Calypso Networks Association

Etat de l'art et perspectives

Paris, 14 mars 2017

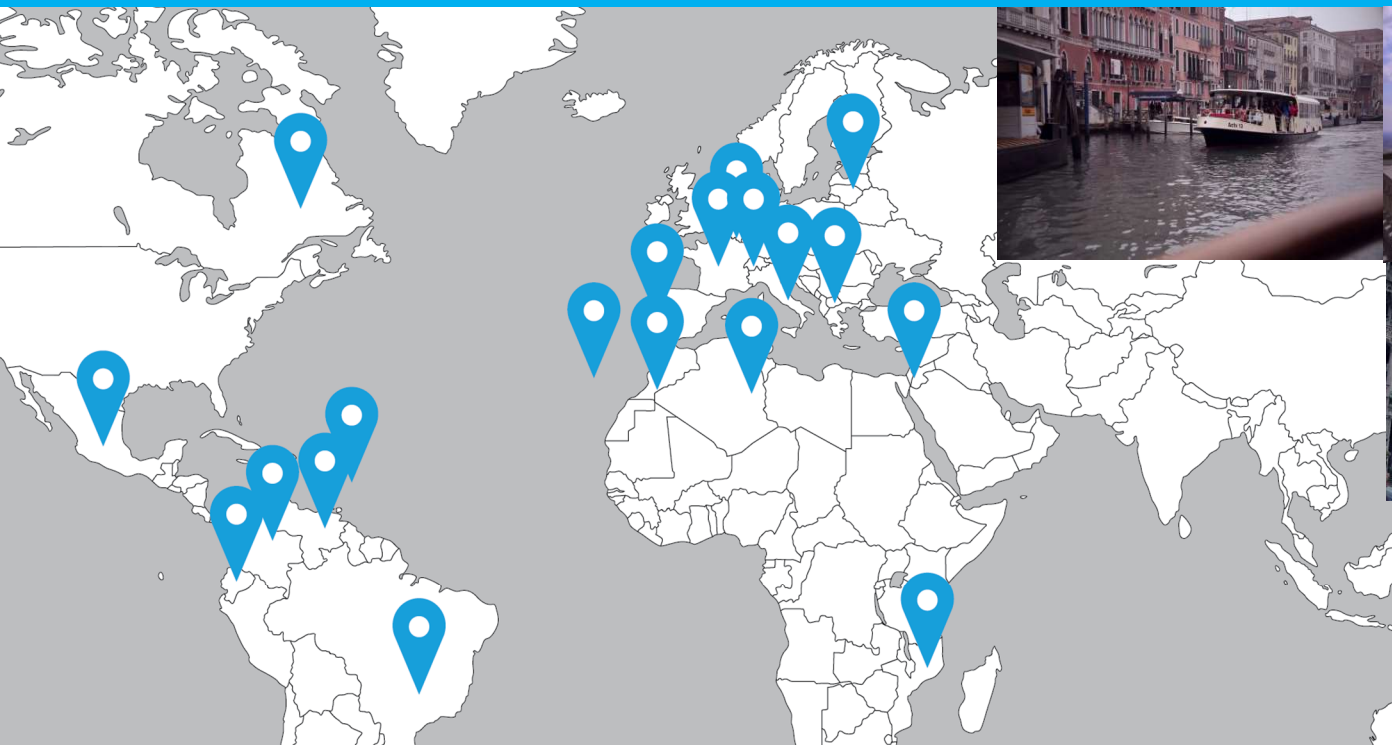
SOMMAIRE

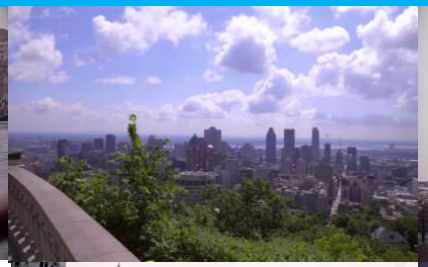
1. Calypso Aujourd'hui
   - Spécifications
   - Triangle 2
   - Applet CNA
   - Certification
2. 2017 : le début d'une nouvelle ère
   - Une diversification des supports sur le Mobile NFC (Ese, HCE)
   - Elargissement de la gamme de produit (CLAP)
   - Fourniture d'un SDK en Open Source
   - Calypso et le Back-office centrique

Calypso Aujourd'hui

Une présence sur tous les continents

125 villes & regions
25 pays





Les spécifications CALYPSO aujourd'hui

Spécifications objet portable:

Dernière version en vigueur, spécifications 3.2 (31/12/2013) :

- Ajout de l'AES comme algorithme cryptographique (avec mode de compatibilité 3.1)
- Possibilité de restreindre la lecture des données par session sécurisée.

Où en est-on sur Triangle 2 ?

Documentation

Dernière version des spécifications Triangle 2 le 28/06/2016,version 2.7:

- Uniquement modifications éditoriales
- Pas de modifications de l'application depuis la version 2.6 publiée le 01/09/2015 (qui intègre la photo)

Dernière version des « Triangle2 Best Practice » 24 juin 2016

- Aide à l'implémentation dans les terminaux

Communication

- Nouveau logo
- Fourniture d'un Kit de communication aux AOTs

Gouvernance

Un collège des utilisateurs Triangle 2 a été mis en place:

- Election d'un comité de direction: CTS (président membre de droit du Board CNA), AFIMB, TEC
- L'utilisation de T2 est gratuite mais liée à la signature d'une charte et réservée aux membres CNA

triangle®

Calypso Networks Association

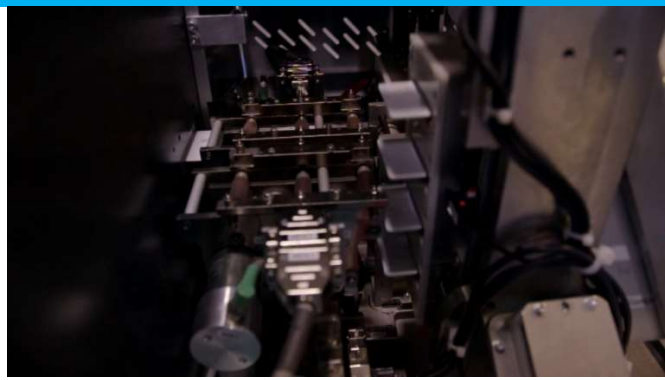
Où en est-on sur L'Applet Calypso ?

CNA offre gratuitement à ses membres via un contrat de licence une Applet JavaCard permettant d'instancier toute application Calypso Révision 3.1 dans un élément sécurisé type Carte SIM, Ese, Carte JAVA.

- Dernière version : 1.2 publiée le 07/07/2015, Certifiée AFSCM
- Prochaine version à venir: mi-2017, travail en concertation avec les opérateurs et l'AFSCM. Prévue pour être pré-chargée dans les dernières versions de cartes SIM (V3) par les Opérateurs mobiles

Calypso Networks Association

Une certification de bout-en-bout



Une politique de certification de bout-en-bout:

- Certification couche RF selon la norme CEN 16794 (ISO 14443 appliquée au transport), conjointement réalisée par CNA et Paycert:
  - Certification cartes disponible depuis juillet 2016
  - Certification terminaux disponible depuis février 2017.
- Certification de conformité aux spécification 3.1 Calypso pour les objets portables
- Audit terminal
- Audit Triangle 2

Calypso Networks Association

2017: Le début d'une nouvelle ère pour Calypso

Afin de pérenniser le standard Calypso sur la durée, les membres de CNA ont décidé d'un plan de transformation de 3 ans pour donner une nouvelle impulsion à la technologie Calypso afin qu'elle puisse s'adapter aux nouveaux enjeux de la billettique:

Pour cela les membres de CNA ont décidé de donner de nouveaux moyens à l'association:

- Une nouvelle gouvernance
- La Constitution d'une équipe permanente à temps plein

Au service d'un programme ambitieux de développement

Diversification des supports sur le mobile NFC
HCE

CNA a publié l'été dernier la version 1.2 de la spécification « Calypso HCE Application » :

- A ce stade, elle est strictement expérimentale et limitée à des pilotes
- Elle doit être complétée par des exigences sécuritaires au niveau du système central
- Ces exigences sont actuellement en cours d'étude et seront publiées mi-2017 dans un nouveau document : « HCE Calypso Guidelines ».
- Ces « HCE Calypso Guidelines » incluront les recommandations issues d'une étude commandée par l'AFIMB, menée par un expert indépendant et pilotée conjointement avec CNA, sur la sécurité de HCE Calypso.

Le déploiement opérationnel et commercial d'un système HCE Calypso devra donc respecter la spécification ainsi que les exigences minimales de sécurité qui seront décrites dans les « HCE Calypso Guidelines ».

Diversification des supports sur le mobile NFC

L'Embedded Secure Element

Des discussions sont actuellement en cours entre CNA et les principaux fabricants de mobiles pour pouvoir intégrer l'Applet CNA dans les « embedded secure element » présents dans les terminaux mobiles.

Calypso Networks Association

Diversification de la gamme de produit

A l'instar d'autres technologies, CNA souhaite pouvoir proposer aux utilisateurs du standard Calypso une gamme d'objet portables « milieu de gamme » ,compatibles avec les systèmes existants à un coût nettement inférieur aux cartes actuelles

CNA a envoyé un RFI (Request For information) aux industriels du marché (principalement encarteurs et fabricants de puces) pour définir les conditions de cette faisabilité en faisant coïncider les contraintes industrielles et les besoins des réseaux de transport avec Les prérequis suivants:

- Carte à microprocesseur sans contact uniquement avec capacité cryptographique
- Protocole de communication ISO14 443 type B ou type A
- 2 kB mémoire de données maximum
- Utilisant des commandes compatibles avec Calypso rev 3.1

Calypso Light Application (CLAP)

Suite aux réponses au RFI, CNA a travaillé sur les spécifications fonctionnelles de ce nouveau produit et a proposé une version DRAFT à ses membres dans un nouveau groupe de travail (WP 12) . Cette nouvelle application a été appelée **CLAP (Calypso Light APplication)**

Ces spécifications sont en cours de finalisation mais en voici quelques principales caractéristiques:

- Jeu de commandes réduit compatible Calypso 3.1
- Sécurité identique aux autres produits Calypso, mais avec 3DES obligatoire
- 2 structures de fichiers possibles (1 proche de T2, l'autre des applications existantes) avec 2 contrats maximum

Les spécifications devraient être publiées en mai 2017, accompagnées de recommandations non fonctionnelles (niveau de sécurité hardware, certification RF, facteur de forme) qui pourront être intégrées dans des appels d'offre pour les réseaux intéressés par ce nouveau produit.

Calypso, vers un modèle Open Source

Au départ une conviction des membres de CNA: La nécessité de confirmer et amplifier le modèle Calypso basé sur l'ouverture et l'interopérabilité:

- Suivre l'exemple de l'Information Voyageur avec l'OPEN DATA
- S'inspirer du modèle Open Source pour faciliter l'implémentation de Calypso et permettre son appropriation par de nouveaux acteurs industriels

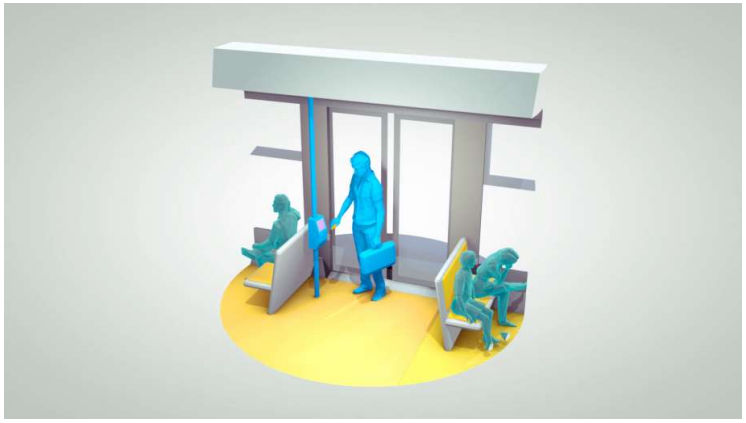
Dans cet esprit CNA offre déjà des outils en accès libre et gratuit à ses membres tels que l'Applet CNA, et Triangle 2.

Afin d'aller plus loin, CNA va offrir un SDK (Kit de développement logiciel) en Open Source (i.e mise à disposition libre et gratuite du logiciel et de son code source, avec la possibilité d'accès payant à des prestations de support et d'assistance) qui permettra l'implémentation de Calypso dans différents types de systèmes billettiques (carte centrique mais également système centrique) ainsi que dans des environnements autres que le transport (ex AMG).
Le modèle Open Source permettra de plus à la communauté de développeurs Calypso d'enrichir ce SDK.

Le SDK Calypso

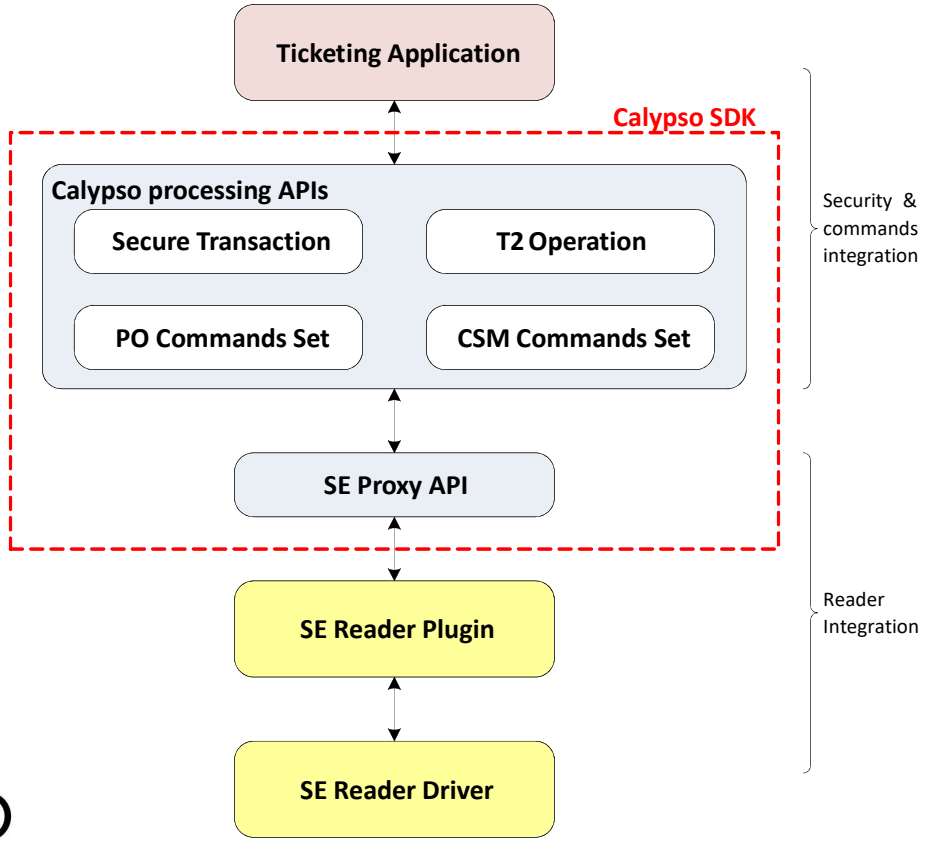
Une librairie pour faciliter l'implémentation de Calypso dans les équipements

- Une bibliothèque open source disponible en Java & C ++:
- Compatible avec n'importe quelle architecture de terminal:
  - mobile / embarqué / serveur
- Interopérable avec n'importe quelle solution de lecteur sans contact:
  - standard / propriétaire
  - local / distant
- Gestion des fonctions de sécurité avancées de Calypso
- Possibilité d'ajouter des extensions pour gérer également des solutions de cartes non-Calypso.



Calypso Networks Association

Le SDK Calypso
Architecture logicielle



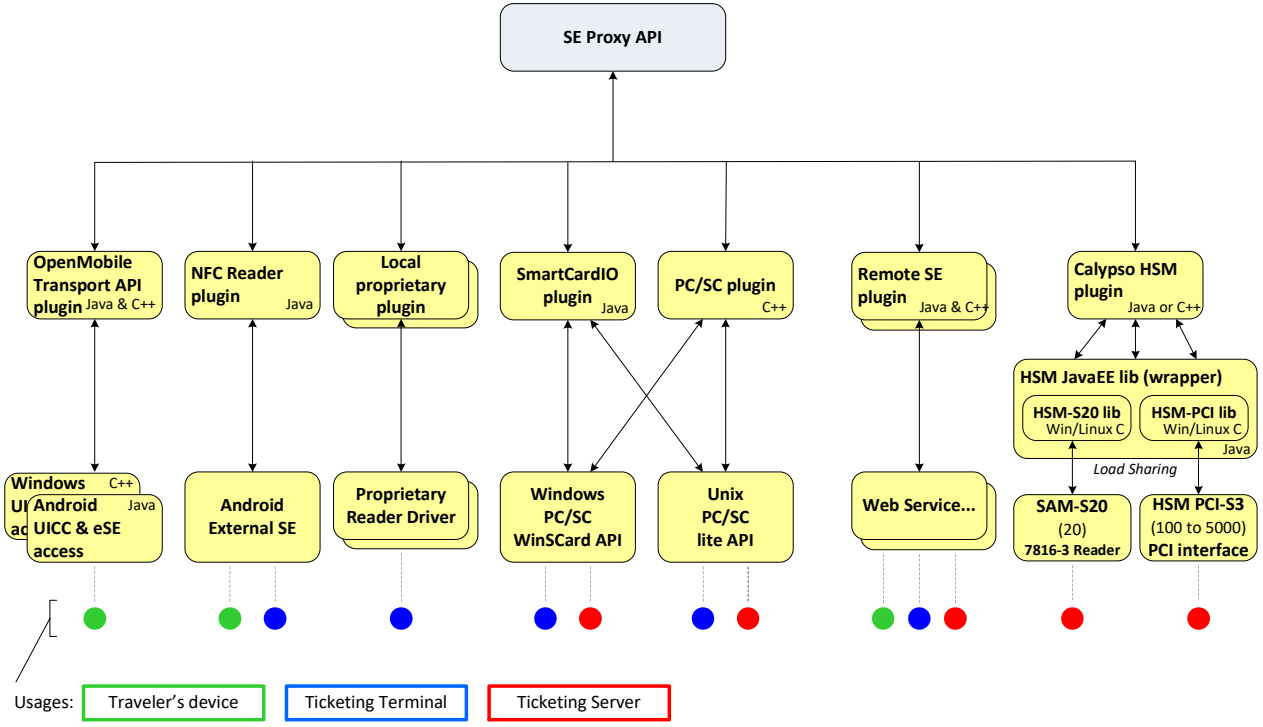
Le SDK proposera 2 API:

- Une API haut niveau (**Calypso processing API**)qui permettra aux applications métier billettiques de faire appel aux commandes et à la sécurité Calypso
- Une API de bas niveau (**SE proxy API**) qui pourra gérer différents types de lecteurs via des plugins adaptés

Calypso Networks Association

Le SDK Calypso

Intégration hardware



- Optimisation des communications avec le SE en groupant les commandes pour s'adapter à des architectures locales ou distantes
- Possibilité d'adaptation aussi bien avec des lecteurs standards ou propriétaires
  - Fourniture avec le SDK de Plugins pouvant gérer des lecteurs sans contact intégrant des API standard (Android NFC Reader, Android SmartCard interface, Windows/Linux PC/SC, Java SmartCard IO PC/SC interface)
  - Possibilité d'intégrer au SDK des plugins fournis par des industriels pour s'intégrer avec leurs API propriétaires

Calypso Networks Association

Calypso et le Système centrique

Le Système centrique ou Account Based Ticketing (ABT) est un concept qui émerge de plus en plus, et Calypso y travaille sur plusieurs aspects:

- Au niveau cas d'usages:
  - Publication d'un livre blanc sur le sujet en avril 2017,
  - Mise en place dans la foulée d'un groupe de travail CNA pour travailler sur les scénarii d'utilisation de Calypso dans le cadre d'un système ABT

- Au niveau de ses spécifications
  - La future version 3.3 devrait inclure un mécanisme de cryptographie asymétrique qui permettra l'authentification forte des objets portables sans SAM.

Calypso

Networks Association

Questions ?