

NEOWAVE

MORPHEO

Solution sécurisée de rechargement
en ligne de supports MIFARE

1 - Serveur de rechargement MIFARE

2 - Web service sécurisé

3 - Couche de sécurité intégrée
au lecteur sans contact

4 - Lecteur sans contact personnalisé

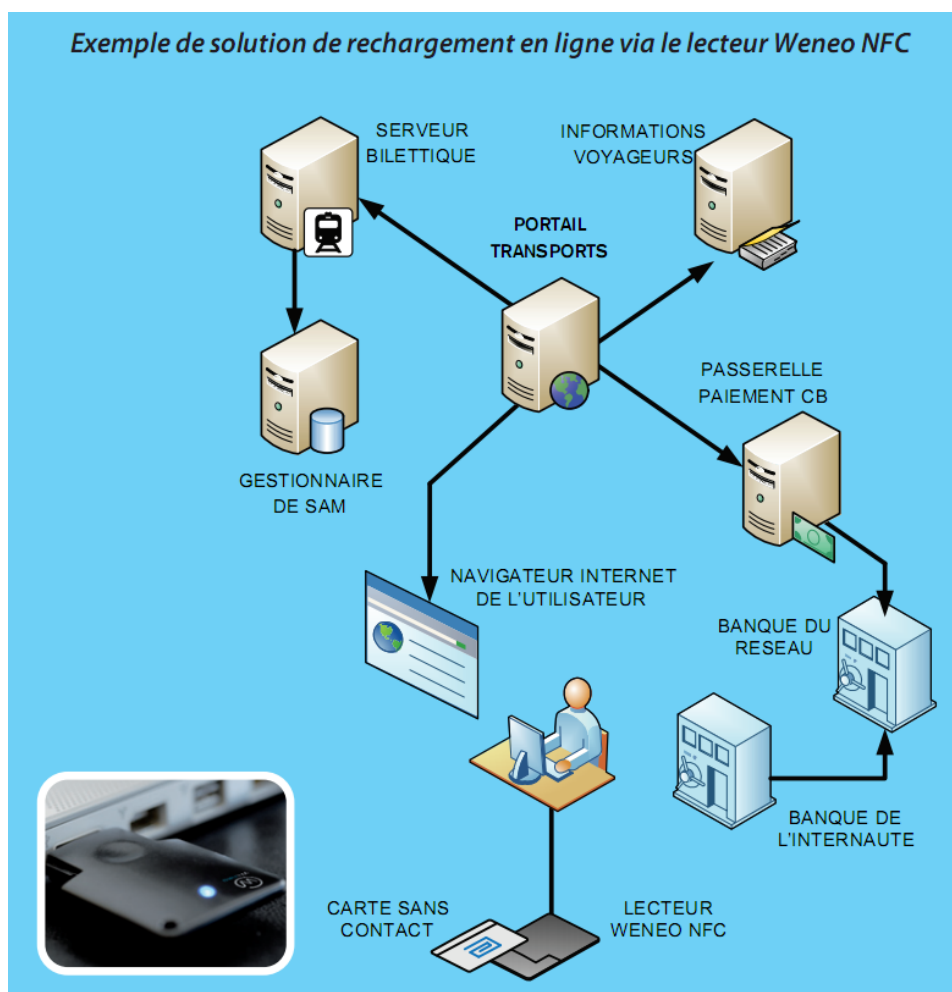
MORPHEO

Solution sécurisée de rechargement en ligne de supports MIFARE

Introduction

Les Smart Objects Weneo de Neowave annoncent l'aube d'une nouvelle ère pour la billetterie Transport et d'autres applications transactionnelles, celle de la dématérialisation et des offres de bouquets de services aux usagers. Les nouveaux supports de dématérialisation comme les Smart Objects (Weneo, téléphone mobile NFC...) constituent une réponse parfaite à l'appétence du grand public vers ces nouveaux bouquets de services. Le déploiement des services s'appuiera sur ces nouveaux supports qui offrent directement la sécurité et l'ergonomie requises pour des transactions en ligne mais devra aussi prendre en compte les supports déjà distribués comme les cartes sans contact ou les cartes duales. Dans le monde du transport, il apparaît comme extrêmement risqué en termes de sécurité de vouloir effectuer du rechargement en ligne à partir de carte MIFARE comme on peut le faire avec des cartes Calypso avec un simple lecteur de carte à puce connecté à un PC.

En effet la sécurité proposée par les cartes MIFARE a été cassée et des méthodes pour accéder aux données sensibles sont disponibles sur internet, donnant naissance à une multitude de fraudeurs potentiels. Dans cette note d'application, Neowave décrit l'architecture qu'elle a mise en place pour offrir un niveau de sécurité suffisant pour autoriser des transactions en ligne à partir de cartes MIFARE Classic. Cette solution constitue une ouverture potentielle vers les services en ligne en toute sécurité pour des centaines de millions de cartes déjà utilisées dans le monde du transport et dans d'autres applications transactionnelles.



La problématique des environnements MIFARE pour le rechargement en ligne

Pourquoi faut-il une architecture de sécurité spécifique dans les environnements MIFARE ?

Cas des autres cartes sans contact (à microprocesseur)

Quand on considère des environnements à base de carte à microprocesseur pour faire du rechargement en ligne comme c'est le cas dans les systèmes Calypso ou Global Platform, on peut mettre en place des mécanismes de sécurité qui s'appuient sur ceux créés pour les transactions sans contact sur les valideurs ou sur les terminaux et qui comprennent généralement :

- Une authentification du terminal
- Une authentification de la carte
- La création d'un canal sécurisé pour réaliser la session de transaction
- L'authentification des données transmises
- La preuve que la carte a correctement réceptionné les données et/ou modification demandées

Pour le rechargement en ligne à domicile de cartes sans contact, le terminal est remplacé par un lecteur simple et transparent, c'est donc directement au niveau du serveur que la sécurité va être gérée et que le dialogue sécurisé avec la carte va pouvoir s'établir. Comme indiqué dans le diagramme d'architecture en page précédente, c'est le serveur en liaison avec le gestionnaire de SAM qui va mettre en œuvre les processus d'authentification réciproque avec la carte et assurer la sécurité de la transaction avec celle-ci.

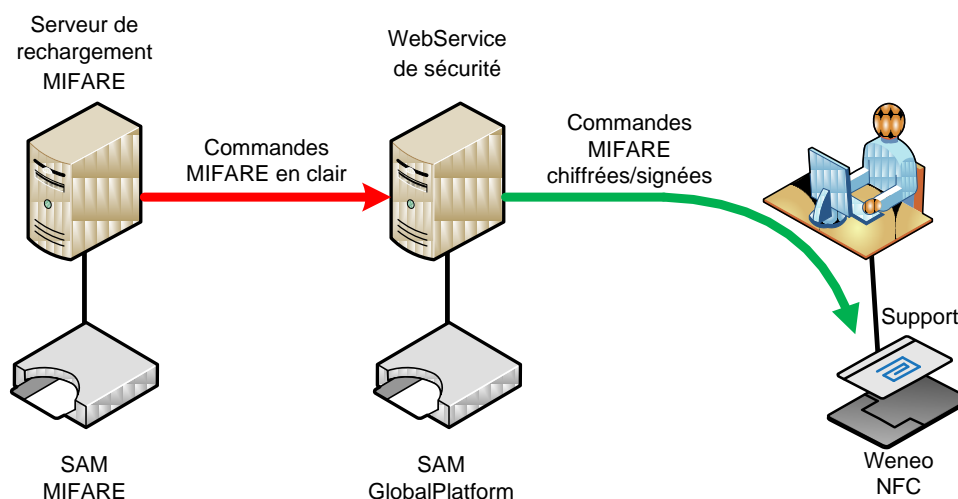
Cas des environnements MIFARE

Cette solution qui a été validée et qui est utilisée dans de nombreuses applications, ne peut malheureusement pas s'appliquer quand on considère un parc de cartes MIFARE. En effet pour lire et écrire dans une carte MIFARE, il faut un lecteur sans contact compatible MIFARE avec un composant frontal RF MIFARE pour mettre en œuvre l'algorithme propriétaire CRYPTO1 de NXP pour réaliser le processus d'authentification mutuelle avec la carte MIFARE. Pour cela il faut fournir au lecteur la clé MIFARE A ou B, et l'on devine aisément la difficulté de transmettre ces clés extrêmement sensibles à travers internet vers un lecteur bas coût dans un environnement grand public et par conséquent non sécurisé. En effet, l'envoi peut être facilement intercepté par un tiers malveillant à de nombreux endroits dans l'architecture système : sur internet, sur l'ordinateur de l'utilisateur, dans la liaison entre l'ordinateur de l'utilisateur et le lecteur, et dans le lecteur lui-même...

MORPHEO

La Solution de Neowave pour le rechargement en ligne de cartes MIFARE

Pour s'affranchir de ce problème de sécurité crucial et pouvoir ouvrir les solutions de rechargement en ligne aux cartes MIFARE, Neowave a créé un protocole de sécurisation de haut niveau qui s'intègre parfaitement dans une solution de vente à distance multi-supports : cartes sans contact ou duale Calypso, clé USB RFID Calypso, cartes MIFARE, clé USB RFID avec émulation MIFARE...)



Ce protocole de sécurité repose sur une implémentation des algorithmes de cryptographie Global Platform largement utilisés dans le monde de la carte à puce. Une clé maître (MK, Master Key) est générée spécifiquement pour les lecteurs lors d'une cérémonie de clés formelle (dans un lieu isolé, avec des officiers de sécurité, etc.), puis déployée dans des SAM (ou HSM) connectés à un Web Service dédié pour la gestion de la sécurité du lecteur. Lorsque la logique de gestion du contenu de la zone MIFARE a besoin de transmettre des commandes MIFARE au support, elle demande leur encapsulation à ce Web Service.

Dans chaque lecteur sans contact comportant la couche de sécurité Neowave MORPHEO, lors de la personnalisation sont injectés un diversifiant unique pour chaque lecteur et trois clés de base (clé de chiffrement, clé de signature, clé de sur-chiffrement) diversifiées à partir de la clé maître et du diversifiant du lecteur. Lors de la phase d'authentification mutuelle du lecteur, ce dernier fournit son diversifiant, ce qui permet au SAM côté Web Service de recalculer les clés de base à partir de la MK présente dans le SAM. Des nombres aléatoires sont alors échangés afin de calculer des clés de session qui seront utilisés pour gérer la confidentialité et l'intégrité des échanges de commandes suivants. L'utilisation de clés de session garantit l'anti-rejeu d'une transaction. Toutes les clés mises en œuvre (clé maître, clés de bases, clés de session) sont des clés Triple-DES à deux clés. Weneo NFC contient également un numéro de série unique qu'il est possible d'obtenir avec une pseudo-commande APDU spécifique.

Le **serveur de rechargement MIFARE** implémente la logique de gestion du contenu du **support MIFARE** (c'est-à-dire, quels sont les blocs MIFARE à lire et écrire lors d'une opération de consultation ou de rechargement d'un titre). Les commandes MIFARE à envoyer au support sont générées par le **SAM MIFARE** puis transmises **en clair** au **Web Service de sécurité** pour encapsulation. A la réception de la première commande MIFARE à transmettre au support, le Web Service de sécurité établit la session sécurisée avec le lecteur sans contact **Weneo NFC** en mettant en œuvre la clé maître Global Platform stockée dans le **SAM Global Platform**. Les commandes MIFARE sont alors transmises **chiffrées et signées** au lecteur Weneo NFC.

Le Webservice de sécurité peut également être mis en œuvre pour la transmission de toute commande destinée à un support sans contact, y compris donc un support Calypso (protocole Type B ou Innovatron).

Une solution ouverte

La technologie de sécurité de bout en bout NORSSOM est implémentée dans les lecteurs sans contact de la gamme Neowave mais peut-être implémentée sous licence dans d'autres lecteurs sans contact ayant les ressources nécessaires pour l'implémentation de la couche de sécurité décrite ci-dessus (comme par ex. le lecteur Prox'N'Roll de SpringCard)

Les composantes de la solution MORPHEO de Neowave

- Serveur de rechargement MIFARE
 - Avec les SAM associés
- Web service de sécurité
 - Avec la cérémonie de clé associée
 - Et la génération des SAM GlobalPlatform
- Couche de sécurité intégrée au lecteur sans contact
 - Option logicielle : le mécanisme de sécurité est implémenté dans le firmware du processeur du lecteur sans contact
 - Option SAM : le mécanisme de sécurité est implémenté dans un SAM spécifique de la solution MORPHEO qui est inséré dans le logement du lecteur sans contact (quand il intègre cette option)
- Lecteur sans contact personnalisé
 - Weneo NFC
 - Prox'N'Roll de SpringCard
 - ... ou tout autre lecteur sans contact intégrant la couche de sécurité MORPHEO

Weneo NFC et MORPHEO



Weneo NFC de Neowave avec sa fonction lecteur sans contact de rechargement intégrant la solution MORPHEO

Les bénéfices de la solution MORPHEO

- Une sécurité de bout en bout pour du rechargement en ligne qui autorise l'utilisation de cartes MIFARE en toute sécurité
- Une solution qui s'adapte à tout type de support sans contact pour la mise en œuvre de transactions sécurisées utilisant des environnements non sécurisés comme le web
- Une solution complète intégrant les modules côté serveur et les modules côté lecteur
- Une solution ouverte qui peut s'implémenter dans de multiples lecteurs sans contact
- Une solution « low-cost » tant au niveau de l'intégration sur le lecteur que de l'intégration sur le serveur