THALES

ProtectServer 3 HSM и ProtectToolkit 7

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

Информация о документе

Последняя редакция	2022-01-06 11:17:18-05:00

Отказ от ответственности
Вся содержащаяся в настоящем документе информация либо является общедоступной, либо принадлежит на правах исключительной собственности Thales Group и/или ее дочерним компаниям, которые обладают исключительным правом подачи заявок на патенты или использования защиты интеллектуальной собственности иного рода в связи с такой информацией.

Ничто из содержащегося в настоящем документе не может рассматриваться как подразумевающее или предоставляющее вам какие-либо права на основании лицензии, концессии или иным образом в отношении любых прав интеллектуальной собственности и/или прав на промышленную собственность или в отношении какой-либо информации, принадлежащей Thales Group.

Настоящий документ может использоваться в информационных целях, не для получения прибыли, внутри компании и в личных целях только при условии, что:

> Сведения об авторских правах, требованиях конфиденциальности и защиты служебной информации, а также полный текст данного предупреждения будут присутствовать на всех экземплярах документа.

> Настоящий документ не будет опубликован ни на каком общедоступном сетевом ресурсе и не будет транслироваться никаким иным образом. При этом любые изменения какой-либо части настоящего документа запрещены.

Использование настоящего документа в каких-либо иных целях явным образом запрещено и может повлечь за собой серьезную административную или уголовную ответственность.

Содержащаяся в настоящем документе информация предоставляется на условиях «КАК ЕСТЬ» без предоставления гарантий любого рода. Если иное не будет оговорено в письменном виде, Thales Group не предоставляет никаких гарантий в отношении ценности или точности содержащейся в настоящем документе информации.

Данный документ может содержать технические неточности или опечатки. В содержание настоящего документа могут периодически вноситься изменения. Вместе с тем, компания Thales сохраняет за собой право в любое время вносить любые изменения или улучшать технические характеристики, информацию и иное содержание настоящего документа.

Thales Group настоящим отказывается от ответственности по любым гарантиям и условиям в отношении содержащейся в настоящем документе информации, включая все подразумеваемые гарантии товарных качеств, пригодности для определенной цели, прав собственности и ненарушения прав. Thales Group ни при каких обстоятельствах не несет ответственности на основании контракта, в связи с правонарушением или на иных основаниях за любые косвенные убытки, фактические убытки, определяемые особыми обстоятельствами, последующие убытки или убытки любого рода, включая, помимо прочего, убытки, возникающие в результате утраты возможности использования, потери данных, прибыли, доходов или клиентов в результате использования информации, содержащейся в настоящем документе, или в связи с ним.

Thales Group не предоставляет и не намерена предоставлять никаких гарантий в отношении того, что настоящий продукт будет устойчив ко всем возможным видам атак и отказывается от любой ответственности в этой связи. Даже если каждый продукт будет соответствовать действующим на дату разработки стандартам безопасности, надежность механизмов защиты непосредственно зависит от уровня развития отрасли информационной безопасности и, в частности, от появления новых видов атак. Thales Group ни при каких обстоятельствах не несет ответственности ни за какие действия третьих лиц, в том числе за успешные атаки на системы или оборудование, использующие продукты компании Thales. Thales Group отказывается от любой ответственности за обеспечение безопасности в связи с возникновением прямых, косвенных, случайных или последующих убытков в результате использования ее продукции.

Также обращаем ваше внимание, что производитель настоятельно рекомендует пользователю продукта самостоятельно проводить его тестирование и проверку, в особенности при любом применении, когда неисправность, ненадлежащая или небезопасная работа могут привести к получению травмы людьми или повреждению имущества, отказу в обслуживании или нарушению конфиденциальности.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ: Информация о руководстве по установке аппаратного модуля безопасности ProtectServer 3 и ProtectToolkit 7

Данное руководство описывает порядок действий по установке и настройке аппаратного обеспечения для приобретенного вами аппаратного модуля безопасности (HSM) ProtectServer, поддерживающего различные криптографические функции, и порядок действий по установке клиентского программного обеспечения ProtectToolkit.
Обратитесь к разделам, относящимся к вашей модели ProtectServer 3 HSM:

> «Установка аппаратного обеспечения PCIe устройства ProtectServer 3» на странице 10

> «Установка и настройка ProtectServer 3 External» на странице 16

> «Установка и настройка ProtectServer 3+ External» на странице 34

> «Установка программного обеспечения ProtectToolkit 7» на странице 70

> «Элементы конфигурации» на странице 94

Во введении также содержится следующая информация о данном документе:

> «Условные обозначения, принятые в документе» в следующем пункте

> «Контактные данные службы технической поддержки» на странице 9

Информация о статусе документа и истории изменений содержится в разделе «Информация о документе» на странице 2.

Условные обозначения, принятые в документе

В настоящем документе используются стандартные условные обозначения для описания пользовательского интерфейса и привлечения вашего внимания к важной информации.

Примечания

Примечания используются для привлечения внимания к важной или полезной информации.
Для примечаний применяется следующий формат:

> **ПРИМЕЧАНИЕ:** Примите к сведению! Содержит важную или полезную информацию.

Предостережения

Предостережения используются для привлечения внимания к важной информации, которая может помочь предотвратить нештатную ситуацию или потерю данных.
Для предостережений применяется следующий формат:

> **ПРЕДОСТЕРЕЖЕНИЕ!** Соблюдайте осторожность! Предостережения содержат важную информацию, которая может помочь предотвратить нештатную ситуацию или потерю данных.

Предупреждения

Предупреждения используются для привлечения внимания к возможности потери критически важных данных или получения травмы. Для предупреждений применяется следующий формат:

> ****ПРЕДУПРЕЖДЕНИЕ** Соблюдайте максимальную осторожность и выполняйте все требования охраны труда и безопасности. В данной ситуации ваши действия могут привести к потере критически важных данных или получению травмы.**

Синтаксис команд и условные обозначения в тексте

Формат	Использование
жирный	Использование жирного шрифта обозначает следующее: > Команды и необязательные параметры консольной программы (Введите «**dir /p**».) > Наименования кнопок (Нажмите кнопку «**Сохранить как» (Save As)**.) > Наименования кнопок-флажков и кнопок-переключателей (Отметьте флажок «**Печать с двух сторон**» (**Print Duplex**).) > Заголовки диалоговых окон (В диалоговом окне **«Защитить документ**» (**Protect Document)** нажмите кнопку «**Да**» (**Yes**).) > Наименования полей («**Имя пользователя**» (**User Name):** Введите имя пользователя.) > Наименования элементов меню (В меню «**Файл**» (**File**) нажмите на пункт «**Сохранить**» (**Save**).) (Нажмите на «**Меню**» (**Menu) > «Перейти» (Go To) > «Папки» (Folders).**) > Пользовательский ввод (В поле «**Дата**» (**Date)** введите «**1 апреля**» (**April 1)**.)
курсив	В печатном тексте курсив используется для того, чтобы подчеркнуть что-либо или выделить перекрестную ссылку на другие документы в пакете документации.
<переменная>	В описаниях команд угловые скобки указывают на переменные. В угловых скобках указываются значения аргументов консольной команды.
[необязательно] [<необязательно>]	Выделение необязательных **ключевых слов** или <переменных> в описании команды. Как вариант, указывайте ключевое слово или <переменную> в квадратных скобках, если это необходимо или рекомендуется для завершения задачи.
{**a**|**b**|**c**} {<a>|<b>|<c>}	Выделение обязательных вариантов **ключевых слов** или <переменных> в описании команды. Необходимо выбрать один аргумент консольной команды из перечисленных в фигурных скобках. Варианты разделяются вертикальной чертой (ИЛИ).
[**a**|**b**|**c**] [<a>|<b>|<c>]	Выделение необязательных вариантов ключевых слов или переменных в описании команды. По желанию выберите один аргумент консольной команды из перечисленных в скобках. Варианты разделяются вертикальной чертой (ИЛИ).

Контактные данные службы технической поддержки

В случае возникновения проблем в ходе установки, регистрации или эксплуатации данного продукта перед обращением в службу технической поддержки ознакомьтесь с документацией по нему. Если проблему устранить не получится, свяжитесь с вашим поставщиком или со Службой поддержки клиентов компании Thales.

Служба поддержки клиентов компании Thales обслуживает клиентов круглосуточно и без выходных дней. Уровень вашего доступа к данной службе определяется тарифным планом технической поддержки, по которому компания Thales обслуживает вашу организацию. Пожалуйста, обратитесь к описанию тарифного плана для получения подробной информации о доступных вам услугах, включая время получения технической поддержки по телефону.

Портал поддержки клиентов

Портал поддержки клиентов, доступный по адресу https://supportportal.thalesgroup.com, предлагает решения наиболее распространенных проблем. Портал поддержки клиентов представляет собой многоцелевую с опцией расширенного поиска базу данных ресурсов технической поддержки, включая загрузку программного обеспечения и встроенного программного обеспечения, комментарии по известным проблемам и путям их временного решения, базу знаний, ответы на часто задаваемые вопросы, документацию по продукции, технические заметки и многое другое. Кроме того, портал может использоваться для создания кейсов клиентской поддержки и управления ими.

> **ПРИМЕЧАНИЕ:** для доступа к Порталу поддержки клиентов требуется регистрация. Для регистрации учетной записи посетите портал и щелкните по ссылке «**РЕГИСТРАЦИЯ**» (**REGISTER**).

Обращение по телефону

На портале поддержки также указаны телефонные номера для голосовой связи (раздел «Контактная информация» (Contact Us)).

РАЗДЕЛ 2: Установка и настройка ProtectServer 3 External

Данный раздел содержит указания по установке и конфигурации аппаратного модуля безопасности (HSM) ProtectServer 3 External, поддерживающего различные криптографические функции. Ниже описывается общая процедура настройки криптопровайдера с использованием ProtectServer 3 External в сетевом режиме.

1. При необходимости ознакомьтесь с информацией в разделе «Краткая информация об изделии» на странице 17.

2. Убедитесь в комплектности поставки согласно разделу «Необходимое оборудование ProtectServer 3 External» на странице 21.

3. Установите ProtectServer 3 External в стандартную серверную стойку и подключите считыватель смарт-карт (см. раздел «Установка оборудования ProtectServer 3 External» на странице 23).

4. Ознакомьтесь с «Рекомендациями по вводу в эксплуатацию» на странице 24 для безопасной эксплуатации изделия.

5. Выполните первоначальное подключение к устройству и убедитесь в надлежащей работе системы (см. раздел «Первый вход в систему и тестирование» на странице 25).

6. Настройте сетевые параметры ProtectServer 3 External (см. раздел «Настройка сетевых параметров» на странице 27).

7. Установите и настройте программное обеспечение ProtectToolkit (см. раздел «Установка программного обеспечения ProtectToolkit 7» на странице 70).

8. Настройте высокоуровневый интерфейс прикладного программирования (API) для работы с криптопровайдером в необходимых режимах. Для этого могут потребоваться следующие действия:

   - организация доверенного канала или системы безопасного обмена сообщениями (SMS) между API и ProtectServer 3+ External.

   - организация передачи данных между сетевым клиентом и ProtectServer 3+ External.

В данном разделе также содержится следующая дополнительная информация/описание действий:

> «Отключение питания ProtectServer 3 External» на странице 32

> «Обновление образа программного обеспечения устройства» на странице 32

Краткая информация об изделии

ProtectServer 3 External представляет собой защищенный сервер в отдельном корпусе, предоставляющий аппаратные криптографические функции в сети TCP/IP. Совместно с ПО высокоуровневого интерфейса прикладного программирования (API) SafeNet, данный продукт используется в качестве криптопровайдера для обширного диапазона защищенных приложений.

Модуль ProtectServer 3 External выполнен на базе ПК. Он помещен в прочный стальной корпус со стандартными для ПК разъемами и элементами управления. В качестве операционной системы используется ОС Linux с предустановленными программными компонентами. Необходимо произвести настройку сетевых параметров, как описано в настоящем документе.

За счет выделенного аппаратного криптоускорителя ProtectServer 3 External поддерживает полный диапазон криптографических сервисов, необходимых пользователям инфраструктуры открытых ключей (PKI). Данные сервисы включают шифрование, расшифровку, генерацию и проверку подписей и управление ключами в защищенном от несанкционированного доступа и оснащенном резервным аккумулятором хранилище ключей.

ProtectServer 3 External необходимо использовать с одним из высокоуровневых криптографических интерфейсов прикладного программирования компании SafeNet. В нижеприведенной таблице перечислены типы криптопровайдеров и соответствующие API компании SafeNet:

API	Необходимый продукт SafeNet
PKCS #11	ProtectToolkit-C
JCA / JCE	ProtectToolkit-J
Microsoft IIS и CA	ProtectToolkit-M

Данные API непосредственно взаимодействуют с системным ядром устройства, сертифицированным по FIPS 140-2 уровня 3 и обеспечивающим высокую скорость аппаратных криптографических преобразований. Хранилище ключей защищено от несанкционированного доступа и оснащено аккумулятором.

Считыватель смарт-карт, которым оснащен HSM, обеспечивает безопасную загрузку и резервное копирование ключей.

Передняя панель

Ниже показаны элементы передней панели устройства ProtectServer 3 External:

Рисунок 1: передняя панель устройства ProtectServer 3 External

Разъемы
На передней панели размещены следующие разъемы:

VGA	Не подключен.
Console	Используется для предоставления доступа к консоли устройства. См. раздел «Первый вход в систему и тестирование» на странице 25.
USB	Не подключен.

eth0 eth1	Порты Ethernet RJ45 (10/100/1000 Мбит/с) с функцией автоматического определения скорости для подключения устройства к сети.
HSM USB	Используется для подключения к устройству считывателя смарт-карт с помощью входящего в комплект поставки кабеля USB-Serial.

Светодиодные индикаторы
На передней панели размещены следующие светодиодные индикаторы:

Power	Индикатор светится зеленым цветом, если питание устройства включено.
HDD	Мигает желтым цветом при обращении к жесткому диску.
Status	Мигает зеленым цветом во время пуска.

Кнопка перезагрузки системы
Кнопка перезагрузки системы располагается между разъемами USB и Ethernet. Нажатие данной кнопки приводит к немедленной перезагрузке устройства. При этом происходит перезапуск программного обеспечения без отключения питания устройства. Перезагрузка прерывает работу устройства и при обычных условиях не рекомендуется.

Задняя панель

Ниже показаны элементы задней панели устройства ProtectServer 3 External:

Рисунок 2: задняя панель устройства ProtectServer 3 External

Защита от вскрытия корпуса
Функция защиты от вскрытия корпуса используется при вводе устройства в эксплуатацию или выводе из эксплуатации для уничтожения любых ключей, хранящихся в аппаратном модуле безопасности.

Если переключатель находится в горизонтальном (Active) положении, аппаратный модуль безопасности работает в обычном режиме. При переводе переключателя в вертикальное (Tamper) положение аппаратный модуль безопасности регистрирует вскрытие и любые ключи, хранящиеся в аппаратном модуле безопасности, уничтожаются.

> **ВНИМАНИЕ!** При повороте переключателя из положения Active в положение Tamper любые хранящиеся в аппаратном модуле безопасности ключи удаляются. Удаленные ключи восстановлению не подлежат. Убедитесь в наличии у вас резервных копий ключей. Чтобы не допустить случайного удаления ключей с используемого устройства ProtectServer 3 External, снимите ключ защиты от вскрытия корпуса после ввода в эксплуатацию и сохраните его в надежном месте.

Криптографическая архитектура

Аппаратная криптографическая система состоит из трех компонентов общего назначения:

> Один или более аппаратных модулей безопасности (HSM) для обработки и хранения ключей защиты.

> ПО высокоуровневого криптографического API. Данное ПО использует криптографический функционал аппаратного модуля безопасности, чтобы приложения могли пользоваться сервисами защиты.

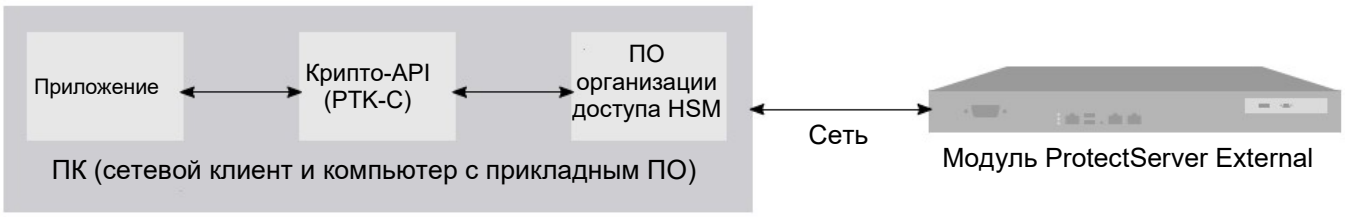
> Программное обеспечение организации доступа, обеспечивающее обмен данными между API и аппаратными модулями безопасности.

Работая в сетевом режиме, устройство ProtectServer 3 External может самостоятельно производить обработку и хранение ключей защиты.

В сетевом режиме ПО организации доступа устанавливается на том же компьютере, на котором установлено ПО криптографического API. ПО организации доступа обеспечивает обмен данными между API и устройством ProtectServer 3 External по протоколу TCP/IP. Таким образом, аппаратный модуль безопасности может быть установлен удаленно, что увеличит защищенность данных криптографических ключей.

На нижеприведенном рисунке схематично показана работа криптопровайдера с использованием устройства ProtectServer 3 External в сетевом режиме.

Рисунок 3: использование устройства ProtectServer 3 External



Технические характеристики

ProtectServer 3 External имеет следующие характеристики:

Аппаратное обеспечение

> Один защищенный USB-разъем для подключения считывателя смарт-карт (необходимо использовать входящий в комплект кабель USB-Serial)
> Защитный корпус из высокопрочной стали промышленной категории
> Процессор Intel® Atom™ E3827 с рабочей частотой 1,74 ГГц
> 2 Гб RAM
> Твердотельный жесткий диск на основе флеш-памяти объемом 4 Гб (DOM)
> Сетевой интерфейс 10/100/1000 Мбит/с с функцией автоматического определения скорости с разъемом RJ45 LAN

Предустановленное программное обеспечение

> Операционная система Linux
> ПО организации доступа ProtectServer HSM Access Provider
> Серверное ПО ProtectServer HSM Net Server

Источник электропитания

> Номинальная мощность: 43 Вт
> Диапазон напряжения питания на входе (перем.): 100 ÷ 240 В
> Диапазон частоты входного напряжения: 50 ÷ 60 Гц

Физические характеристики

> 437 мм (Ш) x 270 мм (Г) x 44 мм (В) (1U)

> 19-дюймовые кронштейны для монтажа в стойке в комплекте
> Масса: 5 кг (11 фунтов)

Условия эксплуатации

> Температура: 0 ÷ 40 °C (32 ÷ 104 °F)
> Относительная влажность: 5 ÷ 85%

Необходимое оборудование ProtectServer 3 External

В данном разделе перечислены компоненты, которые вы должны были получить в комплекте с заказанным вами ProtectServer 3 External.

Комплект поставки

В нижеприведенной таблице перечислено стандартное оборудование, входящее в комплект поставки:

К-во	Наименование
1	**Устройство ProtectServer 3 External в корпусе** 
1	**Соединительный кабель: RJ45 - USB со стандартным модульным разъемом на восемь контактов 8P8C**  **ПРИМЕЧАНИЕ:** внешнее устройство ProtectServer 3 External можно настраивать с терминала, подключенного к порту для доступа к консоли устройства с помощью входящего в комплект поставки кабеля RJ45 – USB. Два USB-разъема и разъем VGA устройства не подключены и не могут быть использованы для подключения клавиатуры, мыши или монитора для настройки устройства.
1	**Считыватель смарт-карт** 

К-во	Наименование
5	**Смарт-карты** (в одном чехле) На одной смарт-карте может храниться 64 килобайта данных. 

ПРИМЕЧАНИЕ!

> Кабели питания более не включаются в комплект поставки. Приобретайте кабели питания у местных поставщиков.

Дополнительное оборудование

Ваш аппаратный модуль безопасности ProtectServer 3 может использоваться с нижеперечисленным оборудованием. Для заказа данного оборудования свяжитесь с торговым представителем компании Thales.

> **OTP-токены SafeNet 110 с ограничением по времени действия пароля** (позволяют использовать многофакторную аутентификацию с токенами ProtectServer 3 HSM)

Компания Thales рекомендует заказывать не менее 2 (двух) OTP-токенов для каждого слота HSM (по одному для работника службы охраны и пользователя токена).

Номер изделия: 955-000237-001

> **Панель для ввода ПИН-кода компании Verifone, совместимая с оборудованием ProtectServer** (позволяет вводить ключ защиты вручную)

Номер изделия: 934-000087-001

Установка аппаратного обеспечения ProtectServer 3 External

Поскольку ProtectServer 3 External поставляется с предустановленным необходимым программным обеспечением, установка дополнительного ПО непосредственно на устройстве не требуется.

После установки следует убедиться, что устройство функционирует надлежащим образом, и настроить сетевые параметры. Данные действия описаны в разделе «Первый вход в систему и тестирование» на странице 25.

Установка аппаратного обеспечения

1. Выберите подходящее место для установки оборудования. Модуль ProtectServer 3 External может быть установлен в стандартной 19-дюймовой стойке.

   ПРИМЕЧАНИЕ: для отключения электропитания устройства используется кабель питания. Необходимо, чтобы основная розетка питания, к которой подключается устройство, была легко доступной.

2. Подключите ProtectServer 3 External к сети с помощью стандартного Ethernet-кабеля, подключаемого к разъемам LAN, располагающимся на передней панели устройства (обозначены *eth0* и *eth1*). Клиентские устройства с установленным криптографическим API компании SafeNet должны располагаться в одной сети с подключаемым модулем.

   ПРИМЕЧАНИЕ: ProtectServer 3 External оснащается двумя сетевыми картами (*eth0* и *eth1*), позволяющими использовать двойной стек протоколов IPv4/IPv6 и, соответственно, присваивать каждому интерфейсу как адреса IPv4, так и адреса IPv6. Если вы планируете использовать обе сетевые карты, подключите Ethernet-кабель к обоим разъемам LAN.

3. Подключите кабель питания к устройству и к надлежащему источнику питания. ProtectServer 3 External оборудовано блоком питания с функцией автоматического определения напряжения, который может работать от сети напряжением 100-240 В и частотой 50-60 Гц.

Установка считывателя смарт-карт

Устройство поддерживает использование смарт-карт с помощью считывателя, поставляемого компанией Thales. Другие считыватели смарт-карт не поддерживаются.

Порядок установки считывателя карт с интерфейсом USB

Просто вставьте кабель считывателя карт в USB-разъем HSM, как показано на рисунке ниже.

Дальнейшие инструкции содержатся в разделе «Первый вход в систему и тестирование» на странице 25.

Рекомендации по вводу в эксплуатацию

Пользователям следует руководствоваться передовым опытом в сфере защиты данных и выполнения нормативных требований при вводе в эксплуатацию ProtectServer 3 External в своей сети / среде прикладной системы:

> «Система безопасного обмена сообщениями (SMS)» – см. ниже

> «Подключение к сети и настройка межсетевого экрана» – см. ниже

> «Разделение уровней доступа» – см. на следующей странице

Система безопасного обмена сообщениями (SMS)

ProtectServer 3 External сохраняет криптографические ключи и другие объекты в защищенной памяти, которая стирается при обнаружении несанкционированного доступа. Для доступа к сохраненным ключам используются вызовы функций PKCS#11 клиентским ПО. Клиентское ПО обращается к ProtectServer 3 External на сетевом уровне (TCP/IP). Устанавливаемый по умолчанию режим защиты не предусматривает шифрования канала обмена данными между HSM и клиентскими программами. Для улучшения защиты канала следует настроить политику безопасности HSM. Описание доступных флагов и их влияния на систему содержится в разделе «Флаги безопасности» на странице 1 *Руководства по администрированию ProtectToolkit-C*.

Система безопасного обмена сообщениями (SMS) увеличивает защищенность канала передачи данных между клиентскими программами и HSM. SMS предоставляет канал с криптографической защитой между клиентскими программами и HSM и обеспечивает контроль подлинности передаваемых по каналу сообщений с помощью кода проверки подлинности сообщений (MAC), соответствующего стандарту FIPS 140-2. Подробное описание функций SMS содержится в разделе «Безопасный обмен сообщениями» в *Руководстве по администрированию ProtectToolkit-C*.

> **ПРИМЕЧАНИЕ:** SMS обеспечивает шифрование и проверку подлинности сообщений между клиентскими программами и HSM и позволяет клиентским программам проверять подлинность учетных данных HSM.
>
> Данный флаг требует наличия действительного идентификационного ключа/сертификата ProtectServer на устройстве HSM. Подробные данные и описание действий содержатся в разделе «Сертификат владельца и идентификационные сертификаты ProtectServer» *Руководства по администрированию ProtectToolkit-C*.

Функция SMS универсальная и может быть настроена на:

> Шифрование/расшифровку всех сообщений

> Подписание/проверку всех сообщений

Для обеспечения максимальной защиты следует активировать все указанные функции. Описания флагов и инструкции по настройке содержатся в разделе «Флаги безопасности» в *Руководстве по администрированию ProtectToolkit-C*.

> **ПРИМЕЧАНИЕ:** включение режима FIPS автоматически включает SMS и блокирует все механизмы, не соответствующие стандарту FIPS. Не включайте режим FIPS, если вы используете не соответствующие данному стандарту механизмы и понимаете последствия своих действий.

Подключение к сети и настройка межсетевого экрана

Клиентская программа PTK аутентифицирует ProtectServer 3 HSM по его идентификационному сертификату ProtectServer (PIC). При этом способа аутентифицировать клиентскую программу на HSM не существует. В связи с этим рекомендуется подключать HSM и компьютер с клиентским ПО к одному защищенному сегменту сети, чтобы не допустить передачи конфиденциальных данных по незащищенным промежуточным сетям.

Необходимо всегда проверять соответствие полученного сертификата ожидаемым данным (серийный номер HSM, дата выпуска и прочие). Такая конфигурация позволяет предотвратить «атаку посредника» (MITM) и другие виды атак. По возможности следует соединять HSM и клиентский компьютер напрямую, с помощью кросс-кабеля.

В ProtectServer 3 External предусмотрены два сетевых разъема, каждый из которых можно подключить к отдельной сети. Настоятельно рекомендуется на постоянной основе изолировать сеть управления и сеть, в которой работают ваши приложения, друг от друга. Дополнительно ограничить передачу данных между сегментами сети можно с помощью статической маршрутизации. Указания по настройке статических маршрутов содержатся в разделе «Настройка сетевых параметров» на странице 27.

ProtectServer 3 External поддерживает использование межсетевого экрана на базе *iptables*. Межсетевой экран следует настраивать с соответствующими правилами, позволяющими разрешить доступ только к определенным сетевым ресурсам. Подробное описание настройки *iptables* содержится в разделе «Настройка сетевых параметров» на странице 27.

Разделение уровней доступа

ProtectServer 3 External обеспечивает два уровня доступа: пользователи устройства и пользователи HSM. Для оптимальной защиты данные уровни доступа и их учетные данные должны быть изолированными, и пользователи не должны совмещать различные уровни доступа. Не используйте одни и те же терминалы для доступа в целях управления устройством, управления HSM и доступа обычных пользователей.

Пользователи устройства
Входить в командную оболочку PSE (PSESH) для настройки и управления устройством могут следующие пользователи:

> admin
> pseoperator
> audit

Функции каждого пользователя описаны в разделе «Использование PSESH» *Справочного руководства по командам PSESH*.

Пользователи HSM
Входить в систему для управления HSM-токеном и выполнения криптографических операций могут следующие пользователи:

> Администратор - сотрудник службы безопасности (ASO)
> Администратор
> Сотрудник службы безопасности (SO)
> Владелец токена (Пользователь)

Функции каждого пользователя описаны в разделе «Уровни доступа пользователей» *Руководства по администрированию ProtectToolkit-C*.

Первый вход в систему и тестирование

При первом пуске ProtectServer 3+ External выполните нижеперечисленные действия:

> «Подключение к консоли, включение питания и вход в систему» – см. следующую страницу
> «Тестирование системы» – см. страницу 27

Подключение к консоли, включение питания и вход в систему

Для тестирования системы и настройки сетевых параметров необходимо сначала подключиться к консоли ProtectServer 3+ External. Терминал следует подключать непосредственно к последовательному порту на задней панели устройства с помощью входящего в комплект адаптера USB-RJ45 компании Prolific Technology Inc. (с разъемом 8P8C). Данным последовательным соединением следует воспользоваться для настройки, по крайней мере, одного из сетевых интерфейсов.

Установка соединения через последовательный порт и первый вход в систему

1. Соедините разъем **Console** на передней панели устройства с терминальным сервером, терминалом ввода-вывода, настольным или портативным компьютером с помощью входящего в комплект адаптера USB-RJ45 компании Prolific Technology Inc. (с разъемом 8P8C).

ПРИМЕЧАНИЕ: не подключайте кабель последовательного интерфейса к одному из портов Ethernet.

2. В случае неудачной загрузки и автоматической установки драйвера адаптера USB-RJ45 компании Prolific Technology Inc. (с разъемом 8P8C) посетите веб-страницу по адресу http://www.prolific.com.tw для загрузки и установки драйвера устройства PL2303 USB-to-Serial для операционной системы Windows.

3. Откройте **Диспетчер устройств** (**Панель управления > Оборудование > Диспетчер устройств**) и раскройте список **Порты** (**COM и LPT**). Если драйвер был успешно установлен, в данном списке будет отображаться запись **Prolific USB-to-Serial Comm Port** с указанием порта, назначенного адаптеру. Например:

```
Prolific USB-to-Serial Comm Port (COM4)
```

   Запишите COM-порт (в данном примере COM4), назначенный адаптеру. Номер порта потребуется вам при установке последовательного соединения.

4. Включите питание устройства ProtectServer 3 External.

5. Воспользуйтесь программой эмуляции терминала, например, *PuTTY*, для установки последовательного соединения с COM-портом, назначенным вашему адаптеру Prolific USB-to-Serial. Установите параметры соединения через последовательный интерфейс следующим образом:

   - **Скорость передачи в бодах** 115200
   - **Биты данных:** 8
   - **Контроль четности:** отсутствует
   - **Стоповые биты:** 1

ПРИМЕЧАНИЕ: для начала сеанса может потребоваться нажать клавишу **ENTER** несколько раз. После открытия сеанса администрирования необходимо войти в систему в течение двух минут, или лимит времени для входа в систему будет превышен.

6. После успешного подключения на экране появится строка ввода имени пользователя устройства HSM:

```
Protect Server External 7.0
PSE login:
```

Вы можете войти в систему под именем **admin** или **pseoperator** для доступа к командной оболочке PSE (PSESH), которая предоставляет интерфейс командной строки для настройки и управления устройством. С синтаксисом команд можно ознакомиться в *Справочном руководстве по использованию PSESH*. Третья учетная запись (**audit)** используется для настройки ведения контрольных журналов устройства. Данная учетная запись не используется для выполнения функций управления устройством.

По умолчанию для пользователей **admin** и **pseoperator** установлен пароль **password**

7. После входа в систему на экран будет выведено предложение изменить пароль учетной записи. Пароль следует запомнить. Чтобы изменить пароль в любое другое время, войдите в учетную запись и введите команду **user password**.

Пользователь с именем **admin** может выполнить сброс паролей всех учетных записей на установленные по умолчанию производителем, введя в командной оболочке PSESH команду **sysconf appliance factory**. Данная команда также сбросит настройки SNMP и сетевые параметры на установленные по умолчанию производителем.

ВНИМАНИЕ! Выполнение команды **sysconf appliance factory** по SSH может привести к обрыву соединения в результате сброса установленного IP-адреса. Чтобы не допустить этого, используйте данную команду при соединении через последовательный интерфейс.

Тестирование системы

Перед испытаниями и развертыванием системы в условиях эксплуатации следует запустить средство диагностики. Войдите в систему как **admin** или **pseoperator** и введите команду **hsm state** для отображения текущего статуса:

```
psesh:>hsm state

HSM device 0: HSM in NORMAL MODE. RESPONDING to requests. Usage Level=0%
State = (0x8000, 0xffffffff)
Host Interface = PSIe3

Command Result: 0 (Success)
```

Вы также можете использовать команду **status** оболочки PSESH для проверки каждого процесса HSM. С синтаксисом команд можно ознакомиться в *Справочном руководстве по использованию PSESH*.

Далее см. раздел «Настройка сетевых параметров».

Настройка сетевых параметров

Устройство ProtectServer 3 External предназначено для установки в центре обработки данных и использования с удаленным доступом по сети. Для подключения к сети используются два порта Ethernet LAN. Устройство ProtectServer 3 External также оснащено консольным портом RJ-45, который используется для доступа к устройству через последовательный интерфейс для первоначальной настройки сетевых параметров.

Сетевые интерфейсы (eth0 и eth1) и консольный порт располагаются на передней панели устройства, как показано на нижеприведенном рисунке:

Консольный порт

Для выполнения первоначальной настройки сетевых параметров с использованием PSESH подключите к ProtectServer 3 External устройство с последовательным интерфейсом. Используя подключение к порту **Console,** настройте, по крайней мере, один из сетевых интерфейсов. После настройки интерфейса вы можете подключить устройство к сети и использовать командную оболочку PSESH для завершения настройки сетевых параметров.

Конфигурация устройства

Следующие сетевые параметры настраиваются на уровне устройства:

> Имя хоста устройства. Имя хоста не является обязательным параметром, если вы не используете DNS.

Конфигурация интерфейсов Ethernet LAN

ProtectServer 3 External оснащен двумя индивидуально конфигурируемыми сетевыми интерфейсами Ethernet LAN. Вы можете задать следующие сетевые параметры для каждого интерфейса:

> Адрес IPv4 или IPv6. Адреса IPv4 можно присваивать с использованием статических адресов или адресации DHCP. Адреса IPv6 настраиваются как статические адреса.

> Сетевой шлюз. Интерфейсы должны использовать соответствующий сети шлюз (IPv4 или IPv6).

> Маска сети. Интерфейсы IPv4 должны использовать формат адресов в виде четырех чисел, разделенных точками (например, 255.255.255.0). Интерфейсы IPv6 могут использовать полную или сокращенную форму записи.

> Статический сетевой маршрут.

> Конфигурация DNS. Хотя конфигурация DNS выполняется на уровне интерфейса, устанавливаемые для него настройки доступны для всех интерфейсов устройства, если сконфигурированный интерфейс подключен к сети. Для доступа к DNS рекомендуется настраивать каждый интерфейс. Настраиваемые параметры:

  - Сервера имен DNS
  - Домены поиска DNS

  Данные настройки применимы только к сетям со статической конфигурацией. При использовании DHCP используются домены поиска DNS и сервера имен DNS, заданные на DHCP-сервере.

> Объединение сетевых интерфейсов

Сбор сетевых данных устройства

Перед началом работы необходимо собрать следующую информацию (большая часть данных может быть получена у администратора сети):

Сетевые параметры модуля HSM

> IP-адрес и маска подсети для каждого порта LAN, который вы желаете использовать (если вы используете статическую IP-адресацию)

> Имя хоста для устройства HSM (зарегистрированное на DNS-сервере сети)

> Имя домена (для каждого порта)

> IP-адрес шлюза по умолчанию (для каждого порта)

> IP-адреса серверов имен DNS (для каждого порта)

> Имена доменов поиска (для каждого порта)

> Маска подсети устройства (для каждого порта)

Записи DNS

> Убедитесь, что на используемых DNS-серверах правильно настроены записи для устройства и клиентского оборудования.

> При использовании DHCP все ссылки на клиентское оборудование и устройство HSM (в соответствии с сертификатами) должны использовать имена хостов.

Настройка параметров сети

Вы можете настроить все сетевые параметры через последовательный интерфейс или настроить один порт и использовать его для доступа к устройству по сети для завершения настройки.

> **ПРИМЕЧАНИЕ:** Для смены IP-адреса устройства используйте локальный терминал, подключенный через последовательный интерфейс, чтобы избежать разрыва SSH-соединения в консоли администратора.

Настройка сетевых параметров устройства и портов

Рекомендуется настраивать и тестировать каждый сетевой интерфейс. Для подключения к устройству по SSH необходимо знать IP-адрес, по крайней мере, одного сетевого интерфейса.

1. Войдите в систему под именем **admin**.

2. Настройте IP-адрес, маску сети и шлюз (опционально), по крайней мере, для одного из портов Ethernet LAN (eth0 или eth1). Вы можете указать статический адрес или использовать адрес, назначенный DHCP-сервером. Каждый порт можно настроить на использование адреса IPv4 или IPv6.

> **ПРИМЕЧАНИЕ:** Адреса IPv6 настраиваются как статические адреса.

Статическая адресация	psesh:> **network interface static -device** <сетевой_интерфейс> **-ip** <IP_адрес> **-netmask** <маска_сети> [**-gateway** <IP_адрес>]
DHCP	psesh:> **network interface dhcp -device** <сетевой_интерфейс>
IPv6	psesh:> **network interface ipv6 -device** <сетевой_интерфейс> **-ip** <IP> **[-gateway** <IP>]

   После выполнения любой из данных команд будет выведен запрос на перезапуск сетевой службы.

3. [Опционально] Настройка объединения сетевых интерфейсов. Данная функция позволяет двум сетевым интерфейсам работать как один интерфейс, с одним MAC-адресом, увеличивая пропускную способность и обеспечивая резервирование.

> **ПРИМЕЧАНИЕ:** Настройка объединения сетевых интерфейсов возможна только со статическими адресами IPv4. При использовании DHCP объединение не будет функционировать, если одному из интерфейсов будет назначен другой IP-адрес.

psesh:>**network interface bonding config -ip** <IP> **-netmask** <IP> **-devices eth0,eth1 [-gateway** <IP>] [**-mode** <режим>]

psesh:>**network interface bonding enable**

psesh:>**sysconf appliance reboot**

Наличие нескольких режимов объединения обеспечивает различные возможности для распределения нагрузки между двумя физическими интерфейсами:

- **0:** Balance Round Robin. Пакеты передаются на каждый интерфейс из объединенных интерфейсов поочередно, обеспечивая распределение нагрузки и отказоустойчивость.
- **1:** Active-Backup. Активен один из объединенных интерфейсов, при этом другой интерфейс выступает в качестве резервного. Резервный интерфейс становится активным, только если активный интерфейс теряет соединение.
- **2:** Balance XOR. Передача данных по формуле XOR, при которой операция XOR выполняется с MAC-адресом отправителя и MAC-адресом получателя. Для каждого MAC-адреса получателя выбирается один и тот же интерфейс из объединенных интерфейсов, что обеспечивает распределение нагрузки и отказоустойчивость.
- **3:** Broadcast. Все пакеты передаются через оба объединенных интерфейса, что обеспечивает отказоустойчивость.
- **4:** 802.3ad (динамическое агрегирование каналов). Создание агрегированных групп с одинаковыми настройками скорости и дуплексного режима. Для данного режима требуется коммутатор, поддерживающий динамические линии связи IEEE 802.3ad. Интерфейс, используемый для отправки исходящего пакета выбирается на основании политики передачи хеша (transmit hash policy) (по умолчанию, простая операция XOR). Для изменения данной политики необходимо изменить параметр xmit_hash_policy. **ПРИМЕЧАНИЕ:** Проверьте по тексту стандарта 802.3ad, соответствует ли используемая вами политика передачи хеша требованиям стандарта. В частности, изучите раздел 43.2.4, описывающий требования в отношении порядка обработки пакетов. Допуски по данным требованиям могут отличаться в зависимости от реализации подключения различных одноранговых узлов.
- **5:** Balance TLB (балансировка нагрузки на передачу). Исходящий трафик распределяется с учетом текущей нагрузки и очереди пакетов на каждом сопряженном интерфейсе. Входящий трафик поступает на активный интерфейс.
- **6:** Balance ALB (адаптивная балансировка нагрузки). Балансировка нагрузки производится для исходящего и входящего трафика аналогично процедуре для исходящего трафика в режиме 5. Балансировка входящей нагрузки осуществляется с помощью ARP-переговоров. Драйвер объединения перехватывает ответы по протоколу ARP, отправляемые устройством, и заменяет аппаратный адрес отправителя уникальным аппаратным адресом одного из объединенных интерфейсов. Таким образом, различные клиенты будут обращаться к устройству по различным аппаратным адресам.

4. [Опционально] Установите имя хоста и доменное имя для устройства.

psesh:> **network hostname** <имя_хоста>

psesh:> **network domain** <домен_сети>

Вам необходимо настроить свой DNS-сервер на преобразование имени хоста в IP-адрес, настроенный для порта Ethernet устройства. Это нужно сделать для каждого порта Ethernet, подключенного к сети. Обратитесь за помощью к сетевому администратору.

5. [Опционально] Добавьте в конфигурацию сети для устройства сервер доменных имен. Сервер имен добавляется в таблицу DNS устройства. На устройстве используется одна таблица DNS, которая относится ко всем сетевым интерфейсам (портам).

psesh:> **network dns add nameserver** <IP_адрес> **-device** <сетевой_интерфейс>

> **ПРИМЕЧАНИЕ:** данные настройки доменного имени применимы только к сетям со статической конфигурацией. При использовании DHCP используются сервера доменных имен, заданные на DHCP-сервере.

При добавлении DNS-сервера к определенному сетевому интерфейсу он будет добавлен в таблицу DNS устройства и станет доступен для обоих интерфейсов при условии, что интерфейс, к которому вы добавили сервер, подключен к сети. Например, если вы добавите DNS-сервер к eth0, eth1 сможет получить доступ к DNS-серверу, если eth0 подключен к сети. Если eth0 отключен от сети, eth1 также утрачивает доступ к DNS-серверу. Чтобы убедиться, что любой добавленный вами DNS-сервер будет доступен при неполадках в сети или неисправности порта, рекомендуется добавлять его к обоим интерфейсам, подключенным к сети.

6. [Опционально] Добавьте к конфигурации сети домен поиска. Они автоматически добавляются к интернет-адресу, указываемому вами в PSESH. Например, если вы добавите домен поиска mycompany.com, при вводе команды **network ping hsm1** начнется поиск домена **hsm1.mycompany.com**. Если домен будет определен, он отправит эхо-запрос на интерфейс с данным именем хоста.

lunash:> **network dns add searchdomain** <домен> **-device** <сетевой_интерфейс>

Сервер поиска добавляется в таблицу DNS устройства.

> **ПРИМЕЧАНИЕ:** данные настройки домена поиска применимы только к сетям со статической конфигурацией. При использовании DHCP используются домены поиска DNS, заданные на DHCP-сервере.

При добавлении домена поиска DNS к определенному сетевому интерфейсу он будет добавлен в таблицу DNS устройства и станет доступен для обоих интерфейсов при условии, что интерфейс, к которому вы его добавили, подключен к сети. Например, если вы добавите DNS-сервер к eth0, eth1 сможет получить доступ к DNS-серверу, если eth0 подключен к сети. Если eth0 отключен от сети, eth1 также утрачивает доступ к DNS-серверу. Чтобы убедиться, что любой добавленный вами DNS-сервер будет доступен при неполадках в сети или неисправности порта, рекомендуется добавлять его к обоим интерфейсам, подключенным к сети.

Если вы решили производить настройку по SSH, вероятно, соединение будет разорвано, когда вы подтвердите изменение установленного по умолчанию IP-адреса.

7. [Опционально] Добавьте в устройство правила iptables ACCEPT и DROP для управления доступом к сети.

По умолчанию на устройстве ProtectServer 3 External разрешен доступ ко всем сетям и узлам. По умолчанию для цепочки INPUT и OUTPUT установлено правило ACCEPT. Для цепочки FORWARD по умолчанию установлено правило DROP, так как ProtectServer 3 External не используется для перенаправления пакетов в качестве маршрутизатора или прокси-сервера.

> **ВНИМАНИЕ!** При настройке iptables по SSH неверно настроенное правило может привести к блокировке.

a. Чтоб добавить правило ACCEPT, укажите узел или сеть:

psesh:> **network iptables addrule accept host -ip** <IP_адрес>

psesh:> **network iptables addrule accept network -net** <IP_адрес> **-mask** <маска_сети>

b. Чтоб добавить правило DROP, укажите узел или сеть:

psesh:> **network iptables addrule drop host -ip** <IP_адрес>

psesh:> **network iptables addrule drop network -net** <IP_адрес> **-mask** <маска_сети>

c. Чтобы просмотреть текущий список правил:

psesh:> **network iptables show**

d. Чтобы удалить правило, укажите номер правила в списке:

psesh:> **network iptables delrule -rulenum** <номер>

Номер правила соответствует его текущему положению в списке, поэтому повторное выполнение команды **network iptables delrule -rulenum 1** в конце концов приведет к удалению всего списка.

e. Сохранение изменений в настройках iptables:

psesh:> **network iptables save**

Данная команда обязательна, в противном случае при следующей перезагрузке устройства изменения не будут сохранены.

8. После изменения конфигурации сетевого соединения перезагрузите устройство:

psesh:> **sysconf appliance reboot**

9. Просмотр новых сетевых настроек:

psesh:> **network show**

Сетевой доступ по протоколу SSH

После завершения настройки сетевых параметров вы можете получить доступ к устройству ProtectServer 3 External по сети по протоколу SSH. Для этого вам потребуется программа SSH-клиент, например, puTTY (можно бесплатно загрузить на www.putty.org).

Отключение питания устройства ProtectServer 3 External

Для отключения питания устройства перед нажатием переключателя питания воспользуйтесь PSESH.

Отключение питания устройства ProtectServer 3 External

1. Войдя в систему PSESH под именем пользователя **admin** или **pseoperator**, выполните команду:

psesh:> **sysconf appliance poweroff**

Дождитесь завершения работы устройства. Вентилятор и светодиодные индикаторы продолжат работать.

2. Переведите переключатель, расположенный на задней панели ProtectServer 3 External в положение «Off» (Отключено). Вентилятор и светодиодные индикаторы отключатся.

Обновление образа программного обеспечения устройства

Компания Thales размещает на Портале поддержки клиентов пакеты безопасного обновления ПО, которые позволяют администратору устройства обновлять образ программного обеспечения на ProtectServer 3 External и пользоваться преимуществами новых функций PSESH.

Нижеописанный порядок действий позволяет вам обновить образ ПО на устройстве ProtectServer 3 External с использованием пакета безопасного обновления.

Необходимые условия

> Загрузить пакет безопасного обновления с Портала поддержки клиентов компании Thales (см. раздел «Контактные данные службы технической поддержки» на странице 9).

> Необходимо иметь доступ к устройству уровня **admin**.

> Инициализируйте токен авторизации пользователя Admin для обслуживания HSM. Для получения повторной информации об инициализации токена обратитесь к описанию утилиты ctconf.