Calypso
Networks Association

GUIDE D'ACCOMPAGNEMENT

à la rédaction d'un appel d'offres de cartes, de billettique mobile NFC et de terminaux basés sur le standard Calypso

- Novembre 2022 -

Ou comment garantir l'ouverture complète
de votre système billettique lors d'un appel d'offres

TABLE DES MATIÈRES

CONTEXTE

Pour les autorités organisatrices et les opérateurs de transport, les systèmes billettiques sont un sujet hautement stratégique car ils traduisent la politique de mobilité au sein de leur territoire et permettent d'en assurer les revenus. Ces systèmes sont conçus pour durer dans le temps et s'adapter aux évolutions, notamment tarifaires, aux extensions de réseau, ainsi qu'à la mise en place de schémas d'interopérabilité.

Pour assurer la pérennité d'un système billettique, il est nécessaire de pouvoir y intégrer, au cours de son cycle de vie, des équipements, des cartes, des logiciels provenant de constructeurs différents. En effet, le fournisseur d'origine du système n'a pas nécessairement la capacité ni la volonté d'assurer les évolutions souhaitées à un prix raisonnable. Pouvoir disposer de plusieurs fournisseurs évite aux réseaux une situation de monopole, synonyme de coûts excessifs, voire d'incapacité à réaliser une évolution par perte de compétence.

Pour assurer la compatibilité et l'inter-opérabilité technique entre différents fournisseurs, il est fondamental de passer d'une logique de produit (figés et généralement propriétaires par essence) à une logique de respect des normes et standards, à condition qu'ils soient ouverts et multisources. Le donneur d'ordre doit alors avoir des exigences de conformité à ces normes et standards, dont la preuve doit être apportée par le fournisseur grâce à la certification de ses produits.

Le standard Calypso est ouvert car il répond à tous les critères fixés par les instances internationales pour bénéficier de cette dénomination : « un standard est dit ouvert quand il e**st mis à la disposition de tous, développé, maintenu et géré dans un processus collaboratif et consensuel. Un standard ouvert facilite l'interopérabilité et l'échange de données entre différents produits ou services et est destiné à être largement adopté** »[1].

Calypso a été créé, est développé, maintenu et géré par des autorités et des opérateurs de transport regroupés dans ce but au sein de l'association Calypso Networks Association (CNA). L'objectif de CNA, association à but non lucratif, est de garantir à tous les utilisateurs de ce standard l'évolutivité, l'interopérabilité et l'indépendance vis-à-vis des fournisseurs.

Calypso est ainsi le seul standard de billettique multisource à tous les niveaux, y compris à celui des composants électroniques des cartes. C'est un facteur majeur de résilience en période de pénurie de composants. Il met à disposition du monde industriel des spécifications de référence et un processus de certification pour attester de la conformité des produits. C'est le standard adopté par la très grande majorité des réseaux français, mais également utilisé par de nombreux réseaux dans le monde. Ainsi de nombreux fournisseurs d'origines différentes proposent des produits Calypso dans un schéma multisource qui porte ses fruits depuis de nombreuses années. Cette véritable concurrence permet de garantir à l'acheteur de se voir proposer des produits Calypso au juste prix.

[1] *Suivant la définition de standard ouvert donnée par l'Union Internationale des Télécommunications*

L'enjeu des appels d'offres billettique, au-delà de la fonction d'achat de matériel, doit être de garantir la compatibilité entre les supports (cartes sans contact, smartphones NFC ...) et les terminaux billettiques (valideurs, appareils de vente et de contrôle, bornes ...) déjà déployés et nouvellement acquis. Sans ce prérequis, il est impossible de déployer des schémas d'interopérabilité.

Le document « **La billettique au service du MaaS : les bonnes pratiques pour un système efficace** » présente l'ensemble des bonnes pratiques à respecter pour spécifier un système billettique. Il y est rappelé en particulier que le modèle de données ne doit pas être intégré dans un appel d'offre de système billettique ou de terminaux mais qu'il doit être géré indépendamment, sous la maîtrise du donneur d'ordre qui s'assure d'en avoir la propriété.

2 OBJET DU DOCUMENT

L'objectif de ce document est de rappeler les exigences à inscrire dans un **appel d'offres de cartes sans contact, de billettique mobile NFC, de terminaux afin de garantir compatibilité et évolutivité.**

Un appel d'offres public doit permettre une concurrence ouverte et équitable à tous les industriels. Ce document a été rédigé en respectant les principes du code des marchés publics français et peut donc être réutilisé dans le contexte d'un appel d'offres.

Ce document rédigé par CNA est libre de droits. Il peut être répliqué intégralement ou partiellement.

CNA propose un support pour la rédaction de vos appels d'offre, en particulier une aide à la définition de la configuration et de la personnalisation de vos cartes Calypso.

Un service de vérification de la configuration et de la personnalisation des cartes Calypso livrés par les industriels est également proposé.

Pour en savoir plus :
contact@calypsonet.org

3 PRINCIPES GÉNÉRAUX

Les principes généraux ci-dessous sont détaillés dans les chapitres dédiés respectivement aux cartes, aux smartphones NFC, aux terminaux :

- Faire référence systématiquement à toutes les normes et tous les standards applicables au domaine,
- Exiger des produits certifiés, preuve de leur conformité aux standards, ou, en absence de certification existante, ayant fait l'objet d'une déclaration de conformité aux standards applicables au domaine,
- Se référer aux référentiels partagés et bonnes pratiques existants (par exemple Intercode, Interbob…),
- De préférence, demander d'intégrer l'application Calypso Hoplink dans les cartes Calypso Prime et dans les modules de sécurité. Ceci n'induit pas de coût supplémentaire et permet une ouverture ultérieure à l'interopérabilité,
- Ne pas faire référence à un nom de produit commercial spécifique à un industriel donné,
- Ne pas faire référence à des technologies, spécifications ou solutions rendues obsolètes, notamment par l'émergence de référentiels partagés.

4 EXIGENCES SPÉCIFIQUES **AUX CARTES SANS CONTACT**

Un système Calypso correctement implémenté permet d'accepter toutes les cartes sans contact certifiées Calypso.

Calypso Networks Association a défini une gamme comprenant trois produits :
Calypso® PRIME, Calypso® LIGHT, Calypso® basic

Tous ces produits sont dotés des mêmes mécanismes de sécurité et peuvent être gérés par un même logiciel dans les terminaux, ce qui garantit leur compatibilité et facilite leur intégration.

- Calypso® PRIME regroupe sur une même carte les fonctionnalités de transports et multi-applications/multiservices.
  Calypso Prime permet de gérer plusieurs contrats billettiques et l'interopérabilité entre les réseaux, y compris à l'échelle internationale. Calypso Prime permet également l'authentification de la carte sans module de sécurité (SAM) dans sa version PKI.

- Calypso® LIGHT est une version allégée qui convient plutôt aux utilisateurs occasionnels, de même niveau de sécurité que Calypso Prime et peut être émise sur support plastique ISO ou support papier. Deux contrats de transport d'un même opérateur peuvent coexister sur une carte. C'est un produit également particulièrement adapté aux architectures ABT (Account Based Ticketing, ou dîtes système centrique).

- Calypso® basic disponible fin 2022, est un titre de transport mono-contrat rechargeable sur support papier sans contact, adapté au voyage unitaire.

Dans le contexte d'un appel d'offres, un donneur d'ordre doit exiger que les cartes soient certifiées à la fois au niveau radiofréquence (matériel/hardware) et au niveau fonctionnel Calypso (logiciel/software), comme décrit dans les deux sous-chapitres suivants. Acheter des cartes non certifiées fait courir un risque grave d'incompatibilité carte/terminal.

4.1. EXIGENCES ET CERTIFICATIONS RADIOFRÉQUENCES (RF)

La première exigence est la conformité **radiofréquence (RF) de la carte sans contac**t à la dernière version de la **norme ISO/IEC TS 24192** (anciennement nommée **CEN/TS 16794**), qui est l'application au domaine du transport de la norme **ISO/IEC 14443**.

La conformité à cette norme garantit une interopérabilité de la carte avec les smartphones NFC conformes aux exigences du NFC Forum, notamment lorsque ceux-ci sont utilisés pour recharger un titre sur cette carte sans contact.

Un programme de certification radiofréquence des cartes développé par la Smart Ticketing Alliance (https://www.smart-ticketing.org/) est en place depuis plusieurs années. La conformité à la norme ISO TS 24192 doit être démontrée par l'obtention d'un certificat auprès d'un organisme de certification approuvé par la Smart Ticketing Alliance.

Cette démarche de certification s'effectue auprès de Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), un organisme de certification indépendant, seul habilité à ce jour à délivrer une certification RF selon le programme de la Smart Ticketing Alliance.

La liste à jour des cartes certifiées ISO/IEC TS 24192 (CEN/TS 16794) par PayCert est publique et se trouve sur le site de PayCert : https://www.cna-paycert-certification.eu/rf-interface/picc/.

IMPORTANT : La certification RF d'une carte porte sur le produit fini, comprenant : le composant avec son logiciel, l'inlay avec antenne et le corps de carte, assemblés.

Il est fortement déconseillé de commander des cartes utilisant le protocole B' (aussi appelé Innovatron). En effet, celui-ci est obsolète car il n'existe aucun produit certifié conforme à ce protocole. Pour rappel, le protocole B' ne permet pas d'intégrer Hoplink. Il ne permet pas non plus le traitement des smartphones NFC (SE et HCE) ni la mise en oeuvre de l'interopérabilité. Si le réseau fonctionne uniquement en B', il est recommandé de commander des cartes bi-mode (B' et ISO 14443) afin de faciliter la migration le moment venu.

Voir la section 6.1.3: Gestion de l'obsolescence pour plus de détails sur les conséquences du maintien du protocole B'.

4.2. EXIGENCES ET CERTIFICATION FONCTIONNELLES CALYPSO

CNA a défini, d'une part, les spécifications de référence auxquelles toute carte Calypso (Prime, Light, Basic) doit être conforme et, d'autre part, un schéma de certification pour garantir cette conformité. Cette certification est gérée par l'organisme de certification PayCert, seul habilité à délivrer les certificats. Il existe une certification dédiée pour chacune des trois cartes (Prime, Light, Basic).
Il est à noter que Calypso Prime peut être configuré selon trois versions. L'appel d'offres doit préciser quelle configuration est demandée :

- Mode normal, « Regular mode », (anciennement rev 3.1) ; ce mode inclut les fonctions de base de Calypso Prime avec cryptographies TDES et DESX.
- Mode étendu, « Extended mode » (anciennement rev 3.2), avec cryptographie AES et cryptage optionnel des données en complément des fonctions du mode normal.
- Mode PKI (anciennement rev3.3), qui ajoute au mode étendu la cryptographie asymétrique PKI, permettant l'authentification de la carte sans module de sécurité (sans SAM) dans le terminal.

Dans un **appel d'offres** :

- Pour des cartes Calypso Prime, il est recommandé d'exiger *a minima* la conformité des cartes à la certification Calypso Prime en mode étendu. Si vous avez besoin d'une authentification de la carte sans module de sécurité, il convient de demander la conformité au mode PKI.
- Pour les cartes Calypso Light, la conformité des cartes à la certification Calypso Light doit être exigée.
- Pour les cartes Calypso Basic, la conformité des cartes à la certification Calypso Basic doit être exigée.

La liste des cartes Calypso certifiées se trouve à l'adresse : https://www.cna-paycert-certification.eu/card/

4.3. CONFIGURATION DES CARTES

Pour toutes les cartes **Calypso (Prime, Light et Basic)**, la configuration demandée doit respecter les règles suivantes :

- Utiliser un identifiant de l'application (appelé également « AID » ou « conteneur ») **normalisé** par l'ISO et référencé par l'AFNOR, propre à l'opérateur du système billettique. Il ne faut pas utiliser les identifiants génériques comme « 1TIC. ICA » pour lesquels l'unicité n'est pas garantie et qui sont incompatible avec les solutions de billettique sur smartphone NFC.

- Utiliser l'identifiant fourni par l'AFNOR tel quel, sans y ajouter de 00 supplémentaires.

Pour les cartes **Calypso Prime**, la configuration doit, en plus, respecter les règles et recommandations suivantes :

- Toujours configurer les applications en mode Regular, Extended ou PKI, selon le besoin (et non plus en émulation de Calypso Révision 2.4 ou inférieur).

- Intégrer l'application Hoplink (recommandé car sans surcoût, et qui permettra la mise en place ultérieure d'un schéma d'interopérabilité).

- De préférence, utiliser les structures de fichier les plus récentes (exemple : Intercode 2.2) et éviter autant que possible les structures de fichier anciennes.
  Une liste de structure de fichier référencée par CNA est disponible dans le document « Calypso File Structure Registry » (ref. 060709-CalypsoFiles).

- Utiliser des jeux de clés dédiés pour chacune des applications avec des cryptographies récentes : **TDES, AES ou PKI** et éviter d'utiliser des cryptographies obsolètes, telles que DES.

- S'il existe un besoin de compatibilité avec un réseau ancien (Calypso révision 2.4), il convient de demander une carte Prime certifiée émulant la révision 2.4.

Pour les cartes **Calypso Light**, la configuration doit, en plus, respecter les règles suivantes :

- Choisir l'une des deux structures de fichier autorisées (Reference ou Classic), en fonction des structures déjà existantes et de vos besoins futurs.
- Utiliser, de préférence, un jeu de clés dédiés pour ce produit. Les cartes Light utilisent uniquement la cryptographie TDES.

Pour les cartes **Calypso Basic**, la configuration doit, **en plus** :

- Utiliser un jeu de clés dédié pour ce produit. Les cartes Basic utilisent uniquement la cryptographie TDES.

Attention : Ne pas confondre la ***structure de fichiers*** d'une carte Calypso et la ***structure des contrats*** définie par Intercode, aussi appelée « instanciation ». Ces deux structures ne recouvrent pas la même notion. La structure de fichier définit l'organisation des fichiers dans la carte. La structure des contrats, « instanciation », sert au codage des titres de transport.
Pour chaque structure de contrat, Intercode précise quelle structure de fichier Calypso est adaptée.

CNA propose un support pour la rédaction de vos appels d'offre, en particulier une aide à la définition de la configuration et de la personnalisation de vos cartes Calypso.

Un service de vérification de la configuration et de la personnalisation des cartes Calypso livrés par les industriels est également proposé.

Pour en savoir plus, contactez-nous : contact@calypsonet.org

4.4. TEXTE POUR APPEL D'OFFRES

Voir fiche pratique n°1

5 EXIGENCES SPÉCIFIQUES À LA BILLETTIQUE MOBILE NFC

5.1. LES SOLUTIONS : SE ET HCE

On appelle **billettique mobile NFC** la technologie qui permet d'utiliser un smartphone NFC pour effectuer des opérations d'achat et/ou de validation de titres de transport. Nous nous intéressons dans ce document à la billettique mobile NFC qui permet à un smartphone NFC d'émuler une carte sans contact.
La billettique mobile NFC se décline en plusieurs modes selon que la sécurité s'appuie sur un élément de sécurité matériel dans le smartphone NFC ou non :

- La billettique mobile NFC **SE** (SE pour Secure Element) utilise un composant microprocesseur identique à celui qu'on trouve dans une carte, et dispose donc du même niveau de sécurité : Critères Communs EAL4+ à minimum pour le SE. Des SE sont présents dans les modèles récents des smartphones NFC de plusieurs fabricants, en particulier ceux des marques Samsung et Apple.

  Une applet Calypso générique (application logicielle) est fournie par CNA pour être chargée dans le SE du smartphone NFC et ainsi émuler pleinement une carte Calypso Prime.

  Cette solution a l'avantage de ne pas nécessiter d'évolution des terminaux billettiques en place, simplement quelques paramétrages, à condition que le système soit conforme à minimum avec la révision 3 de Calypso Prime.

- La billettique mobile NFC **HCE** ne repose pas sur l'utilisation d'un élément sécurisé stocké dans le smartphone NFC, mais sur une sécurité logicielle. Elle est compatible avec tous les smartphones NFC Android. Pour compenser la moindre sécurité, due à la non-utilisation d'un SE pour protéger les données sensibles, un mécanisme (dit de tokenisation) met à jour régulièrement les clés secrètes de l'application Calypso HCE stockée dans le smartphone NFC, limitant ainsi les risques de fraude.

  Comme pour la solution SE, le système doit être conforme à minimum avec la révision 3 de Calypso Prime. Elle nécessite une légère évolution logicielle des terminaux billettiques de validation afin de mettre en place des mesures de sécurité spécifiques à la solution HCE.

5.2. LES EXIGENCES RELATIVES À LA SOLUTION SECURE ELEMENT (SE)

La solution sur SE peut être approvisionnée directement auprès d'un fournisseur dédié ou indirectement via votre intégrateur billettique. Dans les deux cas, le donneur d'ordre doit demander que le fournisseur garantisse :

- Que sa solution billettique mobile NFC est apte à fonctionner avec tout smartphone NFC ayant fait l'objet d'une certification RF, soit sur la base de la certification NFC Forum, soit sur la base de la certification ISO/IEC TS 24192 dernière édition (ou de sa version CEN/TS 16794),

- Que l'applet est chargé uniquement dans des Secure Element (SE) qui ont fait l'objet d'une certification fonctionnelle de conformité à Calypso du couple « Applet/SE ». PayCert, organisme indépendant accrédité, gère cette certification, et la liste des produits certifiés est disponible à l'adresse https://www.cna-paycert-certification.eu/card/applet/. Si un couple « Applet/SE » n'est pas d'ores et déjà certifié, il appartient au fournisseur de demander cette certification.

La conformité aux exigences terminaux, décrites plus loin dans ce document, garantit le respect des exigences spécifiques aux solutions mobiles NFC.

Les solutions sur mobiles NFC, qu'elles soient sur base d'applet dans un SE ou HCE sont commercialisées par des fournisseurs dédiés en charge de l'installation et de l'initialisation de l'application Calypso dans le smartphone NFC.

5.3. LES EXIGENCES RELATIVES À LA SOLUTION HCE CALYPSO

La solution sur HCE peut-être approvisionnée directement auprès d'un fournisseur dédié ou indirectement via votre intégrateur billettique. Dans les deux cas, le donneur d'ordre doit s'assurer que les exigences suivantes sont prises en compte :

- Le fournisseur garantit que sa solution billettique mobile NFC est apte à fonctionner avec tout smartphone NFC ayant fait l'objet d'une certification RF, soit sur la base de la certification NFC Forum, soit sur la base de la certification ISO/IEC TS 24192 dernière édition (ou de sa version CEN/TS 16794).

- La **certification fonctionnelle de conformité aux spécifications HCE Calypso** devra être exigée dès qu'elle sera disponible (fin 2022).

- La **certification de sécurité HCE Calypso**, basée sur un référentiel à l'état de l'art, qui concerne la résistance au hacking des données stockées dans le smartphone. CNA assure la délivrance de ce certificat avec l'assistance de la société Internet of Trust dans un rôle d'organisme indépendant de certification. La liste des fournisseurs ayant satisfait à cette certification est disponible sur le site calypsonet.org. Il est fortement recommandé d'exiger cette certification, même si elle n'est pas rendue, à ce jour, obligatoire par CNA.

- Le respect des spécifications et guidelines HCE établis par CNA quant aux exigences applicables à l'infrastructure du système billettique.

La solution HCE Calypso, purement logicielle, ne peut pas s'appuyer sur la classification de sécurité d'un composant électronique dans le smartphone NFC. Pour assurer un niveau de sécurité conforme aux exigences du standard Calypso, CNA a donc mis en place un ensemble de mesures de sécurité spécifiques à la solution HCE, **que l'on retrouve dans les spécifications et guidelines.**

Tous les fournisseurs HCE Calypso se sont engagés contractuellement, en tant que licencié, au respect de ces spécifications et guidelines. Une certification dédiée est donc inutile.

5.4. TEXTE POUR APPEL D'OFFRES

Voir fiche pratique n°2

6 EXIGENCES SPÉCIFIQUES **AUX TERMINAUX ET AUX LOGICIELS BILLETTIQUES**

On entend par **terminal**, un équipement de vente, de validation, de contrôle ou de personnalisation.
On entend par **logiciel billettique,** un logiciel permettant de faire une transaction billettique. Dans l'environnement Calypso, cela comprend le logiciel du lecteur, la librairie Calypso et l'application billettique, qu'ils soient dans le terminal ou déportés dans un serveur central.

RAPPEL: pour garantir l'interopérabilité entre plusieurs équipements, en particulier cartes et lecteur, il est crucial que chacun soit certifié aussi bien au niveau radiofréquence que fonctionnel.

6.1. EXIGENCES ET CERTIFICATION RADIOFRÉQUENCE (RF)

La première exigence est la conformité **radiofréquence (RF) du terminal sans contact** à la dernière version de la **norme ISO/IEC TS 24192** (anciennement nommée **CEN/TS 16794**), qui est l'application au domaine du transport de la norme **ISO/IEC 14443**.

La conformité à cette norme garantit une interopérabilité du terminal avec les smartphones NFC conformes aux exigences du NFC Forum, notamment lorsque ceux-ci sont utilisés pour émuler une carte de transport sans contact.

Un programme de certification radiofréquence des terminaux développé par la Smart Ticketing Alliance (https://www.smart-ticketing.org/) est en place depuis plusieurs années. La conformité à la norme ISO TS 24192 doit être démontrée par l'obtention d'un certificat auprès d'un organisme de certification approuvé par la Smart Ticketing Alliance.

Cette démarche de certification s'effectue auprès de Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), un organisme de certification indépendant, seul habilité à ce jour à délivrer une certification RF selon le programme de la Smart Ticketing Alliance.

La liste à jour des terminaux certifiés ISO/IEC TS 24192 (CEN/TS 16794) est publique et se trouve sur le site de PayCert : https://www.cna-paycert-certification.eu/rf-interface/pcd/.

IMPORTANT: La certification RF d'un terminal porte :
- Soit sur le produit fini qui comprend le matériel électronique dans son packaging définitif, avec le logiciel,
- Soit sur un sous ensemble du produit fini, dans la mesure où ce sous-ensemble a été intégré dans le produit fini selon les préconisations du constructeur qui garantissent aucune perte.

6.1.1. COMPATIBILITÉ AVEC LES CARTES ET APPLICATIONS DE PAIEMENT SANS CONTACT EMV

Si la mise en place d'un service **Open Payment** est envisagée à court, moyen ou long terme, il convient de demander en complément de la certification RF que les terminaux soit certifié EMVCo niveau 1. **Cette démarche de certification s'effectue auprès d'EMVCo.**

La liste à jour des terminaux certifiés EMVCo L1 est publique et se trouve sur le site d'EMVCo aux pages : https://www.emvco.com/approved-registered/approved-products/

6.1.2. COMPATIBILITÉ AVEC LES PRODUITS NFC APPLE

Si la mise en place d'une **billettique mobile NFC sur iPhone ou Apple Watch** est envisagée à court, moyen ou long terme, il convient de demander en complément de la certification RF que les terminaux gèrent le protocole spécifique à Apple (dénommé ECP) afin de support le mode Express d'Apple (https://support.apple.com/en-us/HT212171). **Cette démarche de certification s'effectue auprès d'Apple Inc.**

Il n'existe pas à ce jour de liste publique des terminaux supportant le mode Express d'Apple.

6.1.3. GESTION DE L'OBSOLESCENCE

Les premières cartes Calypso émises dans les années 2000 utilisaient le protocole Innovatron (appelé aussi « B' » ou « B prime »). Le standard Calypso s'appuie aujourd'hui exclusivement sur la norme ISO/IES 14443 (type A ou B). D'anciennes cartes utilisant le protocole B' sont toujours sur le terrain car les terminaux ne sont parfois pas mis à jour pour l'utilisation des protocoles ISO/IES 14443 type A ou B.

Seuls quelques rares modèles de terminaux intègrent encore le protocole B' en complément du protocole standard, ce qui conduit à un coût nettement supérieur de ces équipements par rapport à des terminaux standards. Il faut donc s'interroger sur la pertinence de maintenir le protocole B' plutôt que de remplacer les cartes B' encore en circulation.
A l'inverse, la grande diversité de terminaux conformes à la norme ISO/IEC TS 24192 (anciennement nommé CEN/TS 16794) garantit un prix optimum pour ces équipements.

Enfin, le protocole B' ne permet pas d'intégrer Hoplink, de traiter des smartphones NFC (SE et HCE), ni de gérer le MaaS.

S'il est vraiment impératif de continuer à gérer les cartes B' existantes, alors dans ce cas seulement, il doit être spécifié un terminal supportant le protocole standard et le protocole B'.

6.2. EXIGENCES SUR LE LOGICIEL DES TERMINAUX

6.2.1. STRUCTURATION EN TROIS COUCHES LOGICIELLES

CNA a défini une structuration des équipements en trois couches logicielles pour assurer l'évolutivité, la modularité et la capacité du terminal à traiter toutes les cartes Calypso certifiées. Ces trois couches sont décrites sur le site https://calypsonet.org/calypso-pour-terminaux/?lang=fr. A chaque couche logicielle correspond un document d'exigences, rédigé par CNA.

6.2.2. READER LAYER (LOGICIEL LECTEUR)

La couche logicielle en charge des échanges entre la carte et le lecteur, dénommée « Reader Layer » permet de gérer tous les types de cartes et de SAM, quelle que soit leur technologie : Calypso, CIPURSE, MIFARE, etc. Cette couche logicielle ne contient aucun élément spécifique à Calypso. La couche logicielle applicative y accède via des APIs (Application Programmable Interface) de référence (Reader API & Card API) définies par CNA.

A ce jour, le donneur d'ordre doit demander au soumissionnaire de présenter la lettre d'enregistrement du lecteur délivrée par CNA, qui atteste, sur base déclarative[3], de la conformité aux exigences décrites dans le document « Reader Layer Requirements », établi par CNA. Fin 2022, une certification « Reader Layer » se substituera au déclaratif.

6.2.3. CALYPSO LAYER (LIBRAIRIE FONCTIONNELLE CALYPSO)

La couche logicielle « Calypso Layer » permet de gérer spécifiquement les cartes et SAM propres à Calypso dans le strict respect des spécifications fonctionnelles de ce standard. Cette couche correspond à la librairie Calypso, la couche logicielle applicative y accède via une API (Application Programmable Interface) de référence (Calypso API) définie par CNA.

A ce jour, le donneur d'ordre doit demander au soumissionnaire de présenter la lettre d'enregistrement de la librairie Calypso délivrée par CNA, qui atteste, sur base déclarative[3], de la conformité aux exigences décrites dans le document « Calypso Layer Requirements ». Fin 2022, une certification « Calypso Layer » se substituera au déclaratif.

Le déclaratif est un simple document d'engagement de l'industriel à respecter les exigences (reader ou Calypso layer). La certification, vérifie à la fois le respect des exigences et la conformité aux APIs de référence définies par CNA ; il y a donc garantie d'interopérabilité.

[3] Il est important de rappeler qu'il s'agit d'une déclaration sur l'honneur faite par les industriels et non le résultat de tests réalisés par un laboratoire indépendant. Lorsque la certification correspondante existera (fin 2022), il conviendra de l'exiger.

6.2.4. TICKETING LAYER (APPLICATION BILLETTIQUE)

La couche billettique « Ticketing Layer » correspond à l'application billettique (règles tarifaires et commerciales, gestion de l'accès, de la signalétique, etc.) présente dans le terminal - ou déportée dans un serveur central (systèmes ABT).

CNA a publié un document nommé **« Ticketing Layer Requirements »**.

C'est à la fois un document d'exigences et de recommandations pour l'utilisation des APIs de référence définis par CNA. Il contient également des bonnes pratiques à suivre dans la réalisation et la gestion d'un système billettique Calypso.

Le document « Ticketing Layer Requirement » ne fera pas l'objet de certification car les applications billettiques sont spécifiques à chaque réseau. Il convient à chacun de demander son respect et son utilisation.

6.2.5. LOGICIEL OUVERT : ECLIPSE KEYPLE

CNA recommande d'inscrire dans les appels d'offres le recours au logiciel open source Eclipse Keyple. Eclipse Keyple est libre de droits (Eclipse Public License 2.0 (ou EPL-2.0))
S'appuyer sur un logiciel open source contribue à la pérennité de la solution, en garantissant la possibilité de faire évoluer le système par n'importe quel autre industriel, au meilleur coût.
L'utilisation de Keyple garantit la capacité du terminal à traiter toutes les cartes Calypso certifiées, même les plus récentes.

Keyple implémentent les API de référence définis par CNA pour les terminaux Calypso et les développements sont réalisés dans le respect des exigences « Reader Layer » et « Calypso Layer ».

Keyple est composé de deux logiciels situés à deux niveaux de la transaction :

- **Keyple Core** correspondant à la couche « Reader layer ». L'intégration avec le matériel hardware (lecteur) se fait via un plugin.
- **Keyple Calypso** correspondant à la couche « Calypso layer ».

En cas d'utilisation de Keyple Calypso, le soumissionnaire pourra fournir directement la lettre d'enregistrement de la librairie Keyple Calypso.

En cas d'utilisation du Keyple Core, le soumissionnaire doit présenter la lettre d'enregistrement du lecteur, qui atteste, sur base déclarative, de la conformité aux exigences décrites dans le document « Reader Layer Requirements ».

Cette lettre d'enregistrement garantit la conformité de l'ensemble «hardware du terminal/ Keyple Plugin/Keyple Core».

Lorsqu'elle sera disponible, la certification se substituera à la lettre d'enregistrement.

L'utilisation d'Eclipse Keyple, en tant que logiciel open source, garantit une totale indépendance entre le matériel et le logiciel du terminal :

• Il est ainsi possible de remplacer un matériel par un autre en gardant les mêmes logiciels (Keyple Core, Keyple Calypso et logiciel applicatif) et en utilisant (ou en développant) le Keyple Plugin *ad hoc* pour le nouveau matériel.

• Il est possible d'intervenir sur le logiciel d'un terminal donné, sans aucune implication sur le matériel, ce qui évite toute propriétarisation de la solution globale matériel/logiciel.

6.3. CERTIFICATION ET DÉCLARATION DE CONFORMITÉ

Le tableau suivant indique les certifications et/ou déclaratifs à exiger en fonction du type de matériel tant que la certification n'est pas disponible.

Type de matériel/logiciel	Certification à exiger	Lettre d'enregistrement à exiger		Lettre d'engagement à exiger
	ISO/IEC TS 24192	Reader layer	Calypso layer	Ticketing layer
Matériel sans librairie Calypso	√	√		
Matériel avec librairie Calypso	√	√	√	
Matériel intégrant l'application billettique du réseau	√	√	√	√
Librairie Calypso seul			√	
Application billettique seule				√

La liste des terminaux et logiciels ayant fait l'objet d'une déclaration de conformité est disponible à l'adresse : https://calypsonet.org/calypso-certification/?lang=fr.

Un équipement est conforme si, et seulement si, **chaque couche est conforme**.

6.4. EXIGENCES SUR LES TERMINAUX CONCERNANT LES MODULES DE SÉCURITÉ

En fonction du terminal, il peut être nécessaire de prévoir des emplacements pour l'intégration de modules de sécurité (SAM).
Le nombre d'emplacements dépend du contexte, du type de terminal et du type de carte Calypso qui seront utilisés.

Pour tous les terminaux, il est recommandé de prévoir a minima deux emplacements, et de préférence quatre, pour de possibles évolutions du système.
Le format courant du module de sécurité (SAM) est le format SIM (ID-1/1FF) dont le format mini SIM (2FF) est détachable. Pour des besoins spécifiques, il est possible d'obtenir les formats micro SIM (3FF), nano SIM (4FF).

6.5. TEXTE POUR APPEL D'OFFRES

Voir fiche pratique n°3

FICHE PRATIQUE N°1

SPÉCIFIER DES CARTES CALYPSO DANS UN APPEL D'OFFRES

On ne mentionne ici que les éléments de texte à insérer dans un appel d'offres, concernant la conformité des cartes Calypso, avec des commentaires explicatifs (en italique). Toutes les autres caractéristiques, physiques, ergonomiques, contraintes spécifiques, exigences complémentaires doivent être ajoutées pour que le soumissionnaire puisse y répondre.

Concernant les cartes Calypso, la conformité à tous les standards de référence ISO 14443, ISO 7816, ISO 24192 (ou CEN 16794) est assurée en faisant simplement référence à l'obligation de certification RF de la carte, qui est un premier prérequis à l'interopérabilité, en demandant au soumissionnaire de remettre le certificat de la carte proposée :

« La carte doit être certifiée ISO/IEC TS 24192 dernière édition (ou par défaut CEN/ TS 16794). Le soumissionnaire remettra le certificat de la carte qu'il propose. Pour rappel, le certificat fourni porte sur le produit fini tel qu'il sera livré, comprenant le composant avec son logiciel, l'inlay avec antenne et le corps de carte, assemblés. Il ne peut en aucun cas s'agir d'un certificat délivré pour un produit différent, dans le cas où l'un de ces éléments a été modifié postérieurement à la certification. Il ne peut pas non plus s'agir d'un certificat délivré par le fournisseur du composant sur la base d'un encartage différent. »

La conformité aux spécifications fonctionnelles Calypso, qui est le deuxième prérequis à l'interopérabilité, est assurée en faisant référence à l'obligation de certification fonctionnelle Calypso, en demandant au soumissionnaire de remettre le certificat de la carte proposée :

« La carte doit avoir fait l'objet de la certification fonctionnelle Calypso. Le soumissionnaire remettra le certificat de la carte qu'il propose. »

- *S'il s'agit d'une Calypso Prime, il faudra préciser le mode demandé : Extended (rev 3.2) ou PKI s'il est fait le choix d'une carte Calypso Prime implémentant une cryptographie asymétrique.*

- *S'il s'agit d'une Calypso Light ou Calypso Basic, il n'y a pas besoin de précision complémentaire.*

En ce qui concerne les aspects de configuration et de personnalisation, les éléments (décrits au paragraphe 4.3) sont à reprendre dans le texte d'appel d'offres.
Pour chaque application contenue dans la carte Calypso Prime (application locale du réseau, Hoplink, AMC…) :

« Les cartes fournies doivent respecter pour l'application ***(mentionner le nom de l'application)*** :

- Utiliser l'identifiant de l'application du réseau (appelé également AID ou conteneur) normalisé par l'ISO et référencé par l'AFNOR : ***(mentionner l'identifiant choisi fourni par l'AFNOR tel quel, sans y ajouter de 00 supplémentaires)***,

- Être configurées en mode Regular / Extended / PKI ***(suivant le besoin, mettre la mention choisie entre ces trois modes, ou mentionner*** « émulation de la révision 2.4 de Calypso » ***uniquement s'il existe un besoin de compatibilité avec un réseau ancien)***,

- Utiliser un jeu de clés TDES / AES dédiés, le jeu de clés sera fourni a posteriori ***(choisir l'une des deux cryptographies en fonction des jeux de clés déjà existantes dans le réseau et des besoins futurs et ne plus utiliser de jeux de clés DES ou DESX)***,

- Utiliser la structure de fichier Intercode 2.2 : structure 11h / 12h / 13h. ***(choisir l'une des 3 structures en fonction du besoin et d'autres structures de fichiers peuvent être demandées pour des raisons de compatibilité avec la structure déjà utilisée sur le réseau)***. »

CNA propose un support pour la rédaction de vos appels d'offre, en particulier une aide à la définition de la configuration et de la personnalisation de vos cartes Calypso.

Un service de vérification de la configuration et de la personnalisation des cartes Calypso livrés par les industriels est également proposé.

Pour en savoir plus, contactez-nous : contact@calypsonet.org

- Novembre 2022 -

« Les cartes fournies doivent respecter pour l'application Hoplink les conditions suivantes ***(si le donneur d'ordre en fait le choix, car sans surcoût)*** :

- Utiliser l'identifiant Hoplink,
- Être configurées en mode Regular,
- Utiliser le jeu de clés TDES Hoplink,
- Utiliser la structure de fichier Hoplink : structure 0Ch,
- Initialiser le fichier environnement selon la spécification Hoplink,
- Imprimer le logo Hoplink (cf. charte graphique Hoplink). »

Pour une carte Calypso Light :

« Les cartes fournies doivent :

- Utiliser l'identifiant de l'application du réseau (appelé également AID ou conteneur) normalisé par l'ISO et référencé par l'AFNOR, propre à l'opérateur du système billettique : ***(mentionner l'identifiant choisi fourni par l'AFNOR tel quel, sans y ajouter de 00 supplémentaires)***,
- Être configurées suivant la structure de fichier Reference / Classic ***(choisir l'une des deux en fonction des structures déjà existantes dans le réseau et des besoins futurs)***,
- Utiliser un jeu de clés TDES dédiés pour ce produit ; le jeu de clés sera fourni a posteriori. »

Pour une carte Calypso Basic :

« Les cartes fournies doivent :

- Utiliser l'identifiant de l'application (appelé également AID ou conteneur) normalisé par l'ISO et référencé par l'AFNOR, propre à l'opérateur du système billettique : ***(mentionner l'identifiant choisi fourni par l'AFNOR tel quel, sans y ajouter de 00 supplémentaires)***,
- Utiliser un jeu de clés TDES dédiées pour ce produit ; le jeu de clés sera fourni *a posteriori*. »

FICHE PRATIQUE N°2

SPÉCIFIER UNE SOLUTION BILLETTIQUE MOBILE NFC CALYPSO DANS UN APPEL D'OFFRES

Pour la solution billettique mobile NFC Calypso sur SE :

« La solution billettique mobile NFC Calypso sur SE proposée doit avoir la capacité à fonctionner sur tout smartphone NFC ayant fait l'objet d'une certification RF, soit sur la base de la certification NFC Forum, soit sur la base de la certification ISO/IEC TS 24192 dernière édition (ou de sa version CEN/TS 16794).

L'applet doit être chargé uniquement dans des Secure Element (SE) qui ont fait l'objet d'une certification fonctionnelle de conformité à Calypso du couple Applet/SE, assurée par PayCert, organisme indépendant accrédité. La liste des produits certifiés est disponible à l'adresse https://www.cna-paycert-certification.eu/card/applet/. Le fournisseur s'engage à s'assurer régulièrement pendant toute la durée du service contractualisé que tous les smartphones NFC dans lesquels l'applet est chargé ont obtenu la certification fonctionnelle Calypso du couple Applet/SE. Si un couple Applet/SE n'est pas d'ores et déjà certifié, il appartiendra au fournisseur de demander cette certification.

A la date de l'offre, le fournisseur donnera la liste exhaustive des smartphones NFC (fournisseur et référence produit) éligibles au service de billettique mobile NFC Calypso qu'il propose. Le fournisseur s'engage à assurer une veille active sur les smartphones NFC éligibles à la solution SE Calypso et il mettra à jour régulièrement cette liste sur toute la durée du service. »

- Novembre 2022 -

Pour la solution billettique mobile NFC HCE Calypso :

« La solution billettique mobile NFC HCE Calypso proposée doit avoir la capacité à fonctionner sur tout smartphone NFC sur système d'exploitation (OS) Android ayant fait l'objet d'une certification RF, soit sur la base de la certification NFC Forum, soit sur la base de la certification ISO/IEC TS 24192 dernière édition (ou de sa version CEN/TS 16794).

Le fournisseur doit fournir les certificats apportant la preuve qu'il obtenu :

- La certification fonctionnelle Calypso du SDK HCE Calypso (à venir),
- La certification de sécurité du SDK HCE Calypso.

La solution billettique mobile NFC doit s'appuyer sur les spécifications et guidelines Calypso, et en respecter toutes les exigences. Le fournisseur doit fournir une déclaration sur l'honneur que sa solution billettique mobile NFC respecte dans leur intégralité les spécifications et les guidelines de la solution HCE Calypso.

A la date de l'offre, le fournisseur donnera la liste exhaustive des smartphones NFC sur système d'exploitation (OS) Android éligibles au service de billettique mobile HCE Calypso qu'il propose. Le fournisseur s'engage à assurer une veille active sur les smartphones NFC éligibles à la solution HCE Calypso et il mettra à jour régulièrement cette liste sur toute la durée du service. »

FICHE PRATIQUE N°3

SPÉCIFIER DES TERMINAUX CALYPSO DANS UN APPEL D'OFFRES

Les textes à insérer dans un appel d'offres de terminaux d'un système billettique concernent uniquement la bonne mise en œuvre du standard Calypso. Un strict respect des exigences définis par CNA et détaillées au paragraphe 6 est nécessaire pour garantir la compatibilité avec toutes les cartes certifiées et les solutions billettique mobile NFC.

Pour rappel, et conformément au document « La billettique au service du MaaS : les bonnes pratiques pour un système efficace », le modèle de données ne doit pas être intégré dans un appel d'offre terminaux mais géré indépendamment sous la maîtrise du donneur d'ordre qui s'assure d'en avoir la propriété.

Par référence au tableau du paragraphe 6.3, le texte ci-dessous correspond à la ligne «Matériel» intégrant l'application billettique du réseau.

« Le terminal proposé doit avoir reçu le certificat de conformité à la norme ISO/IEC TS 24192 (anciennement nommé CEN/TS 16794), que le soumissionnaire joindra à son offre. Il est rappelé que ce certificat radiofréquence du terminal doit porter sur le produit fini qui comprend le matériel électronique dans son packaging définitif, avec le logiciel.
Le logiciel du terminal sera structuré en trois couches logicielles afin d'assurer l'évolutivité, la modularité et la capacité du terminal à traiter toutes les cartes Calypso certifiées. Ces trois couches sont décrites sur le site: https://calypsonet.org/calypso-pour-terminaux/?lang=fr.

Le soumissionnaire devra apporter la preuve de son respect des exigences correspondant à ces trois couches logicielles par la remise de :

- La lettre d'enregistrement du lecteur de cartes du terminal, qui atteste, sur base déclarative de la conformité aux exigences décrites dans le document « Reader Layer Requirements ».

- La lettre d'enregistrement de la librairie Calypso, qui atteste, sur base déclarative, de la conformité aux exigences décrites dans le document « Calypso Layer Requirements ».

- Une lettre d'engagement, qui atteste, sur base déclarative, du respect des exigences, recommandations et des bonnes pratiques décrites dans le document « Ticketing Layer

- Novembre 2022 -

Requirements ».

Les deux premiers alinéas seront remplacés par les deux alinéas ci-dessous dès que la certification sera disponible et se substituera donc à cet enregistrement sur base déclarative :

- Le certificat du lecteur de cartes du terminal, qui atteste de la conformité aux exigences décrites dans le document « Reader Layer Requirements ».

- Le certificat de la libraire Calypso, qui atteste de la conformité aux exigences décrites dans le document « Calypso Layer Requirements ».

Le terminal proposé s'appuiera sur l'utilisation des APIs de référence définis par CNA : Reader API, Card API et Calypso API.

Le terminal proposé s'appuiera préférentiellement sur l'utilisation du logiciel open source Eclipse Keyple.

Eclipse Keyple est libre de droits (Eclipse Public License 2.0 (ou EPL-2.0)).

En cas d'utilisation du module Keyple Core, le soumissionnaire sera tenu à présenter la lettre d'enregistrement du lecteur, qui atteste, sur base déclarative de la conformité aux exigences décrites dans le document « Reader Layer Requirements ». ***(À remplacer par le certificat dès que la certification correspondante sera disponible).***

En cas d'utilisation du module Keyple Calypso, le soumissionnaire fournira directement la lettre d'enregistrement existante de la librairie Keyple Calypso. ***(À remplacer par le certificat dès que la certification correspondante sera disponible).***

Le terminal proposé devra avoir au minimum deux, et de préférence quatre, emplacements réservés pour l'intégration de module de sécurité (SAM) au format suivant : ***(choisir entre SIM (ID-1/1FF), mini SIM (2FF), micro SIM (3FF), nano SIM (4FF)). »***

- Novembre 2022 -

DÉFINITIONS
ET ACRONYMES

- ABT ou Système Centrique

Un système ABT (Account Based Ticketing) est un système billettique où les titres de transport sont stockés dans un serveur central et liés à un compte client, la carte ne servant que de moyen d'identifier le client pour le relier à son compte. Les traitements logiciels des titres de transport sont alors assurés par le serveur central.

- AES

Advanced Encryption Standard (tel que défini dans la norme ISO/IEC 18033-3) : algorithme cryptographique symétrique utilisant des données et une clé de 128 bits.

- AID

Identifiant d'application (appelé également « conteneur ») : valeur unique dans une carte, permettant d'identifier sans ambiguïté une application de la carte, telle que définie dans les normes ISO/IEC 7816-4 et ISO/IEC 7816-5.

- AMC

Application Multi-services Citoyenne : norme ayant pour objectif de permettre l'utilisation d'un seul et même support (carte ou application mobile) pour accéder à différents services de la vie citoyenne (transport, culture, déchetterie, stationnement, tourisme...). La référence AFNOR de la norme est NF 99-508.

- API pour Terminal

Une API (Application Programmable Interface) pour terminal définit une interface commune de gestion d'application logicielle. Au niveau d'un terminal billettique, plusieurs API peuvent exister, de la gestion du coupleur sans contact aux applications billettiques de plus haut niveau.

- APPLET

Application qui peut être chargée dans une carte (généralement associée à l'environnement Java).

- Carte sans contact

Un support sans contact, par exemple une carte à puce, une carte java, un smartphone NFC, une clé USB avec une interface sans contact, ou tout autre support sans contact à disposition des clients.

- CNA

Calypso Networks Association.

- CEN

Le CEN (Comité Européen de Normalisation) est une association qui regroupe les organismes nationaux de normalisation de 34 pays européens. Le CEN est un organisme de normalisation reconnu par l'Union européenne comme étant responsable de l'élaboration et de la définition de normes au niveau européen en collaboration avec l'ISO.

- Chip

Puce ou composant électronique, conçu et fabriqué par des industriels spécialisés du domaine du silicium, dénommés fondeurs. Le chip est intégré dans les cartes dont il constitue l'élément intelligent qui stocke les données et les traite.

- DES

Algorithme de chiffrement produisant 8 octets de données à partir de 8 octets d'entrée, en utilisant une clé de 7 octets (tel que défini dans ANSI X3.92-1981). Également appelé «DES simple», maintenant déprécié.

- DESX

Algorithme de chiffrement produisant 8 octets de données à partir de 8 octets d'entrée, en utilisant une clé de 15 octets, maintenant obsolète.

- Eclipse

La fondation Eclipse est une organisation à but non lucratif supervisant le développement de l'IDE open source Eclipse et des projets gravitant autour, et qui aide à cultiver une communauté open source et un écosystème de produits et de services complémentaires autour d'Eclipse.

- ECP

Apple VAS Enhanced Contactless Polling (ECP), est une extension propriétaire d'Apple de l'EMV level 1 et de l'ISO/IEC 14443.

- EMVCo

EMVCo est un organisme technique mondial qui facilite l'interopérabilité et l'acceptation des transactions de paiement sécurisées dans le monde entier en gérant et en faisant évoluer les spécifications EMV et les processus de test associés. EMVCo est la propriété collective d'American Express, Discover, JCB, Mastercard, UnionPay et Visa.

- HCE

Host Card Emulation – Émulation de la carte hôte. Fin 2013, Google a publié la version 4.4 d'Android, appelée «KitKat», qui introduit plusieurs fonctionnalités pour les applications Android, dont l'API Host Card Emulation (ou «HCE»), destinée à faciliter et à encourager l'utilisation des smartphones NFC comme «cartes sans contact». Avec le HCE, une application Android dans le smartphone NFC peut directement recevoir, traiter et répondre à des commandes sans contact, sans avoir besoin du soutien d'un élément sécurisé (SE). Cependant, le HCE est beaucoup moins sûr qu'une carte à puce sans contact ou une carte SIM. Par conséquent, des exigences de sécurité spécifiques sont nécessaires pour mettre en œuvre une application sécurisée (telle qu'une application Calypso) afin d'atteindre un niveau de sécurité acceptable.

- HOPLINK

Hoplink est l'application de billettique interopérable développée par CNA. Certaines données et noms de fichiers et de champs peuvent utiliser l'acronyme de Triangle 2, l'ancienne dénomination de Hoplink.

- Interopérabilité

L'interopérabilité est la capacité d'un système ou d'un produit à fonctionner avec d'autres systèmes ou produits sans nécessiter des actions supplémentaires de la part du voyageur.

- ISO

L'ISO (International Standardization Organization) est une organisation internationale non gouvernementale, indépendante, dont les 164 membres sont les organismes nationaux de normalisation. Elle réunit des experts de tous pays pour élaborer des normes internationales.

- Logiciel Open Source

Un logiciel Open Source est un logiciel dont le code source est librement et gratuitement accessible, utilisable et modifiable, distribué sous une licence approuvée par l'Open Source Initiative et qui garantit le respect des règles qui y sont relatives.

- Modèle de données

Le modèle de données a pour objet de décrire comment les informations sont codées et stockées dans la carte ainsi que leurs règles de gestion. Le modèle de données constitue un langage commun qui permet l'interopérabilité entre acteurs de la mobilité partageant un même media client.

- Module de sécurité (SAM)

Le module de sécurité authentifie la carte, le terminal et toutes les données échangées entre eux. À la base, c'est une carte à puce, mais les services étant aujourd'hui souvent assurés par des serveurs distants, il peut également s'agir d'un composant hardware intégré à un serveur (HSM).

- NFC

Le NFC (Near Field Communication) est une technologie de communication sans-fil dont l'atout principal, dans ce cas précis, est sa courte portée, jusqu'à 10 cm.

- PKI

Public Key Infrastructure : Infrastructure à clé publique : système assurant la sécurité des informations basé sur la cryptographie asymétrique, qui permet de protéger les données en partageant uniquement des clés publiques.

- SE

Secure Element : élément sécurisé : microprocesseur sécurisé capable de stocker et d'exploiter des logiciels, notamment des applications ISO/IEC 7816-4.

- Système Carte Centrique

Dans un système billettique « carte centrique », les titres de transport sont stockés dans la carte du voyageur. Même en cas de recopie des titres sur un serveur central, c'est le contenu de la carte qui fait foi. Les traitements logiciels temps réel des titres de transport sont généralement assurés par les terminaux front office du système.

- TDES

L'algorithme de cryptographie symétrique est constitué de trois opérations DES successives (telles que définies dans la norme ISO/IEC 18033-3), également appelé «Triple-DES», ou «3DES».

Calypso
Networks Association

www.calypsonet.org

contact@calypsonet.org

Headquarters:
Calypso Networks Association,
Rue Royale 76,
1000 Bruxelles, Belgium

Paris:
Calypso Networks Association,
2 rue de la Roquette, Escalier Avril,
75011 Paris, France