Spirtech

SECURE & SMART

La sécurité dans les systèmes cartes à puce sans-contact

Mai 2011

Le dossier

Ce qu'il faut retenir

Triangle 2 : application Calypso permettant l'interopérabilité des supports billettiques entre différentes régions et pays.

Calypso Révision 3 : version la plus récente des spécifications du standard ouvert billettique Calypso. Triangle 2 est conforme à ces spécifications.

Gestion des clés : les clés Triangle doivent être inscrites dans le SAM maître (SAM-SP) du bassin d'interopérabilité lors de la cérémonie de création des clés.

Triangle 2: l'interopérabilité transrégionale et transfrontalière

Projet initié par *Belgium Mobility Card*, intégré aux travaux de *Calypso Networks Association (CNA)* et soutenu par l'Union Européenne, l'application ***Triangle*** permet de bâtir simplement une interopérabilité billettique des déplacements entre régions et pays frontaliers.

Afin de permettre des déplacements au-delà d'un seul bassin d'interopérabilité, Triangle définit des ***clés de sécurité***, une ***structure de fichiers*** et un ***modèle de données*** communs.

Triangle est protégée par des clés de sécurité ***DESX*** et ***Triple DES*** administrées par CNA et présentes dans les SAM des équipements. Le modèle de données permet de charger des contrats de transport de tout type et de toute durée. Chaque contrat est sécurisé par une signature : l'identifiant unique de l'émetteur du contrat, présent dans les données du contrat, est non falsifiable et sécurisé par un SAM.

Triangle est une application billettique ***Calypso Révision 3*** présente dans un objet portable (carte, téléphone NFC, clé USB, etc.). Elle peut être utilisée de façon autonome, ou en complément d'une application billettique locale.

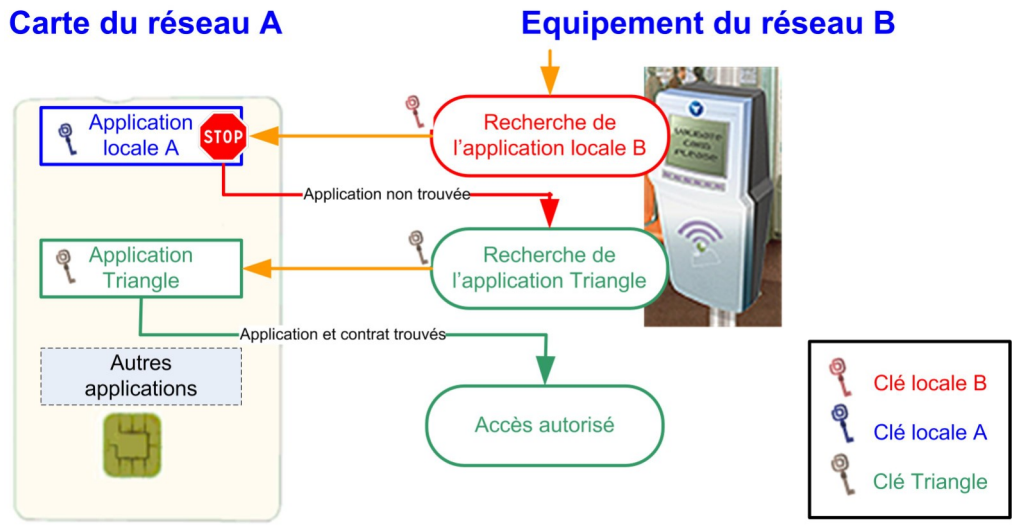
Hors du bassin d'émission de l'objet portable, les réseaux partenaires peuvent directement utiliser l'application Triangle pour gérer des titres locaux ou interrégionaux.

Dans le bassin d'émission, le mécanisme Calypso de ***partage de fichiers*** permet d'accélérer les flux en validant un contrat Triangle depuis l'application de transport locale : lorsqu'un objet portable est présenté à un équipement billettique, celui-ci sélectionne l'application locale et peut y valider un titre de transport local ou Triangle, avec les clés locales.

L'inscription de nouveaux contrats nécessite l'utilisation des clés Triangle. Elle a pour seule limite les capacités du support retenu. Le voyageur peut, lorsque l'espace disponible est insuffisant, procéder à la suppression de titres dont il n'a plus l'utilité.

Triangle ne nécessite pas de système billettique commun, il permet donc facilement aux *autorités organisatrices* de différents bassins d'interopérabilité d'étendre leur offre de transport interopérable et multimodale. Elles doivent alors simplement se mettre d'accord sur une offre tarifaire commune couvrant les nouveaux déplacements interrégionaux.

L'application Triangle est mise gracieusement à disposition par CNA.



Validation hors de la zone d'émission

En savoir plus

Pour en savoir plus sur le standard Calypso et sur Triangle 2:

Calypsonet-asso.org

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

CalypsoTechnology.net

Calypso Networks Association (CNA) : Association regroupant les opérateurs et les autorités organisatrices ayant adopté le standard Calypso pour leur billettique interopérable et multimodale.

Clés : cf. Secure & Smart février 2011.

Clés locales : clés sécurisant l'application transport du bassin d'interopérabilité émetteur du support. Elles sont partagées par l'ensemble des partenaires de l'interopérabilité locale.

Clés Triangle : clés sécurisant l'application transport interopérable Triangle. Ces clés, partagées par les réseaux partenaires Triangle, sont administrées par CNA.

DESX : algorithme de chiffrement utilisant une clé de 120 bits, et offrant une sécurité équivalente au Triple DES.

Modèle de données : description du codage des données inscrites dans les objets portables.

Partage de fichiers : mécanisme défini par Calypso et permettant un partage contrôlé et sécurisé de données entre applications différentes du même objet portable.

SAM (Secure Application Module) : cf. Secure & Smart février 2011.

Signature : données cryptographiques ajoutées aux informations des contrats afin de permettre leur authentification et l'identification sécurisée de l'émetteur du contrat.

Structure de fichiers : description des fichiers (nombre, identifiants, taille, sécurité) présents dans une application Calypso.

Triple DES : Algorithme de chiffrement reposant sur un triple chiffrage DES et une double clé DES (112 bits).

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.

www.spirtech.com

Spirtech Conseil. L'interopérabilité en Belgique et au-delà.

La Société des Transports Intercommunaux de Bruxelles (STIB) a initié le projet de télébillettique interopérable belge ***MOBIB***.

En choisissant le standard télébillettique ***Calypso*** pour la carte MOBIB, les quatre sociétés de transport public (De Lijn, SNCB, STIB et TEC), réunies dans ***Belgian Mobility Card*** (BMC) ont montré une volonté forte de conserver leur indépendance vis-à-vis des industriels, tout en garantissant l'interopérabilité billettique nationale.

De plus, MOBIB est une ***carte multiservices***. Elle est utilisée non seulement pour les transports publics, mais aussi pour le stationnement, l'accès aux musées et spectacles, la location de vélos. Elle reste ouverte à de futurs services.

De façon innovante, un titre de transport MOBIB peut être acheté par téléphone, Internet ou par tout autre moyen. Puis, lors du passage devant un valideur, le titre est automatiquement chargé dans la carte.

MOBIB permet de gérer de nombreux titres de transports (carnets, abonnements), ainsi que différentes réductions (scolaires, étudiant, chômeur, senior), qui peuvent également varier selon le lieu de résidence par exemple.

BMC a également fait inscrire les clés ***Triangle*** dans les SAM MOBIB. Les travaux en cours entre les autorités organisatrices belges et celles du nord de la France devraient faciliter à terme les déplacements transfrontaliers.

Spirtech Conseil assiste la STIB depuis les prémisses du projet, afin de l'aider à en maîtriser la complexité. En complément de son assistance au projet, Spirtech a notamment rédigé les documents techniques et sécuritaires, procédé aux tests d'interopérabilité et optimisé les temps de transactions entre un terminal et une carte MOBIB.

Cette expérience permet à Spirtech Conseil d'accompagner avec succès BMC dans la rédaction du référentiel d'interopérabilité nationale.

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	v0025	041115SDI-SE-SAMS1E v1.4
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 être obtenues sous NDA sur : www.CalypsoTechnology.net.

Evènements

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 organise à Lyon (France) les 6 et 7 octobre 2011 les assises consacrées à la télébillettique et la dématérialisation.

www.adcet.com

Cartes & Identification
Du 15 au 17 novembre 2011, Paris Villepinte (France) accueille le plus grand salon dédié à la sécurité numérique et aux technologies intelligentes.

www.cartes.com

Liens utiles

www.spirtech.fr

www.calypsonet-asso.org

www.calypsotechnology.net

www.stib.be

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 - Mai 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.