

Доверенное устройство управления payShield (TMD)

Безопасное, гибкое и эффективное управление ключами для платежных HSM

- Шифрование ключевой чувствительной информации при выводе на защищенный сенсорный экран.
- Обеспечение строгой аутентификации на основе ролей для критических задач.
- Поддержка выбора форматов вывода для ключей и компонентов
- Использование QR-кодов для упрощения обмена ключами и уменьшения количества ошибок при вводе данных.
- Представление компактных, интуитивно понятных, автономных решений PCI HSM v3 KLD для использования в любом месте



Обзор

PayShield Trusted Management Device (TMD) от Thales - это компактное, интуитивно понятное, автономное безопасное криптографическое устройство (SCD), которое позволяет вам безопасно управлять симметричными ключами. TMD генерирует ключи в соответствии с соответствующими стандартами безопасности, включая X9 TR-31, ANSI X9.24-1 и PCI PIN Security. В отличие от традиционных подходов, все критически важные задачи управления ключами могут выполняться без какого-либо физического подключения к производственному HSM, что обеспечивает большую операционную гибкость без ущерба для безопасности. Один TMD может формировать ключи для нескольких платежных HSM, распределенных по нескольким центрам обработки данных, что позволяет крупным платежным системам, создавать и распространять тысячи симметричных ключей одновременно и безопасно, устраняя при этом ошибки ввода данных.

Функции управления ключами

TMD использует один или несколько ключей, известных как Master Zone Master Keys или MZMK, с HSM, чтобы облегчить безопасный обмен ключевыми материалами. Это избавляет TMD от необходимости запрашивать доступ к локальным мастер-ключам (LMK), используемым производственными HSM. Ключи, сгенерированные TMD, передаются в HSM в зашифрованном виде с использованием соответствующего MZMK, откуда они могут быть импортированы.

- Использование до 20 MZMK на TMD: поддержка криптографических ключей DES (двойная и тройная длина) и AES (128, 192 и 256 бит)
- Смарт-карты TMD, используемые для хранения компонентов каждого MZMK - минимум 2, максимум 9 для авторизации
- Отдельные роли администратора, оператора и аудитора, управляемые с помощью смарт-карт TMD.
- Гибкий набор методов безопасного обмена ключами и компонентами между TMD и HSM - QR-коды, смарт-карты, USB-токены и бумажные компоненты

Администраторы

- Роли администраторов создают владельцы компонентов MZMK.
- Администраторы назначают роли операторам и аудиторам
- Операторы могут выполнять функции в соответствии с ролью, назначенными администраторами.
- Двойное управление для всех функций оператора
- Функции включают управление ключами и работу системы

Типичные варианты использования

- Формирование ключей из компонентов
- Разделение существующих ключей на компоненты
- Обмен симметричными КЕК внутри организации или извне с доверенными третьими сторонами.

Функции безопасности

- Конфиденциальные данные сразу же удаляются в случае атаки - конструкция, отвечающая за несанкционированный доступ, независимо сертифицирована PCI
- Надежная аутентификация на основе ролей (минимум двойного контроля)
- Защищенный сенсорный экран заменяет традиционную клавиатуру - конфиденциальная ключевая информация, зашифрованная в точке захвата
- Подробный журнал аудита

Особенности устройства

- Компактное, интуитивно понятное, автономное решение - без дополнительных аксессуаров.
- QR-коды упрощают обмен ключами - нет необходимости в ручном вводе данных
- Встроенный принтер быстро распечатывает компонент или криптограмму, избегая записи экранной информации
- Встроенная камера облегчает раздачу ключей - нет необходимости ручного ввода

Характеристики продукта

- 7-дюймовый полноцветный емкостный сенсорный экран TFT IPS с разрешением 1280 x 800 пикселей
- Перезаряжаемый и сменный литий-ионный аккумулятор емкостью 5200 мАч
- Дополнительные блоки питания для США, Великобритании, Европы и Австралии
- Встроенный считыватель смарт-карт, соответствующий ISO / IEC 7816-1 / 2/3
- Встроенный термопринтер (ширина печати 48 мм с отрывной полосой)
- USB-кабель (тип C - тип A)

Сертификаты безопасности и соответствие требованиям

- Сертифицированный KLD PCI HSM v3
- Соответствие аудиту безопасности PCI PIN

Физические характеристики

- Высота 72 мм
- Ширина 114 мм
- Длина 231 мм
- Вес 625 г
- Импульсный адаптер питания 5 В / 2 А, литий-ионный аккумулятор
- Рабочая температура: от 0 до 50 ° C
- Рабочая температура зарядки аккумулятора: от 0 до 45 ° C.
- Температура хранения: от -20 до 60 ° C.
- Влажность при эксплуатации: от 5 до 85% (без конденсации)

Соответствие требованиям безопасности и охраны окружающей среды

- TUV CB, cTUVus, FCC, IC, CE, RCM
- RoHS, REACH, WEEE

О компании Thales

Люди, на которых вы полагаетесь для защиты вашей конфиденциальности, полагаются на Thales для защиты своих данных. Когда дело доходит до безопасности данных, организации сталкиваются с растущим количеством решающих моментов. Является ли момент строением стратегии шифрования, переходом в облако или соблюдением требований, вы можете положиться на Thales, чтобы обеспечить безопасность вашей цифровой трансформации. Решающие технологии для решающих моментов.

> thalesgroup.com <    

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com