



System i
Security
Secure Sockets Layer

Версия 6, выпуск 1





System i
Security
Secure Sockets Layer

Версия 6, выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 23.

Это издание относится к версии 6, выпуску 1, модификации 0 i5/OS (5761–SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

© Copyright International Business Machines Corporation 2002, 2008. Все права защищены.

Содержание

Secure Sockets Layer 1

Новое в выпуске V6R1 1

Файл PDF с информацией по SSL 1

Сценарии: SSL 2

Сценарий: Защита соединения клиента с сервером централизованного управления с помощью протокола SSL 2

 Подробные сведения о настройке: Защита соединения клиента с системой централизованного управления с помощью SSL 4

 Шаг 1: Выключите SSL для клиента System i Navigator. 4

 Шаг 2: Задайте уровень идентификации для сервера централизованного управления. 5

 Шаг 3: Перезапустите систему Централизованного управления в центральной системе. 5

 Шаг 4: Включите SSL для клиента System i Navigator. 5

 Необязательный шаг: Выключите SSL для клиента System i Navigator 5

Сценарий: Защита всех соединений сервера централизованного управления с помощью SSL 5

 Подробные сведения о настройке: Защита всех соединений с системой централизованного управления с помощью SSL 9

 Шаг 1: Настройте центральную систему для идентификации сервера 10

 Шаг 2: Настройте конечные системы для идентификации сервера 10

 Шаг 3: Перезапустите систему Централизованного управления в центральной системе 11

 Шаг 4: Перезапустите систему Централизованного управления во всех конечных системах 11

Шаг 5: Включите SSL в System i Navigator. 11

Шаг 6: Настройте центральную систему для идентификации клиента (необязательный шаг). 11

Шаг 7: Настройте конечную систему для идентификации клиента 12

Шаг 8: Скопируйте контрольный список в конечные системы 12

Шаг 9: Перезапустите систему Централизованного управления в центральной системе 13

Шаг 10: Перезапустите систему Централизованного управления во всех конечных системах 13

Общие сведения о SSL 13

 Принципы работы SSL. 13

 Поддержка протоколов SSL и Transport Layer Security (TLS). 14

 Системный SSL 15

 Свойства системного SSL 16

 Идентификация сервера 18

 Идентификация клиента 18

Предварительные требования к SSL 19

Защита приложений с помощью SSL 19

Устранение неполадок SSL 20

Связанная информация по SSL 21

Приложение. Примечания 23

Товарные знаки 24

Terms and conditions 25

Secure Sockets Layer

В этом разделе приведена информация о применении протокола Secure Sockets Layer (SSL) на сервере.

Протокол Secure Sockets Layer (SSL) стал отраслевым стандартом, который применяется приложениями для установления защищенных соединений в незащищенной сети, например, в Internet.

Новое в выпуске V6R1

Описание новой и значительно измененной информации в разделах, посвященных протоколу Secure Sockets Layer (SSL).

Новая информация: Системный SSL

Системный SSL - это набор базовых служб из Лицензионного внутреннего кода (LIC) i5/OS, предназначенных для защиты соединений TCP/IP с помощью протокола SSL/TLS. Системный SSL тесно взаимодействует с операционной системой и кодом сокетов, обеспечивая дополнительную производительность и более надежную защиту.

Для описания системного SSL добавлены следующие разделы:

- “Системный SSL” на стр. 15
- “Свойства системного SSL” на стр. 16



Новые системные значения для системного SSL

Добавлены следующие системные значения:

- Системное значение SSL: QSSLPCL
- Системное значение SSL: QSSLCSLCTL
- Системное значение SSL: QSSLCSL

Условное обозначение новой и измененной информации

В этом документе новая и измененная информация обозначается следующим образом:

- Значок  отмечает начало новой или измененной информации.
- Значок  отмечает конец новой или измененной информации.

В файлах PDF новая и измененная информация может обозначаться значками ревизий ({}).

Дополнительная информация об изменениях, связанных с выпуском, приведена в документации Информация для пользователей.

Файл PDF с информацией по SSL

Можно просмотреть и распечатать файл PDF с данной информацией.


Для просмотра или загрузки этого документа в формате PDF выберите ссылку Secure Sockets Layer (SSL).

Сохранение файлов PDF

Для сохранения файла в формате PDF на рабочей станции с целью последующего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
2. Щелкните на опции локального сохранения PDF.
3. Выберите каталог, в котором следует сохранить файл PDF.
4. Щелкните на **Сохранить**.

Загрузка Adobe Reader

Для просмотра и печати файлов PDF требуется программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html) .

Сценарии: SSL

Сценарии SSL помогут вам получить максимальной пользы от протокола SSL в платформе System i.

Сценарии SSL помогают понять работу SSL в системе i5/OS на примерах использования SSL.

Информация, связанная с данной

Сценарий: Защита Telnet с помощью SSL

Сценарий: Защита личных ключей криптографическим аппаратным обеспечением

Сценарий: Защита соединения клиента с сервером централизованного управления с помощью протокола SSL

Этот сценарий описывает применение SSL для защиты соединения между удаленным клиентом и сервером централизованного управления модели System i, играющей роль центральной системы функции централизованного управления System i Navigator.

Задача:

В состав локальной сети, развернутой в офисе компании, входит несколько систем i5/OS. Системный администратор этой компании выбрал одну из систем i5/OS в качестве центральной системы сети (далее мы будем называть этот сервер системой А). Он использует запущенный в этой системе сервер централизованного управления для управления всеми остальными конечными системами сети.

Администратор хочет обеспечить возможность подключения к серверу централизованного управления в системе А из внешней сети. Он часто бывает в командировках и ему требуется безопасное соединение с сервером централизованного управления во время отсутствия. Он хочет, чтобы соединение между его компьютером и сервером централизованного управления было надежно защищено, даже когда его нет в офисе. Администратор решает использовать SSL на своем компьютере и на сервере централизованного управления системы А. Настроив поддержку SSL, он может быть уверен, что сервер централизованного управления надежно защищен.

Цели:

Администратор хочет защитить только соединение между своим компьютером и сервером централизованного управления. Ему не требуется дополнительная защита для соединений между этим сервером и конечными системами сети. Другие сотрудники компании также не нуждаются в дополнительной защите своих подключений к серверу централизованного управления. Администратору предстоит настроить свой компьютер и сервер централизованного управления так, чтобы его клиентское подключение использовало идентификацию сервера. При этом подключения других компьютеров-клиентов и других систем i5/OS к серверу централизованного управления не будут защищены с помощью SSL.

Подробности:

Следующая таблица иллюстрирует типы идентификации, применяемые в зависимости от того, включена ли поддержка SSL на компьютере-клиенте:

Таблица 1. Необходимые элементы для защищенного соединения SSL между клиентом и сервером централизованного управления

Состояние SSL на компьютере администратора	Выбранный уровень идентификации для сервера централизованного управления в системе А.	Применяется ли соединение SSL?
Поддержка SSL выключена	Безразлично	Нет
Включена поддержка SSL	Безразлично	Да (идентификация сервера)

Идентификация сервера означает, что компьютер администратора идентифицирует сертификат сервера централизованного управления. Компьютер администратора в соединении с сервером играет роль клиента SSL. Сервер централизованного управления играет роль сервера SSL и должен подтвердить свою идентификацию. Для этого он предоставляет сертификат, выданный сертификатной компанией (CA), которой доверяет компьютер администратора.

Предварительные требования и предположения

Для того чтобы защитить соединение между своим компьютером и сервером централизованного управления в системе А, администратор должен выполнить ряд задач по настройке:

1. System А отвечает предварительным требованиям SSL.
2. System А работает под управлением i5/OS V5R3 или более позднего выпуска.
3. Компьютер клиента работает под управлением System i Navigator for System i Access for Windows V5R3 или более позднего выпуска.
4. Получите сертификатную компанию (CA) для систем i5/OS.
5. Создайте для системы А сертификат, подписанный CA.
6. Отправьте сертификаты сервера и сертификатной компании в систему А и импортируйте их в базу данных ключей.
7. С помощью функции идентификации серверов Централизованного управления назначьте сертификат системам i5/OS. Центральный сервер TCP, сервер базы данных, сервер очереди данных, файловый сервер, сервер сетевой печати, сервер обработки удаленных команд и сервер входа в систему - все это системы i5/OS.
 - a. В системе А запустите IBM DCM. Теперь администратор может получить или создать сертификаты, а также внести другие изменения в систему сертификатов.
 - b. Нажмите кнопку **Выбрать хранилище сертификатов**.
 - c. Выберите ***SYSTEM** и нажмите кнопку **Далее**.
 - d. Введите *пароль хранилища сертификатов*, и нажмите кнопку **Далее**. После обновления меню разверните папку **Управление приложениями**.
 - e. Нажмите **Обновить присвоение сертификата**.
 - f. Выберите **Сервер** и нажмите кнопку **Далее**.
 - g. Выберите **Сервер Централизованного управления** и нажмите **Обновить присвоение сертификата**. Теперь серверу централизованного управления присвоен сертификат.
 - h. Нажмите **Назначить новый сертификат**. DCM снова откроет страницу Обновить присвоение сертификата с подтверждающим сообщением.
 - i. Нажмите кнопку **Готово**.
 - j. Присвойте сертификат всем серверам, к которым имеет доступ клиент.
8. Загрузите CA на компьютер-клиент.

Перед применением SSL в функции централизованного управления администратор должен выполнить все предварительные требования для установки SSL и настроить цифровые сертификаты в системе. После выполнения всех предварительных требований администратор может активировать SSL на сервере централизованного управления.

Шаги настройки

Для защиты соединения с сервером с помощью SSL, необходимо выполнить следующие действия:

1. “Шаг 1: Выключите SSL для клиента System i Navigator”
2. “Шаг 2: Задайте уровень идентификации для сервера централизованного управления” на стр. 5
3. “Шаг 3: Перезапустите систему Централизованного управления в центральной системе” на стр. 5
4. “Шаг 4: Включите SSL для клиента System i Navigator” на стр. 5
5. “Необязательный шаг: Выключите SSL для клиента System i Navigator” на стр. 5

Понятия, связанные с данным

“Предварительные требования к SSL” на стр. 19

Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

Информация, связанная с данной

Настройка DCM

Запуск DCM

Подробные сведения о настройке: Защита соединения клиента с системой централизованного управления с помощью SSL

Этот раздел содержит подробное описание шагов по настройке защиты клиентских соединений с сервером централизованного управления с помощью SSL.

Эта информация предполагает, что вы ознакомились с разделом Сценарий: Защита соединения клиента с сервером централизованного управления с помощью SSL.

В этом сценарии модель System i выбрана в качестве центральной системы локальной сети компании. Администратор использует сервер централизованного управления, работающий в центральной системе (до этого момента называвшейся системой A), для управления конечными системами сети. Ниже приведены инструкции по настройке защищенного подключения внешнего клиента к этому серверу. Вы можете вслед за администратором нашей гипотетической сети выполнить все необходимые операции.

Понятия, связанные с данным

“Предварительные требования к SSL” на стр. 19

Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

“Сценарий: Защита всех соединений сервера централизованного управления с помощью SSL” на стр. 5

Этот сценарий описывает применение SSL для защиты всех соединений с сервером централизованного управления для модели System i, играющей роль центральной системы функции централизованного управления System i Navigator.

Информация, связанная с данной

Первичная настройка сертификатов

Шаг 1: Выключите SSL для клиента System i Navigator:

Этот шаг необходим только в том случае, если SSL уже включен для клиента System i Navigator.

1. В окне System i Navigator разверните **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **Защита** и отмените выбор опции **Применять SSL для соединения**.
4. Перезапустите System i Navigator.

Из контейнера Централизованное управление в Навигаторе System i Navigator исчезнет значок замка. Это значит, что соединение между клиентом и центральной системой компании теперь не защищено.

Шаг 2: Задайте уровень идентификации для сервера централизованного управления:

1. В окне System i Navigator щелкните правой кнопкой мыши на записи **Централизованное управление** и выберите **Свойства**.
2. Перейдите на вкладку **Защита** и выберите опцию **Применять SSL**.
3. Выберите **Любой** в качестве уровня идентификации (System i Access for Windows).
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Шаг 3: Перезапустите систему Централизованного управления в центральной системе:

1. В окне System i Navigator разверните **Мои соединения**.
2. В системе A откройте **Сеть --> Серверы** и выберите **TCP/IP**.
3. Щелкните правой кнопкой мыши на **Централизованное управление** и выберите **Остановить**. Список под именем центральной системы будет свернут. Появится сообщение о том, что соединение с сервером прервано.
4. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 4: Включите SSL для клиента System i Navigator:

1. В окне System i Navigator разверните **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **SSL** и выберите опцию **Применять SSL для соединения**.
4. Перезапустите System i Navigator.

В System i Navigator рядом с сервером центрального управления появится значок замка, означающий, что соединение защищено с помощью SSL. Таким образом, администратор успешно установил защищенное соединение между своим клиентом и центральной системой компании.

Примечание: Эта процедура защищает только соединение между одним компьютером и системой централизованного управления. Соединения остальных клиентов и конечных систем сети с этим сервером не будут защищены. Для того чтобы защитить подключения других клиентов, убедитесь, что для них выполнены предварительные требования и повторите “Шаг 4: Включите SSL для клиента System i Navigator”. Для того чтобы защитить другие соединения с сервером централизованного управления, обратитесь к разделу Сценарий: Защита всех соединений с сервером централизованного управления с помощью SSL.

Необязательный шаг: Выключите SSL для клиента System i Navigator:

Когда администратор работает в офисе, то он может отключить SSL, что позволит несколько повысить производительность компьютера. Для выключения SSL выполните следующие действия:

1. В окне System i Navigator разверните **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **Защита** и отмените выбор опции **Применять SSL для соединения**.
4. Перезапустите System i Navigator.

Сценарий: Защита всех соединений сервера централизованного управления с помощью SSL

Этот сценарий описывает применение SSL для защиты всех соединений с сервером централизованного управления для модели System i, играющей роль центральной системы функции централизованного управления System i Navigator.

Ситуация:

Недавно была создана глобальная сеть (WAN) фирмы, содержащая несколько удаленных моделей System i (конечных систем). Для управления этими системами применяется центральная система, расположенная в главном офисе компании. В этой компании предусмотрена должность администратора системы безопасности. Он хочет использовать SSL для защиты соединений между сервером централизованного управления центральной системы и всеми серверами и клиентами i5/OS.

Подробности:

С помощью SSL администратор может **безопасно** осуществлять все соединения с сервером централизованного управления. Для применения SSL он должен настроить защиту System i Navigator на том персональном компьютере, на котором запущена функция Централизованное управление.

Можно выбрать один из двух уровней идентификации для сервера централизованного управления:

Идентификация сервера

Обеспечивает идентификацию сертификата сервера. Клиент должен проверить сервер, будь то клиент System i Navigator на PC или сервер централизованного управления в центральной системе. Когда System i Navigator подключается к центральной системе, то PC выступает как клиент SSL, а сервер централизованного управления, работающий в центральной системе - как сервер SSL. Центральная система выступает в соединении с конечной системой в роли клиента SSL. Конечная система выступает в роли сервера SSL и должна предъявить удостоверение личности в виде сертификата, выданного сертификатной компанией, зарегистрированной в клиенте. Для каждого сервера SSL необходим сертификат, выданный уполномоченной сертификатной компанией.

Идентификация сервера и клиента

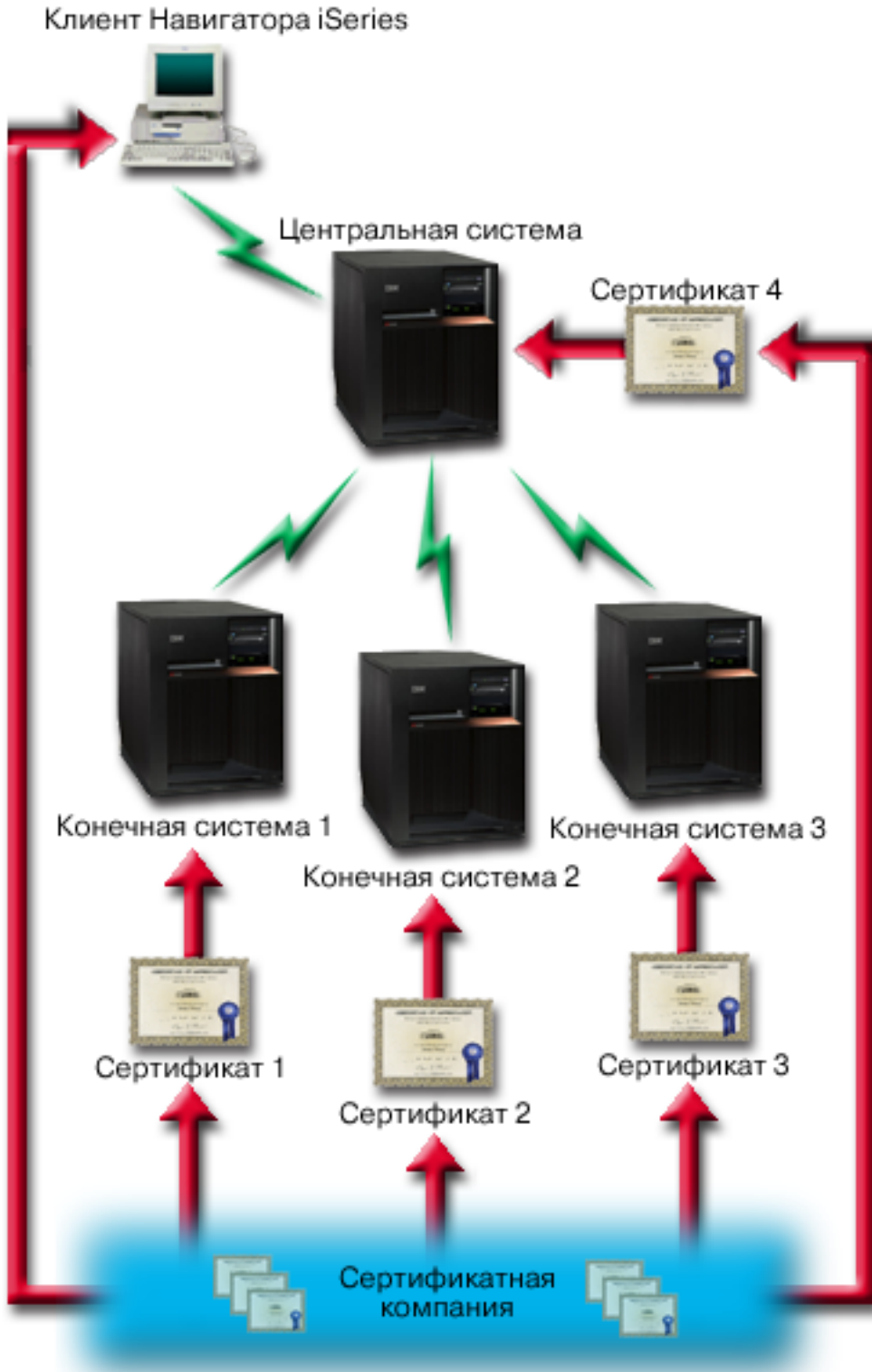
Обеспечивает идентификацию сертификатов центральной и конечной систем. Это более высокий уровень защиты, чем идентификация сервера. В других приложениях это называется идентификацией клиента, так как клиент должен предоставить надежный базовый сертификат. Когда центральная система (клиент SSL) устанавливает соединение с конечной системой (сервером SSL), обе системы проверяют подлинность сертификатов друг друга.

Примечание: Идентификация сервера и клиента поддерживается только между двумя моделями System i. Идентификация клиента не выполняется сервером, когда клиент - это PC.

В отличие от других приложений, Централизованное управление также поддерживает идентификацию с помощью контрольного списка, называемого контрольным списком Уполномоченной группы. Обычно в контрольном списке хранится информация, идентифицирующая пользователя, такая как ИД пользователя и информация идентификации: пароль, личный идентификационный номер или цифровой сертификат. Информация идентификации зашифрована.

В большинстве приложений нет опций для настройки идентификации клиента и сервера, поскольку идентификация сервера почти всегда происходит в процессе установления сеанса связи SSL. Во многих приложениях можно дополнительно настроить идентификацию клиента. В Централизованном управлении вместо идентификации клиента применяется термин "идентификация клиента и сервера", так как центральная система выполняет в сети две функции. Когда персональный компьютер устанавливает связь с центральной системой, она играет роль сервера. Однако при соединении центральной системы с другой конечной системой центральная система является клиентом. Ниже приведен пример выполнения центральной системой функций клиента и сервера в сети.

Примечание: В этом примере копия сертификата, связанного с сертификатной компанией, должна храниться в базах данных ключей центральной системы и всех конечных систем. Служба сертификации должна распознаваться центральной системой, всеми конечными системами, а также PC.



Предварительные требования и предположения:

Для применения SSL в Централизованном управлении администратор должен выполнить следующие задачи настройки и администрирования:

1. Система А отвечает предварительным требованиям SSL.
2. Центральная система и все конечные системы работают под управлением OS/400 V5R2 или i5/OS V5R3 или более поздних выпусков.

Примечание: Операционная система i5/OS V5R4 и более поздних выпусков не поддерживает соединения с системами OS/400 V5R1.

3. Компьютер клиента работает под управлением System i Navigator for System i Access for Windows V5R3 или более позднего выпуска.
4. Получите сертификатную компанию (CA) для моделей System i.
5. Создайте для системы А сертификат, подписанный СА.
6. Отправьте сертификаты сервера и сертификатной компании в систему А и импортируйте их в базу данных ключей.
7. С помощью функции идентификации приложений Централизованного управления назначьте сертификаты системам i5/OS. Центральный сервер TCP, сервер базы данных, сервер очереди данных, файловый сервер, сервер сетевой печати, сервер обработки удаленных команд и сервер входа в систему - все это системы i5/OS.
 - a. Запустите Администратор цифровых сертификатов IBM на сервере централизованного управления. Если администратору требуется создать или получить сертификаты, либо выполнить другие действия с сертификатами, он должен сделать это сейчас.
 - b. Нажмите кнопку **Выбрать хранилище сертификатов**.
 - c. Выберите ***SYSTEM** и нажмите кнопку **Далее**.
 - d. Введите пароль хранилища сертификатов, и нажмите кнопку **Далее**. После обновления меню разверните папку **Управление приложениями**.
 - e. Нажмите **Обновить присвоение сертификата**.
 - f. Выберите **Сервер** и нажмите кнопку **Далее**.
 - g. Выберите Сервер Централизованного управления и нажмите **Обновить присвоение сертификата**. Теперь системе централизованного управления присвоен сертификат.
 - h. Выберите сертификат, который следует присвоить приложению, и нажмите **Присвоить новый сертификат**. DCM снова откроет страницу **Обновить присвоение сертификата** с подтверждающим сообщением.
 - i. Нажмите **Отмена**, чтобы вернуться к списку приложений.
 - j. Повторите эту процедуру для всех систем i5/OS.
8. Загрузите СА на клиент System i Navigator.

Действия по настройке

Перед применением SSL в функции централизованного управления администратор должен установить все необходимые программы и настроить цифровые сертификаты в центральной системе. Перед тем, как продолжить, обратитесь к предварительным требованиям и предположениям этого сценария. После выполнения всех предварительных требований администратор может выполнить следующие действия для защиты всех соединений с сервером централизованного управления:

Примечание: Если функция SSL включена в System i Navigator, то администратор должен выключить ее перед активацией SSL в Централизованном управлении. Если функция SSL будет включена в System i Navigator и не будет включена в Централизованном управлении, то System i Navigator не удастся подключиться к центральной системе.

1. “Шаг 1: Настройте центральную систему для идентификации сервера” на стр. 10
2. “Шаг 2: Настройте конечные системы для идентификации сервера” на стр. 10
3. “Шаг 3: Перезапустите систему Централизованного управления в центральной системе” на стр. 11
4. “Шаг 4: Перезапустите систему Централизованного управления во всех конечных системах” на стр. 11

5. “Шаг 5: Включите SSL в System i Navigator” на стр. 11
6. “Шаг 6: Настройте центральную систему для идентификации клиента (необязательный шаг)” на стр. 11
7. “Шаг 7: Настройте конечную систему для идентификации клиента” на стр. 12
8. “Шаг 8: Скопируйте контрольный список в конечные системы” на стр. 12
9. “Шаг 9: Перезапустите систему Централизованного управления в центральной системе” на стр. 13
10. “Шаг 10: Перезапустите систему Централизованного управления во всех конечных системах” на стр. 13

Понятия, связанные с данным

“Предварительные требования к SSL” на стр. 19

Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

“Защита приложений с помощью SSL” на стр. 19

Список приложений платформы System i, которые можно защитить с помощью протокола SSL.

Задачи, связанные с данной

“Подробные сведения о настройке: Защита соединения клиента с системой централизованного управления с помощью SSL” на стр. 4

Этот раздел содержит подробное описание шагов по настройке защиты клиентских соединений с сервером централизованного управления с помощью SSL

“Подробные сведения о настройке: Защита всех соединений с системой централизованного управления с помощью SSL”

Этот раздел содержит сведения о защите всех соединений с сервером централизованного управления с помощью SSL

Информация, связанная с данной

Настройка DCM

Первичная настройка сертификатов

Подробные сведения о настройке: Защита всех соединений с системой централизованного управления с помощью SSL

Этот раздел содержит сведения о защите всех соединений с сервером централизованного управления с помощью SSL

Эта информация предполагает, что вы ознакомились с пунктом Сценарий: Защитить все подключения к серверу централизованного управления с помощью SSL.

Ниже приведены инструкции по настройке защищенного подключения всех клиентов к серверу централизованного управления. Вы можете вслед за администратором нашей гипотетической сети выполнить все необходимые операции.

Перед применением SSL в функции централизованного управления администратор должен установить все необходимые программы и настроить цифровые сертификаты в модели System i. После выполнения всех предварительных требований администратор может активировать all для применения в Централизованном управлении, выполнив описанные ниже действия.

Примечание: Если функция SSL включена в System i Navigator, то администратор должен выключить ее перед активацией SSL в Централизованном управлении. Если функция SSL будет включена в System i Navigator и не будет включена в Централизованном управлении, то System i Navigator не удастся подключиться к центральной системе.

С помощью SSL администратор может обеспечить защиту данных, передаваемых по соединению между центральной и конечной системами, а также по соединению между System i Navigator и центральной системой. SSL обеспечивает передачу и идентификацию сертификатов и шифрование данных. Соединение SSL может быть установлено только между центральной и конечной системами, поддерживающими SSL. Прежде чем настраивать идентификацию клиента, необходимо настроить идентификацию сервера:

Понятия, связанные с данным

“Предварительные требования к SSL” на стр. 19

Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

“Сценарий: Защита всех соединений сервера централизованного управления с помощью SSL” на стр. 5

Этот сценарий описывает применение SSL для защиты всех соединений с сервером централизованного управления для модели System i, играющей роль центральной системы функции централизованного управления System i Navigator.

Информация, связанная с данной

Первичная настройка сертификатов

Шаг 1: Настройте центральную систему для идентификации сервера:

1. В окне System i Navigator щелкните правой кнопкой мыши на записи **Централизованное управление** и выберите **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. Выберите уровень идентификации **Сервер**.
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Примечание: НЕ перезапускайте сервер централизованного управления, пока не дойдете до соответствующего прямого указания. Если перезапустить сервер сейчас, то вы не сможете связаться с конечными серверами. Необходимо выполнить задачи настройки до перезапуска сервера и активировать SSL. Конфигурация SSL должна быть распространена на конечные системы задачей Сравнить и обновить.

Шаг 2: Настройте конечные системы для идентификации сервера:

После настройки идентификации сервера в центральной системе администратор должен настроить идентификацию сервера во всех конечных системах. Для этого необходимо выполнить следующие действия:

1. Откройте представление **Централизованное управление**.
2. Сравните и обновите системные значения в конечных системах.
 - a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр → Собрать**.
 - b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций. Нажмите **ОК** и дождитесь завершения работы задачи реестра.
 - c. Правой кнопкой мыши щелкните на пункте **Группы систем → Создать группу систем**.
 - d. Определите группу систем, включающую все конечные системы, с которыми планируется устанавливать соединения SSL. Назовите новую группу систем "Группой защиты".
 - e. Новая группа появится в списке групп систем.
 - f. После создания реестра щелкните правой кнопкой мыши на группе систем и выберите пункт **Системные значения → Сравнить и обновить**.
 - g. Убедитесь, что в поле **Модельная система** указана Центральная система.
 - h. В поле **Категория** выберите **Централизованное управление**.
 - i. Проверьте, задано ли значение **Использовать SSL** равным **Да** и выберите **Обновить**, чтобы передать это значение 'Группе защиты'.
 - j. Проверьте, задано ли значение **Уровень защиты SSL** равным **Сервер** и выберите **Обновить**, чтобы передать это значение 'Группе защиты'.

Примечание: Если эти значения не указаны, выполните Шаг 1: Настройте центральную систему для идентификации сервера.

- k. Нажмите **ОК**. Дождитесь завершения задачи **Сравнить и обновить** перед переходом к следующему шагу.

Шаг 3: Перезапустите систему Централизованного управления в центральной системе:

1. В окне System i Navigator разверните **Мои соединения**.
2. Разверните значок центральной системы.
3. Разверните **Сеть** → **Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **Централизованное управление** и выберите **Остановить**. Список под именем центральной системы будет свернут и появится сообщение о том, что соединение с сервером прервано.
5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 4: Перезапустите систему Централизованного управления во всех конечных системах:

1. В окне System i Navigator разверните **Мои соединения**.
2. Разверните значок конечной системы, в которой нужно перезапустить сервер.
3. Разверните **Сеть** → **Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **Централизованное управление** и выберите **Остановить**.
5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.
6. Выполните эту процедуру во всех конечных системах.

Шаг 5: Включите SSL в System i Navigator:

1. В окне System i Navigator разверните **Мои соединения**.
2. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.
3. Перейдите на страницу **SSL** и выберите опцию **Применять SSL для соединения**.
4. Перезапустите System i Navigator.

Примечание: После этих шагов идентификация сервера настроена в центральной и конечных системах. Можно также по выбору настроить идентификацию клиента в центральной и конечных системах. Для включения идентификации клиента требуется завершить шаги с 6 по 10.

Шаг 6: Настройте центральную систему для идентификации клиента (необязательный шаг):

При необходимости после настройки идентификации сервера администратор может попытаться выполнить следующие процедуры настройки идентификации клиента. При идентификации клиента выполняется проверка Сертификатной компании и уполномоченной группы как центральной, так и конечных систем. Когда центральная система (клиент SSL) пытается установить соединение SSL с конечной системой (сервером SSL), то и центральная, и конечная системы идентифицируют сертификаты друг друга с помощью процедуры идентификации и сервера, и клиента. Эту процедуру называют также идентификацией сертификатной компании или защищенной группы.

Примечание: Настроить идентификацию клиента можно только после того, как настроена идентификация сервера. Если идентификация сервера не настроена, вернитесь назад и настройте ее.

1. В окне System i Navigator щелкните правой кнопкой мыши на записи **Централизованное управление** и выберите **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. Выберите уровень идентификации **Клиент и сервер**.
4. Нажмите кнопку **ОК**, чтобы сохранить это значение в центральной системе.

Примечание: **НЕ** перезапускайте сервер централизованного управления, пока не дойдете до соответствующего прямого указания. Если перезапустить сервер сейчас, то вы не сможете связаться с конечными серверами. Необходимо выполнить задачи настройки до

перезапуска сервера и активировать SSL. Конфигурация SSL должна быть распространена на конечные системы задачей Сравнить и обновить.

Шаг 7: Настройте конечную систему для идентификации клиента:

Сравните и обновите системные значения в конечных системах.

1. Откройте представление **Централизованное управление**.
2. Сравните и обновите системные значения в конечных системах.
 - a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр → Собрать**.
 - b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций. Нажмите ОК и дождитесь завершения работы задачи реестра.
 - c. После создания реестра щелкните правой кнопкой мыши на "Группе защиты" и выберите пункт **Системные значения → Сравнить и обновить**.
 - d. Убедитесь, что в поле **Модельная система** указана Центральная система.
 - e. В поле **Категория** выберите **Централизованное управление**.
 - f. Проверьте, задано ли значение **Использовать SSL** равным **Да** и выберите **Обновить**, чтобы передать это значение 'Группе защиты'.
 - g. Проверьте, задано ли значение **Уровень защиты SSL** равным **Клиент и сервер** и выберите **Обновить**, чтобы передать это значение 'Группе защиты'.

Примечание: Если эти значения не указаны, выполните Шаг 6: Настройте центральную систему для идентификации клиента..

- h. Нажмите **ОК**. Дождитесь завершения задачи **Сравнить и обновить** перед переходом к следующему шагу.

Шаг 8: Скопируйте контрольный список в конечные системы:

Эта задача предполагает, что в центральной системе установлен выпуск операционной системы i5/OS V5R3 или выше. В системах i5/OS до V5R3 QYPSVLDL.VLDL располагался в QUSRSYS.LIB, а не QMGTC2.LIB. По этой причине, если вы отправляете контрольный список в системы выпусков до V5R3, то его необходимо будет поместить в QUSRSYS.LIB, а не в QMGTC2.LIB. В V5R3 и выше выполните следующие действия:

1. В окне System i Navigator разверните запись **Централизованное управление → Определения**.
2. Щелкните правой кнопкой мыши на **Пакет** и выберите **Создать определение**.
3. В окне **Создать определение** задайте следующие значения:
 - a. **Имя:** Введите имя определения.
 - b. **Исходная система:** Введите имя центральной системы.
 - c. **Выбранные файлы и папки:** Щелкните мышью в поле и введите /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL.
4. Перейдите на страницу **Опции** и выберите пункт **Заменить существующий файл на отправленный файл**.
5. Нажмите кнопку **Дополнительно**.
6. В окне **Дополнительные опции** разрешите наличие различий в объектах при выполнении операции восстановления. Для этого выберите **Да** и задайте значение **Целевой выпуск** равным самому раннему выпуску конечных систем.
7. Нажмите кнопку **ОК**. Будет обновлен список определений и показан новый пакет.
8. Щелкните на новом пакете правой кнопкой мыши и выберите опцию **Отправить**.
9. В окне **Отправить** разверните **Группы систем->Уполномоченная группа** в списке **Доступные системы и группы**. Эта группа была определена в "Шаг 2: Настройте конечные системы для идентификации сервера" на стр. 10.

Примечание: Задача **Отправить** не будет выполнена в центральной системе, так как она является исходной системой. Во всех конечных системах задача **Отправить** должна быть успешно выполнена.

10. Если в **Группу защиты** входят системы i5/OS версии ниже чем V5R3, то вручную в этих системах переместите объект QYPSVLDL.VLDL из QMGTC2.LIB в QUSRSYS.LIB. Если версия QYPSVLDL.VLDL уже есть в QUSRSYS.LIB, то удалите ее и замените новой из QMGTC2.LIB

Шаг 9: Перезапустите систему Централизованного управления в центральной системе:

1. В окне System i Navigator разверните **Мои соединения**.
2. Разверните значок центральной системы.
3. Разверните **Сеть** → **Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **Централизованное управление** и выберите **Остановить**. Список под именем центральной системы будет свернут и появится сообщение о том, что соединение с сервером прервано.
5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Шаг 10: Перезапустите систему Централизованного управления во всех конечных системах:

Примечание: Выполните эту процедуру во всех конечных системах.

1. В окне System i Navigator разверните **Мои соединения**.
2. Разверните значок конечной системы, в которой нужно перезапустить сервер.
3. Разверните **Сеть** → **Серверы** и выберите **TCP/IP**.
4. Щелкните правой кнопкой мыши на **Централизованное управление** и выберите **Остановить**.
5. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Общие сведения о SSL

Содержит дополнительную информацию, в том числе некоторые базовые сведения о протоколах SSL.

Протокол SSL позволяет устанавливать защищенные соединения между приложениями клиента и сервера, которые обеспечивают идентификацию одной или обеих конечных систем. SSL гарантирует секретность и целостность данных, которыми обмениваются клиент с сервером.

Принципы работы SSL

SSL представляет собой, фактически, два протокола. Это протокол согласования и протокол передачи данных. Протокол передачи данных управляет потоком данных между двумя конечными системами соединения SSL.

Протокол согласования служит для идентификации одной или обеих конечных систем соединения SSL и создания уникального симметричного ключа, с помощью которого генерируются ключи для шифрования и расшифровки данных, передаваемых по этому соединению. Для идентификации конечных систем в протоколе SSL применяется асимметричное шифрование, цифровые сертификаты и процедуры согласования SSL. Обычно SSL идентифицирует сервер, но может использоваться и для идентификации клиента. Цифровой сертификат, выданный сертификатной компанией, может быть связан с каждой из конечной систем или с приложениями, применяющими протокол SSL в конечных системах.

Цифровой сертификат состоит из общего ключа и идентификационной информации с цифровой подписью уполномоченной сертификатной компании (CA). С каждым общим ключом связан частный ключ. Частный ключ не входит в состав сертификата и хранится отдельно от него. При идентификации клиента или сервера конечная система должна предоставить доказательство наличия частного ключа, соответствующего общему ключу цифрового сертификата.

Применение общих и частных ключей в операциях шифрования обуславливает высокие требования согласований SSL к производительности системы. После установления первого соединения SSL между двумя конечными системами информация об этом соединении и приложениях может быть занесена в кэш в защищенной памяти для ускорения последующих согласований SSL. При возобновлении соединения SSL конечные системы проверяют наличие доступа к уникальной информации путем выполнения сокращенной процедуры согласования без применения общего и частного ключей. Если обе системы предоставят доказательства наличия доступа к этой информации, будут созданы новые симметричные ключи и соединение SSL возобновится. Кэшированная информация соединений TLS версии 1.0 и SSL версии 3.0 будет удалена из защищенной памяти по истечении 24 часов. В выпуске OS/400 V5R2 и последующих, или в i5/OS, влияние процедуры согласования SSL на центральный процессор можно минимизировать, установив аппаратное обеспечение для шифрования.

Информация, связанная с данной

Цифровые сертификаты - концепции

Криптографическое аппаратное обеспечение

Поддержка протоколов SSL и Transport Layer Security (TLS)

Список версий протоколов Secure Sockets Layer (SSL) и Transport Layer Security (TLS), поддерживаемых реализацией i5/OS.

Существует несколько версий протокола SSL. Последней из них является протокол Transport Layer Security (TLS). Он основан на протоколе SSL версии 3.0 и был разработан Рабочей группой Internet (IETF).

Реализация i5/OS поддерживает следующие версии протоколов SSL и TLS:

- TLS версии 1.0
- TLS версии 1.0, с поддержкой SSL версии 3.0

Примечание:

1. TLS версии 1.0 с поддержкой SSL версии 3.0 означает, что будет выполняться согласование TLS, а если это невозможно, то согласование SSL версии 3.0. Если согласование SSL версии 3.0 выполнить нельзя, то процедура согласования SSL не будет выполнена.
2. Кроме того, System i поддерживает TLS версии 1.0 с SSL версии 3.0, включая совместимость с SSL версии 2.0. Этой функции соответствует значение протокола **ALL**, при котором будет выполняться процедура согласования TLS, а если это невозможно, то процедура согласования SSL версии 3.0. Если применить процедуру согласования SSL версии 3.0 невозможно, то выполняется согласование SSL версии 2.0. Если согласование SSL версии 2.0 выполнить нельзя, то процедура согласования SSL выполнена не будет. SSL версии 2.0 по умолчанию не применяется, однако его можно включить путем изменения системного значения QSSLPC. Системное значение QSSLPC позволяет включить и выключить любые протоколы.

- SSL версии 3.0
- SSL версии 2.0
- SSL версии 3.0 с поддержкой SSL версии 2.0

Сравнение SSL версии 3.0 с SSL версии 2.0

Протоколы SSL версии 3.0 и SSL версии 2.0 имеют мало общего. Наиболее важные отличия этих двух протоколов перечислены ниже:

- Потоки процедуры согласования SSL версии 3.0 отличаются от соответствующих потоков согласования SSL версии 2.0.
- SSL версии 3.0 применяет реализацию BSAFE 3.0 компании RSA Data Security, Incorporated. BSAFE 3.0 содержит исправления, защищающие от атак с нарушением синхронизации, и применяют алгоритм

хэширования SHA-1. Алгоритм хэширования SHA-1 считается более надежным, чем алгоритм MD5. Применение SHA-1 позволяет SSL версии 3.0 поддерживать дополнительные сеансы шифрования с SHA-1 вместо MD5.

- Протокол SSL версии 3.0 защищает от атак типа man-in-the-middle (MITM) в процессе согласования SSL. В SSL версии 2.0 существовала небольшая вероятность успешного ослабления шифра с помощью атаки MITM. Ослабление шифра может позволить постороннему пользователю взломать ключ сеанса SSL.

Сравнение TLS версии 1.0 и SSL версии 3.0

Протокол Transport Layer Security (TLS) версии 1.0, основанный на SSL версии 3.0, является последним отраслевым стандартом SSL. Его спецификация определена рабочей группой IETF в документе RFC 2246, *Протокол TLS*.

Цель создания TLS - повышение защиты SSL и более точное и полное определение протокола. TLS обладает следующими преимуществами по сравнению с SSL версии 3.0:

- Более надежный алгоритм MAC
- Более детальные предупреждения
- Более четкие определения спецификаций "серой области"

Все приложения System i, поддерживающие SSL, автоматически поддерживают TLS, если явно не указано, что приложение должно применять SSL версии 3.0 или 2.0.

TLS предоставляет следующие усовершенствованные способы защиты:

- **Хэширование ключей для идентификации с помощью сообщений** - TLS применяет в коде идентификации сообщения (HMAC) хэширование, предотвращающее от изменения записи при передаче по незащищенной сети, например в Internet. SSL версии 3.0 также поддерживает идентификацию сообщений с помощью ключей, но HMAC считается более надежным, чем функция MAC, применяемая в SSL версии 3.0.
- **Улучшенная псевдослучайная функция (PRF)** С помощью PRF создаются данные ключа. В TLS функция PRF определена с помощью HMAC. PRF применяет два алгоритма хэширования, обеспечивающих ее защиту. Если один из алгоритмов будет взломан, данные будут защищены вторым алгоритмом.
- **Улучшенная проверка сообщения "Готово"** - Протоколы TLS версии 1.0 и SSL версии 3.0 отправляют обеим конечным системам сообщение "Готово", означающее, что доставленное сообщение не было изменено. Однако в TLS эта проверка основана на значениях PRF и HMAC, что обеспечивает более высокий уровень защиты по сравнению с SSL версии 3.0.
- **Согласованная обработка сертификатов** - В отличие от SSL версии 3.0, TLS пытается указать тип сертификата, который может применяться различными реализациями TLS.
- **Особые предупреждающие сообщения** - TLS предоставляет более точные и полные предупреждения о неполадках, обнаруженных одной из конечных систем. TLS также содержит информацию о том, когда какие сообщения с предупреждениями следует отправлять.

Информация, связанная с данной



Протокол TLS

Системный SSL

Системный SSL - это набор базовых служб из Лицензионного внутреннего кода (LIC) i5/OS, предназначенных для защиты соединений TCP/IP с помощью протокола SSL/TLS. Системный SSL тесно взаимодействует с операционной системой и кодом сокетов, обеспечивая дополнительную производительность и более надежную защиту.

Разработчики приложений могут обратиться к системному SSL с помощью следующих API и реализации JSSE:

- API Global Secure Toolkit (GSKit)
 - API ILE C доступны из других языков ILE

- Интегрированные API i5/OS SSL_
 - API ILE C доступны из других языков ILE
 - Вместо этого набора API в качестве интерфейса C рекомендуется использовать GSKit.
- Интегрированная реализация i5/OS JSSE
 - Реализация JSSE для JDK 1.4 по умолчанию
 - Реализация i5/OS JSSE доступна для JDK 1.5 и JDK 1.6, однако она не является реализацией по умолчанию.

Приложения SSL, созданные IBM, деловыми партнерами IBM, независимыми вендорами программного обеспечения (ISV) и заказчиками, использующие один из трех указанных выше интерфейсов системного SSL, будут использовать системный SSL. В качестве примеров приложений IBM, использующих системный SSL, можно привести FTP и Telnet. Не все приложения System i с поддержкой SSL используют системный SSL.

Свойства системного SSL

Свойства системного SSL описывают поддерживаемые функции SSL, а также функции SSL, применяемые по умолчанию.

Каждое приложение проверяет, следует ли использовать функции по умолчанию или переопределить их в соответствии с конфигурацией приложения. Многие приложения используют функции системного SSL по умолчанию для реализации новых возможностей системного SSL без внесения изменений в код.

Начиная с i5/OS V6R1, системный SSL предоставляет администраторам точный механизм управления протоколами SSL и комплектами шифров, поддерживаемыми в системе. Перед тем, как приступить к работе с системным SSL, необходимо получить представление о двух основных концепциях. Первая концепция относится к поддерживаемым значениям. Поддерживаемые значения - это функции, поддерживаемые системным SSL. В поставляемой системе активированы не все поддерживаемые функции. Вторая концепция связана со значениями по умолчанию. Значения по умолчанию представляют собой подмножество поддерживаемых значений. Значения по умолчанию применяются, если приложение запрашивает набор функций по умолчанию. Для защиты приложений IBM, использующих значения по умолчанию, от попыток применения более низкого уровня защиты доступ к значениям по умолчанию разрешен только администраторам. Поддержка по умолчанию ограничена поставляемыми значениями по умолчанию. Администратор может дополнительно ограничить функции, поддерживаемые по умолчанию, путем отмены поддержки конкретных функций.

Протоколы SSL

Системный SSL поддерживает следующие протоколы:

- Secure Sockets Layer версии 2.0 (SSLv2)
- Secure Sockets Layer версии 3.0 (SSLv3)
- Transport Layer Security версии 1.0 (TLSv1)

Поставляемые протоколы SSL

Системный SSL поставляется вместе со следующими протоколами:

- Secure Sockets Layer версии 3.0 (SSLv3)
- Transport Layer Security версии 1.0 (TLSv1)

Примечание: Протокол Secure Sockets Layer версии 2.0 (SSLv2) по умолчанию выключен. SSLv2 можно включить путем изменения системного значения QSSLPCL. Системное значение QSSLPCL позволяет включить и выключить любые протоколы.

Поставляемые протоколы SSL по умолчанию

Следующие протоколы по умолчанию применяются по запросу приложений:

- Secure Sockets Layer версии 3.0 (SSLv3)
- Transport Layer Security версии 1.0 (TLSv1)

Примечание: Протокол SSLv2, добавленный администратором в список поддерживаемых протоколов, не добавляется в число протоколов по умолчанию. Удаление протокола по умолчанию из списка поддерживаемых протоколов приводит к его удалению из списка протоколов по умолчанию.

Комплект шифров SSL

Системный SSL поддерживает три комплекта шифров. Комплекты шифров указываются разными способами для каждого программного интерфейса. Ниже указано соглашение об именах системных значений.

Системный SSL может поддерживать следующие комплекты шифров:

- *RSA_NULL_MD5
- *RSA_NULL_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_RC4_128_MD5
- *RSA_RC4_128_SHA
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_DES_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_AES_256_CBC_SHA
- *RSA_RC2_CBC_128_MD5
- *RSA_DES_CBC_MD5
- *RSA_3DES_EDE_CBC_MD5

Поставляемый список спецификаций шифров SSL

Список спецификаций шифров содержит список комплектов шифров. Системный SSL поставляется вместе с десятью поддерживаемыми комплектами шифров. Администратор может управлять поддерживаемыми шифрами с помощью системных значений QSSLCSL и QSSLCSLCTL. При необходимости поддержку комплекта шифров можно отменить в соответствии с требованиями протокола SSL.

Следующие комплекты шифров поставляются в качестве поддерживаемых:

- *RSA_AES_256_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5

Список спецификаций поддерживаемых шифров может изменяться в соответствии с требованиями протоколов SSL, а также с помощью системного значения QSSLCSL. Системное значение QSSLCSL позволяет просмотреть список спецификаций шифров системы.

Поставляемый список спецификаций шифров SSL по умолчанию

Ниже перечислены записи из списка спецификаций шифров по умолчанию:

- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA

При необходимости список спецификаций шифров по умолчанию можно уменьшить или переупорядочить с помощью системного значения QSSLCSL. Добавление дополнительных комплектов шифров запрещено.

Информация, связанная с данной

Системное значение SSL: QSSLPCL

Системное значение SSL: QSSLCSLCTL

Системное значение SSL: QSSLCSL

Идентификация сервера

При идентификации сервера клиент проверяет подлинность сертификата сервера и наличие в нем подписи сертификатной компании, уполномоченной клиентом.

С помощью асимметричного шифрования и протокола согласования SSL генерирует симметричный ключ, который будет применяться только для данного соединения. С помощью этого ключа создается набор ключей для шифрования и расшифровки данных, передаваемых через соединение SSL. По окончании процедуры согласования SSL будет идентифицирована одна или обе конечные системы соединения, и будет создан уникальный ключ для шифрования и расшифровки данных. После согласования данные уровня приложения будут передаваться через соединение SSL в зашифрованном виде.

Идентификация клиента

Многие приложения поддерживают опцию идентификации клиента. При идентификации клиента сервер проверяет подлинность сертификата клиента и наличие в нем подписи сертификатной компании, уполномоченной сервером.

Идентификацию клиента поддерживают следующие приложения System i:

- IBM HTTP Server for i5/OS
- Сервер FTP
- Сервер Telnet
- Конечная система Централизованного управления
- IBM Tivoli Directory Server for i5/OS

Информация, связанная с данной

Поддержка протоколов SSL и TLS на сервере каталогов

Защита клиента FTP с помощью Transport Layer Security или Secure Sockets Layer

Защита Telnet с помощью SSL

Настройка SSL на сервере администрирования (ADMIN) для сервера HTTP

Предварительные требования к SSL

Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

Перед настройкой SSL установите следующие продукты:

- IBM Digital Certificate Manager (DCM) (5761-SS1, компонент 34)

Примечание: DCM не требуется для IBM Java Secure Socket Extension (JSSE) и OpenSSL.

- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
- IBM HTTP Server for i5/OS (5761-DG1)
- Если при работе с DCM вы планируете применять сервер HTTP, необходимо установить продукт IBM Developer Kit for Java (5761-JV1). В противном случае вам не удастся запустить сервер администрирования HTTP.
- Вы также можете установить аппаратное обеспечение для шифрования, которое позволяет ускорить процесс согласования SSL. Если вы решите установить аппаратное обеспечение шифрования, то вам потребуется установить Cryptographic Service Provider.

Примечание: 5722 - это код продукта для компонентов и продуктов i5/OS до V6R1.

Понятия, связанные с данным

“Устранение неполадок SSL” на стр. 20

В этом разделе приведены общие рекомендации по устранению неполадок, которые могут возникнуть в системах System i при работе с протоколом SSL.

Информация, связанная с данной

Криптографическое аппаратное обеспечение

Личные сертификаты и открытые сертификаты

Настройка DCM

Защита приложений с помощью SSL

Список приложений платформы System i, которые можно защитить с помощью протокола SSL.

С помощью SSL можно защитить следующие приложения System i:

- Преобразование идентификаторов в рамках предприятия (EIM)
- Сервер FTP
- IBM HTTP Server for i5/OS
- System i Access for Windows
- IBM Tivoli Directory Server for i5/OS
- Сервер архитектуры распределенных реляционных баз данных (DRDA) и управления распределенными данными (DDM)
- Централизованное управление
- Сервер Telnet
- Websphere Application Server - Express
- Приложения, написанные с использованием интерфейсов прикладных программ (API) System i Access for Windows
- Приложения, созданные с применением API защищенных сокетов, поддерживаемых платформой System i. Поддерживаются API из Global Secure Toolkit (GSKit) и API SSL_System i.

Понятия, связанные с данным

“Сценарий: Защита всех соединений сервера централизованного управления с помощью SSL” на стр. 5
Этот сценарий описывает применение SSL для защиты всех соединений с сервером централизованного управления для модели System i, играющей роль центральной системы функции централизованного управления System i Navigator.

Информация, связанная с данной

Преобразование идентификаторов в рамках предприятия (EIM)

Работа с SSL для защиты сервера FTP

Сервер HTTP

Администрирование SSL (раздел iSeries Access для Windows)

Сценарий Telnet: Защита Telnet с помощью SSL

API защищенных сокетов

Устранение неполадок SSL

В этом разделе приведены общие рекомендации по устранению неполадок, которые могут возникнуть в системах System i при работе с протоколом SSL.

Данный раздел является не полным руководством по устранению неполадок, а всего лишь подсказывает, как решать часто встречающиеся задачи.

Убедитесь, что выполнены следующие условия:

- Выполнены предварительные требования протокола SSL для платформы System i.
- Убедитесь, что срок действия сертификатной компании и сертификатов не истек, и сертификатная компания является уполномоченной CA.

Если несмотря на соблюдение всех перечисленных выше условий на вашем сервере возникла неполадка SSL, попробуйте выполнить следующие действия:

- Найдите код ошибки SSL в протоколе задания сервера, а затем найдите дополнительную информацию об ошибке в таблице ошибок по ее коду. Например, если в протоколе задания сервера указан код ошибки -93, то по таблице можно определить, что он соответствует константе `SSL_ERROR_SSL_NOT_AVAILABLE`.
 - Отрицательный код возврата (есть дефис перед значением кода) означает, что применялся `SSL_API`.
 - Положительный код возврата означает, что применялся `API GSKit`. Для получения краткого описания кода возврата, свидетельствующего об ошибке, в программах могут применяться `API gsk_strerror()` и `SSL_strerror()`. С помощью этих API приложение может занести в протокол задания сообщение с описанием ошибки.

Для получения более подробной информации просмотрите сообщение с идентификатором, указанным в таблице, в модели System i. В этом сообщении описана возможная причина ошибки и перечислены действия по ее исправлению. Дополнительную информацию с описанием кодов ошибок можно найти в документации по тому API защищенных сокетов, который вернул код ошибки.

- Имена констант, соответствующие системным кодам возврата SSL, перечислены и в указанных ниже файлах заголовков (без ссылки на ИД сообщения):
 - `QSYSINC/H.GSKSSL`
 - `QSYSINC/H.QSOSSL`

Хотя все имена констант, перечисленные в этих файлах, уникальны, один код возврата может соответствовать разным ошибкам.

Понятия, связанные с данным

“Предварительные требования к SSL” на стр. 19



Содержит список предварительных требований, которые должны быть выполнены в системе System i для поддержки SSL, а также некоторые полезные советы и рекомендации.

Информация, связанная с данной

Связанная информация по SSL

Список других информационных ресурсов, связанных с протоколом Secure Sockets Layer (SSL).

Web-сайты

- RFC 2246: "The TLS Protocol Version 1.0"  (ftp://ftp.isi.edu/in-notes/rfc2246.txt)
содержит подробное описание протокола TLS.
- RFC2818: "HTTP Over TLS"  (ftp://ftp.isi.edu/in-notes/rfc2818.txt)
Содержит информацию о защите соединений HTTP в Internet с помощью TLS.

Прочая информация

- SSL и Java Secure Socket Extension
- IBM Toolbox for Java

Приложение. Примечания

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

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Consult your local IBM representative for information on the products and services currently available in your area. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

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

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

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

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

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

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

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

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

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

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

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

- | Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы
- | предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного
- | соглашения о лицензии на программу IBM, Лицензионного соглашения о машинном коде IBM или любого
- | другого эквивалентного соглашения.

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

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

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

Эта информация содержит примеры данных и отчетов, применяемых в повседневной работе. Для того чтобы примеры были максимально наглядными, в них указаны имена людей, а также названия компаний, товарных знаков и продуктов. Все они являются вымышленными, и любое совпадение с реально существующими именами и названиями случайно.

Лицензия на продукты, защищенные авторским правом:

Эта информация содержит примеры приложений на исходном языке, иллюстрирующие приемы программирования в различных операционных платформах. Разрешается бесплатно копировать, изменять и распространять в любой форме эти примеры с целью разработки, использования и распространения прикладных программ для интерфейсов, соответствующих той операционной платформе, для которой созданы примеры. Они не проверялись для работы во всех условиях. По этой причине, IBM не может гарантировать их надежность и пригодность.

Любая копия или часть этих примеров программ, а также произведений, созданных на их основе, должна содержать следующее заявление об авторских правах:

© (название вашей фирмы) (год). Этот код частично создан на основе примеров программ фирмы IBM Corp.
© Copyright IBM Corp. _год или годы. Все права защищены.

В электронной версии данной документации фотографии и цветные иллюстрации могут отсутствовать.

Товарные знаки

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

- | DRDA
- | i5/OS
- | IBM
- | OS/400
- | System i
- | Tivoli

| Adobe, эмблема Adobe, PostScript и эмблема PostScript являются товарными знаками или зарегистрированными товарными знаками Adobe Systems в США и/или других странах.

Java и все товарные знаки Java-based являются товарными знаками корпорации Sun в Соединенных Штатах и/или других странах.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Напечатано в Дании