

THALES payShield 9000



je prvým hardvérovým bezpečnostným modulom (Hardware Security Module; HSM) vo svete, ktorý je špeciálne navrhnutý pre bezpečné platobné systémy, ktorý ponúka dva samostatné napájacie zdroje, poskytuje vysokú odolnosť nevyhnutnú

pre vysokokapacitnú zdieľanú infraštruktúru v kritických (mission-critical) bezpečnostných systémoch v moderných dátových centrách.

Podporuje tiež nárast v celkových objemoch uskutočnených transakcií širokou škálou výkonnostných verzií, ktorá zahŕňa aj najvýkonnejšiu súčasnú verziu pre túto oblasť, ktorá je schopný vykonať až 1500 transakcií za jednu sekundu (TPS)

Navrhnutý, tak aby spĺňal požiadavky bezpečnosti pre finančný priemysel, včítane štandardu FIPS 140-2 Level 3 a najnovšieho PCI HSM je payShield 9000 ideálnym výberom pre nadobúdateľov, výrobcov a vydavateľov v oblasti kartových systémov na vydávanie a spracovávanie všetkých typov kariet s magnetickou páskou resp. čipových kariet (EMV).

HSM technológia Thales chráni celosvetovo technológie ATM, POS, korporáčného bankovníctva, vydávania kariet, prevodov finančných prostriedkov a obchodovania s akciami. Je využívaná všetkými hlavnými kartovými systémami a v súčasnosti chráni 70 percent svetových transakcií vykonaných prostredníctvom kariet.

VÝHODY

- Integrovaťelný so všetkými rozhodujúcimi softvérovými produktmi pre finančné transakcie
- Komplexný balík softvérových balíkov ušitý pre vydavateľov, spracovateľov a nadobúdateľov kariet
- Spätná kompatibilita s HSM 8000
- Široká škála protokolov/pripojení k hostiteľským systémom

CHARAKTERISTIKA

Ochrana finančných transakcií

Navrhnutý špeciálne pre naplnenie potrieb priemyslu platobných kariet s kryptografickou podporou na vydávanie platobných kariet a na výmenu a autorizáciu transakcií.

Vysoká odolnosť a dostupnosť

Celá škála hardvérových a softvérových vlastností vrátane duálneho napájania umožňujúca nepretržitú prevádzku dátových centier aj v prípade výpadkov.

Komplexná bezpečnosť optimalizovaná pre platobné systémy

Navrhnutý špeciálne za účelom splnenia požiadaviek platobných systémov s bohatým súborom kryptografických funkcií pokrývajúcim všetky aspekty transakčných procesov a vydávania kariet

Škálovateľná vzdialená správa

Umožňuje, aby samostatný bezpečnostný tím umiestnený v jednej lokalite manažoval payShield zariadenia vo viacerých dátových centrách bez potreby cestovania

Modulárny softvér

Široká škála softvérových balíkov navrhnutá pre spracovateľov a nadobúdateľov umožňujúca znížiť náklady ich vlastníkom.

Preukázateľná integrácia s aplikáciami pre platobné systémy

Komplexná predpripravená podpora pre všetky najpoužívannejšie platobné aplikácie.

Flexibilné možnosti modernizácie

Široká škála jednotlivých softvérových licencií spolu so službou individuálneho nastavenia softvéru navrhnutá na doplnenie štandardných softvérových balíkov.



ŠPECIFIKÁCIA

Manažment kľúčov (Key Management)

Možnosť viacerých Local Master Keys (LMKs) ma bezpečné uchovávanie a distribúciu kľúčov, ktorá poskytuje úplné oddelenie používaných typov kľúčov, aplikácií alebo zákazníckych aktív podľa požiadaviek používateľa.

- Testovacie LMK na použitie mimo produkčného prostredia
- Podpora Thales Key Block (súčasť ANSI X9.24)\
- Podpora X9 TR-31 Key Block
- RSA public key

- DUKPT (DES a Triple-DES)
- Master/Session Key; Racal Transaction Key; AS2805 Key (DES a Triple-DES)

Podpora kryptografických algoritmov

- DES a Triple-DES (dva resp. tri kľúče)
- RSA (až do 2048 bits)
- AES a ECC prostredníctvom upgrade softvéru

Výkonnostné parametre

- Škála výkonnostných modelov až do 1500 Triple-DES PIN block transakcií/sekundu s použitím key blocks
- Multi-threading na využitie dostupných výkonnostných možností
- Možnosť klastrovania v spojení s Thales Security Resource Manager (SRM)

Konektivita

- Asynchronous (v.24, RS-232)
- TCP/IP a UDP (10/100/1000 Base-T) - duálne porty na dosiahnutie redundancie
- FICON (future factory fitted option)

Certifikáty

- Thales Secure Processing Platform (TSPP) má certifikát FIPS 140-2 Level 3
- prebieha certifikácia payShield 9000 v zmysle požiadaviek MEPS, APCA a PCI HSM

Štandardy pre finančný priemysel

- American Express/Mastercard/Visa PIN a funkcie na overovanie kariet
- EMV 3.x a 4.x transakcie a správy (včítane zmeny PIN)
- Vzdialené nahrávanie kľúčov do NCR, Diebold and Wincor-Nixdorf ATMs
- Europay Security Platform (MasterCard stand-in processing)
- Integrácia so všetkými najpoužívanejšími aplikáciami na „payment authorisation“ a „transaction switching“

Nástroje na manažment

- Konzola pre 'dumb' terminály
- Možnosť grafického rozhrania (GUI) pre štandardné PC prostredníctvom Ethernet pripojenia - podpora lokálneho a vzdialeného módu
- Možnosť manažovania klastra payShield 9000 zariadení prostredníctvom externého Thales Security Resource Manager (SRM)

Bezpečnosť

- Dvojfaktorová autentizácia operátora za použitia čipovej karty
- Zdvojený fyzický zámok resp. použitie dvoch čipových kariet k nastaveniu režimu práce
- Ochrane pred nežiaducou manipuláciou navrhnutá na vyššej úrovni ako je požadované FIPS 140-2 Level 3
- Detekcia otvorenia krytu
- Mnohonásobné mechanizmy upozornenia pri pokuse o premiestnenie zariadenia, problémoch s napájaním a teplotou
- Umožnený 'hardening' zariadenia - možnosť odstavenia funkcií, ktorých využívanie nie je potrebné pre nasadenú aplikáciu

Fyzická charakteristika

- Prevedenie ako: 2U 19" rack mount
- Hmotnosť: 7.3 kg (7.5 kg so zdvojeným zdrojom)
- Pripojenie: 100 to 240V AC
- Spotreba : 100W (maximum)
- Prevádzková teplota: 10 až 40 °C
- Vlhkosť: 10% až 90% (bez prítomnosti kondenzátu)