



**ENTRUST**

# Услуга nShield as a Service

## Простой и эффективный доступ к криптографии как услуге

### ОБЗОР

- Используйте удаленно размещенные и удаленно управляемые аппаратные модули безопасности для облачных решений
- Сохраняйте полный контроль над материалом ключей независимо от источника нагрузок приложений
- Расширяйте облачную криптографию и управление ключами на несколько облачных ресурсов
- Обеспечьте безопасное выполнение кода для облачных рабочих процессов
- Упростите работу с бюджетом на критически важные сферы безопасности бизнеса
- Сократите затраты времени на обслуживание и мониторинг

В нынешней изменчивой корпоративной IT-среде распространенной стратегической целью многих организаций становится принцип «приоритета облачной инфраструктуры». Те времена, когда компании по умолчанию размещали свою критически важную IT-инфраструктуру локально, остались в прошлом. Переход на облачные среды дает организациям масштабируемость, гибкость и отказоустойчивость, которые может предоставить поставщик облачных услуг, при этом снижая потребность в обслуживании и обеспечивая более предсказуемые ежемесячные эксплуатационные расходы. Такой сдвиг в бизнесе создает определенную напряженность, когда облачные приложения полагаются на аппаратные модули безопасности (HSM) — физические устройства для защиты криптографических ключей, выполняющие функцию основы доверия для зашифрованных данных

организации. HSM, традиционно размещаемые в локальных центрах обработки данных и управляемые местным отделом безопасности, помогают клиентам соблюдать нормативные или сертификационные требования и являются неотъемлемой частью критически важной инфраструктуры организации. Учитывая растущие требования к корпоративным отделам безопасности, постоянно возникает проблема поиска квалифицированных специалистов по безопасности для администрирования HSM. С помощью услуги nShield as a Service мы предлагаем те же функции и возможности, которые имеются в локальных HSM, но дополненные преимуществами облачной службы. Это позволяет клиентам решать свои первоочередные задачи в сфере облачных вычислений, оставляя управление и обслуживание устройств специалистам Entrust.

### Криптография как услуга

nShield as a Service — это решение на основе подписки, предназначенное для создания, доступа и защиты материала криптографических ключей отдельно от конфиденциальных данных. Для этого решения используются выделенные аппаратные модули безопасности nShield Connect, сертифицированные по стандартам FIPS 140-2 и eIDAS (EN 419 221-5). Эта облачная модель дает организациям возможность дополнять или заменять HSM в своих центрах обработки данных, при этом пользуясь всеми преимуществами, как при владении физическими устройствами. Услуга nShield as a Service позволяет более предсказуемо распределять средства на меры безопасности, управлять техническим ресурсом в зависимости от спроса, уменьшать центры обработки данных и сокращать время, затрачиваемое на плановое обслуживание и мониторинг.

# Услуга nShield as a Service

Клиенты, приобретающие подписку, взаимодействуют с облачными HSM nShield так же, как и с устройствами в своих собственных центрах обработки неструктурированных данных, но без необходимости получать, устанавливать и обслуживать физическое оборудование. Нередко это позволяет сократить время между первоначальной закупкой и началом использованием HSM и, следовательно, ускорить развертывание защищенных приложений.

## Полное соответствие вашей стратегии и требованиям к безопасности

Использование nShield as a Service позволяет полностью учитывать любую стратегию обеспечения безопасности независимо от того, ориентирована ли организация на облачные среды для выполнения своих криптографических функций, переносит ли выборочно определенные службы в облако или просто расширяет технические возможности HSM, чтобы справляться с периодическими скачками рабочих нагрузок.

Поскольку для услуги nShield as a Service используется та же уникальная архитектура Security World, что и для локальных решений nShield, вы можете использовать гибридный подход, сочетая nShield as a Service с локальными HSM. Архитектура nShield Security World — это масштабируемая система управления ключами, охватывающая все клиентские устройства nShield и обеспечивающая единый интерфейс для администратора и пользователя и гарантированную возможность взаимодействия независимо от того, используется ли подписка или собственные локальные мощности.<sup>1</sup> Это позволяет клиенту просто и эффективно масштабировать использование HSM с учетом конкретной среды, операционных подходов и потребностей в области безопасности.

Кроме того, уникальная безопасная среда выполнения CodeSafe по запросу дает доступ к расширенным защищенным вычислительным мощностям. Только nShield as a Service позволяет легко переносить безопасное выполнение кода с локального HSM в облако.

## Отличие nShield as a Service

Решение nShield as a Service обладает несколькими ключевыми преимуществами по сравнению с другими вариантами:

- У клиентов имеются ресурсы и ключи Security World, которые они могут использовать в своей среде nShield как в рамках услуги на условиях подписки, так и на локальном оборудовании.
- Только nShield as a Service дает возможность удаленного управления по требованию при необходимости переноса и увеличения производительности для безопасного выполнения кода с локального HSM в облако.
- nShield as a Service обеспечивает безопасность ключей на основе сертификатов FIPS 140-2 уровня 3 и eIDAS (профиль защиты по EN 419 221-5), которая недоступна в некоторых облачных решениях по защите ключей
- Заказчики могут и далее использовать те же приложения со своими облачными HSM nShield, но с возможностью увеличения производительности HSM на случай всплесков рабочей нагрузки.
- nShield as a Service может использоваться при работе с различными поставщиками облачных услуг, в отличие от услуг с использованием HSM, предлагаемых индивидуальными поставщиками, которые стремятся ограничить клиентов своими облачными средами.

Примечание 1. Дополнительная информация содержится в нашем техническом документе по архитектуре nShield Security World.



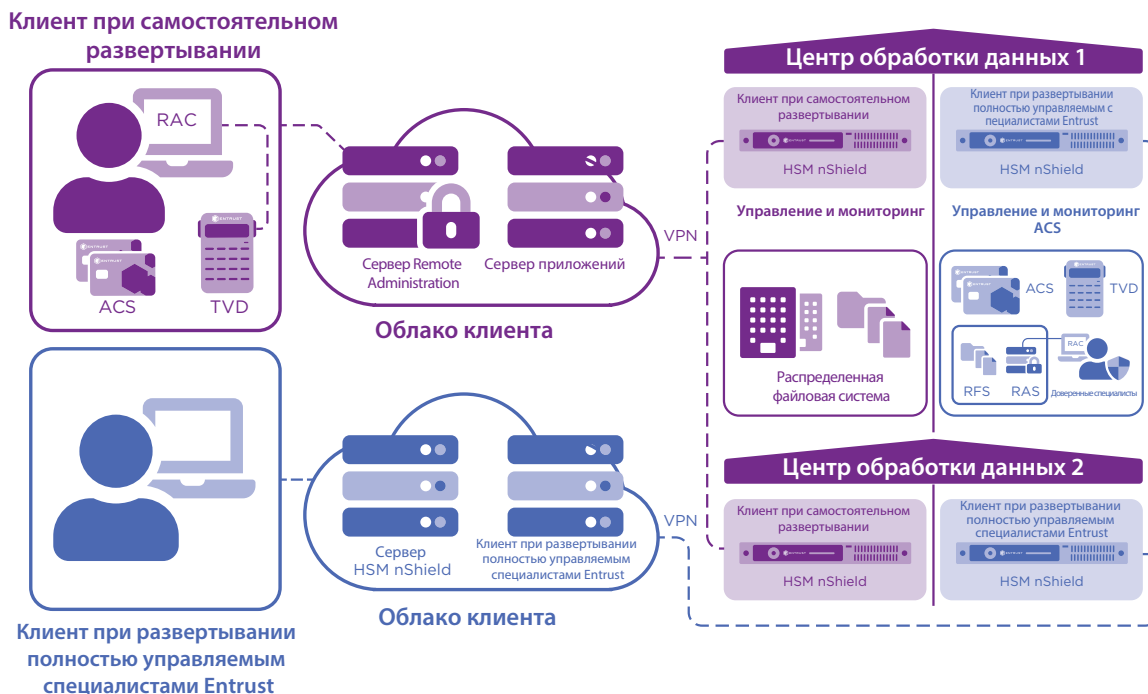
# Услуга nShield as a Service

- nShield as a Service поддерживает развертывание гибридного облака и позволяет легко перенести ключи, если потребуется вернуть данные от поставщика облачных услуг в локальную среду.
- nShield as a Service дает клиентам возможность воспользоваться выделенным аппаратным модулем безопасности. Клиенты получают полный контроль над своими криптографическими ключами: мы предусмотрели двойной контроль и полное разделение обязанностей

## Варианты и особенности развертывания nShield as a Service

Для nShield as a Service предусмотрено как самостоятельное, так полностью управляемое развертывание, как показано на схеме.

### Варианты развертывания nShield as a Service



Условные обозначения: ACS — набор карт администратора. TVD — доверенное устройство проверки. RAS — сервер удаленного администрирования. RFS — удаленная файловая система. RAC — клиент удаленного администрирования.

Особенности развертывания nShield as a Service	Самостоятельное	Полностью управляемое
Доступ заказчика к выделенному оборудованию nShield Connect, размещенному в защищенном центре обработки данных	✓	✓
Комплект для удаленного администрирования nShield Remote Administration, позволяющий безопасно подключаться к одному или нескольким облачным аппаратным модулям безопасности nShield и взаимодействовать с ними	✓	✓
Техобслуживание и поддержка <ul style="list-style-type: none"> <li>• Мониторинг услуги</li> <li>• Предварительно протестированные обновления/исправления, применяемые во время ежегодного или аварийного обслуживания</li> <li>• Поддержка — круглосуточно и без выходных</li> </ul>	✓	✓
Полное управление ходом установки <ul style="list-style-type: none"> <li>• Роль специалиста по безопасности, выполняется доверенным сотрудником <ul style="list-style-type: none"> <li>– Создание архитектуры nShield Security World</li> <li>– Регистрация HSM</li> <li>– Процедуры подписания</li> </ul> </li> </ul>		✓
<ul style="list-style-type: none"> <li>• Политика и процедуры, соответствующие ISO/IEC 27001: 2013 (сертификат о регистрации предоставляется по запросу)</li> <li>• Реестр по безопасности, доверию и предоставлению гарантий (STAR) Федерации информационной облачной безопасности (CSA), Уровень 1</li> </ul>	✓	✓
<ul style="list-style-type: none"> <li>• Все специалисты по операциям прошли проверку согласно процедуре BS7858 (только для центров обработки данных в Великобритании)</li> </ul>	✓	✓

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**

