cpl.thalesgroup.com

THALES

La gestion des transactions avec les HSM payShield

Contents

Présentation

payShield de Thales est le leader en matière de HSM de paiement dans le monde, contribuant à sécuriser environ 80 % des transactions en point de vente dans le monde. HSM privilégié par les fournisseurs de solutions de paiement et les distributeurs de technologie de paiement, il offre une intégration éprouvée à toutes les applications de paiement principales. Il accélère la mise sur le marché pour différents participants, y compris les émetteurs et les acquéreurs, qui exigent une sécurité solide lors du traitement des transactions de commerce de détail. Depuis son déploiement initial, au début des années 1980, la famille de HSM de paiement Thales a continué d'évoluer afin de répondre aux besoins de l'industrie du paiement en matière de transactions, pendant la transition des bandes magnétiques aux cartes à puce EMV, puis à l'arrivée des paiements de proximité, basés sur les cartes sans contact et les appareils mobiles NFC.

Si l'on compare avec les premiers HSM de paiement Thales, la variante payShield utilisée aujourd'hui comprend un ensemble de commandes plus complet, des mécanismes de sécurité plus sophistiqués pour éviter les fraudes sur l'appareil, et fournit les niveaux de performance plus élevés nécessaires afin de sécuriser des volumes de transaction à augmentation exponentielle. Un service de surveillance et de gestion à distance complet est disponible pour réduire les coûts d'exploitation et améliorer la visibilité de l'environnement HSM. Les communications de l'hébergeur sécurisées permettent de déployer des appareils dans des environnements plus ouverts, plutôt que des segments de réseau privé dédiés.

L'importance et l'influence croissantes des organismes de normalisation internationaux, dont EMVCo et PCI SSC, ont contribué à des avancées considérables en matière de technologie de chiffrement requise dans les HSM de paiement, et à l'émergence de normes et de mandats de sécurité plus stricts. payShield a toujours adopté les dernières méthodes de sécurité et offert une prise en charge des nouvelles applications mobiles et de carte de plusieurs marques de paiement internationales. Ce document fournit un aperçu des caractéristiques et des avantages de la fonctionnalité de gestion des transactions payShield utilisée pour sécuriser l'écosystème des paiements dans le commerce de détail.

Les défis de la sécurisation des paiements de bout en bout

Tous les commerçants, les acquéreurs, les processeurs, les passerelles de paiement ou les émetteurs impliqués dans le traitement des transactions sont tout à fait conscients de la complexité accrue, depuis l'époque où il leur suffisait de prendre en charge les transactions en face à face par carte en plastique à bande magnétique, puis par carte de débit et de crédit à puce. Avant le déploiement, il est nécessaire d'établir de nombreuses zones de chiffrement de confiance, de confirmer la fiabilité de nombreux appareils d'acceptation côté client, ainsi que des HSM pour le traitement en arrière-plan, et enfin de prendre en charge une gamme de plus en plus variée de méthodes de paiement, des transactions en face à face aux transactions à distance.

À l'heure actuelle, nous sommes confrontés à la sécurisation des paiements « par carte » depuis les dispositifs des consommateurs (smartphones et tablettes, par exemple) qui ne sont pas émis par la banque, contrairement aux cartes de paiement matérielles. L'acceptation des paiements émis par les dispositifs IoT est une exigence récente et en rapide évolution, qui présente de nouveaux risques et de nouvelles menaces. La numérisation des cartes et leur utilisation pour les transactions a suscité récemment une augmentation considérable de l'activité dans le secteur de la sécurisation des paiements, avec un impact sur tous les acteurs impliqués dans l'acceptation des paiements.

Les « intermédiaires de paiement » traditionnels gérés et exploités par les réseaux de paiement majeurs (y compris des organisations internationales telles qu'American Express, Mastercard et Visa) doivent évoluer en permanence afin de prendre en charge des techniques de gestion des risques et de sécurité de plus en plus sophistiquées pour s'assurer que l'industrie réduit au maximum les risques de fraude au paiement et entretient ainsi la confiance des clients envers les systèmes de paiement. Le traitement des transactions est une activité de volume (qui repose sur un besoin d'efficacité intrinsèque), mais le gain en flexibilité pour les consommateurs et l'amélioration de l'expérience de paiement requièrent la mise en place d'un niveau de sécurité approprié, nécessitant souvent l'implémentation d'algorithmes cryptographiques plus forts, de longueurs de clé et d'une utilisation plus généralisée du chiffrement.

Parmi les défis du traitement (et par conséquent de la sécurisation) des paiements du commerce de détail on retrouve notamment :

- Couvrir toutes les applications récentes, y compris les cas d'utilisation de transactions en ligne et hors ligne issus des outils de paiement émis par les banques ou des appareils côté client : les conséquences quant aux besoins de chiffrement, aux données à protéger et à la gestion des risques diffèrent, même si la majorité repose sur un numéro de compte client ou un numéro PAN
- S'assurer que l'infrastructure est solide, protégée contre les attaques frauduleuses (les données sensibles en particulier) et capable d'accommoder les pics de volume de transactions : les efforts nécessaires à l'implémentation des changements nécessaires afin de s'adapter aux dernières menaces et à la surveillance efficace du bon fonctionnement des opérations pour garantir une disponibilité 24 h/27, 7 j/7 peuvent s'avérer considérables
- Se conformer à tous les derniers mandats de sécurité des marques de paiement qui tirent parti de plusieurs spécifications des organisations, y compris EMVCo et PCI SSC : de nombreuses organisations exigent désormais l'utilisation de HSM qui nécessitent la mise en application de politiques et de procédures de gestion de clé strictes

Tous les acteurs de la sécurisation des paiements, du point de départ, ou de la capture, à l'autorisation finale par la banque émettrice de la carte ou le processeur émetteur, doivent impérativement déployer des bases flexibles, sécurisées et fiables qui peuvent évoluer en fonction de leurs besoins.

payShield offre des solutions de traitement pour de nombreux types d'outils de paiement

payShield a aidé une variété de participants à simplifier leurs efforts d'intégration et à réduire leurs coûts d'exploitation pour une vaste gamme de transactions initiées par des outils de paiement anciens et récents, parmi lesquels :

- Cartes de débit et de crédit à bande magnétique
- Cartes de débit et de crédit à puce EMV (avec et sans contact)
- Appareils mobiles avec cartes numérisées (basés sur les éléments sécurisés, l'émulation de la carte d'hébergement ou les applications natives)
- e-Wallet, ou portefeuille électronique
- Carte sur fichier (y compris les identifiants tokénisés)
- IoT et appareils connectés utilisés pour les paiements

Le logiciel payShield de base en vente libre contient les fonctionnalités principales essentielles à l'infrastructure de traitement, indépendamment du type de paiement traité ou de l'outil de paiement utilisé pour la transaction :

- Gestion de clé et de certificat
- Clés symétriques (DES, TDES, AES) et asymétriques (RSA)
- Chiffrement/déchiffrement de messages
- Authentification de messages (MAC, CMAC, HMAC, hachage)
- Signatures et vérification numériques
- Audits

Avantages clés de payShield pour le traitement des transactions

Si vous êtes impliqué dans la gestion d'une infrastructure de traitement des transactions, vous savez à quel point les notions d'agilité, de flexibilité, d'évolutivité, de rentabilité et de sécurité sont cruciales pour votre solution. Afin de répondre constamment à vos besoins, payShield continue d'évoluer, proposant une vaste gamme d'avantages immédiats, parmi lesquels :

- **Prise en charge anticipée des dernières applications de carte et mobiles : permet d'étendre votre acceptation de paiement**
- **Intégration éprouvée à toutes les solutions d'application de paiement certifiées majeures : réduit la durée nécessaire aux tests**
- **Mise à niveau des performances sans changement de matériel : facilite la croissance de vos activités**
- **Capacités de gestion et surveillance à distance exhaustives : réduit vos coûts d'exploitation**
- **Certifié aux normes de sécurité régionales et mondiales : vous aide à réussir les audits de sécurité audits**

Au logiciel principal s'ajoute une gamme d'ensembles de fonctions complémentaires spécifiques qui, dans leur ensemble, couvrent l'intégralité des transactions par carte, mobiles ou IoT effectuées aujourd'hui. La liste suivante est examinée et complétée constamment dès que des nouvelles méthodes de paiement ou exigences en matière de sécurité émergent :

- Vérification et traduction de PIN
- Codes de vérification de carte/vérification des valeurs
- Vérification et génération de cryptogrammes EMV
- Authentification de l'utilisateur
- HMAC et CAP/DPA pour 3-D Secure
- Déchiffrement de messages pour les solutions P2PE (y compris le chiffrement conservateur de format)

Offre une résilience et une disponibilité élevées

payShield a toujours été pionnier en matière de résilience élevée, bilan renforcé par une fiabilité éprouvée. Parmi les fonctions principales qui aident à entretenir votre environnement de HSM payShield :

- Utilise des unités de doubles blocs d'alimentation et ventilateurs remplaçables à chaud et de ports d'hôte doubles, pour une résilience et une redondance améliorées
- Réduit au minimum la durée d'indisponibilité planifiée (grâce à une gestion, une configuration et des mises à jour des HSM efficaces)
- Évite l'empreinte client pour supprimer toute dépendance de système d'exploitation pouvant autrement entraîner des mises à jour ou des correctifs de sécurité continus
- Réduit les interactions physiques avec les HSM par le biais d'une approche sans contact à l'aide d'un centre de données « dark data »
- Prend en charge les communications sécurisées entre l'application et le HSM pour s'assurer que seules les applications vérifiées ont accès à ses services
- Conservation de pistes de vérification pour toute opération de sécurité importante afin de simplifier les exigences de rapports d'audit obligatoires
- Propose en option le contrôleur payShield Monitor pour aider à la planification de capacité

Permet des mises à niveau logicielles et de performance pour se conformer aux nouvelles exigences

L'environnement de traitement est toujours en mouvement : c'est vrai aussi bien pour le nombre croissant de transactions nécessitant traitement que pour les types de paiement effectués. De par son étroite collaboration avec les différentes marques de paiement, les organisations de normalisation et les organismes de certification de sécurité des paiements, Thales garantit que sa plateforme payShield soit constamment mise à jour, afin que vous puissiez procéder au traitement de tous les types de paiement de la manière la plus efficace et la plus sécurisée possible. Parmi les avantages principaux d'adopter la normalisation des HSM de paiement payShield pour les exigences actuelles et à venir :

- Les mises à jour logicielles et de licences sont très simples et rapides : vous n'avez même pas besoin de visiter le centre de données si vous utilisez la fonction de gestion à distance du gestionnaire payShield
- Les nouvelles fonctionnalités sont disponibles rapidement : en collaborant étroitement avec plusieurs marques de paiement, nous obtenons leurs spécifications les plus récentes et distribuons la fonctionnalité en avance à notre liste grandissante de partenaires de technologie, pour une intégration anticipée à leur logiciel d'application de paiement
- Des mises à jour de licence logicielle sont disponibles pour vous permettre d'optimiser vos performances et votre capacité de traitement globale : nous offrons une vaste gamme de niveaux de performance ; vous pouvez ainsi commencer à un niveau bas et faire les mises à jour nécessaires ultérieurement pour éviter tout changement de matériel

Prise en charge d'applications de carte et mobiles pour toutes les marques de paiement principales

En tant que processeur ou acquéreur de volume de transactions de paiement du commerce de détail, vous devez disposer de la prise en charge des applications de paiement la plus étendue possible afin d'optimiser votre volume, et ainsi vos profits. Les HSM payShield contiennent une fonctionnalité de prise en charge des exigences en matière de sécurité des transactions pour tous les systèmes de paiement principaux, sur plusieurs outils de paiement. La liste des éléments couverts, revue fréquemment, comprend actuellement :

- La prise en charge des applications de carte avec et sans contact pour American Express, Discover, JCB, Mastercard, UnionPay et Visa (cartes à bande magnétique et carte à puce EMv, le cas échéant)
- Les transactions mobiles NFC basées sur les éléments sécurisés et l'émulation de la carte d'hébergement conformes aux spécifications propriétaires d'American Express, de Mastercard et de Visa
- Les services de tokénisation d'American Express, Discover, Mastercard et Visa conformes à la norme EMVCo
- Les services de tokénisation des acquéreurs (ou de non-paiement) conformes à la spécification et aux directives PCI DSS

Offre des nouveaux services

Les HSM payShield sont au cœur de l'infrastructure solide des intermédiaires de paiement, déployés sur plusieurs nœuds des différents réseaux, y compris ceux associés aux commerçants, aux processeurs des commerçants, aux facilitateurs de paiement, aux banques acquéreuses, aux réseaux de paiement, aux processeurs émetteurs et aux banques émettrices.

Différents participants peuvent avoir des besoins légèrement différents dans leur stratégie de consolidation de leur posture de sécurité et de réduction des risques. La numérisation constante des paiements dans le commerce de détail a stimulé l'innovation afin de trouver de nouvelles approches de sécurité pour la protection de l'infrastructure de traitement. payShield est mis à jour régulièrement afin de prendre en charge les exigences en matière de gestion de clé et du chiffrement de plusieurs solutions, parmi lesquelles :

- Numérisation de cartes, que l'outil de destination soit, par exemple, un appareil mobile, une carte de commerçant sur un système de fichier ou un appareil IoT ou connecté
- Prise en charge du chiffrement P2PE principalement pour les segments du commerçant à l'acquéreur ou au processeur, dont l'objectif principal est d'améliorer la protection des données de paiement en mouvement et, en même temps, de réduire la portée de la conformité PCI DSS pour les commerçants
- Tokénisation des paiements qui, en plus d'être un composant essentiel de certaines formes de numérisation de cartes, est utilisé de manière dynamique afin de changer le numéro PAN en token pour l'essentiel de la transaction, afin de protéger les données de paiement en mouvement.

Dans tous les cas, l'utilisation intensive de fonctionnalités de haut niveau dans la plateforme payShield a permis, en offrant des solutions de paiement au marché, de simplifier les opérations, aussi bien pour les équipes de développement bancaire en interne que pour les intégrateurs. De plus, la création de partitions de HSM (par le biais de la prise en charge de plusieurs clés principales locales ou LMK) est une option utilisée efficacement par les clients payShield afin de proposer une séparation sécurisée des applications et des locataires.

Simplification de l'intégration

Depuis leur création, l'un des buts principaux des HSM de paiement Thales est de simplifier l'opération pour quiconque souhaite effectuer une intégration avec eux, ou les utiliser pour sécuriser les transactions. Voici les principales avancées que nous avons réalisées au fil de ce processus :

- Nous nous assurons d'éliminer l'empreinte de l'hôte ou la dépendance du système d'exploitation : nous souhaitons empêcher le besoin de toute mise à jour de logiciel HSM si votre système d'exploitation, application ou base de données hôte, par exemple, doit appliquer un correctif de sécurité ou une mise à jour fonctionnelle forcée
- Nous prenons en charge toutes les méthodes de gestion de clé des systèmes de paiement : simplifie la génération, le partage et l'utilisation de clés de chiffrement solides
- Nous présentons des fonctions de haut niveau de sécurité pour l'intégration : élimine la complexité, évite de devoir lire et comprendre des centaines de pages de spécifications de sécurité complexes en réduisant en même temps le nombre d'appels HSM nécessaires pour compléter une tâche particulière (ce qui contribue à sécuriser davantage le système en évitant toute exposition à des étapes de traitement intermédiaires)
- Nous permettons aux clés de chiffrement dont vous avez besoin pour le traitement d'être stockées sous la forme de cryptogrammes sur des bases de données externes sous le contrôle de votre application : garantit l'absence de problèmes de synchronisation ou d'évolutivité lorsque que le besoin se présente de prendre en charge des HSM supplémentaires au fur et à mesure que le volume de traitement augmente
- Nous conservons la rétrocompatibilité lorsque nous introduisons de nouveaux HSM de paiement à notre portefeuille ou que nous étendons notre ensemble de commandes : permet d'assurer que vos applications fonctionnent en toute fluidité sur les modèles actuels de HSM Thales tout comme les nouveaux modèles
- Nous distribuons des logiciels de base riches en fonctionnalités que vous pouvez utiliser en vente libre : nous faisons en sorte que notre service de personnalisation en option ne soit pas généralisé

Réduction des coûts d'exploitation

En choisissant payShield comme plateforme de HSM de paiement, vous profiterez d'une multitude d'avantages vous permettant de réduire vos coûts d'exploitation :

- Si vous utilisez l'interface graphique du gestionnaire payShield Manager, la configuration est simplifiée : nous faisons tout ce que nous pouvons pour simplifier l'expérience utilisateur
- Les niveaux de performances peuvent être mis à jour ultérieurement : nous vous offrons la possibilité de limiter votre investissement jusqu'à ce que vous ayez vraiment besoin d'augmenter votre puissance de traitement
- La gestion du HSM à distance élimine la nécessité de se rendre aux centres de données : nous avons sécurisé la gestion à distance des tâches généralement effectuées en face à face (lorsque cela vous convient)
- La surveillance en arrière-plan avec le contrôleur payShield Monitor fournit une grande visibilité pour tous vos HSM, 24 h/24, 7 j/7 : nous facilitons la détection rapide de problèmes potentiels et réels, vous permettant de planifier plus facilement vos besoins en matière de capacité de traitement
- Le HSM payShield est certifié conforme à toutes les normes de sécurité internationales et régionales : nous aidons à accélérer la conformité aux audits, particulièrement aux cinq spécifications PCI SSC qui exigent l'utilisation de HSM (sécurité du PIN PCI, PCI P2PE, PCI TSP, PCI 3DS et PCI SPoC), dont la plupart s'appliqueront à votre situation

Thales est l'entreprise de HSM de paiement pour le long terme. Nous sommes réputés pour encourager l'optimisation du cycle de vie actif de notre gamme de produits HSM. Cette réputation est renforcée par nos services de support supérieurs, locaux, gérés par notre équipe interne d'experts dans l'industrie du paiement aux connaissances étendues, auxquels s'ajoute notre réseau de partenaires de technologie. Il est temps de normaliser votre infrastructure HSM avec Thales payShield pour toutes vos exigences en matière de transaction.

payShield : une plateforme flexible et sécurisée pour tous vos besoins de traitement des transactions

- Accélère la mise sur le marché de nouveaux services de paiement
- Réduit les coûts de gestion continue et des audits de sécurité
- Permet à l'environnement essentiel à votre mission de fonctionner 24 h/24, 7 j/7 en toute sécurité

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.

THALES

Nous contacter

Retrouvez nos coordonnées sur notre site Internet
cpl.thalesgroup.com/fr/contact-us

> cpl.thalesgroup.com <