Spirtech

SECURE & SMART

La sécurité dans les systèmes cartes à puce sans-contact

Avril 2012

Le dossier

Ce qu'il faut retenir

Multiplication des canaux de distribution : avec le déploiement des mobiles NFC et l'achat de titres de transport par Internet, les transporteurs facilitent l'accès à leurs services et améliorent le service rendu à leur clients.

Sécurité : l'utilisation de l'application Calypso pour Java Card garantit un niveau de sécurité élevé, basé sur la session Calypso et sur des standards cryptographiques solides.

Démarche partenariale : les objets portables Java Card permettent à plusieurs prestataires de services de partager un même support. Ainsi, des applications de transport, de contrôle d'accès ou de paiement peuvent être installées sur une même carte. Pour utiliser la carte sim du téléphone mobile, un accord avec l'opérateur du téléphone doit être conclu.

En savoir plus

Pour en savoir plus sur le standard Calypso :

calypsonet-asso.org

Les spécifications Calypso sont disponibles sur le site de support technique Calypso :

CalypsoStandard.net

Des compléments d'information sur l'utilisation de Calypso et de Java Card sont accessibles sur :

spirtech.fr

Calypso pour téléphones mobiles et cartes Java

Un ***téléphone NFC***, une ***carte Java*** ou une ***clé USB NFC*** permettent à plusieurs prestataires de services de partager un même support.

En effet, l'environnement standard appelé ***Java Card**** permet à une application (transport, paiement, services universitaires, etc.) d'être installée dynamiquement, y compris après l'émission de l'objet, sans compromettre la sécurité des autres applications déjà présentes.

L'application d'un partenaire (***fichier CAP****) est chargée dans un ***domaine de sécurité*** étanche. Ce domaine protège l'accès aux données du prestataire en exigeant l'utilisation de ses clés cryptographiques secrètes. Les clés assurent l'***authenticité***, l'***intégrité*** et la ***confidentialité*** de ses données.

GlobalPlatform* est la spécification qui standardise et sécurise la gestion du cycle de vie de l'objet portable dans un environnement comportant de multiple prestataires et différents types d'acteurs : émetteurs de supports, fournisseurs d'applications, gestionnaires (tiers de confiance). GlobalPlatform spécifie comment charger, installer, personnaliser et, éventuellement supprimer une application dans le support Java Card. Ces opérations peuvent se faire à distance, à travers Internet ou une liaison GSM (dans ce dernier cas, on parle de liaison « OTA »: *Over The Air*).

Depuis un ***système central****, administré, soit par l'émetteur du support, soit par un tiers de confiance, un logiciel GlobalPlatform gère le *chargement d'une application*, la *création d'une* ***instance****, sa *personnalisation* et, si nécessaire, sa suppression.

Calypso Networks Association (CNA) a défini les règles permettant de charger et d'activer une application Calypso en toute sécurité, conformément à GlobalPlatform et Calypso Révision 3.

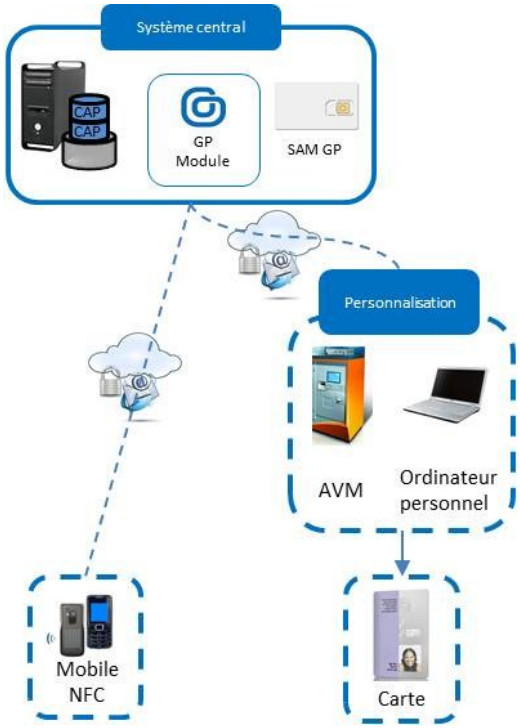
Une fois certifié par CNA, le logiciel Calypso peut être remis sous forme de fichier CAP à un tiers de confiance ou à l'émetteur du support. Le ***chargement sécurisé*** dans un objet portable est réalisé en local ou à distance, avec les clés GlobalPlatform nécessaires.

Le logiciel Calypso est ensuite ***instancié et activé*** : une application Calypso est créée avec ses clés, ses fichiers et ses données spécifiques (par exemple pour un carnet de tickets pour un réseau de transport spécifique). Il est possible de créer plusieurs applications indépendantes dans un objet portable à partir d'un même logiciel Calypso.

L'instanciation et l'activation sont sécurisées par un ***module d'activation Calypso****.

Le module d'activation, intégré au système central, sécurise le chargement des clés Calypso de personnalisation, de vente, et de validation.

Spirtech peut fournir l'application Calypso pour Java Card, le ***Module GP**** et le ***SAM GP**** associé, ainsi que des outils de test.



Fichier CAP : contient un logiciel Java Card correspondant à une application spécifique. Par exemple l'application Calypso.

GlobalPlatform : spécifications interopérables d'administration des cartes Java et Multos. Basées sur le système OpenPlatform élaboré par la société Visa, elles sont maintenant gérées par l'association GlobalPlatform.

Instance : données relatives à une application spécifique dans une carte. Plusieurs instances peuvent utiliser le même fichier CAP (par exemple plusieurs applications Calypso).

Java Card : langage et système d'exploitation permettant la réalisation de logiciels embarqués sur des cartes à puce. Un logiciel Java Card (« applet ») peut théoriquement fonctionner dans toute carte Java.

Module d'activation Calypso : module de sécurité nécessaire pour activer un applet Calypso.

Module GP : librairie logicielle permettant au système central de gérer la sécurité et la cryptographie des domaines de sécurité, des applications et des instances.

SAM GP : module de sécurité contenant les clés GlobalPlatform de gestion des objets portables Java. Le SAM sécurise les opérations GlobalPlatform.

Système central de gestion des supports : système de gestion centralisée des objets portables. Il permet, à distance ou localement, de charger des logiciels, de créer des instances, et de modifier ou supprimer ces logiciels et leurs instances présents dans le support.

En savoir plus

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

Spirtech réalise des missions d'Assistance à Maîtrise d'Œuvre et d'expertise pour les Autorités Organisatrices de Transport. 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.

spirtech.com

Spirtech Conseil : RUNN, Java Card et GlobalPlatform

Le projet ***RUNN***, Réseau Universitaire Numérique Normand, rassemble les établissements d'enseignement supérieur des deux régions normandes, les CROUS et les Conseils Généraux.

Piloté par l'***ENSICAEN*** et initié par Marc Pasquet, ce projet prévoit un ***espace numérique de travail*** qui donnera aux étudiants un ***accès centralisé aux services des universités***, des ***points d'accès numériques*** ainsi qu'une ***carte multiservice***.

La carte multiservice de l'Université Numérique en région est une initiative ambitieuse qui devrait permettre le déploiement de 65 000 cartes sans contact auprès des étudiants et du personnel universitaire normand.

La carte multiservice est une carte Java fonctionnant selon les standards ***Java Card*** et ***GlobalPlatform***. Ces standards permettent le déploiement sécurisé d'applications de prestataires différents sur le même support, tels que: transport, contrôle d'accès, porte-monnaie électronique, bibliothèques, etc.

Avec la société Monecarte, Spirtech participe aux travaux de réalisation du système de gestion centralisé RUNN.

Grâce à sa connaissance technique approfondie des spécifications Java Card et GlobalPlatform, Spirtech accompagne l'ENSICAEN dans l'intégration de ces technologies à leur système.

Spirtech a également réalisé un ***module logiciel GlobalPlatform*** (appelé *Module GP*) permettant d'administrer facilement les cartes Java afin d'y ajouter des logiciels et applications, de les mettre à jour, et éventuellement de les supprimer. Ce module est intégré au système central fournit par Monecarte.

Spirtech fournit également le ***logiciel Java Card Calypso***, permettant d'utiliser la carte universitaire comme carte de transport Calypso.

Ce logiciel met en œuvre la chaîne de sécurité Calypso dans les objets portables sans contact, notamment dans les cartes SIM des téléphones NFC, les clés USB et les cartes Java.

Cette application, compatible avec les SAM et HSM Calypso, possède donc un haut niveau de performance et de sécurité.

En savoir plus...

Vous pouvez accéder gratuitement aux spécifications liées au standard Calypso sur le site technique :

CalypsoStandard.net

Versions actuelles des principaux produits Spirtech

Produit	Version	Spécification
SAM-S1 Type D	v1.11	000522-SE-SDI-SAMS1D v2.4
SAM-S1 Type E	v0025	041115SDI-SE-SAMS1E v1.5
SAM-C1	v0003	101010-SAM Calypso v1.1
Librairies HSM/SAM S20	v63	090225-MU-LibCsm v1.9
Librairies CAS/DAM	v79	110620CHY-MU-LibCas v1.2

Les spécifications des SAM sont confidentielles ; elles peuvent être obtenues sous NDA sur: www.CalypsoStandard.net.

Evènements

CNA - Visite technique
3 mai 2012, visite du LRT de Jérusalem (Israel) pour découvrir comment Calypso répond aux besoins d'interopérabilité des réseaux israéliens.

www.calypsonet-asso.org

NFC World Congress
19-21 septembre 2012, Nice (France) salon dédié au NFC et à ses évolutions, permettant de rencontrer les acteurs de la chaîne de valeur du NFC.

www.nfcworldcongress.com

Cartes & Identification
6-8 novembre 2012, Paris Villepinte (France) accueille le plus grand salon dédié à la sécurité numérique et aux technologies intelligentes.

www.cartes.com

Nous contacter et vous abonner

Spirtech
1, rue Danton
75006 PARIS - France

spirtech.com

Liens utiles

www.spirtech.fr

www.calypsonet-asso.org

www.calypsotechnology.net

www.unr-runn.fr

www.adcet.com

Spirtech

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

Secure & Smart - Avril 2012
Lettre d'information éditée par Spirtech - 1, rue Danton - 75006 Paris - France.

Créée en 2000, la société Spirtech est un bureau d'études indépendant, expert 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.