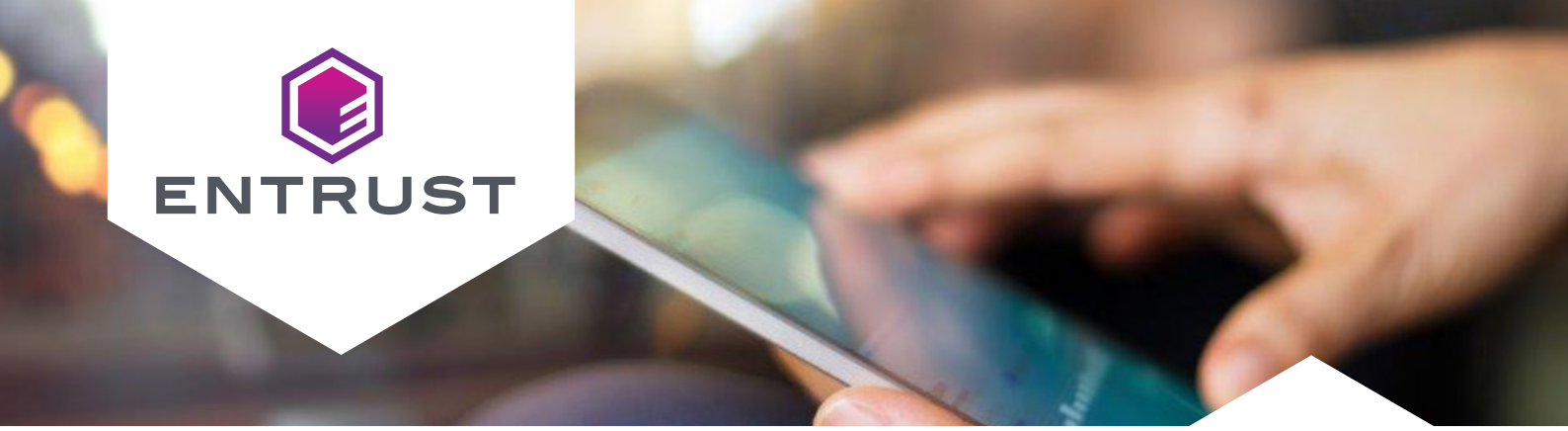


# Пакет nShield Web Services Option Pack

## Оптимизированный для облачной среды интерфейс на REST-правилах для аппаратных модулей безопасности высокой надежности

### ОБЗОР

- Доступ из облачной среды, центра обработки данных или локальных приложений к решению, обеспечивающему высокий уровень безопасности данных
- Простое оптимизированное подключение к криптографическим службам аппаратного модуля безопасности nShield
- Быстрое и масштабируемое динамическое развертывание приложений
- Гибкая поддержка ОС и архитектуры

Пакет nShield Web Services Option Pack (WSOP) — это интерфейс прикладного программирования на REST-правилах[1], предназначенный для взаимодействия между приложениями, требующими криптографического ключа и служб защиты данных, и аппаратными модулями безопасности (HSM) nShield, сертифицированными по стандарту FIPS. HSM nShield выполняют множество криптографических функций, включая шифрование, дешифрование, подписание, проверку и создание ключей. Теперь приложения могут получить доступ к этим важнейшим функциям через простой интерфейс веб-службы, использующий универсальный протокол HTTPS.

### ОСНОВНЫЕ СВОЙСТВА И ПРЕИМУЩЕСТВА

- **Эффективный доступ к удаленным криптографическим службам из облачной среды, центра обработки данных или локальных приложений** Независимо от своего расположения, будь то облако, удаленный центр обработки данных или локальное оборудование, приложения могут получать доступ к службам nShield посредством вызова веб-сервисов по протоколу HTTPS через API на REST-правилах, чем достигается более высокая гибкость, востребованная в разнообразных современных вычислительных средах.
- **Оптимизированный процесс разработки** Эффективный современный интерфейс веб-служб ускоряет разработку приложений для доступа к службам шифрования аппаратных модулей безопасности nShield.
- **Нет необходимости в интеграции на стороне клиента** Обычно для интеграции приложений с HSM nShield требуется привязка к локальным библиотекам хоста и развертывание локальных служб, однако API веб-служб на REST-правилах значительно упрощает разработчикам задачу по развертыванию.

# Пакет nShield Web Services Option Pack

- **Гибкая поддержка ОС и архитектуры** Интерфейс веб-служб на REST-правилах не зависит от инфраструктуры клиентских приложений и не требует локального программного обеспечения, зависящего от конкретной ОС, что упрощает интеграцию, особенно в пользовательских средах

- **Динамическая масштабируемость** Реализуйте новые или дополнительные рабочие нагрузки приложений без необходимости в дополнительной настройке HSM, установке вспомогательного программного обеспечения или клиентских лицензиях; увеличивайте или уменьшайте производительность по потребности, в том числе используя узлы WSOP при развертывании в контейнерной архитектуре

- **Поддержка балансировки нагрузки с использованием специально назначенных коммерчески доступных устройств** Пакет WSOP позволяет управлять рабочей нагрузкой HSM с помощью коммерчески доступных балансировщиков нагрузки (COTS), упрощая развертывание/настройку HSM и обеспечивая максимально эффективное использование пула аппаратных модулей безопасности

## Начало работы с пакетом nShield Web Services Option Pack

Необходимые ресурсы:

- Программное обеспечение Security World версии 12.6x или более новой
- HSM nShield серии Solo или Connect HSM или подписка на nShield as a Service

Чтобы использовать API на REST-правилах, пакет nShield WSOP устанавливается на клиентском сервере nShield, активируя службу и открывая ее для прямых мгновенных подключений из приложений.

По умолчанию в пакете WSOP настроен набор временных краткосрочных сертификатов TLS, исключительно для целей тестирования. Данная конфигурация должна быть обновлена путем установки соответствующих сертификатов для продолжения тестирования или начала практического использования.

Для аппаратных модулей безопасности nShield Connect: стандартная клиентская лицензия требуется только для клиентского сервера, на котором запущена веб-служба. Для подключения приложений клиентские лицензии не требуются.

Примечание 1. REST (REpresentational State Transfer — передача состояния представления) — это архитектура, основанная на веб-стандартах и использующая для передачи данных универсальный протокол HTTP. HTTP считается протоколом, не использующим информацию о состоянии, поскольку каждая команда выполняется независимо, без каких-либо сведений о командах, которые ей предшествовали. Архитектура REST основана на ресурсах, где каждый компонент считается ресурсом, доступ к которому осуществляется через общий интерфейс с помощью вызовов по протоколу HTTP.

Характеристики RESTful-архитектуры пакета WSOP:

- Четко определенные URI, которые однозначно идентифицируют «ресурсы», например: /keys (ключи) /sign (подписать) /verify (проверить) и т. д.
- HTTP-методы как команды для выполнения действий с этим ресурсом, например, GET — для операций чтения, таких как перечисление ключей, POST — для операций записи, таких как создание ключей, DELETE — для операций удаления, таких как удаление ключей.

**БОЛЕЕ ПОДРОБНАЯ ИНФОРМАЦИЯ РАЗМЕЩЕНА ПО ССЫЛКЕ ENTRUST.COM/RU/HSM**

# Пакет nShield Web Services Option Pack

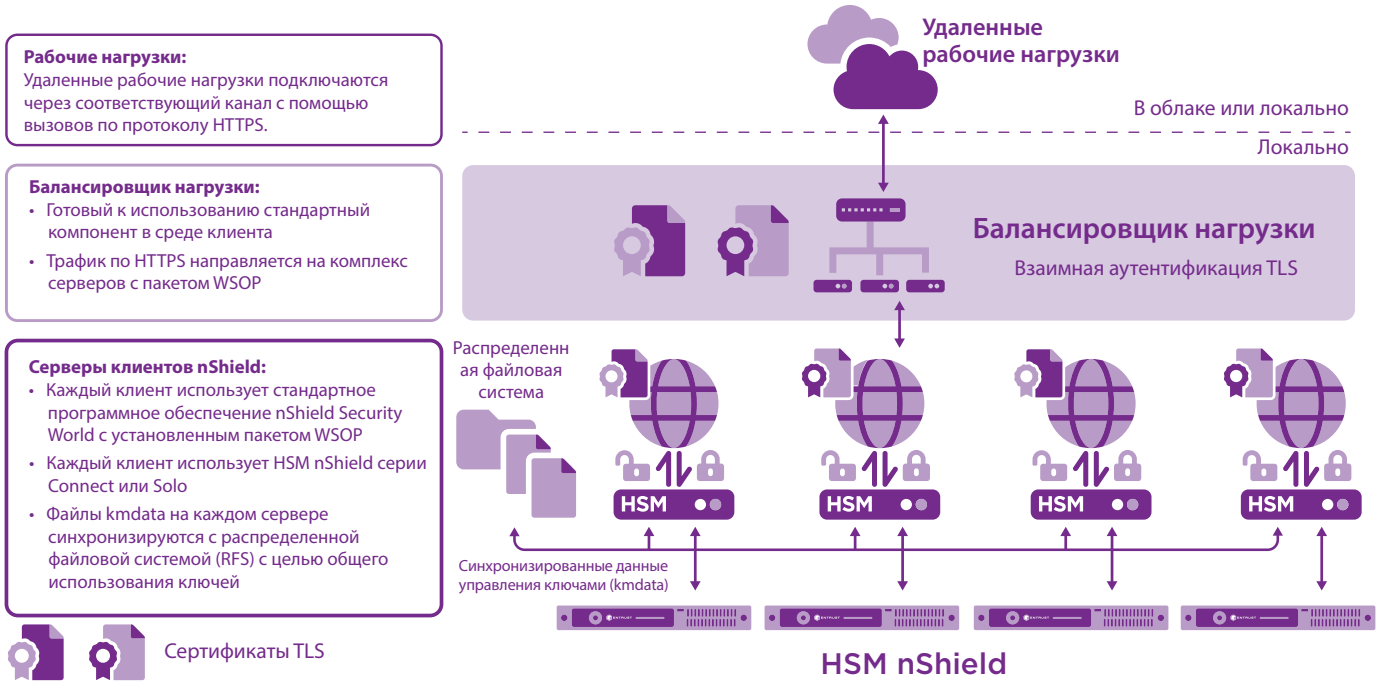
## ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

### Совместимость с решениями nShield

Пакет nShield WSOP совместим со всеми моделями HSM nShield серий Solo и Connect. Пакет WSOP должен устанавливаться на хосте с поддерживаемой версией ОС Linux и установленным программным обеспечением nShield Security World. WSOP поддерживает ключи, защищенные набором карт оператора и программными картами. WSOP также совместим с пакетом nShield Container Option Pack, позволяющим развертывать WSOP в контейнерной среде.

### Совместимость API

Аппаратные модули безопасности nShield могут поддерживать приложения, использующие API веб-служб, в сочетании с приложениями, использующими другие поддерживаемые API (PKCS#11, Java, CNG и др.).




Типовое развертывание пакета WSOP

## 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**