

Thales payShield 9000 - сетевой аппаратный модуль безопасности (HSM) для защиты платежных систем

Thales payShield 9000 обеспечивает защиту более 80 % платежных транзакций в мире.

Thales payShield 9000 – сетевой аппаратный модуль для обеспечения безопасности платежных приложений. Он предназначен для создания, защиты и хранения криптографических ключей шифрования и PIN-кодов пользователей. Это критически важный и необходимый элемент защиты транзакций по платежным и кредитным картам через банкоматы и POS-системы. payShield 9000 соответствует требованиям обеспечения безопасности большинства международных платежных систем, включая American Express, Discover, JCB, MasterCard и Visa. Широкий выбор возможностей позволяет настроить модуль под любые требования. Гибкость и функциональность обеспечили Thales payShield 9000 мировую популярность. Более 80% платежных транзакций в мире осуществляется при помощи этого модуля.

Преимущества payShield 9000

- Комплексная система безопасности выпуска карт и обработки платежей
- Интегрируется с большинством существующих банковских приложений
- Возможность апгрейда функционала и производительности «на месте» программными средствами (без замены модуля)
- Соответствие стандартам FIPS 140-2 Level 3 и PSI HSM
- Модульная программная архитектура
- Возможность изменения программной составляющей
- Интерфейсная совместимость с предыдущим поколением HSM 8000



Thales payShield 9000

Управление ключами

Большое количество локальных мастер-ключей (LMK) для разделения типов ключей, приложений и клиентских данных
Блоки ключей Thales (в соответствии с ANSI X.9; X.9 TR-31)
Поддержка блоков ключей X.9 TR-31
Публичные ключи RSA
Ключи DUKPT для защиты PIN-кодов
Схема основного/сеансового ключей
Схема ключей транзакций Rasal
Поддержка AS2805

Поддержка механизмов криптографии

DES и Triple-DES (2 и 3 ключа)
AES (128, 192 и 256 бит)
RSA (до 2048 бит)
FIPS 198-1, MD5, SHA-1, SHA-2

Производительность

Диапазон производительности до 1500 операций (Triple-DES операций с PIN блоками)
Многопоточный режим работы для оптимизации производительности
Кластеризация при помощи приложения Security Resource Manager

Подключение хостов

Асинхронное (v.24, RS-232)
TCP/IP и UDP (10/100/1000 Base-T)
FICON

Сертификация

140-2 Level 3, 46, 81, 180-3, 186-3, 198
PCI HSM v1
APCA
MEPS
NIST SP800-20, SP800-90(A)



Поддержка стандартов финансовой индустрии

ISO 9564, 10118, 11568, 13491, 16609,
ANSI X3.92, X9.8, X9.9, X9.17, X9.24, X9.31,
X9.52, X9.97
X9 TR-31, X9 TG-3/TR-39, APACS 40 & 70,
AS2805 Pt 14
Список постоянно расширяется

Работа с платежными картами

Функции проверки PIN-кодов и карт American Express/MasterCard/VISA
Транзакции и сообщения EMV.3X и 4X (включая смену PIN)
Удаленная загрузка ключей в банкоматы NCR, Diebold и Wincor Nixdorf
Платформа безопасности Europay Security Platform
Интеграция с большинством существующих банковских приложений

Средства управления

Консольный интерфейс для «немых» терминалов
Графический пользовательский интерфейс (GUI) для стандартного программного обеспечения через Ethernet; поддержка локальных и удаленных режимов
Кластеризация посредством приложения Security Resource Manager (SRM)
SNMP
Встроенный журнал ошибок

Функции безопасности

Двухфакторная аутентификация при помощи смарт-карт
Два физических замка и изменение режимов работы с помощью смарт-карт
Взломостойчивый корпус, соответствующий требованиям FIPS 140-2 Level 3
Контроль попыток снятия крышки, датчики движения, напряжения и температуры
Возможность отключить функции безопасности, не востребованные хостовыми приложениями
Журналы аудита

Физические характеристики

Габариты: 2U для монтажа в 19" серверную стойку
85x478x417 мм
Вес 7.3 кг с одним блоком питания, 7.5 – с двумя
Напряжение: 100-240V
Частота: 40-63Гц
Потребляемая мощность: 100W
Температура эксплуатации: 10...40C°
Влажность: 10-90% (без конденсации)

