Cartes sans contact Mifare DESFire EV1

Frédéric Pauget
DSI Télécom ParisTech
46, rue Barrault
75 013 Paris

Résumé

Les carte sans contact sont de plus en plus présentes dans notre environnement. Elles ont l'avantage d'une grande simplicité pour l'usager et permettent un bon niveau de sécurisation. De nombreuses technologies existent, mais suite au basculement du système de monétique du CNOUS depuis Moneo vers Izly, une d'entre elle va entrer dans de nombreux établissements d'enseignement supérieur : la carte Mifare.

La gamme Mifare se décline en plusieurs produits et nous allons nous intéresser plus particulièrement à sa version la plus avancée : la Mifare DESFire EV1. Ce type de carte permet de stocker ses propres données de manière sécurisée et structurée. Une même carte peut sans problème être utilisée pour plusieurs applications en ayant une totale étanchéité entre elles.

Cet article abordera les points suivants :

- *les technologies de cartes ;*
- *les cartes Mifare DESFire EV1 ;*
- *les outils mis en œuvre et le retour d'expérience sur l'utilisation de ces cartes depuis 2013 à Télécom ParisTech ;*
- *l'utilisation future au sein d'un environnement multi-établissements : l'Université Paris Saclay.*

Mots clefs

carte sans contact, Mifare, DESFire, carte d'étudiant

1 Technologies de carte sans contact

Les cartes sans contact actuellement sur le marché peuvent être classées :

- selon la bande de fréquence utilisée :
  - $13,56MHz$ pour des accès à très courte distance (quelques centimètres), dans cette bande on trouvera notamment les cartes Mifare, Calypso (technologie utilisée notamment pour les cartes Navigo) et les cartes banquaires avec paiement sans contact,
  - $125kHz$: pour des accès à courte distance (une dizaine de centimètres), historiquement cette bande de fréquence est utilisée par les systèmes de contrôle d'accès tel que HID Prox ou les badges Nedap historiques ;
- selon leurs fonctionnalités :
  - cartes contenant un simple identifiant unique non modifiable garanti par le fabriquant (ex : badges Nedap historiques),
  - cartes permettant un stockage des donnés et/ou d'effectuer des opérations sur celles-ci (ex : cartes Mifare).

Afin de faciliter les transitions de technologies une même carte peut embarquer simultanément des puces utilisant les bandes de fréquences $13,56MHz$ et $125kHz$.

1.1 La famille Mifare

La technologie Mifare est une famille de composants qui contient notamment :

— *Mifare classic* : c'est la première version des cartes Mifare développée par la société Mikron (rachetée par Phillips, maintenant NXP) sortie en 1994. Ces cartes offrent un stockage structuré en blocs avec une capacité de $1ko$ ou $4ko$. Elles sont basées sur de la logique câblée. Un système d'authentification propriétaire permet de sécuriser l'accès aux données mais celui-ci a été cassé en 2008, actuellement quelques minutes suffisent pour le contourner, NXP déconseille son utilisation pour tout nouveau déploiement depuis 2008 ;

— *Mifare DESFire et DESFire EV1* : ces cartes sont basées sur la plate-forme NXP SmartMX qui embarque microprocesseur, mémoire, stockage et coprocesseur cryptographique. Elles utilisent le système d'exploitation DESFire développé spécialement pour cet usage. Cette carte introduit une nouvelle méthode de stockage sans utilisation de blocs permettant à l'utilisateur un formatage personnalisé. Elles sont disponibles en capacité de $2ko$, $4ko$ et $8ko$. Dans la version initiale elles proposent un chiffrement DES 56 bits et triple DES $112bits$ (2K3DES), la version EV1 introduit notamment le chiffrement triple DES $168bits$ (3K3DES) et AES $128bits$;

— *Mifare Plus* : cette carte permet de bénéficier des possibilités de la carte DESFire EV1 en ayant en plus une compatibilité Mifare Classic, elle est destinée à faciliter la migration vers la DESFire EV1 pour les systèmes existants ;

— *gamme Mifare ultralight* : une carte sur le modèle de la Mifare avec très peu de stockage ($512bits$) avec ou sans sécurisation suivant les versions, elle sert principalement pour des tickets jetables.

La carte Mifare DESFire EV2 devrait sortir très prochainement, elle sera rétro-compatible avec la version EV1 et apportera notamment une souplesse dans la gestion des clefs et des fichiers, la suppression de la limite du nombre d'applications et une meilleure résistance aux attaques.

2 La technologie Mifare DESFire EV1

Une carte Mifare DESFire permet le stockage d'*applications* qui vont contenir des *fichiers* dans lesquels seront stockés les données et les *clefs* permettant de gérer l'accès à ces fichiers. La carte possède en plus une clef maître permettant son paramétrage. La figure 1 donne une représentation schématique de cette structure.

2.1 Communiquer avec la carte

Un moyen simple de communiquer avec la carte est d'utiliser un lecteur compatible ISO 14443A utilisant la bande $13,56MHz$ exposant une interface PC/SC. Cela permet ensuite d'envoyer et recevoir des données avec la carte en s'affranchissant de tous les aspects matériels.

La carte maintient en permanence un état composé :

— du numéro de l'application courante ;

— du statut d'authentification : non authentifié ou authentifié avec la clef n^0X, l'authentification est perdue lorsque la carte est réinitialisée (sortie du lecteur), lorsque la clef utilisée est changée ou lors de la sélection d'une auttre application.

En fonction de la commande et de l'authentification réalisée la communication est soit en clair, soit authentifiée (signature cryptographique) soit chiffrée.

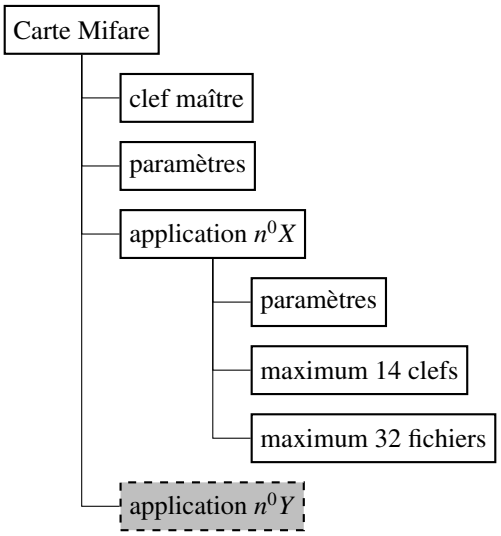

Figure 1 - Structure de la carte

2.2 Paramètres de la carte

La carte possède une clef maître, celle-ci permet notamment de changer le paramétrage de la carte. Il faut noter que en aucun cas cette clef ne peut permettre l'accès aux données.

Les paramètres positionables sont :

- authentification nécessaire ou non pour lister les applications présentes ;
- authentification nécessaire ou non pour créer ou effacer des applications ;
- possibilité de bloquer les futurs changement de clef maître ou de configuration ;
- activation du mode « identifiant aléatoire » (irréversible) ;
- interdiction de la commande permettant la destruction de toutes les applications (irréversible).

Le mode « identifiant aléatoire » permet de présenter un numéro de série différent à chaque initialisation (donc à chaque fois que la carte est posée sur un lecteur). Dans ce mode le numéro de série devient inutilisable comme authentification du porteur, ce qui a plusieurs avantages :

- la sécurité : il est possible de trouver dans le commerce des fausses cartes Mifare avec leur numéro de série programmable ;
- la confidentialité : la lecture du numéro de série se faisant en clair, un attaquant se positionnant à proximité d'un lecteur pourrait facilement collecter ceux-ci.

Il est toutefois encore possible d'accéder au vrai numéro de série après authentification, il sera alors transmis chiffré.

2.3 Application

Une application est caractérisée par :

- un AID (Application Id) : c'est un identifiant unique numérique codé sur $24bits$, ces identifiants sont attribués par NXP [1] ;
- le nombre d'emplacement de clefs, au maximum 14 ;
- le type de clef utilisé par l'application (DES, 2K3DES, 3K3DES, AES), toutes les clefs sont du même type.

Ces paramètres sont fixés à la création de l'application et ne peuvent plus être modifiés ensuite. S'il y a besoin de plus de clefs ou d'utiliser un autre algorithme de chiffrement il faudra détruire l'application puis la recréer.

La clef $n^0 0$ est la clef maître de l'application et permet de régler les paramètres de l'application :

— obligation d'une authentification par la clef maître ou non pour lister les fichiers présents ;

— obligation d'une authentification par la clef maître ou non pour créer ou effacer des fichiers ;

— blocage des changements de clef ou de configuration ;

— choix du numéro de clef nécessaire pour avoir le droit de changer une clef.

Une application peut contenir 32 fichiers et une carte 28 applications. Il y a une totale étanchéité entre les différentes applications.

2.4 Fichier

Le fichier est l'élément stockant les données. Plusieurs types de fichiers sont disponibles en fonction du besoin. Les opérations possibles sur un fichier dépendent de son type.

2.4.1 Standard Data File et Backup Data File

Ces types de fichiers sont destinés au stockage de données brutes.

Pour ces deux types la taille est définie à la création du fichier. Deux opérations sont possibles sur ce type de fichier : l'écriture et la lecture. Trois numéros de clefs de l'application peuvent être choisis pour contrôler ces opérations : clef permettant uniquement la lecture, clef permettant uniquement l'écriture, clef permettant les deux.

L'exemple typique d'utilisation est le stockage d'un identifiant. Une clef avec les droits lecture et écriture sera utilisée par le service d'édition des cartes alors qu'une clef permettant uniquement la lecture sera diffusée pour tous ceux ayant besoin de lire l'identifiant.

La variante backup prend deux fois plus de place sur la carte mais permet de garantir le contenu du fichier en cas de coupure lors de la transaction notamment si la carte est retirée ou en cas d'échec. Cela est utile par exemple en cas de besoin d'écriture depuis une borne libre service.

2.4.2 Value File

Ce type de fichier est destiné au stockage de données numériques.

Les valeurs limites inférieure et supérieure sont définies à la création. Il est possible de réaliser des opérations de lecture de la valeur, crédit et débit. Trois numéros de clefs de l'application peuvent être choisis pour contrôler ces opérations, ces trois clefs permettent la lecture et le débit. L'une d'elle permet en plus un crédit limité par une valeur décidée à la création et une autre un crédit illimité.

L'exemple typique d'utilisation est la réalisation d'une carte gérant un solde tel que des photocopies ou un nombre de trajets.

2.4.3 Linear Record Files and Cyclic Record Files

Ces types de fichier permettent de stocker de multiples enregistrements de même taille.

La taille et le nombre d'enregistrements sont fixés à la création du fichier. Les opérations possibles sont l'ajout d'un enregistrement, la lecture ou l'effacement de tous les enregistrements. Une clef permet de lire, une clef d'ajouter et une clef de lire, ajouter et effacer.

La version « linear » nécessite un effacement total lorsque le nombre maximal d'enregistrements est atteint (pour une application de carte de fidélité par exemple) alors que la version « cyclic » réécrit sur le premier enregistrement une fois le dernier atteint (pour le stockage de journaux par exemple).

2.5 Augmenter la sécurité des clefs

2.5.1 SAM : Secure Access Module

Programmer les clefs ou lire le contenu d'un fichier nécessite de posséder la clef en clair sur le système interagissant avec la carte. Afin de protéger les clefs contre les attaques sur ce système il est possible de stocker les clefs sur un SAM. Celui-ci prend la forme d'une carte à puce et va réaliser les calculs cryptographiques nécessaires aux interactions avec la carte sans jamais donner accès à une version en clair de la clef. La sécurisation de la clef revient à une sécurisation physique du SAM.

2.5.2 Diversification de clef

La diversification d'une clef est l'obtention d'une nouvelle clef à partir d'une clef maître, d'un diversifiant et d'un algorithme. L'algorithme et la clef maître sont fixés et le diversifiant provient d'une donnée lue sur la carte (le numéro de série par exemple). Cela permet de calculer une clef unique par carte. L'avantage est qu'en cas de découverte d'une clef d'une carte, cela ne donne pas d'accès à la clef maître mais uniquement à la clef d'une seule carte.

2.6 Principe d'utilisation

Nous allons prendre le cas d'usage suivant :

— les cartes sont reçues vierges ;

— il faut écrire un identifiant pour l'accès à la bibliothèque et un pour l'utilisation des copieurs multifonctions, ces deux identifiants sont connus au moment de l'écriture.

Pour ce type d'usage nous pouvons utiliser le formatage suivant : création d'une application avec un identifiant propre à l'établissement (demande à NXP ou prise sauvage d'un identifiant) utilisant le chiffrement AES (à moins d'un besoin de compatibilité avec d'anciens systèmes rien ne peut justifier l'emploi de DES ou triple DES) avec trois clefs. Dans cette application deux fichiers de type « standard datafile » seront créés, le fichier 1 lisible par la clef $n^0 1$ sera destiné à la bibliothèque, le fichier 2 lisible par la clef $n^0 2$ sera destiné aux multifonctions, ces deux fichiers seront écrits par la clef $n^0 0$ de l'application. Cette clef aura donc trois usages : paramétrage de l'application, écriture sur le fichier 1, écriture sur le fichier 2.

Avec ce formatage les lecteurs de la bibliothèque posséderont la clef $n^0 1$ et les lecteurs des multifonctions la clef $n^0 2$, chacun de ces deux système ne pourra lire que l'identifiant qui lui est propre.

En plus de ces opérations il faudra mettre en place une clef maître de la carte permettant d'éviter que l'application ne puisse être détruite par un tiers.

La procédure de programmations est le suivant :

1. Configuration de la carte
    a. Sélection application 0,
    b. Authentification clef 0 par défaut,
    c. Changement clef 0,
    d. Authentification nouvelle clef 0,
    e. Paramétrage de la carte ;

2. Création application établissement
    a. Création application X avec 3 clefs AES,
    b. Authentification clef 0 par défaut,
    c. Changement clef 0,
    d. Authentification nouvelle clef 0,
    e. Changement clef 1,
    f. Changement clef 2,
    g. Création fichier 1,
    h. Création fichier 2,
    i. Écriture fichier 2.

Dans une implémentation réelle on ajouterait des opérations d'introspection avant les opération d'écriture afin de pouvoir agir correctement si la carte n'est pas vierge en effectuant une mise à jour ou remontant une erreur.

3 Utilisation à Télécom ParisTech

3.1 Programmation des cartes

3.1.1 Bases logicielles

Deux pistes sont explorées : un logiciel intégré permettant de gérer l'impression et la programmation des cartes ou l'utilisation de librairies logicielles pouvant s'intégrer au système de gestion des personnes existant programmé en python.

La piste du logiciel intégré est vite abandonné : le temps nécessaire pour son achat (procédure de marché) et son intégration étant aussi consommateur en jours-hommes que le temps nécessaire à un développement direct par nos soins.

Aucune librairie python satisfaisante n'a été trouvée pour exploiter les cartes Mifare DESFire EV1. Nous avons étudié la librairie LibLogicalAccess [2] qui est écrite en C++ et finalement avons opté pour un développement interne d'une librairie purement en python basée sur pyscard [3].

Cette librairie permet une communication de haut niveau avec les cartes permettant de réaliser les opérations élémentaires sans se soucier des opérations de chiffrement ou des limites sur la taille des trames. Toutes les fonctionnalités de la carte ne sont pas encore implémentées mais le minimum permettant de paramétrer, changer les clefs, créer des applications et des fichiers, lire les fichiers standard, effacer la carte est présent. Elle peut-être transmise aux établissements nous en faisant la demande.

Un projet futur est l'utilisation de SAM pour le stockage des clefs.

Cette librairie est en production depuis fin 2013 à Télécom ParisTech et depuis 2015 à l'ENS Cachan.

3.1.2 Programmation libre-service

En prévision de la mise en place d'un service d'impression centralisée courant 2014 Télécom ParisTech a distribué des cartes Mifare DESFire EV1 à la rentrée 2013 pour tous les étudiants. A ce moment là aucune application n'exploite les technologies sans contact au sein de l'école et le mode de programmation n'est pas encore défini. Les cartes sont donc données électriquement vierges.

La maîtrise totale de la chaîne de programmation nous a permis de créer et mettre en service deux bornes de programmation libre-service pour les étudiants. Ces bornes sont constituées d'un PC et d'un lecteur de

carte. L'étudiant pose la carte vierge sur le lecteur, entre son identifiant et mot de passe puis la carte est programmée. Le PC est sous GNU/Linux et exporte le socket du service pcscd vers un serveur par ssh, c'est ce dernier qui réalisera tous les calculs cryptographiques afin de ne pas stocker les clefs sur le PC.

3.1.3 Programmation et impression

Pour la rentrée 2014 l'école a investi dans des imprimantes à cartes dotées de lecteur Mifare connectées sur Ethernet : des Fargo HDP5000 du fabriquant HID.

Le pilotage est confié à un serveur Windows (pour des raisons de disponibilité des drivers) depuis lequel le lecteur intégré à l'imprimante est vu comme un lecteur local PC/SC.

L'impression est déclenchée via le système de gestion de la scolarité, la carte est programmée et imprimée en une seule opération. Tous les élèves en sont donc dotés (l'école renouvelle annuellement toutes les cartes d'étudiant).

Fin 2014 le système est étendu à tous les personnels de l'école en utilisant la même infrastructure.

Pour la rentrée 2015 nous avons choisi d'ajouter l'application monétique du CNOUS (Izly) sur les cartes de nos étudiants. Le CNOUS s'appuie sur une SAM et une dll dédiée pour la création de cette application. Nous pouvions donc soit demander à disposer de ces informations pour effectuer l'intégration nous mêmes, soit sous-traiter cette partie. Par soucis de facilité nous avons préféré cette dernière solution, les cartes nous sont livrées par la SELP (prestataire retenu par l'appel d'offre du CNOUS) avec l'application Izly déjà programmée.

3.2 Lecture des cartes

L'école utilise actuellement les cartes pour quatre usages : l'utilisation du système d'impression centralisé, le système de prêt de la bibliothèque, l'accès au restaurant et le contrôle d'accès.

Trois solutions sont possibles pour lire les cartes, chacune avec ses avantages et inconvénients.

Le premier mode est la lecture par un lecteur basique compatible PC/SC et l'utilisation d'un logiciel spécifique pour gérer la communication DESFire. Dans ce cas soit les clefs de lecture sont connues du logiciel soit il faut avoir recours à un SAM. Cette solution est la plus complexe à mettre en œuvre mais en cas d'utilisation avec un SAM c'est la plus sécurisée.

Les deux autres modes font appel à un lecteur intelligent pouvant gérer tous les aspects de la communication avec la carte et transmettant uniquement les données. On trouve ce type de lecteur pour un peu plus d'une centaine d'euros. L'école utilise actuellement les lecteurs HID Omnikey 5427 CK USB. Le lecteur doit être programmé en lui indiquant quelle donnée lire avec quelle clef. Il peut effectuer des opérations simples de formatage sur ces données. Deux modes d'utilisation sont possible :

— mode d'émulation clavier : le lecteur est vu comme un clavier standard, aucun driver spécifique n'est nécessaire mais par contre, dans le cas de l'utilisation sur un PC, le résultat dépend du mode d'entrée du clavier (disposition et verrouillage majuscule activé ou non) et si l'utilisateur n'est pas dans la zone de saisie dédiée l'identifiant lu sera collé un peu n'importe où. Ce mode est utilisé à Télécom ParisTech sur des systèmes ne disposant pas de vrai clavier et prévus pour recevoir ce type de périphérique : les caisses du restaurant et les copieurs multifonctions ;

— mode CCID : un driver est nécessaire sur le poste sur lequel est connecté le lecteur, dans ce mode il est possible de traiter les données reçues et d'effectuer les opérations nécessaires sans avoir les inconvénients du mode précédent. Ce mode est utilisé à Télécom ParisTech à la bibliothèque et au poste de sécurité en association avec le logiciel autohotkey [4] : la présentation de la carte déclenche l'ouverture du navigateur directement sur la page correspondant à l'usager (bibliothèque ou fiche de droits d'accès).

4 Utilisation au sein d'un environnement multi-établissements : l'Université Paris Saclay

L'Université Paris Saclay récemment créée regroupe 19 membres fondateurs (2 universités, 10 grandes écoles et 7 organismes de recherche).

Un groupe de travail avec des représentants des établissements a été constitué afin de travailler sur la carte d'étudiant pour la rentrée 2015. Outre le travail sur le visuel unifié des cartes le groupe de travail a également étudié les aspect services liés à cette nouvelle carte.

Courant 2015 le choix a été fait de déployer des cartes Mifare DESFire EV1 pour tous les étudiants et de programmer l'application Izly sur ces cartes en plus des applications propres établissement. Chaque établissement de l'Université reste totalement autonome dans l'éditions et la programmation de ses cartes.

A terme il est prévu qu'un étudiant de l'Université puisse utiliser sa carte émise par un des établissements de l'Université pour accéder à des services d'un autre établissement. Une réflexion a été menée sur les service pouvant être implémentés sur la carte ayant un intérêt inter-établissements :

- la restauration ;
- le contrôle d'accès ;
- les systèmes d'impression et photocopie ;
- l'accès aux bibliothèques.

Hormis le cas des restaurants gérés par des CROUS qui est résolu grâce au système Izly, un inventaire des systèmes utilisés pour les services ci-dessus montre une très grande diversité de solutions mises en œuvre dans les différents établissements.

Le groupe de travail à choisi de travailler en premier sur le point d'accès aux bibliothèques : un service existant dans tous les établissements et qui aura prochainement des moyens mutualisés au sein de l'Université. L'objectif est qu'un lecteur puisse aller emprunter des ouvrages dans n'importe quel établissement de l'Université. Le groupe est arrivé aux conclusions suivantes :

- création d'une application dédiée Université Paris Saclay sur la carte avec une demande d'identifiant à NXP ;
- écriture d'un identifiant unique dans un fichier de cette application lisible par une clef partagée entre les établissements. Le format de cet identifiant est choisi en fonction des contraintes de tous les SIGB (Système Intégré de Gestion de Bibliothèque) recensés : identifiant numérique à 12 chiffres. Ces identifiants étant distribués localement par les établissements les deux premiers chiffres sont utilisés pour identifier l'établissement émetteur qui est alors responsable de la gestion de l'unicité de cet identifiant ;
- les demandes inter-bibliothèques étant pour le moment très faibles l'intégration dans les SIBG des utilisateurs de l'Université hors établissement sera faite manuellement par les documentalistes sur présentation de la carte ;
- pour des usages futurs l'identifiant généré sera remonté dans le méta-annuaire de l'Université.

Les opérations prévues ci-dessus n'ont pas été réalisées pour la rentrée 2015 malgré la bonne volonté de tous les établissements :

- l'AID n'a pas été encore attribué par NXP ;
- une livraison des cartes hors délais par la SELP et donc des personnalisations réalisées en urgence ;
- la mise en place de la technologie Mifare n'est pas encore effective dans toutes les bibliothèques ;

L'année scolaire 2015-2016 va être mise à profit pour réaliser les tests afin de pouvoir mettre en service cette solution pour la prochaine rentrée.

Bibliographie

[1] liste des identifiants d'applications mifare. http://www.nxp.com/documents/other/MAD_list_of_registrations.pdf.

[2] liblogicalaccess. http://liblogicalaccess.islog.com/.

[3] pyscard. http://pyscard.sourceforge.net/.

[4] autohotkey. http://www.autohotkey.com/.