Spirtech

SECURE & SMART

La sécurité dans les systèmes cartes à puce sans-contact

Février 2011

Le dossier

Ce qu'il faut retenir:

Indépendance : le prestataire en charge de la définition de l'architecture doit être indépendant des industriels, et notamment des encarteurs et intégrateurs. L'Autorité Organisatrice (AO) conserve ainsi la maîtrise de sa sécurité billettique.

SAM maître (SAM-SP) : l'AO doit exiger la création d'un SAM -SP demeurant en sa possession. Elle pourra ainsi être indépendante de son fournisseur de SAM.

En savoir plus:

La multiplication des canaux de vente (internet, terminaux portables, mobile NFC, etc.) peut nécessiter l'utilisation d'un module de sécurité centralisé HSM (non représenté ci -contre).

spirtech.fr

Les spécifications Calypso, incluant la sécurité et les SAM, sont disponibles sur le site de support technique Calypso :

CalypsoTechnology.net

L'architecture de sécurité Calypso

Calypso est le standard de la dématérialisation billettique : transports publics, multiservices, applications de vie quotidienne. Dans ces secteurs, la sécurité du système est primordiale.

L'***architecture de sécurité*** définit les moyens d'authentification et de sécurisation des objets portables Calypso (cartes, mobiles NFC, etc.) et de leur contenu. Elle repose sur des *clés secrètes*, propres à chaque application ou bassin d'interopérabilité. Ces clés interdisent l'utilisation de supports non conformes.

Pour rester secrètes, ces clés sont conservées et utilisées à l'intérieur des *modules de sécurité* (SAM). Configurés pour chaque type d'équipement, les SAM sécurisent les transactions et l'authentification des objets portables.

Les clés sont créées lors de la ***cérémonie de création des clés***, et inscrites dans un SAM maître, le **SAM-SP**, utilisé pour fabriquer les autres SAM du système de manière sécurisée.

Lors de la ***pré-personnalisation***, les clés sont chargées dans les objets portables sans-contact à l'aide du **SAM-CPP**.

Durant la ***personnalisation***, le **SAM-CP** sécurise l'écriture des données du réseau et du porteur dans les supports.

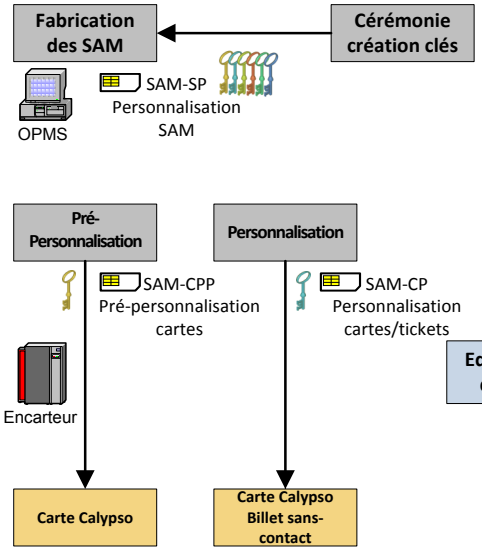
Un ***équipement de vente*** (distributeurs automatiques, guichets, etc.) utilise un **SAM-CL**. Sans ses clés sécrètes, il est impossible d'émettre un contrat.

Un ***équipement de validation*** délivre le service (entrée du voyageur, délivrance d'un bien, etc.). Il possède un **SAM-CV** qui autorise le contrôle, le débit et la validation de titres.

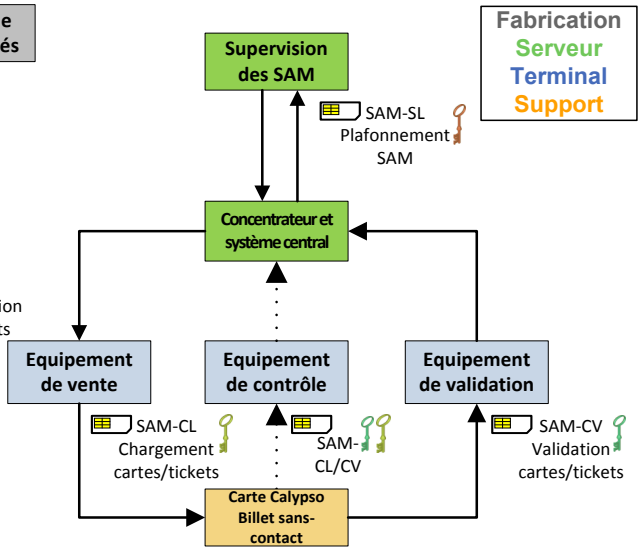
Un ***équipement de contrôle*** utilise également un **SAM-CV** pour garantir à l'exploitant l'authenticité des droits et fournir une preuve de contrôle.

Enfin, dans le système central, le ***superviseur de SAM*** et son **SAM-SL** autorisent les SAM-CL à continuer les ventes. Ainsi, un SAM-CL volé sera bloqué et pourra n'émettre qu'un nombre limité de titres.

Toutes ces transactions sont critiques puisque soumises à des enjeux sécuritaires et de performance forts. L'architecture Calypso garantit l'intégrité du système et améliore l'expérience client. L'indépendance du fournisseur de cette architecture garantit l'autonomie des gestionnaires et responsables.



Initialisation: de la cérémonie des clés à la création d'une carte Calypso.



Exploitation: de la vente à la validation, un système billettique sécurisé

Glossaire

Calypso : standard international de billettique interopérable et multi fournisseurs, créé et géré par ses utilisateurs (Calypso Networks Association).

Cérémonie de création des clés : moment de création des clés qui sécurisent l'ensemble de la chaîne billettique. Les clés sont inscrites dans le SAM-SP.

Clés : éléments secrets protégés dans les SAM et les cartes. Elles garantissent l'authenticité des SAM, des objets portables et de leur contenu. Elles peuvent autoriser à modifier ces contenus.

OPMS : Outil de Personnalisation des Modules de Sécurité.

SAM (Secure Application Module) : puce électronique présente dans les équipements billettiques (personnalisation, vente, validation, contrôle...) et renfermant de façon protégée les clés secrètes.

SAM-CV : SAM de validation, de débit et de contrôle. Utilisé par les équipements de validation et de contrôle.

SAM-CL : SAM de chargement de contrats (droits). Utilisé par les équipements de vente.

SAM-CP : SAM de personnalisation. Utilisé par les équipements de production des objets portables pour charger les données d'environnement et éventuellement un premier contrat.

SAM-CPP : SAM de pré-personnalisation. Utilisé par l'encarteur lors de la production pour charger les clés dans les objets portables .

SAM-SP : SAM de personnalisation des SAM. Utilisé par l'OPMS lors de la fabrication des autres SAM.

En savoir plus

Spirtech Conseil accompagne les acteurs de la télébillettique dans la réussite de leurs projets.

Spirtech Conseil réalise des missions d'Assistance à Maîtrise d'Œuvre et d'expertise pour les Autorités Organisatrices. Elle conseille les industriels dans la conception et la réalisation de leurs solutions Calypso. Elle réalise les tests d'interopérabilité des supports et équipements billettiques.

spirtechconseil.fr

Spirtech Conseil : projet télébillettique LMCU et interopérabilité billettique

Dans le cadre du débat sur la mobilité organisé en 2008 et 2009, *Lille Métropole Communauté Urbaine* (LMCU) a lancé de grands travaux de rénovation de son système de transport. Avec pour objectif de rendre l'ensemble des réseaux de la périphérie urbaine de Lille interopérables, LMCU s'est fixée un programme ambitieux.

Quel que soit le mode de transport public choisi (métro, vélo, bus, train) et peu importe le transporteur, l'usager doit pouvoir utiliser son titre de transport *Transpole*. Le système doit donc être *interopérable* et *multimodal*. Le choix du standard *Calypso s'imposait donc*, gage de sécurité et de performance, pour l'amélioration du service aux usagers.

La *sécurité* est un enjeu prioritaire dans la réalisation des ambitions de LMCU. La réduction de la fraude et la fiabilité des statistiques remontées vers le système central jouent ainsi un rôle important dans la mise en œuvre du nouveau système.

L'interopérabilité régionale étant indispensable, la sécurité doit être conforme aux standards définis par la Région Nord-Pas-de-Calais. L'intégrité du système doit être garantie auprès de chacun des partenaires.

Le souhait de permettre à terme une *interopérabilité transfrontalière* avec la Belgique (qui utilise le standard Calypso pour son interopérabilité nationale), est une autre ambition forte du projet.

Les cartes Transpole pourront aussi fédérer, dans le futur, des *services de vie quotidienne* (bibliothèques, piscines, aide à la personne, etc.), facilitant l'accès des usagers aux services publics.

Spirtech Conseil assiste LMCU dans la réussite de ce projet. Expertise technique et sécuritaire, gestion du multi-applicatif, vente à distance, multi-modalité, sont les sujets autour desquels nous collaborons pour réaliser le meilleur compromis entre performance et sécurité.

En savoir plus

Site technique de Calypso donnant accès aux spécifications liées à ce standard :

CalypsoTechnology.net

Versions stables des principaux produits Spirtech

Produit	Version	Spécification
SAM-S1 Type D	v1.11	000522-SE-SDI-SAMS1D v2.4
SAM-S1 Type E	v0024	041115SDI-SE-SAMS1E v1.3
SAM-S20	v0104	081110FGR-SE-SAM-S20 v1.1
Librairies HSM/SAM S20	v5.1	090225-MU-LibCsm v1.8

Les spécifications des SAM sont confidentielles, elles peuvent cependant être obtenues sous NDA sur : www.CalypsotecTnology.net.

Evènements

UITP Mobility & City
Au Qatar du 11 au 14 avril 2011, rencontres internationales de la mobilité avec la participation de Calypso Networks Association.

www.uitp.org

NFC World Congress
19-21 septembre 2011, les acteurs de la sphère NFC se rencontrent à Sophia-Antipolis (France).

www.nfcworldcongress.com

6èmes Assises des TECT
L'ADCET vous accueille à Lyon (France) les 6 et 7 octobre 2011 pour des assises consacrées à la télébillettique et la dématérialisation.

www.adcet.com

Liens utiles

www.spirtech.com

www.calypsonet-asso.org

www.CalypsoTechnology.net

www.lillemetropole.fr

www.adcet.com

Nous contacter et vous abonner

Spirtech
1, rue Danton
75006 PARIS - France

www.spirtech.com

Spirtech

Le spécialiste de la carte à puce et de la télébillettique.

Secure & Smart - Février 2011
Lettre éditée par Spirtech - 1, rue Danton - 75006 Paris - France.

Créée en 2000, la société Spirtech est un bureau d'étude indépendant, spécialisé dans les domaines de la carte à puce, de la cryptographie et de la technologie sans-contact, en particulier appliqués au monde du transport public.