несанкционированные изменения. Кроме того, некоторые заказанные вами приложения могут быть подписаны деловыми партнерами или другими вендорами. Следовательно, даже если вы не планируете подписывать собственные объекты, вам нужно знать, как нужно работать с подписанными объектами и каким образом такие объекты влияют на выполнение стандартных задач по администрированию системы.

Сильнее всего наличие объектов с подписью влияет на задачи резервного копирования и восстановления, в частности на способ сохранения и восстановления объектов в системе.

Системные значения и команды, связанные с подписанными объектами
Ознакомьтесь с системными значениями и командами, предназначенными для работы с подписанными объектами и управления ими.

Рекомендации по сохранению и восстановлению подписанных объектов
Узнайте о том, как объекты с подписью влияют на сохранение и восстановление данных в системе.

Применение команд для проверки целостности подписи
Информация о том, какие команды позволяют проверить подпись объекта и убедиться в его целостности.

Системные значения и команды, связанные с подписанными объектами

Для работы с подписанными объектами необходимо знать о том, какие системные значения и команды предназначены для управления такими объектами. Системное значение **Проверять подписи объектов при восстановлении** (QVFYOBJRST) указывает, каким образом некоторые команды восстановления влияют на объекты с подписью, и каким образом система обрабатывает объекты с подписью во время восстановления данных. В системе iSeries нет специальных команд CL для работы с подписанными объектами. Для работы с подписанными объектами и вспомогательными объектами, применяемыми при создании подписей, могут применяться обычные команды CL. Существует ряд команд, которые удаляют подпись объекта, таким образом нейтрализуя защиту, которую обеспечивает подпись.

Системные значения, связанные с подписанными объектами

Системное значение **Проверять подписи объектов при восстановлении** (QVFYOBJRST), относящееся в OS/400 к категории системных значений восстановления, определяет, каким образом команды влияют на объекты с подписью. Это системное значение задает способ проверки подписей во время восстановления данных. Для работы с ним применяется Навигатор iSeries. Помимо этого системного значения, еще два системных значения влияют на выполнение операций восстановления

в системе. Это системное значение разрешает или запрещает восстанавливать различные категории объектов с подписью. (Например, объекты без подписи, объекты с недействительной подписью, объекты с надежной подписью и т.д.) По умолчанию это значение разрешает восстанавливать только объекты без подписи и объекты с действительной подписью. 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. Оно влияет только на восстановление исполнимых объектов, в том числе программ (*PGM), команд (*CMD), служебных программ (*SRVPGM), пакетов SQL (*SQLPKG) и модулей (*MODULE). Кроме того, оно применяется к потоковым файлам (*STMF), с которыми связаны программы на Java, созданные командой Создать программу на Java (CRTJVAPGM). Это системное значение не относится к файлам сохранения (*SAV) и файлам IFS.

Дополнительная информация о применении этого и других системных значений приведена в разделе Программа поиска системных значений справочной системы Information Center.

Команды CL, связанные с подписанными объектами

Существует несколько команд CL, служащих для работы с подписанными объектами на сервере iSeries и управления ими. С их помощью можно просмотреть информацию о подписи объекта, проверить подпись объекта, а также сохранить и восстановить объекты средств защиты, необходимые для проверки подписей. Кроме того, существует ряд команд, которые могут удалить подпись объекта и, таким образом, нейтрализовать защиту, которую обеспечивает эта подпись.

Команды для просмотра информации о подписи объекта

- Команда Показать описание объекта (DSPOBJD).
  Эта команда показывает атрибуты перечисленных объектов из указанной библиотеки или из библиотек, входящих в список библиотек нити. С ее помощью можно узнать, подписан ли объект, а также просмотреть информацию о подписи.
- Команды интегрированной файловой системы Показать связи с объектом (DSPLNK) и Работа со связями с объектом (WRKLNK) .
  С помощью этих команд можно просмотреть информацию о подписи объекта, расположенного в интегрированной файловой системе.

Команды для проверки подписи объекта

- Команда Проверить целостность объекта (CHKOBJITG).
  Эта команда позволяет проверить целостность объектов системы. С ее помощью можно проверить подписи объектов. Принцип действия этой команды аналогичен принципу действия антивирусной программы, которая обнаруживает файлы и другие объекты, поврежденные вирусом. Дополнительная информация о применении этой команды для объектов с подписью и объектов, допускающих создание подписи, приведена в разделе Применение команд для проверки целостности подписи.
- Команда Проверить компонент продукта (CHKPRDOPT).
  Эта команда сравнивает текущую структуру программного продукта с правильной структурой. Например, команда сообщает об ошибке в случае, если был удален объект установленного продукта. С помощью параметра CHKSIG можно задать способ обработки ошибок в подписях объектов продукта. Дополнительная информация о применении этой команды для объектов с подписью и объектов, допускающих создание подписи, приведена в разделе Применение команд для проверки целостности подписи.
- Команда Сохранить лицензионную программу (SAVLICPGM).
  Эта команда сохраняет копии объектов, входящих в состав лицензионной программы. Сохраненную копию можно восстановить с помощью команды Восстановить лицензионную

программу (RSTLICPGM). С помощью параметра CHKSIG можно задать способ обработки ошибок в подписях объектов продукта. Дополнительная информация о применении этой команды для объектов с подписью и объектов, допускающих создание подписи, приведена в разделе Применение команд для проверки целостности подписи.

- Команда Восстановить (RST).
  Эта команда восстанавливает копии указанных объектов интегрированной файловой системы (IFS). Кроме того, она позволяет восстановить в системе хранилища сертификатов и их содержимое. Исключение составляет хранилище сертификатов *SIGNATUREVERIFICATION. То, каким образом команда обрабатывает объекты с подписью и объекты, допускающие создание подписи, зависит от системного значения Проверять подписи объектов при восстановлении (QVFYOBJRST).
- Команда Восстановить библиотеку (RSTLIB).
  Эта команда восстанавливает библиотеку или группу библиотек, которая была сохранена с помощью команды Сохранить библиотеку (SAVLIB). Команда RSTLIB восстанавливает все данные библиотеки, в том числе описание библиотеки, описание объектов и содержимое объектов библиотеки. Способ обработки объектов с подписью и объектов, допускающих создание подписи, зависит от системного значения Проверять подписи объектов при восстановлении (QVFYOBJRST).
- Команда Восстановить лицензионную программу (RSTLICPGM).
  Эта команда загружает, или восстанавливает, лицензионную программу для исходного или нового выпуска системы. Способ обработки объектов с подписью и объектов, допускающих создание подписи, зависит от системного значения Проверять подписи объектов при восстановлении (QVFYOBJRST).
- Команда Восстановить объект (RSTOBJ).
  Эта команда восстанавливает объекты из общей библиотеки, которые были сохранены одной командой на дискете, магнитной ленте, оптическом томе или в файле сохранения. Способ обработки объектов с подписью и объектов, допускающих создание подписи, зависит от системного значения Проверять подписи объектов при восстановлении (QVFYOBJRST).

Команды для сохранения и восстановления хранилищ сертификатов

- Команда Сохранить (SAV).
  Эта команда позволяет сохранить копию объектов интегрированной файловой системы, в том числе хранилищ сертификатов. Исключение составляет хранилище сертификатов *SIGNATUREVERIFICATION, к которому эта команда неприменима.
- Команда Сохранить данные защиты (SAVSECDTA).
  Эта команда позволяет сохранить всю информацию о защите, не переключая систему в состояние с ограничениями. С ее помощью можно сохранить хранилище сертификатов *SIGNATUREVERIFICATION и все расположенные в нем сертификаты. Эта команда сохраняет только это хранилище сертификатов.
- Команда Сохранить систему (SAVSYS).
  Эта команда позволяет сохранить копию лицензионного внутреннего кода и библиотеки QSYS в формате, совместимом с текущей конфигурацией сервера iSeries. Эта команда не сохраняет объекты из других библиотек. Она позволяет сохранить объекты, содержащие информацию о защите и конфигурации, которые также сохраняются командами SAVSECDTA и SAVCFG. С ее помощью можно сохранить хранилище сертификатов *SIGNATUREVERIFICATION и все расположенные в нем сертификаты.
- Команда Восстановить (RST).
  Эта команда позволяет восстановить хранилища сертификатов и их содержимое. Исключение составляет хранилище сертификатов *SIGNATUREVERIFICATION, которое не восстанавливается этой командой.
- Команда Восстановить пользовательские профайлы (RSTUSRPRF).
  Эта команда позволяет восстановить основные компоненты пользовательского профайла или набора пользовательских профайлов, сохраненного с помощью команды Сохранить систему (SAVSYS) или Сохранить данные защиты (SAVSECDTA). С ее помощью можно восстановить хранилище сертификатов *SIGNATUREVERIFICATION и сохраненные пароли для всех хранилищ

сертификатов. Для того чтобы восстановить хранилище сертификатов *SIGNATUREVERIFICATION без информации о пользовательских профайлах, укажите в параметре SECDTA значение *DCM, а в параметре USRPRF - значение *NONE. Для того чтобы восстановить информацию о пользовательских профайлах, хранилища сертификатов и их пароли, укажите в параметре USRPRF значение *ALL.

Команды, которые могут удалить подписи объектов

Перечисленные ниже команды в некоторых случаях удаляют подпись обрабатываемого объекта. Это может привести к возникновению ошибок при работе с объектом. Кроме того, будет невозможно идентифицировать источник объекта и проверить подпись, для того чтобы убедиться, что объект не был изменен. Эти команды можно вызывать только для тех объектов с подписью, которые были созданы вами, но не следует вызывать для тех объектов, которые были от кого-то получены, например, от IBM или ее вендора. Если подпись объекта была удалена командой, вызовите команду Показать описание объекта (DSPOBJD) и узнайте, сохранилась ли подпись в системе. Если да, заново подпишите объект.

Примечание: Для того чтобы узнать, была ли удалена подпись объекта командой Сохранить, восстановите объект в библиотеке, отличной от той, в которой объект был сохранен (например, в библиотеке QTEMP). Для того чтобы узнать, есть ли подпись у объекта, расположенного на носителе резервной копии, вызовите команду DSPOBJD.

- Команда Изменить программу (CHGPGM).
  Эта команда изменяет атрибуты программы без ее повторной компиляции. Кроме того, с ее помощью можно заново создать программу, в частности, программу с теми же атрибутами.
- Команда Изменить служебную программу (CHGSRVPGM).
  Эта команда изменяет атрибуты служебной программы без ее повторной компиляции. Кроме того, с ее помощью можно заново создать служебную программу, в частности, программу с теми же атрибутами.
- Команда Очистить файл сохранения (CLRSAVF).
  Эта команда очищает файл сохранения. Она удаляет все записи из файла сохранения, за счет чего сокращается объем памяти, занимаемый файлом.
- Команда Сохранить (SAV).
  Эта команда сохраняет копии объектов интегрированной файловой системы. — Она удаляет подписи объектов команд (*CMD) во время их записи на носитель резервной копии, если в параметре TGTRLS указан выпуск младше V5R2M0. Это связано с тем, что в выпусках младше V5R2M0 для объектов команд запрещено создавать подписи.
- Команда Сохранить библиотеку (SAVLIB).
  Эта команда позволяет сохранить копию одной или нескольких библиотек. Она удаляет подписи объектов команд (*CMD) во время их записи на носитель резервной копии, если в параметре TGTRLS указан выпуск младше V5R2M0. Это связано с тем, что в выпусках младше V5R2 для объектов команд запрещено создавать подписи.
- Команда Сохранить объект (SAVOBJ).
  Эта команда сохраняет копию объекта или группы объектов, расположенных в одной библиотеке. Она удаляет подписи объектов команд (*CMD) во время их записи на носитель резервной копии, если в параметре TGTRLS указан выпуск младше V5R2M0. Это связано с тем, что в выпусках младше V5R2 для объектов команд запрещено создавать подписи.

Рекомендации по сохранению и восстановлению подписанных объектов

На сервере iSeries предусмотрено несколько системных значений, влияющих на операции восстановления. Одним из них является системное значение **Проверять подписи объектов при восстановлении (QVFYOBJRST)**. Оно указывает, каким образом система обрабатывает объекты с

подписью во время их восстановления. В частности, с его помощью можно указать, каким образом во время восстановления должны обрабатываться объекты без подписи и объекты с недействительными подписями.

Некоторые команды сохранения и восстановления изменяют объекты с подписью и задают способ обработки объектов с подписью и без подписи во время сохранения и восстановления. Для того чтобы избежать ошибок, необходимо знать, каким образом эти команды влияют на объекты с подписью.

Ниже перечислены команды, позволяющие проверить подписи объектов во время сохранения или восстановления:

- Сохранить лицензионную программу (SAVLICPGM).
- Восстановить (RST).
- Восстановить библиотеку (RSTLIB).
- Восстановить лицензионную программу (RSTLICPGM).
- Восстановить объект (RSTOBJ).

Ниже перечислены команды, которые позволяют сохранить или восстановить хранилища сертификатов (объекты, содержащие сертификаты, применяющиеся для создания и проверки подписей):

- Сохранить (SAV).
- Сохранить данные защиты (SAVSECDTA).
- Сохранить систему (SAVSYS).
- Восстановить (RST).
- Восстановить пользовательские профайлы (RSTUSRPRF).

Существует ряд команд, которые при определенных значениях параметров удаляют подписи объектов во время их записи на носитель резервной копии, то есть нейтрализуют защиту, которую обеспечивает подпись. Например, *любая* команда сохранения, вызванная для объекта команды (*CMD), удалит подпись этого объекта, если в качестве целевого выпуска будет указан выпуск младше V5R2M0. Удаление подписи может привести к ошибкам при работе с объектом. Кроме того, будет невозможно идентифицировать источник объекта и проверить подпись, для того чтобы убедиться, что объект не был изменен. Такие команды следует вызывать только для созданных вами объектов, но не для объектов с подписью, полученных от кого-либо еще, например, от фирмы IBM или ее вендора.

Примечание: Для того чтобы узнать, была ли удалена подпись объекта командой Сохранить, восстановите объект в библиотеке, отличной от той, в которой объект был сохранен (например, в библиотеке QTEMP). Для того чтобы узнать, есть ли подпись у объекта, расположенного на носителе резервной копии, вызовите команду DSPOBJD.

Возможность удаления подписи следует учитывать при работе со всеми командами сохранения, и, в частности, при работе со следующими командами:

- Сохранить (SAV).
- Сохранить библиотеку (SAVLIB).
- Сохранить объект (SAVOBJ).

За дополнительной информацией о том, каким образом эти команды обрабатывают подписанные объекты и сами подписи во время сохранения и восстановления, обратитесь к разделу Системные значения и команды, связанные с подписанными объектами.

Применение команд для проверки целостности подписи

Для проверки подписи объекта можно воспользоваться Диспетчером цифровых сертификатов (DCM) или соответствующими API. Кроме того, можно вызвать одну из команд проверки подписей. Принцип действия этих команд аналогичен принципу действия антивирусной программы, которая обнаруживает файлы и другие объекты, поврежденные вирусом. Как правило, подписи проверяются при восстановлении объектов в системе, например, с помощью команды RSTLIB.

Для того чтобы проверить подпись объекта, хранящегося в системе, можно воспользоваться одной из трех команд. Среди них только одна команда, Проверить целостность объекта (CHKOBJITG), специально предназначена для проверки подписей объектов. Опция проверки подписей в этих командах задается в параметре CHKSIG. Этот параметр позволяет проверить подписи всех объектов, допускающих создание подписи, проигнорировать все подписи или проверить только те объекты, у которых есть подпись. Последний вариант проверки применяется по умолчанию.

Команда Проверить целостность объекта (CHKOBJITG)

Команда Проверить целостность объекта (CHKOBJITG) позволяет найти в системе те объекты, целостность которых нарушена. С ее помощью можно проверить целостность объектов, принадлежащих определенному пользовательскому профайлу, объектов с указанным именем или всех объектов системы. При выполнении одного из перечисленных ниже условий команда заносит в протокол запись о нарушении целостности объекта:

- Был изменен объект команды, программы или модуля, либо атрибуты библиотеки.
- Цифровая подпись объекта недействительна. Подпись - это зашифрованный результат применения математической функции к содержимому объекта. Подпись считается верной и действительной, если содержимое объекта во время проверки совпадает с содержимым объекта на момент создания подписи. Проверка подписи выполняется путем сравнения результата применения функции, полученного при создании подписи, и текущего результата применения функции. В зависимости от результатов сравнения, подпись признается действительной или недействительной. Если значения не совпадают, значит содержимое объекта изменилось с момента создания подписи, поэтому подпись считается недействительной.
- Атрибут домена, заданный для объекта, несовместим с типом объекта.
-

При обнаружении объекта, целостность которого нарушена, команда заносит имя объекта, имя библиотеки (или путь), тип объекта, имя владельца объекта и тип ошибки в протокол базы данных. Существует еще ряд случаев, не связанных с нарушением целостности, в которых команда заносит данные в протокол. Например, команда добавляет в протокол запись при обнаружении объекта без подписи, для которого можно создать подпись, объекта, который не удалось проверить, а также объектов, формат которых необходимо изменить для их применения в текущей реализации системы (выполнить преобразование IMPI в RISC).

Способ обработки цифровых подписей объектов задается в параметре команды CHKSIG. Допустимы следующие значения параметра:

- *SIGNED – Команда проверит объекты с цифровыми подписями. В протокол будут добавлены записи обо всех объектах, подписи которых недействительны. Это значение применяется по умолчанию.
- *ALL – Команда проверит все объекты, допускающие создание подписи. В протокол будут добавлены записи обо всех объектах без подписи, для которых можно создать подпись, а также обо всех объектах, подписи которых недействительны.
- *NONE – Команда не проверит цифровые подписи объектов.

Команда Проверить компонент продукта (CHKPRDOPT)

Команда Проверить компонент продукта (CHKPRDOPT) сравнивает текущую структуру программного продукта с правильной структурой. Например, команда сообщает об ошибке в случае, если был удален объект установленного продукта.

Способ обработки цифровых подписей объектов задается в параметре команды CHKSIG. Допустимы следующие значения параметра:

- *SIGNED – Команда проверит объекты с цифровыми подписями. Будут проверены подписи всех подписанных объектов. При обнаружении объекта с недействительной подписью команда отправит сообщение в протокол задания и укажет, что продукт находится в недопустимом состоянии. Это значение применяется по умолчанию.
- *ALL – Команда проверит все объекты, допускающие создание подписи, на наличие подписи, а также проверит подписи таких объектов. При обнаружении объекта без подписи, для которого можно создать подпись, команда отправит сообщение в протокол задания, однако не укажет, что продукт находится в недопустимом состоянии. При обнаружении объекта с недействительной подписью команда отправит сообщение в протокол задания и укажет, что продукт находится в недопустимом состоянии.
- *NONE – Команда не проверит цифровые подписи объектов продукта.

Команда Сохранить лицензионную программу (SAVLICPGM)

Команда Сохранить лицензионную программу (SAVLICPGM) позволяет сохранить копию объектов, входящих в состав лицензионной программы. Сохраненную копию можно восстановить с помощью команды Восстановить лицензионную программу (RSTLICPGM).

Способ обработки цифровых подписей объектов задается в параметре команды CHKSIG. Допустимы следующие значения параметра:

- *SIGNED – Команда проверит объекты с цифровыми подписями. Будут проверены подписи всех подписанных объектов. Объекты без подписи проверяться не будут. При обнаружении объекта с недействительной подписью команда добавит в протокол задания сообщение с именем объекта и прервет выполнение операции сохранения. Это значение применяется по умолчанию.
- *ALL – Команда проверит все объекты, допускающие создание подписи, на наличие подписи, а также проверит подписи таких объектов. При обнаружении объекта без подписи, для которого можно создать подпись, команда отправит сообщение в протокол задания, однако не прервет процесс восстановления. При обнаружении объекта с недействительной подписью команда добавит сообщение в протокол задания и прервет выполнение операции сохранения.
- *NONE – Команда не проверит цифровые подписи объектов продукта.

Устранение неполадок, связанных с подписями объектов

В приведенной ниже таблице содержится информация об устранении наиболее распространенных ошибок, которые возникают при создании и проверке подписей объектов iSeries.

Стандартные ошибки, возникающие при создании подписей

Ошибка	Исправление
При вызове API Подписать объект для целевого выпуска V4R5 или младше возникает ошибка, а подпись для объекта не создается (сообщение об ошибке CPFB721).	Подписи объектов поддерживаются в системе iSeries, начиная с выпуска V5R1. Если при обработке объекта было получено сообщение об ошибке CPFB721, заново создайте объект для целевого выпуска V5R1 или выше, а затем создайте подпись для этого объекта.

Стандартные ошибки, возникающие при проверке подписей

Ошибка	Исправление
При попытке восстановить объект без подписи возникает сбой.	Если у объекта действительно не должно быть подписи, убедитесь, что системное значение QVFYOBJRST не равно 5. Значение 5 запрещает восстанавливать объекты без подписи. Измените системное значение на 3 и повторите операцию восстановления.
При попытке восстановить объект с подписью возникает сбой.	Такая ошибка может возникать в том случае, если в систему было передано хранилище сертификатов *SIGNATUREVERIFICATION, после чего его пароль не был изменен с помощью DCM. Сертификаты из такого хранилища запрещено применять для проверки подписей при восстановлении объектов. Измените пароль хранилища сертификатов с помощью DCM. Если вы не знаете пароль, вам придется удалить хранилище сертификатов, создать его заново, а затем изменить пароль с помощью DCM.
Во время восстановления или установки продукта возникает ошибка при проверке подписи.	Если при проверке подписи была обнаружена ошибка, то, скорее всего, объект был изменен с момента создания подписи. Если вам необходимо обеспечить целостность объекта, не изменяйте системное значение QVFYOBJRST и не выполняйте другие действия, позволяющие восстановить объект. Это может привести к нейтрализации защиты, которую обеспечивает подпись, и сохранению опасного объекта в системе. Для устранения такой ошибки рекомендуется обратиться к пользователю, создавшему подпись объекта.

Дополнительная информация о подписях объектов и их проверке

Создание и проверка подписей объектов - это сравнительно новые способы защиты. Ниже приведен краткий перечень источников дополнительной информации об этих способах защиты и их применении:

- **Web-сайт VeriSign Help Desk**
  Этот Web-сайт фирмы VeriSign содержит большую библиотеку информации о цифровых сертификатах, в частности, сертификатах объектов, и защите информации в сети Internet.
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  Это руководство фирмы IBM содержит информацию о новых способах защиты данных в сети, предусмотренных в выпуске V5R1. В нем затронуты многие темы, в том числе вопрос применения подписей объектов в iSeries, способы применения Диспетчера цифровых сертификатов (DCM) и т.п.

Напечатано в Дании