

# payShield 10K

Le module de sécurité matériel qui sécurise les paiements du monde entier

---

## payShield 10K

- Simplifie le déploiement dans des centres de données « dark data »
- Offre une résilience et une disponibilité élevées
- Propose le support rapide le plus étendu de cartes et applications mobiles
- Prend en charge la mise à niveau des performances sans changement de matériel
- Assure la rétrocompatibilité avec tous les HSM de paiement existants de Thales



## Fiche technique

payShield 10K est un module de sécurité matériel (HSM) largement utilisé dans l'écosystème de paiement global par les émetteurs, les prestataires de services, les acquéreurs, les processeurs et les réseaux de paiement. Il joue un rôle de sécurité fondamental dans la sécurisation de la fourniture de données d'identification de paiement, de l'authentification des utilisateurs, des cartes et des processus de protection des données sensibles pour les paiements en personne et à distance.

## Cas d'usage courants

- Fourniture de données d'identification : cartes, éléments sécurisés mobiles, dispositifs portables, dispositifs connectés et applications d'émulation de la carte d'hébergement (HCE)
- Routage PIN
- Chiffrement point à point (P2PE)
- Tokénisation de la sécurité (pour conformité PCI DSS)
- Tokénisation de paiement EMV
- Autorisation de paiement par carte et mobile
- Gestion de clé POS, mPOS et SPoC
- Validation des cryptogrammes PIN et EMV
- Chargement de clé distante

## Le choix d'intégrateurs

- Intégration à toutes les applications d'autorisation de paiement et de commutation principales
- Vous pouvez trouver toutes les informations des partenaires technologiques à cette adresse : [cpl.thalesgroup.com/partners/technology-partners](http://cpl.thalesgroup.com/partners/technology-partners)

## Support de paiement par carte/mobile

- payShield 10K propose une gamme complète de fonctions répondant aux besoins des principales marques de paiement (American Express, Discover, JCB, MasterCard, UnionPay et Visa) dans un certain nombre de domaines, notamment :
  - Fonctions de vérification du code PIN et des cartes pour toutes les grandes marques de paiement
  - Autorisation de transaction EMV et messagerie
  - Autorisation de transaction de paiement mobile et gestion de clé
  - Chargement de clé à distance pour les distributeurs automatiques de billets et les dispositifs POS
  - Gestion de clé régionale/nationale (incluant l'Australie, l'Allemagne et l'Italie)
  - Prise en charge de la gestion de clé (OBKM) pour le compte de MasterCard
  - Préparation et personnalisation de données à bande magnétique et à base EMV, y compris l'approvisionnement mobile
  - Génération et impression de code PIN

## Algorithmes cryptographiques

- Longueurs de clé DES et Triple-DES 112 et 168 bits
- Longueur de clé AES 128, 192 et 256 bits
- RSA (jusqu'à 4 096 bits)
- HMAC, MD5, SHA-1, SHA-2

## Normes de services financiers

- ISO : 9564, 10118, 11568, 13491, 16609
- ANSI : X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97
- ASC X9 TR-31, X9 TG-3/TR-39
- APACS 40 et 70

## Sécurité physique

- Design inviolable et réactif
- Données sensibles effacées immédiatement en cas d'attaque de sabotage
- Déclencheur d'alarme de mouvement, de tension et de température

## Sécurité logique

- Options de la clé principale locale (LMK) : variante et bloc de clé
- Authentification à deux facteurs (2FA) des responsables de la sécurité utilisant des cartes à puce
- Autorisation à double contrôle : clés physiques ou cartes à puce
- Paramètres de sécurité informatique les plus forts implémentés par défaut
- Pistes de vérification avec contrôle de l'utilisateur de la portée des événements enregistrés

## Options et modèles de produits

- Unités de doubles blocs d'alimentation et ventilateurs remplaçables à chaud sur tous les modèles
- Plage de niveaux de performance : 25, 60, 250, 1 000 et 2 500 appels par seconde (cps)
- Options de gestion et de surveillance à distance via le Gestionnaire payShield, le Moniteur payShield et le Dispositif de gestion de confiance payShield (TMD)
- Options de chiffrement conservateur de format (FPE)
- Plusieurs options LMK : jusqu'à 20 partitions par HSM

## Connectivité hôte

- TCP/IP et UDP (1 Gbps) : ports doubles
- Option de gestion des communications de l'hébergeur sécurisée pour les sessions authentifiées TLS sur le port host Ethernet

## Certifications de sécurité

- FIPS 140-2 niveau 3 (sous-système de sécurité) en cours
- PCI HSM v3 (versions du logiciel sélectionnées) en cours

## Caractéristiques physiques

- Facteur de forme : montage en baie 1U 19 pouces
- Dimensions : 482,6 × 736,6 × 44,5 mm
- Poids : 15,9 kg
- Alimentation électrique : 90 à 264 VCA
- Consommation électrique : 60 W (maximum)
- Température en fonctionnement t: 0 °C à 40 °C
- Température de transport : -25 °C à 70 °C
- Température de stockage : -5 °C à 45 °C
- Humidité : 10 % à 90 % (sans-condensation)

## Conformité aux normes relatives à la sécurité et à l'environnement

- UL, UL/CA, UL-AR, CE, BIS, FCC, Canada ICES, RCM, KC, VCCI
- RoHS2, REACH, WEEE

## À propos de Thales

Les personnes à qui vous accordez confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.