Аппаратные модули безопасности общего назначения nShield®

ENTRUST

SECURING A WORLD IN MOTION

Содержание

Безопасность, внушающая доверие **3**

Семейство решений nShield **4**

Серия nShield Connect 4

Серия nShield Edge 4

Серия nShield Solo 4

Услуга nShield as a Service 4

Широчайший спектр применения **5**

Особенности семейства nShield **5**

Оптимизированные для облачной среды интерфейсы веб-сервисов 5

Поддержка локальных и облачных контейнеров 6

nShield BYOK: более надежное управление ключами для облачных данных 6

Оптимизация операций благодаря удаленному мониторингу и управлению 7

Удаленная настройка 7

Архитектура с высокой степенью гибкости — Security World 7

CodeSafe — безопасная среда выполнения от nShield 8

Партнерство с лидерами отрасли **9**

Универсальность и высокая производительность **10**

Сертификация по отраслевым стандартам **10**

FIPS 140-2 (Федеральный стандарт США по обработке информации) 10

Соответствие общим критериям и Регламенту в области электронной идентификации и удостоверительных служб для электронных транзакций (eIDAS) 11

Безопасность, внушающая доверие

Аппаратные модули безопасности nShield (HSM) от компании Entrust — это надежные, устойчивые к взлому устройства, призванные защитить наиболее чувствительные данные вашей компании. Сертифицированные по стандарту FIPS 140-2 модули выполняют функции криптографического преобразования, такие как создание, управление и хранение ключей шифрования и подписи, а также ряд других задач по сохранению конфиденциальности в пределах своей защищенной среды.

Модули nShield станут мощным дополнением к вашей системе безопасности:

- Повышайте свой уровень безопасности и доверия к данным
- Будьте уверены, что вы не только соблюдаете важные нормативные стандарты, но и превосходите их
- Поддерживайте высокий уровень обслуживания и гибкость бизнеса

Семейство решений nShield

Семейство HSM общего назначения от nShield способно полностью охватить среду вашей компании благодаря ряду своих модулей:

Серия nShield Connect

Сетевые устройства

HSM nShield Connect обеспечивают службы криптографического преобразования для распределенных по сети приложений. HSM nShield Connect предлагаются в двух сериях: классические HSM nShield Connect+ и высокопроизводительные HSM nShield Connect XC.

Серия nShield Edge

Портативные USB-модули

HSM nShield Edge — это удобные и экономичные настольные устройства. nShield Edge идеально подходят для разработчиков и поддерживают такие функции, как генерация корневого ключа малого объема.

Серия nShield Solo

Карты PCIe для встраивания в устройства или серверы

HSM nShield Solo — это низкопрофильные модули на основе карт PCI-Express, предоставляющие криптографические ключи приложениям, размещенным на сервере или устройстве. Модули nShield Solo предлагаются в двух сериях: классические HSM nShield Solo+ и высокопроизводительные HSM nShield Solo XC.

Услуга nShield as a Service

Решение на условиях подписки для доступа к HSM nShield в облаке

Услуга nShield as a Service обеспечивает доступ на условиях подписки к выделенным HSM nShield Connect XC, сертифицированным по FIPS 140-2 уровня 3. Это решение предлагает те же функции и возможности, что и локальные HSM, дополненные преимуществами облачной службы. Оно позволяет клиентам решать свои первоочередные задачи в сфере облачных вычислений, оставляя обслуживание устройств специалистам Entrust. Доступны как самостоятельно управляемые, так и полностью управляемые специалистами Entrust варианты обслуживания.

Широчайший спектр применения

Клиенты Entrust используют HSM nShield в качестве основы доверия в различных сферах, включая инфраструктуру открытых ключей (PKI), защиту ключей шифрования SSL/TLS, подписание кода, цифровую подпись и блокчейн. По мере распространения Интернета вещей и увеличения спроса на идентификаторы и сертификаты устройств HSM nShield продолжат обеспечивать важные меры безопасности, такие как аутентификация устройств с использованием цифровых сертификатов.

HSM nShield также поддерживают широкий спектр криптографических алгоритмов, включая алгоритмы шифрования на основе эллиптических кривых, обеспечивающие высокоскоростные операции и идеально подходящие для современных компактных вычислительных сред и распространенных отраслевых операционных систем и API.

Особенности семейства nShield

Оптимизированные для облачной среды интерфейсы веб-сервисов

Дополнительный пакет nShield Web Services Option Pack оптимизирует интерфейс между вашими приложениями и HSM за счет выполнения команд через вызовы веб-служб. Этот инновационный подход упрощает развертывание без необходимости интеграции приложений напрямую с nShield, тем самым устраняя зависимость от ОС и конфигурации архитектуры. Оптимизированный для облачной среды пакет Web Services Option Pack взаимодействует с приложениями, размещенными как в облаке, так и в традиционных центрах обработки данных.

Поддержка локальных и облачных контейнеров

Пакет nShield Container Option Pack гарантирует эффективную разработку и развертывание контейнерных приложений и процессов при поддержке высоконадежных аппаратных модулей безопасности Entrust. Это решение включает в себя комплект готовых сценариев, существенно упрощающих интеграцию HSM nShield в среду контейнерных приложений и учитывающих потребность в динамической масштабируемости клиентских приложений и контейнерных хостов.

nShield BYOK: более надежное управление ключами для облачных данных

nShield BYOK (Bring Your Own Key — создание собственных ключей) позволяет генерировать надежные ключи в локальном HSM nShield и безопасно экспортировать их в свои облачные приложения независимо от используемых веб-служб: это могут быть Amazon, Google Cloud Platform, Microsoft Azure или все сразу. nShield BYOK повышает безопасность методов управления ключами, усиливает контроль над ключами и обеспечивает общую ответственность за безопасность ваших данных в облаке.

Преимущества nShield BYOK:

- Более защищенные методы управления ключами, повышающие безопасность ваших конфиденциальных данных в облаке
- Более надежное создание ключей с использованием генератора случайных чисел с высокой энтропией от nShield, который защищен аппаратным обеспечением, сертифицированным по стандарту FIPS
- Более глубокий контроль над ключами: создавайте и безопасно экспортируйте ключи в облако с помощью собственных HSM nShield

Чтобы обеспечить максимальную надежность и строгий контроль за транспортировкой и использованием криптографических ключей, используйте nCipher BYOK с платформой Microsoft Azure. Если требуется помощь на месте с интеграцией и развертыванием, выберите пакет BYOK Deployment Service Package. Он включает в себя nShield Edge, реализацию интеграции специалистами Entrust Professional Services и договор на один год обслуживания.

Оптимальным вариантом для BYOK в Amazon Web Services и Google Cloud Platform станет пакет Cloud Integration Option Pack (CIOP) от Entrust. Он содержит все необходимое для использования локальных HSM nShield при создании и аренде ваших ключей в Amazon Web Services или Google Cloud Platform. Кроме того, пакет CIOP предусматривает поддержку механизма BYOK новой открытой платформы Microsoft Azure.

Оптимизация операций благодаря удаленному мониторингу и управлению

Сокращайте эксплуатационные расходы благодаря подробному информированию и круглосуточному управлению своими HSM с помощью решений nShield Monitor и nShield Remote Administration для HSM nShield серий Solo и Connect.

- Либо убрать двоеточие после этого текста, либо вынести его из списка
- Оптимизация производительности HSM, планирования инфраструктуры и времени безотказной работы с помощью функции nShield Monitor, предоставляющей информацию о динамике нагрузок, статистику использования, данные о попытках несанкционированного доступа, предупреждения и оповещения
- Сокращение командировочных расходов и экономия времени благодаря управлению HSM через полнофункциональный безопасный интерфейс nShield Remote Administration

Удаленная настройка

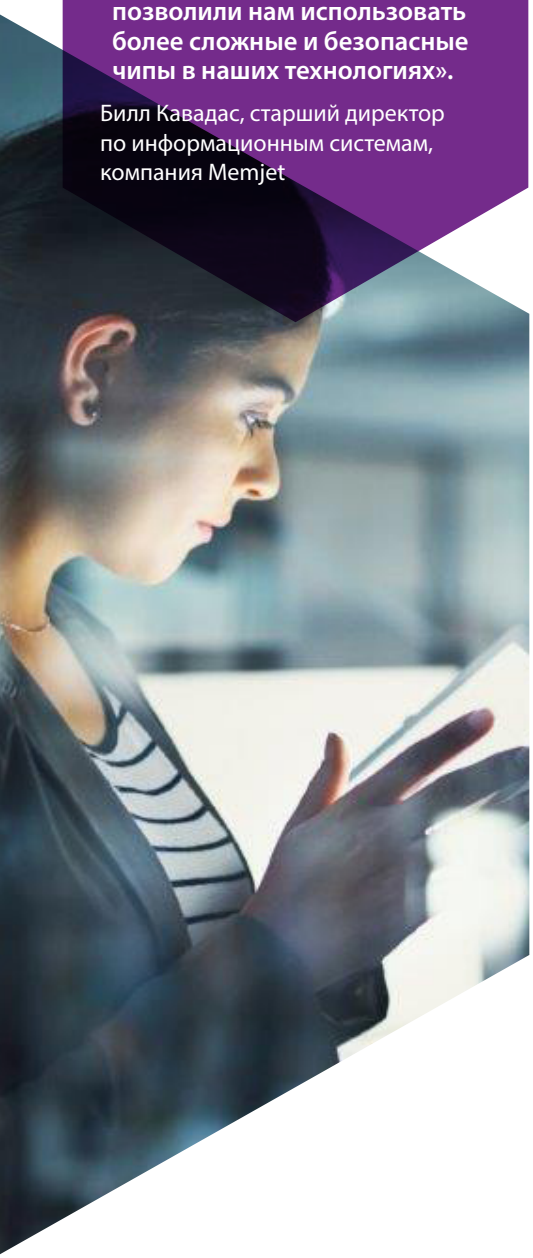
В моделях линейки nShield Connect XC предусмотрена функция последовательной консоли, упрощающая физическую установку HSM в стойки, прокладку кабелей и подачу питания. Все остальные настройки HSM и сети можно выполнять дистанционно. Это упрощает как первоначальное, так и повторное развертывание без необходимости посещения центра обработки данных. В данной функции поддерживается модель «поставщик – арендатор», в рамках которой поставщик контролирует конфигурацию сети, а арендатор полностью контролирует свой материал ключа.

Архитектура с высокой степенью гибкости — Security World

Архитектура nShield Security World поддерживает HSM nShield от Entrust путем создания уникальной гибкой среды управления ключами. С помощью nShield Security World можно объединить разные модели HSM nShield в унифицированную экосистему с возможностью ее масштабирования, эффективной отработки отказов и балансировки нагрузок.

«Сверхсовременные аппаратные модули безопасности nShield от Entrust позволили нам использовать более сложные и безопасные чипы в наших технологиях».

Билл Кавадас, старший директор по информационным системам, компания Memjet



Архитектура nShield Security World гарантирует операционную совместимость независимо от количества развертываемых HSM и позволяет управлять неограниченным количеством ключей, в том числе автоматически и удаленно резервировать и восстанавливать материал ключа.

Преимущества nShield Security World:

- Простое масштабирование оборудования аппаратных модулей безопасности nShield по мере роста потребностей вашей компании
- Обеспечение отказоустойчивости системы
- Экономия времени, поскольку больше нет необходимости в долгом создании резервных копий HSM

CodeSafe — безопасная среда выполнения от nShield

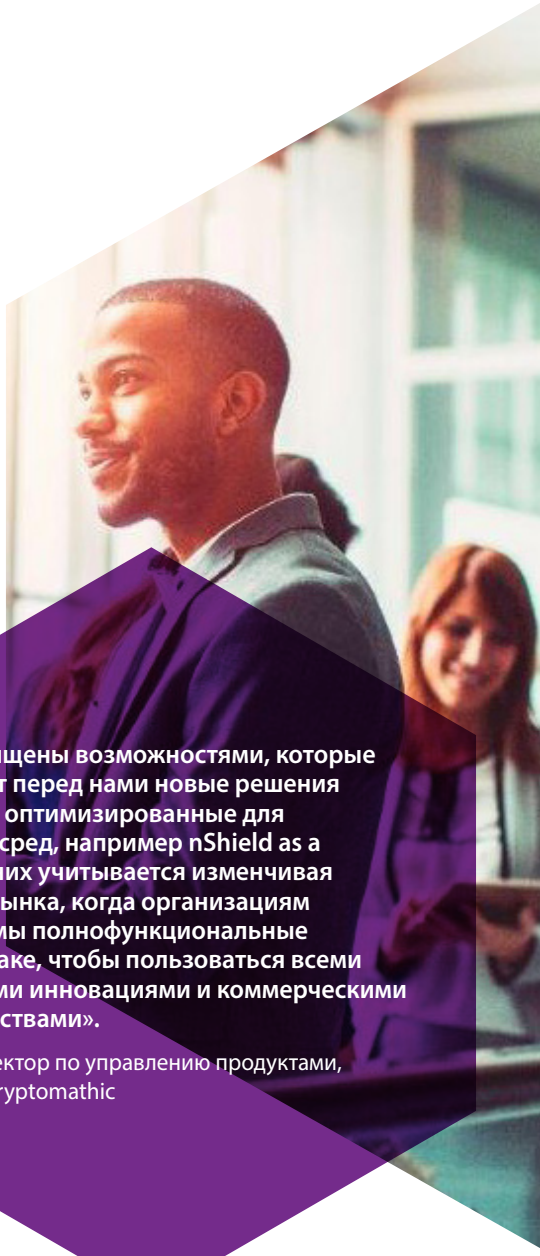
Помимо защиты ключей, HSM nShield серий Connect и Solo также предоставляют безопасную среду для работы приложений вашей компании. Функция CodeSafe позволяет разрабатывать и выполнять код в среде nShield, соответствующей требованиям FIPS 140-2 уровня 3, чтобы защитить приложения от потенциальных атак.

Преимущества CodeSafe:

- Гарантия высокой надежности благодаря выполнению конфиденциальных приложений и защите конечных точек данных приложений в сертифицированной среде
- Защита особо чувствительных приложений от угроз, таких как внутренние кибератаки, вредоносное ПО и постоянные целенаправленные угрозы
- Устранение риска несанкционированного изменения приложений или заражения вредоносным ПО с помощью подписи кода

Партнерство с лидерами отрасли

Чтобы предоставлять более комплексные продукты, позволяющие клиентам решать широкий спектр специфических проблем безопасности и успешно переходить на цифровые технологии, Entrust сотрудничает с ведущими поставщиками отрасли. В рамках своей программы партнерства с поставщиками технологий компания Entrust привлекает их к интеграции HSM nShield в различные сферы безопасности, включая решения по предоставлению учетных данных и инфраструктуру открытых ключей, безопасность баз данных, подписание кода, цифровые подписи, управление привилегированными учетными записями и доставку приложений, а также облачные вычисления и аналитику больших данных. HSM nShield поддерживают приложения безопасности своих партнеров, обеспечивая максимально надежную криптографическую обработку, защиту и управление ключами и одновременно гарантируя соблюдение государственных и отраслевых норм безопасности данных.

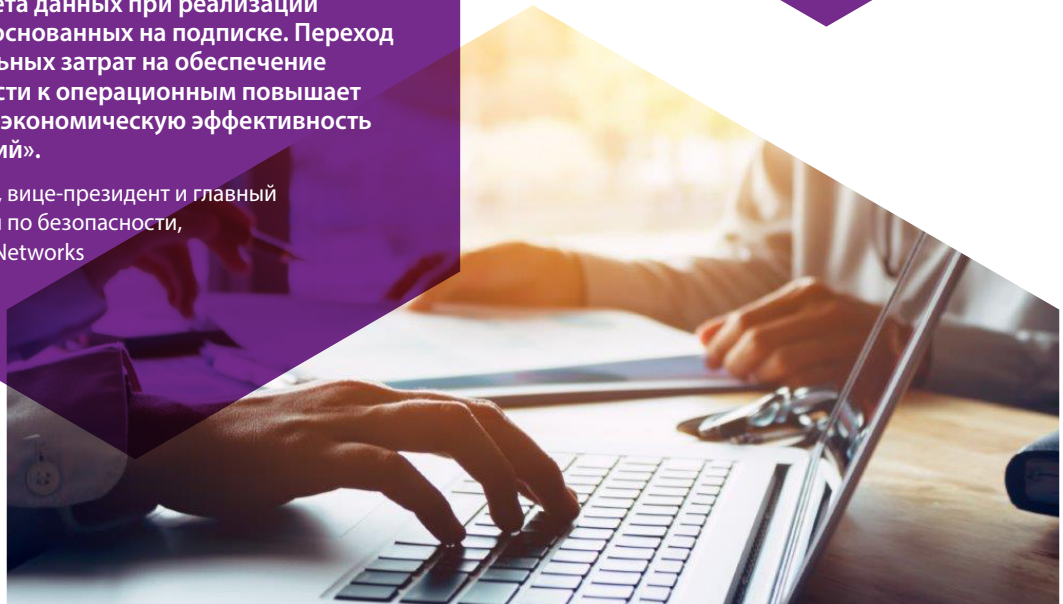


«Мы восхищены возможностями, которые открывают перед нами новые решения от nShield, оптимизированные для облачных сред, например nShield as a Service. В них учитывается изменчивая природа рынка, когда организациям необходимы полнофункциональные HSM в облаке, чтобы пользоваться всеми доступными инновациями и коммерческими преимуществами».

Эд Вуд, директор по управлению продуктами, компания Cryptomathic

«Благодаря nShield as a Service от Entrust клиенты F5 получают расширенные опции безопасности с возможностью достижения суверенитета данных при реализации сервисов, основанных на подписке. Переход от капитальных затрат на обеспечение безопасности к операционным повышает гибкость и экономическую эффективность организаций».

Джон Морган, вице-президент и главный управляющий по безопасности, компания F5 Networks



Универсальность и высокая производительность

Аппаратные модули безопасности nShield серий Connect и Solo предлагаются с тремя уровнями производительности, чтобы при их выборе вы могли учитывать особенности своей среды, то есть вы можете ориентироваться как на умеренную скорость операций, так и на высокую пропускную способность. Наше решение на основе подписки nShield as a Service для доступа к HSM nShield в облаке опирается на высочайшую производительность линейки nShield Connect XC.

Сертификация по отраслевым стандартам

Благодаря приверженности Entrust строгим стандартам вы гарантируете себе соответствие нормативно-правовым требованиям в контролируемых средах наряду с уверенностью в безопасности и целостности HSM nShield. Ниже приведен частичный перечень стандартов, которым мы соответствуем. Полные перечни доступны на нашем сайте и в листах технических данных наших продуктов.

FIPS 140-2 (Федеральный стандарт США по обработке информации)

FIPS 140-2 — это всемирно признанный правительственный стандарт Национального института по стандартизации и технологиям США (NIST), подтверждающий надежность и безопасность криптографических модулей. Все аппаратные модули безопасности Entrust nShield имеют сертификаты FIPS 140-2 уровней 2 и 3.

Соответствие общим критериям и Регламенту в области электронной идентификации и удостоверительных служб для электронных транзакций (eIDAS)

Аппаратные модули безопасности nShield серий XC и nShield+ имеют сертификаты соответствия Общим критериям уровня 4+ (Common Criteria EAL 4+) и признаны соответствующими критериям устройствами для создания подписей (QSCD) по требованиям Регламента eIDAS. Кроме того, модули nShield серий Solo XC и Connect XC соответствуют стандарту EN 419 221-5 «Криптографические модули для удостоверительных служб», применяемому к профилям защиты по общим критериям. Таким образом, nShield могут служить основой для обеспечения безопасности в процессах перехода государств-членов ЕС и коммерческих организаций ЕС на цифровые технологии. В том числе, они могут использоваться в таких сферах, как государственные схемы идентификации и трансграничные услуги, службы подписи электронных документов и операций, а также услуги аутентификации, проставления метки времени, защищенной электронной почты и долгосрочного хранения документов. Несмотря на то, что эти сертификаты относятся к европейскому регулированию, они действуют во многих регионах мира.

Дополнительная информация

Чтобы узнать больше о том, как мы можем защитить важную для вашего бизнеса информацию и приложения на вашем оборудовании, в облаке и в виртуальных средах, перейдите по ссылке **entrust.com/HSM**.

Более подробная информация об аппаратных модулях безопасности nShield от Entrust:

HSMinfo@entrust.com
entrust.com/ru/HSM

ОБ ENTRUST CORPORATION

Корпорация Entrust стоит на страже безопасности в сферах идентификационной информации, платежей и защиты данных по всему миру. Сегодня требования к бесперебойной и безопасной работе как никогда высоки и проявляются во всех аспектах жизни: во время зарубежных поездок, совершения покупок, получения доступа к услугам электронного правительства, входа в корпоративную сеть. Entrust предлагает беспрецедентно широкий спектр решений в области цифровой безопасности и выдачи учетных данных, на которых основано любое такое взаимодействие. Нам доверяют самые надежные организации мирового масштаба, и это неудивительно: мы предлагаем поддержку от более чем 2500 сотрудников и глобальную партнерскую сеть, которую уже оценили клиенты в более чем 150 странах.

Более подробная информация размещена по ссылке
entrust.com/HSM

ENTRUST

Пишите нам:
HSMinfo@entrust.com