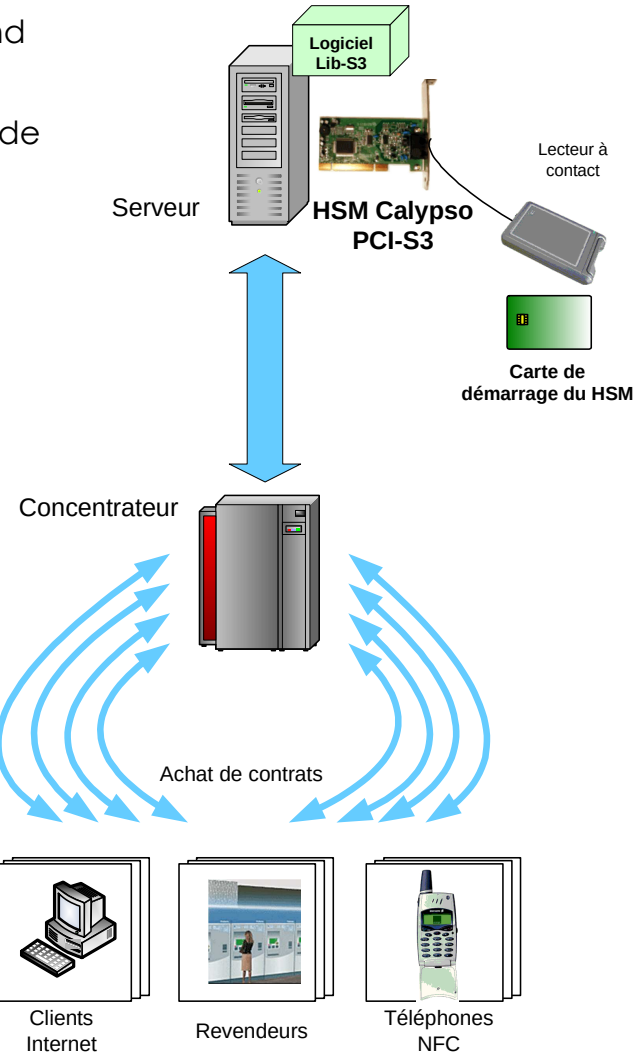
HSM CALYPSO PCI-S3

Gestion centralisée des transactions CALYPSO

Le ***HSM Calypso PCI-S3*** gère la sécurité d'un grand nombre de transactions Calypso simultanées.

Un PCI-S3 remplace avantageusement une baie de SAM utilisés pour les opérations de vente et de personnalisation à distance.



TRANSACTIONS CALYPSO A DISTANCE : GESTION DE LA SECURITE

La billettique sans contact permet au possesseur d'un objet portable (carte sans contact, téléphone NFC, etc.) d'entrer et de voyager dans un réseau de transport.

Pour cela, les titres de transports sont chargés auparavant dans les objets portables par les automates de vente, ou à un guichet.

Ce chargement est protégé par un module de sécurité (SAM-CL) normalement présent dans chaque terminal émettant des contrats de transport. Ce SAM contient les clés cryptographiques nécessaires aux opérations de vente.

Le SAM est peu coûteux, mais il est relativement lent et ne gère qu'une transaction à la fois.

Un serveur de vente à distance peut avoir à traiter de nombreuses demandes simultanément (par exemple pendant les débuts et fins de périodes d'abonnement).

La gestion centralisée de ces ventes nécessiterait alors la disponibilité d'un grand nombre de SAM connectés au serveur, ce qui serait peu pratique à gérer.

De plus la durée de vie d'un SAM est limitée à moins de 17 millions d'opérations.

Le HSM Calypso PCI-S3 est un module sécurisé, remplaçant avantageusement 100 à 5000 SAM (selon la configuration).

Principales fonctions

- Compatible avec le SAM-S1.
- Jusqu'à 5.000 transactions simultanées : vente, personnalisation ou chargement de clés.
- Gestion sécurisée des clés cryptographiques.
- Compteurs internes non falsifiables de traçabilité des opérations.
- Gestion de la cryptographie Calypso.
- Gestion de la sécurité de fonctions propres aux produits CD21, Tango, CD97.

Spirtech

CARACTERISTIQUES TECHNIQUES

La session sécurisée Calypso

L'authentification et la modification des données d'un objet portable Calypso est normalement réalisée par une session qui comprend :

1) L'ouverture de session, qui transmet un aléa généré par le SAM vers l'objet portable.
2) Les lectures et écritures vers l'objet portable.
3) La fermeture de session, qui transmet un certificat émis par le SAM vers l'objet portable afin d'authentifier le terminal et les données écrites.
4) L'envoi d'un certificat par l'objet portable vers le terminal afin d'authentifier les données lues et de prouver que les écritures ont bien été réalisées.

La gestion centralisée des sessions Calypso

Pendant toute une session entre une carte et un SAM Calypso (SAM-S1), le SAM reste dédié à cette session.

La gestion centralisée de multiples sessions Calypso (par exemple de ventes par Internet ou de rechargements sur des mobiles NFC Calypso) nécessiterait donc autant de SAM-S1 que de transactions simultanées.

Les sessions distantes pouvant durer plus de 10 secondes (en fonction des temps d'acheminement réseau), le nombre de SAM à gérer devient prohibitif dès la montée en puissance du système.

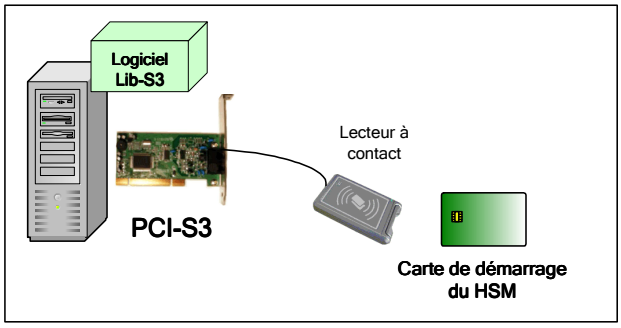
Un HSM Calypso PCI-S3, remplace cette batterie de SAM et permet de réaliser de nombreuses transactions Calypso simultanées, simplifiant ainsi la gestion de la sécurité Calypso sur le système central.

Une version plus légère (SAM-S20), destinée aux expérimentations, pilotes et petits systèmes, offre les mêmes fonctions pour un nombre réduits de transactions simultanées (20).

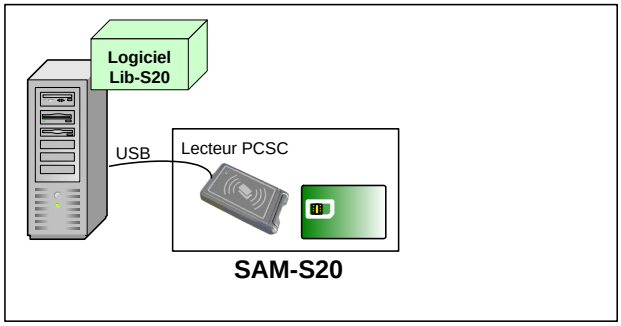
Les deux configurations comprennent une librairie logicielle compatible (Windows ou Linux) assurant les fonctions suivantes :

- Ouverture d'un canal (équivalent à une réservation de SAM-S1).
- Envoi de commandes au format APDU SAM-S1.
- Fermeture de session (libération du SAM-S1 réservé).
- Gestion de plusieurs groupes de clés indépendants.
- Gestion des clés (transfert, suppression, invalidation).
- Mise en service sécurisée par carte à puce (déportable dans un coffre fort).

Configuration PCI-S3



Configuration SAM-S20



Gamme de produits

Les fonctions du HSM Calypso sont disponibles sous deux configurations :
- PCI-S3 : carte PCI pour PC
- SAM-S20 : carte à puce ISO 7816 à insérer dans un lecteur PCSC.

CONFIGURATION PCI-S3

- PCI-S3 : carte HSM, évaluée FIPS 140-2 Level 3, au format PCI (ou PCI Express) pour installation dans un compatible PC.
- S3-Lib : Logiciel fournissant les fonctions d'accès au PCI-S3 (Linux, Windows).
- Un PCI-S3 remplace de 100 à 5000 SAM-S1, selon la configuration choisie (à évaluer en fonction de la charge prévue et des délais réseaux) :
  - PCI-S3/100
  - PCI-S3/500
  - PCI-S3/1000
  - PCI-S3/5000

CONFIGURATION SAM-S20

Plus simple à installer et moins couteuse qu'une configuration PCI-S3, la configuration SAM-S20 est logiciellement compatible et permet de gérer jusqu'à 20 transactions simultanées.
Attention : la durée de vie du SAM-S20 nécessite le changement physique du SAM après 16 millions d'opérations.

- SAM-S20 : carte à puce ISO7816 (découpe ID000), basée sur un composant évalué EAL 5+, gérant jusqu'à 20 transactions simultanées, connectée par un lecteur PCSC au PC.
- S20-Lib : Logiciel fournissant les fonctions d'accès au SAM-S20 (Linux, Windows), présentant une interface compatible avec la configuration PCI-S3.
- Chaque SAM-S20 remplace jusqu'à 20 SAM-S1.

Informations pratiques

Disponible.
Prix : nous consulter.

Droits d'utilisation

Le HSM Calypso est commercialisé sous licence Calypso.
Vous êtes ainsi libre d'utiliser tout terminal pour effectuer vos transactions, y compris des terminaux non licenciés.

Spirtech
1, Rue Danton - 75006 Paris - FRANCE
tel : +33 1 40 46 36 20
email : mail@spirtech.com
web : www.spirtech.com