

THALES



➤ Module de Sécurité HSM8000

Securing your future

>> MODULE DE SÉCURITÉ HSM

Le module HSM est un appareil infalsifiable qui offrant les fonctions cryptographiques nécessaires à la sécurisation des transactions sur les réseaux financiers.

Le module HSM est utilisé pour protéger une multitude d'applications financières dans le monde, allant des réseaux de guichets automatiques et de points de vente aux systèmes de virement interbancaire et d'échanges d'actions. Il est disponible en version standard ou à haut débit avec une grande variété d'options et de protocoles de connexion permettant une liaison avec tous les types de systèmes.

Le module de sécurité HSM:

- est utilisé pour 70 % des transactions réalisées par carte dans le monde ;
- est utilisé par les principales associations de cartes de crédit ;
- est utilisé pour les guichets automatiques bancaires (GAB), les points de vente, les services bancaires aux entreprises, l'émission de cartes, les virements et les opérations sur actions ;

- Fonctions de vérification de carte et de PIN Visa/MasterCard/American Express
- Messagerie sécurisée et traitement des transactions EMV 3.1.1 et EMV 4.0 (comprenant la modification des codes PIN)
- Chargement des clés à distance pour les guichets NCR et Diebold
- Schémas DUKPT et « Australian Transaction Key » Triple DES
- Création, signature et vérification des clés RSA
- Prise en charge Async, Ethernet, SNA sur tous les modèles
- Option ESCON disponible

- peut être facilement personnalisé pour les applications utilisateur ;
- prend en charge un grand nombre d'options de connexion et de protocoles de transaction ;
- est disponible en plusieurs versions afin d'offrir le niveau de débit requis ;
- prend en charge Triple DES à deux et trois clés pour toutes les fonctions, y compris le traitement de blocs PIN ;
- s'intègre aux principales applications des fournisseurs de solutions financières ;
- est conforme aux normes de sécurité les plus rigoureuses.

Applications HSM typiques

Interchange GAB

Le module HSM est conçu pour l'environnement d'interchange GAB et est utilisé dans la plupart des réseaux mondiaux d'interchange GAB. Il peut être personnalisé en fonction des caractéristiques du réseau et, si nécessaire, des exigences propres à chaque membre du réseau. La gamme variée et évolutive d'interfaces host du module HSM permet de prendre en compte les besoins du système de chaque membre. Les commandes AMEX, VISA et MasterCard font notamment partie des fonctionnalités standard.

EFTPOS

Le module HSM prend en charge de multiples systèmes Terminaux de paiement EFTPOS (Electronic Funds Transfer at Point of Sale) utilisés dans le monde entier. Thales a été précurseur dans la mise au point de la plupart des concepts de gestion de clés requis pour sécuriser les EFTPOS, comme le schéma « Racal Transaction Key », et leur intégration dans le module HSM. Les versions Single et Triple DES des schémas DUKPT (Derived Unique Key Per Transaction) et « Australian Transaction Key » sont également disponibles.

Fonction de fabrication de carte

Le module HSM peut être utilisé dans le cadre de la production de carte client. Il permet de générer en toute sécurité des valeurs de carte cryptographique comme CVV (Card Verification Value) pour VISA, CVC (Card Verification Code) pour MasterCard et CSC (Card Security Code) pour American Express, ainsi que des codes PIN et des courriers d'envoi de codes PIN.

Prise en charge de cartes à puce

Le module HSM prend en charge les cartes à puce de type débit/crédit et porte-monnaie électronique de Visa et MasterCard. Le logiciel HSM standard offre des commandes de traitement des transactions pour les systèmes EMV 3.1.1 et EMV 4.0.

Porte-monnaie électronique

Le module HSM peut prendre en charge les technologies Cash, CLIP et VCEPS de VISA, permettant aux détenteurs de cartes de les recharger en toute sécurité à partir d'un guichet automatique ou d'un terminal de rechargement.

Intégrité des données

L'intégrité des informations transmises et stockées au sein de systèmes est d'une importance capitale pour les utilisateurs. L'intégrité des informations générées au niveau des terminaux à distance peut être assurée à l'aide de codes d'authentification de message (MAC). Le module HSM est compatible avec les terminaux WebSentry™ et Smart Card. Des applications comme la gestion de trésorerie (Cash Management) et le réconciliation des obligations (Bond Reconciliation) peuvent être sécurisées de cette manière.

Caractéristiques du module HSM

Options de performance

L'adoption de plus en plus fréquente de systèmes de sécurité basés sur des cartes à puce et des codes PIN dans les milieux financiers et bancaires s'accompagne d'un accroissement de la demande de systèmes de traitement des transactions plus rapides.

Dans sa version à haut débit, le module HSM fournit les meilleures performances du marché (800 fonctions de conversion de blocs PIN Triple DES par seconde), ce qui réduit de manière significative le temps de traitement des transactions et diminue leur coût unitaire.

Système flexible de gestion de clés

En pratique, le niveau de sécurité offert par une application est aussi bon que le système de gestion de clés conçu à cet effet. Le module HSM prend en charge un large éventail de schémas de gestion de clés, comme Master/Session Key, Racal Transaction Key, Australian Transaction Key, DUKPT et Public Key.

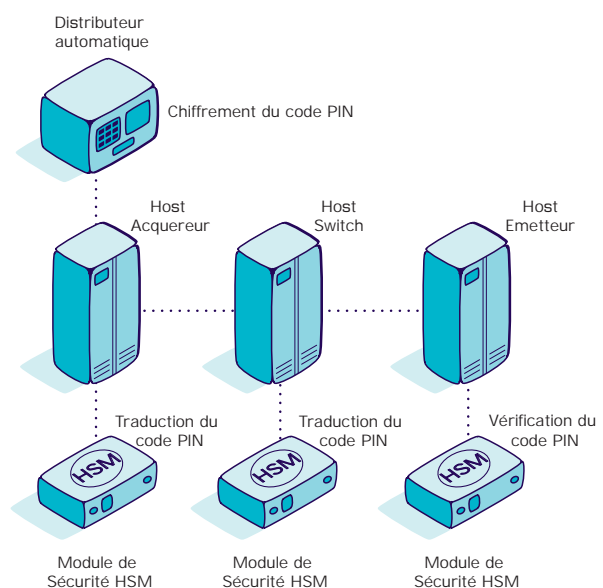
Prise en charge de la clé publique RSA

Le module HSM offre un sous-système de clé publique à haut débit. La cryptographie à clé publique RSA a deux fonctions principales :

1. Générer et vérifier des signatures numériques
2. Distribuer des clés DES chiffrées avec une clé publique RSA

Le module HSM prend en charge des longueurs de clé RSA allant de 320 à 2 048 bits.

Application typique d'un interchange GAB



Cette fonctionnalité permet d'intégrer le module HSM à des systèmes où des longueurs de clé différentes sont utilisées pour des fonctions différentes, comme les signatures électroniques et la gestion des clés. En outre, elle anticipe une augmentation prévisible des exigences en matière de longueur de clé afin de conserver une avance sur les menaces plus fréquentes.

Chargement à distance des clés des guichets automatiques

Des fonctions RSA permettent de traiter le chargement à distance des clés pour les guichets automatiques NCR et Diebold, permettant l'initialisation automatique des clés maître GAB, ce qui réduit les coûts de manière significative.

Certification en matière de sécurité

Le module HSM 8000 a obtenu l'agrément CB nécessaire à la sécurisation des transactions sur les réseaux bancaires français.

Le module HSM utilise le sous-système SGSS (Secure Generic Sub-System) de Thales pour tous les traitements cryptographiques et sécuritaires. Ce sous-système est conforme à la norme FIPS 140-1 niveau 4 et est soumis actuellement à l'évaluation FIPS 140-2*, connue comme l'une des plus rigoureuses.

Le module HSM surpasse les besoins de sécurité des réseaux financiers actuels.

Création et stockage des clés sécurisées

Une fois la clé LMK (Local Master Key) créée au sein du module HSM, toutes les autres clés sont stockées sous cette clé sous forme chiffrée sur et éventuellement dans le module HSM lui-même. Ce dernier utilise la technologie Smart Card pour stocker les principaux composants de la clé LMK.

Prise en charge d'un système hôte étendu

Le module HSM s'intègre aux applications développées par les principaux fournisseurs de solutions financières.

De nombreux protocoles de communication sont acceptés. La version standard du module HSM 8000 prend en charge TCP/IP et UDP (via une interface Ethernet 10/100 l'host auto-sensible), ainsi que les connexions SNA et Async. ESCON est disponible en option pour les gros systèmes IBM.

SRM (Security Resource Manager)

Les gestionnaires SRM sont des produits logiciels disponibles en option pour les systèmes IBM MVS, Tandem Guardian et UNIX®. Ils permettent à un grand nombre d'applications d'utiliser une interface de programmation (API) unique pour accéder aux ressources cryptographiques fournies par un jeu de modules HSM. Le gestionnaire SRM permet d'utiliser différents modèles HSM de manière transparente avec les applications des clients.

- Version IBM - fonctionne sous OS/390 et prend en charge les applications CICS, IMS et Batch. Les programmes en langage d'assemblage et les langages évolués comme COBOL et PL/1 sont également supportés.
- Version Tandem - fonctionne sous le système d'exploitation Guardian en tant qu'application Pathway et accepte les requêtes soit via un module d'interface d'application soit via une interface de serveur. Peut également fournir aux applications une base de données de clés pouvant être gérée par l'application ou par une interface utilisateur de gestion de clés.
- Version UNIX – fonctionne sous différentes versions d'UNIX, en tant que serveur prenant en charge des applications clientes sur plusieurs ordinateurs de réseau. L'API prend en charge les applications écrites en C ou C++.

Spécifications techniques

Performance standard (Conversion PINBlock Triple DES)	HSM8-SM 220 HSM8-EM 220 HSM8-SH 800 HSM8-EH 800
Prise en charge cryptographique	<p>Algorithmes DES et Triple DES – Fonctions d'authentification de messages et de chiffrement PIN.</p> <p>Algorithme RSA – Fonctions avancées de gestion de clés, comme le chargement à distance pour les guichets automatiques, et prise en charge de la création et de la validation des signatures numériques. La longueur des clés RSA peut aller de 320 à 2 048 bits.</p> <p>Composants LMK (Local Master Key) – Stockés sur des cartes à puce (ISO 7816) afin de sécuriser le stockage ou la distribution.</p>
Interfaces de communication	<p>HSM8-SM / HSM8-SH TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232, SNA (v.24/RS-232)</p> <p>HSM8-EM / HSM8-EH ESCON; TCP/IP and UDP, Ethernet 10/100Base-T; Async, RS232, SNA (v.24/RS-232)</p>
Certificat de sécurité	<p>Le module HSM utilise le sous-système SGSS (Secure Generic Sub-System) de Thales pour tous les traitements cryptographiques et sécuritaires. Ce sous-système est conforme à la norme FIPS 140-1 niveau 4 et est soumis actuellement à l'évaluation FIPS 140-2*, connue comme l'une des plus rigoureuses.</p>
Puissance	<p>Tension 90-132 V AC et 175-264 V AC, sélection automatique</p> <p>Fréquence 47-63 Hz</p> <p>Fusible 1,6 A, temporisation</p>
Environnement	<p>Température d'exploitation de 10 à 40 °C</p> <p>Humidité de 10 à 90 %, sans condensation</p>
Dimensions	<p>Hauteur 88 mm (2U)</p> <p>Largeur 480 mm (adaptée au bâti de 19")</p> <p>Profondeur 400 mm</p> <p>Poids 12 kg</p>

*Vérifier le statut de cette validation sur le site Web de NIST.



THALES

160, Boulevard de Valmy, BP 82
92704 Colombes Cedex, France
Tel: +33 (0)1 46 13 28 37 Fax: +33 (0)1 46 13 22 83
e-mail: Security@fr.thalesgroup.com

EUROPE, MIDDLE EAST, AFRICA

Meadow View House, Crendon Industrial Estate
Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, UK
Tel: +44 (0)1844 201800 Fax: +44 (0)1844 208550
e-mail: emea.sales@thales-esecurity.com

FIPS 140-1™ : marque de validation de NIST, qui n'implique pas l'approbation du produit par le NIST, ou les gouvernements des Etats-Unis et du Canada. MasterCard est une marque déposée de MasterCard International Incorporated. Visa est une marque déposée de Visa International Service Association. IBM est une marque déposée de International Business Machines Corporation. American Express et Amex sont des marques déposées de American Express Company. UNIX est une marque déposée de The Open Group. HP et Tandem sont des marques déposées de Hewlett-Packard Company. NCR est une marque déposée de NCR Corporation. Diebold est une marque déposée de Diebold Corporation. Tous les autres logos et noms de produit sont des marques ou des marques déposées de leurs propriétaires respectifs. Thales fonde sa stratégie sur le développement continu. Les détails concernant les équipements peuvent donc varier par rapport aux descriptions et spécifications contenues dans cette publication.



Certificate no. EMS 73838



Certificate no. FS69836