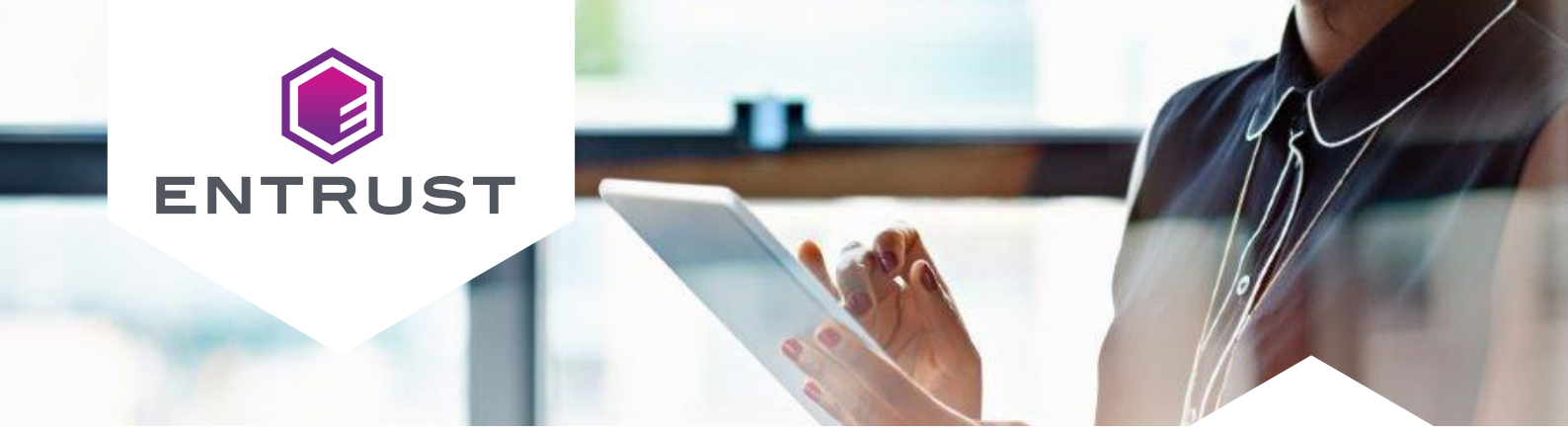

Пакет nShield Database Security Option Pack

Полная интеграция баз данных Microsoft SQL Server с высоконадежными аппаратными модулями безопасности nShield

ОБЗОР

Надежный корень доверия для развертывания баз данных Microsoft SQL Server

- Защита криптографических ключей базы данных с помощью передовых аппаратных модулей безопасности (HSM), сертифицированных по стандартам FIPS и Common Criteria
- Шифрование как на уровне ячейки, так и прозрачное шифрование данных (TDE)
- Защитите от несанкционированного доступа критически важные данные

В большинстве организаций базы данных — это важное хранилище конфиденциальной информации. В корпоративных базах содержатся данные о кредитных картах клиентов, конфиденциальная информация о конкурентах и объекты интеллектуальной собственности. Потеря или кража данных создают существенный риск для репутации и бренда, а также могут привести к серьезным штрафным санкциям. Защита критически важных данных от внутренних и внешних угроз снижает риск несанкционированного доступа к данным и повышает уровень нормативно-правового соответствия, включая соблюдение Стандарта безопасности данных индустрии платежных карт (PCI DSS). В частности, в разделе 3.6 стандарта PCI DSS в последней редакции (версия 3.2.1) указывается, что «криптографические ключи должны надежно храниться ... в защищенном криптографическом устройстве, таком как аппаратный модуль безопасности». Кроме того, в Разделе 3.6 определены передовые методы управления ключами, которое реализуется как функция HSM, например в форме двойного контроля.

Защитите свою базу данных, опираясь на высочайший уровень надежности

Шифрование данных в вашей базе защищает данные, но следует также защитить и ключи шифрования, которые отвечают за разблокировку этих данных. Аппаратные модули безопасности (HSM) защищают ключи шифрования за счет хранения их отдельно от данных на безопасной и надежной платформе. HSM nShield усиливает вашу внутреннюю политику безопасности, требуя авторизации на основе ролей и разделяя функции безопасности и администрирования базы данных, что упрощает демонстрацию соответствия нормам при проверке.

Это решение может быть реализовано как выделенная карта PCIe для отдельного сервера или как общее сетевое устройство для виртуализированных сред.

Пакет nShield Database Security Option Pack (для Microsoft SQL Server), также известный как поставщик SQLEKM, представляет собой API расширенного управления ключами (EKM) для Microsoft SQL Server.

Пакет nShield Database Security Option Pack

Microsoft SQL Server предусматривает две встроенные функции шифрования для защиты ваших данных: TDE и шифрование на уровне ячеек. Эти функции позволяют защитить всю базу данных или только конфиденциальные поля базы данных и могут быть активированы без нарушения работы ваших текущих приложений, структуры базы данных и процессов.

Защитите и данные, и свой бренд

Аппаратные модули безопасности nShield от Entrust, проверенные на соответствие самым высоким стандартам безопасности, таким как FIPS и Common Criteria, защитят ваши данные даже в самых сложных и нестандартных ситуациях. Детализированные элементы управления доступом HSM nShield позволяют также управлять ключами шифрования для Microsoft SQL Server. Чтобы принять во внимание особенности ваших политик, мы предусмотрели разделение функций безопасности и административных функций.

Преимущества аппаратных модулей безопасности nShield от Entrust:

- **Аппаратная защита ключей**: ключи шифрования базы данных хранятся в безопасной среде с защитой от несанкционированного доступа, чтобы предотвратить их копирование или взлом
- **Назначение пользователей и ролей**: обеспечивает более строгий контроль доступа к зашифрованным данным в Microsoft SQL Server
- **Строгий контроль ключей**: используется аутентификация администраторов с помощью смарт-карт, чтобы обеспечить надежный контроль за использованием ключей шифрования базы данных
- **Разделение ролей**: ответственность за важные задачи и процедуры разделена между несколькими администраторами
- **Простая установка и интеграция**: аппаратные модули безопасности nShield от Entrust легко интегрируются с Microsoft SQL Server, обеспечивая:
  - TDE и режимы шифрования на уровне ячейки с защитой применяемых ключей шифрования

HSM nShield масштабируются в соответствии с вашими потребностями и сразу интегрируются с другими ведущими корпоративными приложениями, включая веб-серверы, серверы приложений и инфраструктуры открытых ключей (ИОК).

Сетевые аппаратные модули безопасности nShield Connect могут совместно использоваться несколькими серверами, чем обеспечивается:

- **Поддержка виртуализированных сред**: аппаратное хранилище ключей для виртуализированных серверов, включая Hyper-V и VMware
- **Поддержка отказоустойчивого кластера**, включая группу доступности AlwaysOn
- **Упрощенное администрирование**: управление ключами шифрования для многочисленных баз данных, а также ключами, используемыми другими приложениями
- **Возможность аварийного переключения**: когда критически важна высокая доступность, а HSM становится недоступным, пользователи могут автоматически переключаться на другой HSM
- **Аварийное восстановление**: простые и безопасные процессы архивирования и восстановления ключей
- **Экономичность**: совместное использование модуля на нескольких серверах снижает расходы на оборудование, лицензирование и эксплуатацию

Пакет nShield Database Security Option Pack

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Поддерживаемые конфигурации

- Требуется ПО nShield Security World, версии 12.40.2 или 12.60.x или более поздние.
- Microsoft SQL Server (корпоративное издание), версии 2019 x64, 2017 x64
- Поддержка ОС Windows Server 2019 R2 x64, 2016 R2 x64
- Поддерживаемые аппаратные модули безопасности
  - Совместим со всеми моделями HSM nShield серий Solo и Connect

Поддерживаемые криптографические алгоритмы

- Асимметричные, включая RSA с длиной ключа 2048, 3072 и 4096 бит
- Симметричные, включая AES с длиной ключа 128, 192 и 256 бит

ПОДДЕРЖИВАЕМЫЕ ФУНКЦИИ NSHIELD

При интеграции HSM nShield с Microsoft SQL Server вы получаете доступ к следующим функциям:

Функции	Поддержка
Набор карт «1 из N»	Да
Набор карт «K из N»	Нет
Программные карты	Да
Только ключ модуля	Нет
Восстановление ключа	Да
Импорт ключа	Частично[1]
Балансировка нагрузки	Да
Аварийное переключение	Да
Строгое соответствие стандарту FIPS (FIPS 140-2 уровня 3)	Да[2]

1. Поддерживается только импорт ключей nCore. nCore API — это собственный программный интерфейс приложений для модулей nShield
2. Подробнее описано в примечаниях к выпуску и в руководстве пользователя.

Подробнее

Более подробная информация об аппаратных модулях безопасности nShield от Entrust размещена по ссылке **entrust.com/HSM**. Подробнее о решениях Entrust в области цифровой безопасности для выполнения задач идентификации, обеспечения доступа, информационного взаимодействия и использования данных можно узнать на сайте **entrust.com**

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