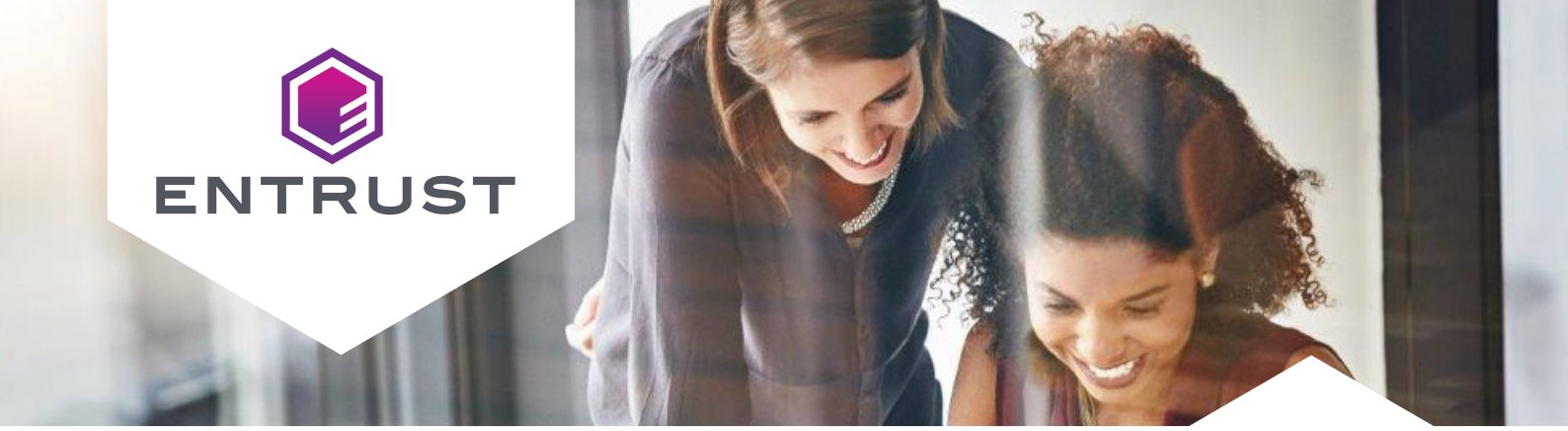

Пакет Cloud Integration Option Pack

Создавайте и управляйте криптографическими ключами в своем аппаратном модуле безопасности, сертифицированном по стандарту FIPS 140-2, а затем безопасно экспортируйте их в облако

ОБЗОР

Пользователи общедоступных облачных сервисов получают возможность генерировать криптографические ключи в своей собственной среде и управлять ими, при необходимости предоставляя к ним доступ для использования в облаке по своему выбору.

- Контроль ваших криптографических ключей с поддержкой мультиоблачной или гибридной облачной стратегии
- Безопасное создание ключей с использованием источника с мощной энтропией
- Долгосрочная защита ключей с помощью аппаратного модуля безопасности, сертифицированного по стандарту FIPS
- Поддержка Amazon Web Services, Google Compute Engine и Microsoft Azure

Защитите свои ключи, опираясь на высочайший уровень надежности

Защитите и данные, и свой бренд

Аппаратные модули безопасности nShield от Entrust, проверенные на соответствие высочайшим стандартам безопасности, таким как FIPS 140-2 и Common Criteria, защитят данные даже в самых сложных и нестандартных ситуациях, возникающих как локально, так и в облачной среде.

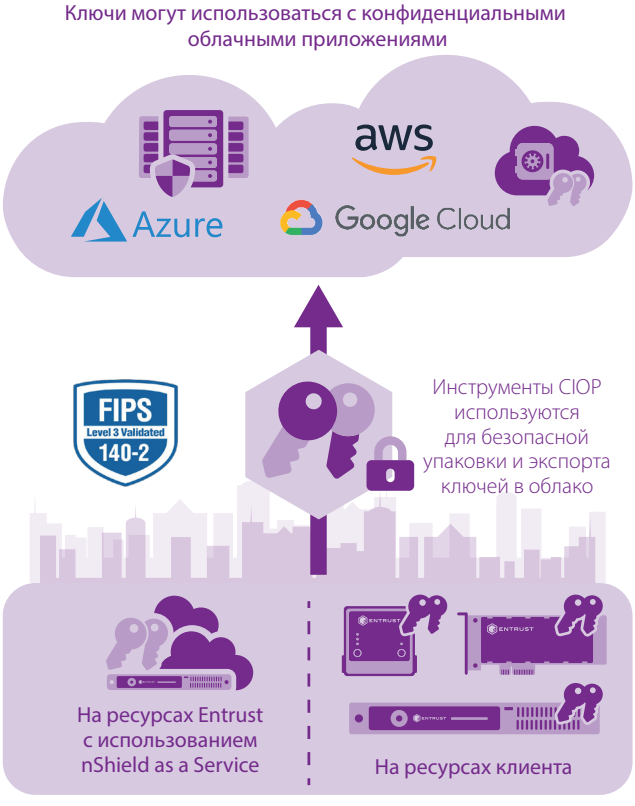

Рисунок 1. Ключи шифрования создаются в HSM nShield, надежно упаковываются и экспортируются в облако

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

Пакет Cloud Integration Option Pack

Поддерживаемые поставщики облачных услуг

Пакет Cloud Integration Option Pack (CIOP) содержит инструменты, позволяющие создавать криптографические ключи с помощью HSM nShield, а затем упаковывать и безопасно экспортировать их в службы ряда поставщиков облачных услуг:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (с использованием механизма Azure BYOK)

Если требуется более высокий уровень надежности, Microsoft предлагает BYOK от nCipher. BYOK от nCipher дает дополнительную уверенность в том, что разрешения для ключей, заданные во время их создания, сохраняются во время передачи ключей в Microsoft Azure Key Vault. Кроме того, Microsoft использует архитектуру Entrust nShield Security World, чтобы ограничить использование ключей заданной зоной Azure. Для такого варианта не требуется приобретать пакет CIOP. Подробнее об этом написано в документе «**Импорт ключей, защищенных аппаратными модулями безопасности, для Key Vault (nCipher)**».

Управление ключами в гибридных и мультиоблачных средах

Пакет Cloud Integration Option Pack обеспечивает контроль и уверенность при развертывании гибридной облачной стратегии, мультиоблачной стратегии или использовании одного поставщика облачных услуг. Предоставление своих криптографических ключей поставщику облачных услуг позволяет избежать трудностей, обусловленных привязкой к одному поставщику, которая может осложнить смену поставщика облачных услуг.

Поддерживаемые конфигурации

- Требуется программное обеспечение nShield Security World версии 12.60 и прошивка версии не ниже 12.60 для Azure BYOK
- Требуется программное обеспечение nShield Security World версии 12.40 для AWS и Google Compute Engine
- Это решение было протестировано на совместимость с рядом платформ, в том числе:
  - Microsoft Windows Server 2019 x64 и 2016 x64
  - Microsoft Windows 10 x64 и 7 x64
  - Red Hat Enterprise Linux 7 x64 и AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 и 11 x64
  - Oracle Enterprise Linux 7.6 x64 и 6.10 x64
- Поддерживаемые аппаратные модули безопасности
  - Совместим со всеми моделями HSM nShield, существующими в данный момент

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 размещена по ссылке
entrust.com/HSM

Пишите нам:
HSMinfo@entrust.com