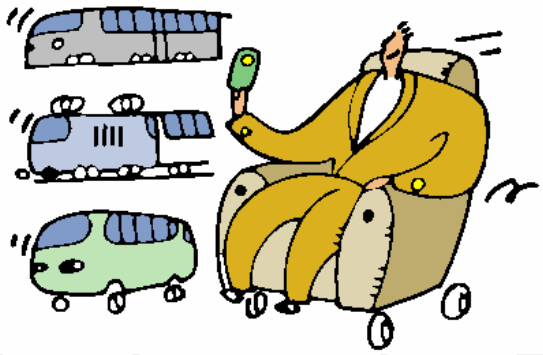
Technologie cartes sans contact et lecteurs associés



Sommaire

- Marchés, généralités
- Standardisation internationale
- Evolution des cartes
- Architecture et fonctionnement d'une carte type
- Organisation mémoire
- Gestion de la sécurité
- Caractéristiques particulières
- Architecture du lecteur
- Jeu de commandes
- Application porte-monnaie

Généralités (1/2)

- Plusieurs standards de cartes sans contact co-existent :
  - ISO/IEC 10536 : Close coupled cards. Portée : 1 à 3 mm.
  - **ISO/IEC 14443 : Proximity cards** (Cartes à puce sans contact de proximité). Portée : 10 cm. Couplage inductif à 13,56 Mhz. Débit supérieur à 100 kbit/s (→ 847 kbits)
  - ISO/IEC 15693 : Vicinity cards (Cartes de voisinage). Portée : 1m. Couplage inductif à 125 khz (Produits propriétaires) et 13,56 Mhz. Débit faible : 26 kbit/s.

Généralités (2/2)

- D'autres solutions techniques sont présentes :
  - Normalisées ISO 11784/785 : Identification animale. Fréquence : 134,5 khz. Distance : 1 m.
  - Non normalisées : Etiquettes longue portée actives (alimentées). Systèmes propriétaires. Tendance pour le 5,75 Ghz. Distance : quelques m.

Diversité des solutions techniques et des applications

- Les systèmes actuels fonctionnent dans 4 bandes de fréquences :
  - 125 - 135 khz. Identification par RF. Portée jusqu'à 1 m.
  - 13,56 Mhz Portée 10 cm.
  - Les UHF : 862 / 928 Mhz
  - Les Hyperfréquences à 2,45 Ghz et 5,8 Ghz, 915 Mhz (EU) : Etiquettes (Tags) électroniques alimentées. Distances de plusieurs m.

Identification à distance par radiofréquences (RFID)

- Désigne les transpondeurs* passifs (puce + enroulement) utilisés pour l'identification et l'enregistrement
  - Fonctionnent à 125 khz (jusqu'à plusieurs m) norme 15693
  - également à 135 khz, 13,56 Mhz, UHF 860 Mhz, 2,45GHz (Iso 18000)
  - Implants de marquage des animaux (Animal ID régi par ISO 11784/85), numéro unique sur 128 bits, capsule de verre.
  - identification d'objets (logistique, agroalimentaire, papeterie), clés de voiture. EAS (Electronic Article Surveillance)
  - Formes et matériaux divers (Plastiques en cartes, disques, barrettes, bâtonnets, capsules de verre)
  - Domaines d'application : Contrôle d'accès, suivi de fabrication, logistique, services, traçabilité des services. Gestion de la chaîne logistique (SCM)

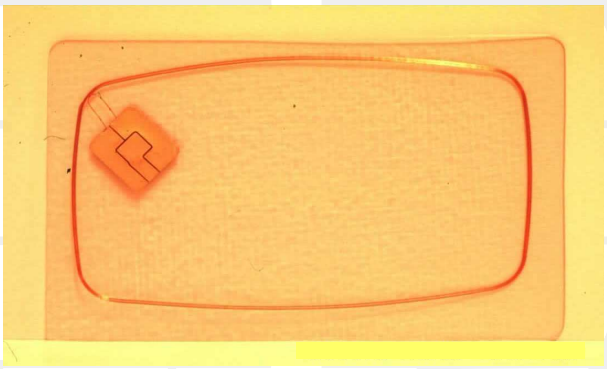
* Mot fabriqué à partir de transmettre et répondre. Appareil de réponse au signal d'un émetteur.

Différentes technologies sans contact

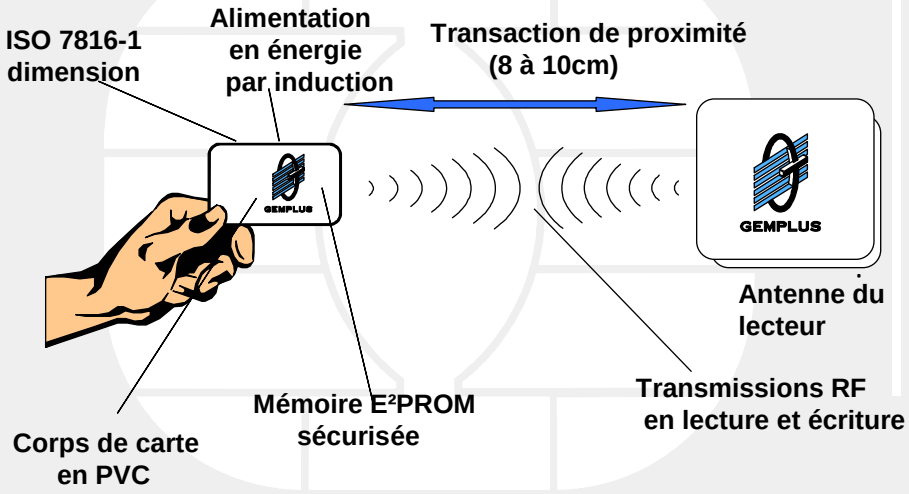
- Sans contact

- Sans contact et avec contacts

Carte échantillon



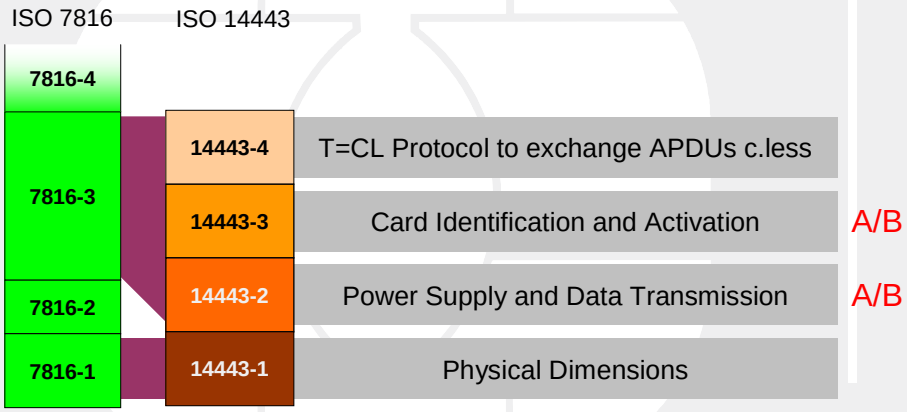
Caractéristiques des cartes sans contact



La Standardisation internationale

- La norme ISO 14443 pour les cartes de proximité regroupe les 4 parties suivantes :
  - 14443-1 : Caractéristiques physiques
  - 14443-2 : Signal radio fréquence, transfert d'énergie
  - 14443-3 : Identification et activation
  - 14443-4 : Protocole de transmission sans contact

Normes



Les 2 Interfaces RF dans le standard 14443

Type A

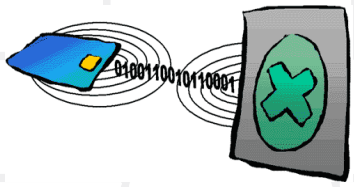
- Supporté par Philips, Siemens, Hitachi
- Mieux ciblé pour les cartes RF à logique câblée
- Standard Mifare de facto
- Applications de transport
- 106 Kbps

Type B

- Supporté par ST Micro, Inside Contactless, Motorola et Sony
- Système CALYPSO
- Davantage conçu pour les cartes à microprocesseur
- Débit plus élevé (→ 847 Kbps)

Les 2 types ne sont pas compatibles, mais l'interopérabilité est possible à travers des lecteurs multistandards (DUAL READERS)

Les 2 Interfaces RF dans le standard 14443



Type A

- Fréquence porteuse :13,56 Mhz
- Modulation lecteur --> carte (Downlink) : ASK 100%
- Codage bits : Miller modifié
- Voie montante (Uplink) carte --> lecteur : Sous-porteuse 847 khz
- Modulation de charge ASK
- Codage bits : Manchester

Type B

- 13,56 Mhz
- Modulation lecteur --> carte : ASK 10%
- Codage NRZ
- Voie montante carte --> lecteur : sous-porteuse 847 khz
- Modulation de phase BPSK
- Codage bits NRZ

Intérêt des cartes sans contact

Les cartes à contacts posent certains problèmes

- Maintenance (connecteurs)
- Coûts (encartage plus complexe)

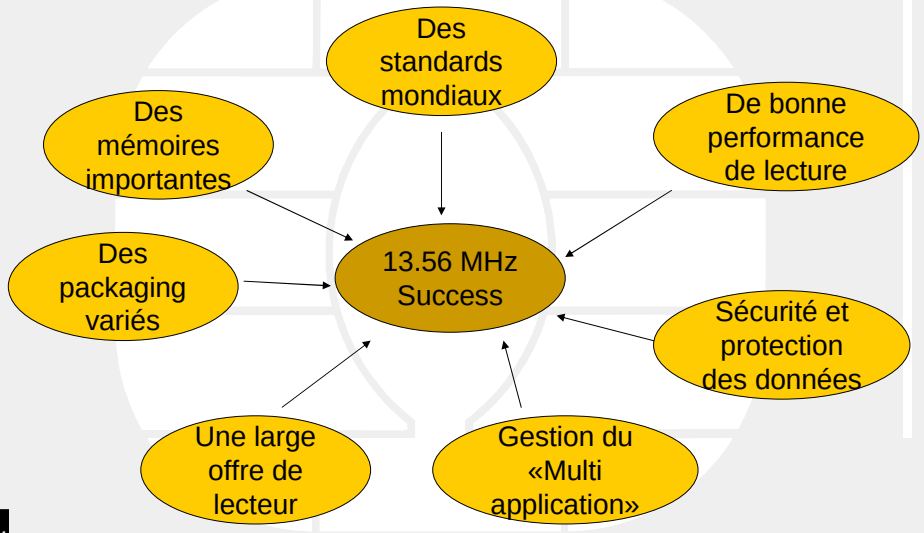
La solution : les cartes sans contact

- Pas de parties mécaniques dans les lecteurs.
- Fiabilité : Pas de dommages physiques pour la carte
- Facilité d'utilisation pour les usagers
- Vitesse de transaction optimum
- Coûts de maintenance presque nuls

Contraintes spécifiques des cartes sans contact

- Besoin d'une transaction en 150 ms (à contact jusqu'à 2s)
- Passage à la volée
- Transactions en limite de champ
- Risques de trous dans le champ
- Nécessité de technologie faible consommation

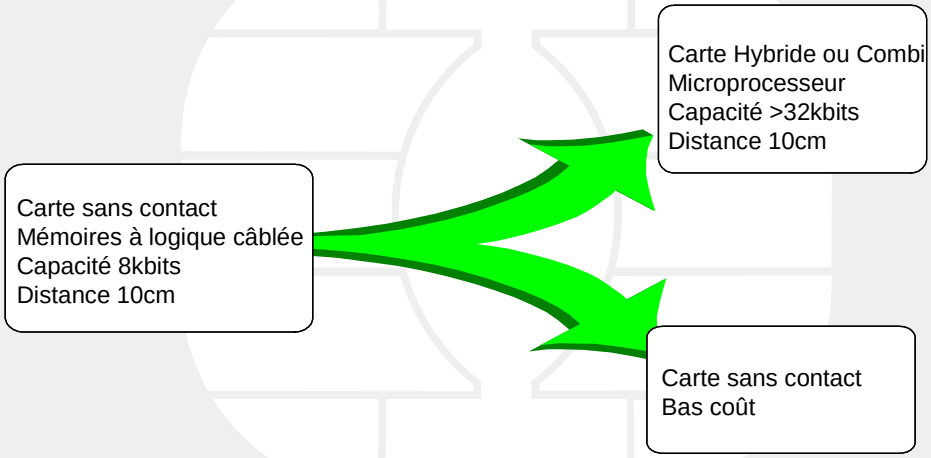
Les Raisons du succès du 13,56 Mhz



Une technologie mature

- Développée depuis plus de 10 ans
- Par de grandes sociétés de SC : Philips, Infineon
- Plus de 400 millions de puces vendues dans le monde par an
- Utilisée chaque jour dans de nombreuses applications
  - Contrôle d'accès (physique et logique)
  - Identification (carte d'étudiant, permis, etc
  - Transport
  - Paiement

Evolution des besoins

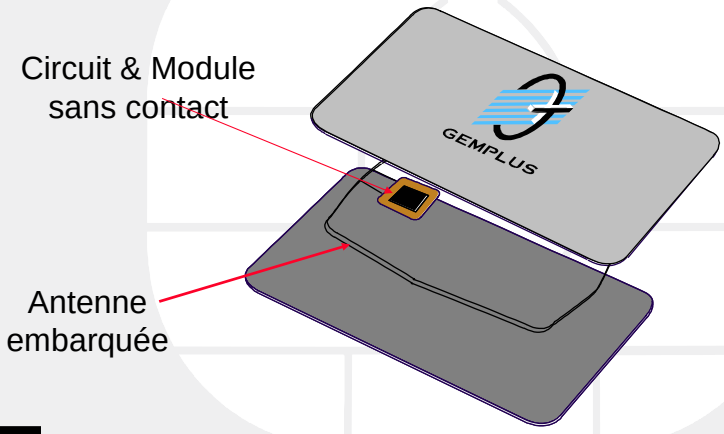


Les principaux fabricants

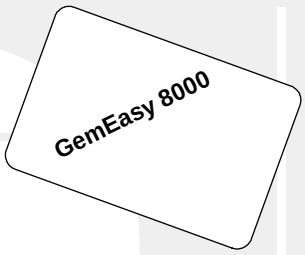
- En 2007, 4,5 milliards de cartes dont environ 15 % sans contact !
- **NXP** (lancé par Philips, est le leader mondial). (Cartes → 64 KO)
  - Mifare 1K, 4K, Mifare DESFire (3DES)
- **ASK**
  - Cartes à mémoire : CT3000 (Mifare ProX dédié au transport)
  - Cartes à microprocesseur (TanGO OS), cartes CALYPSO
- **INSIDE CONTACTLESS**
  - Picopass (2K, 32K) produit compatible avec normes 14443B et 15693
- **GEMALTO**
  - Cartes à double interface (NavigoTM
- **OBERTHUR**
  - Cartes à microprocesseur

Architecture et fonctionnement d'une carte type

GemEasy

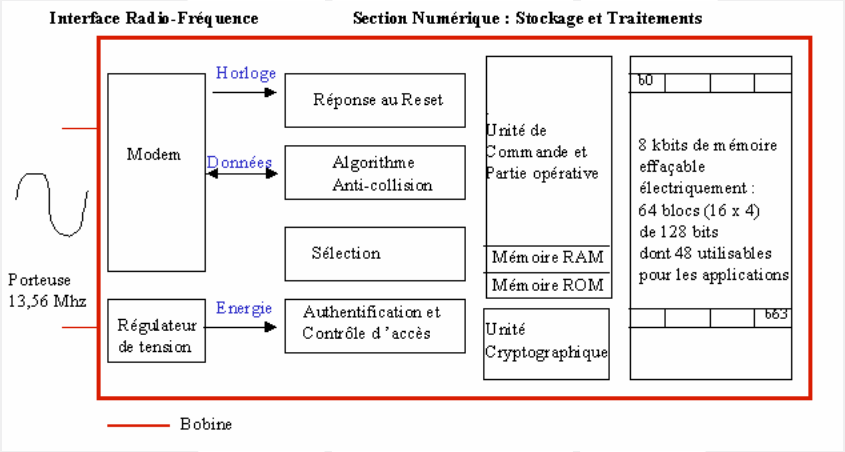


GemEasy 8000



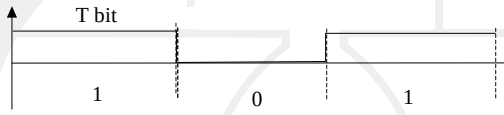
- Logique câblée (Technologie Mifare)
- Sécurité
  - Clés Secrètes (48 bits)
  - Authentification mutuelle carte-lecteur (ISO 9798-2)
  - Cryptage de l'échange
- **Multi-application**
  - 8KBit EEPROM partitionnée en 16 secteurs
  - Conditions d'accès et clés individualisées par secteur
- Gestion de porte-monnaie (Débit/Crédit)

Architecture interne de la GCL8K



Codage en bande de base (1/2)

Code NRZ

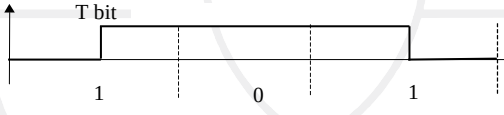


Le signal peut ne pas donner d'informations de rythme lors de longues séquences de 0 ou de 1

Code Manchester

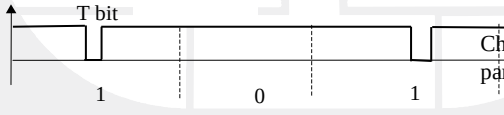
Transitions à chaque durée de bit. Extraction d'horloge facile

Code de Miller



Une transition au plus toutes les deux durées de bit. Permet la récupération du rythme

Code de Miller modifié



Chaque transition est remplacée par une transition négative (tp<<Tbit)

Codage en bande de base (2/2)

- **Code NRZ** : Le 1 binaire est représenté par un signal haut et le 0 par un signal bas
- **Code Manchester** : Le 1 est représenté par une transition négative au milieu de la période bit et le 0 est représenté par une transition positive.
- **Code Miller** : Le 1 est représenté par une transition de type quelconque au milieu de la période bit. Le 0 est représenté par la continuité du niveau 1 précédent pour la période bit suivante. Une suite de 0 crée une transition au départ d'une période bit.
- **Code Miller modifié** : Chaque transition est remplacée par une impulsion négative. Ceci permet d'assurer une alimentation en énergie du transpondeur par le lecteur même pendant les transferts de données.

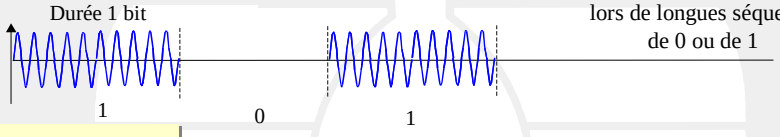
Procédés de modulation

- L'énergie est propagée depuis une antenne sous la forme d'ondes électromagnétiques. La modulation d'une porteuse par un des 3 paramètres du signal (Amplitude, fréquence ou phase) permet de coder et transmettre des messages à l'intérieur d'une zone d'influence.
- Les procédés de modulation utilisés sont :
  - ASK (Amplitude Shift Keying) : Modulation d'amplitude
  - FSK (Frequency Shift Keying) ou MDF (Modulation par déplacement de fréquence)
  - BPSK (Binary Phase Shift Keying) ou MDP (Modulation par déplacement de phase)
  - Modulation procedure with subcarrier (Load Modulation) ou modulation de charge

Codage et modulation

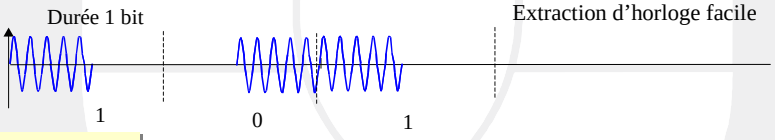
Code NRZ

Le signal peut ne pas donner d 'informations de rythme lors de longues séquences de 0 ou de 1



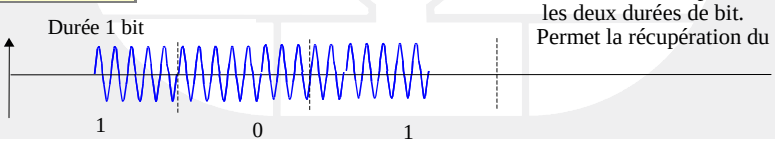
Code Manchester)

Transitions à chaque durée de bit. Extraction d'horloge facile



Code de Miller

Une Transition au plus toutes les deux durées de bit. Permet la récupération du rythme



J. Leroux Les Jardins (leroux@enst.fr)

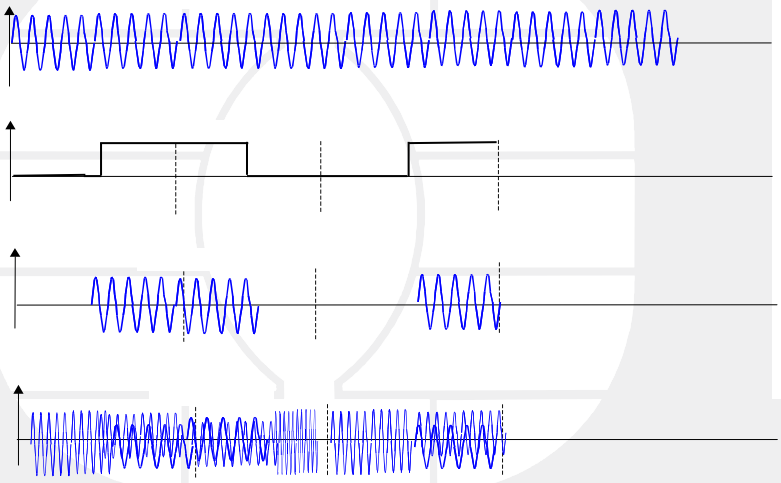
Modulation de charge (Carte vers lecteur)

Sous porteuse

Flux de données (Bande de base)

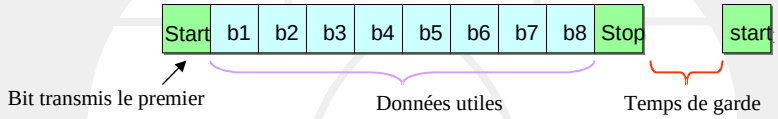
Sous porteuse modulée

Signal modulé avec sous porteuse



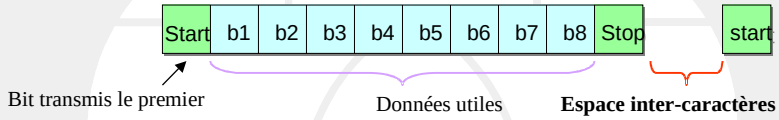
J. Leroux Les Jardins (leroux@enst.fr)

Format de transmission des données



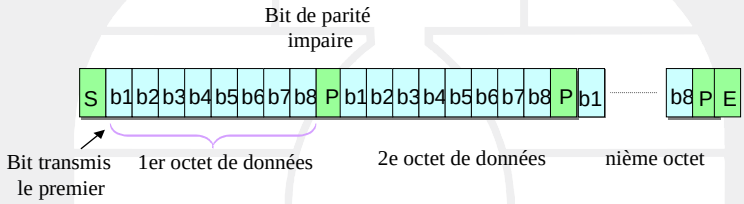
- Le format utilisé pour la transmission et la réception de données entre la carte et le lecteur est le suivant :
  - Un bit de Start à l'état bas
  - 8 bits de données transmis les poids faibles en tête
  - Un bit d'arrêt à l'état haut
- La transmission d'un octet nécessite 10 temps élémentaires (10 ETU)
  - Remarque : 1 etu (elementary time unit) = 128/fréquence porteuse
  - Avec 13,56 Mhz, 1 etu = 9,4µs

Format de transmission des données (1/2)



- Un caractère est séparé du suivant par un temps de garde EGT (Extra Guard Time)
- L'espace EGT entre 2 caractères consécutifs envoyés par le lecteur à la carte peut varier entre 0 et 6 ETU
- L' espace EGT entre 2 caractères consécutifs envoyés par la carte au lecteur peut varier entre 0 et 2 ETU

La trame standard transmise (2/2)

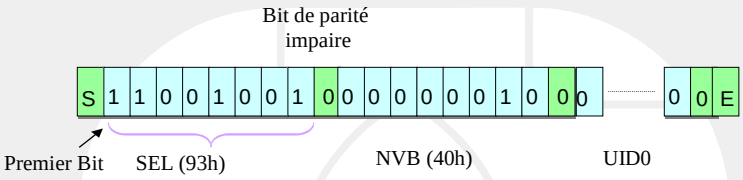


- Les trames standards sont utilisées pour l'échange des données. Elles contiennent des trames de données suivies d'une trame CRC (format bloc) :
  - Un bit de début de communication (Start) à l'état bas.
  - N fois (8 bits de données + bit de parité impaire). La transmission de chaque octet commence par le bit de plus faible poids (lsb)
  - Un bit de fin de communication (End) à l 'état haut.

Délimiteurs de trames

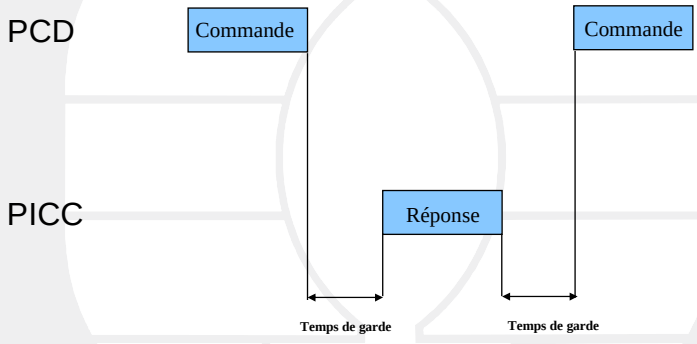
- Les commandes envoyées par le lecteur sont transportées par les trames (Composées de caractères de données suivies des trames CRC).
- Les trames utilisées dans les deux sens (Transmission et réception entre lecteur et carte) pendant la séquence d'anticollision utilisent les identifiants SOF et EOF pour les deux sens de communication.

La trame anticollision



- Les trames anti-collision sont des trames standards de 7 octets utilisées pendant la boucle anticollision . Elles sont divisées en deux parties :
  - Partie 1 pour la transmission du lecteur à la carte.
  - Partie 2 pour la transmission de la carte au lecteur
  - Trois règles s'appliquent :
    - La somme des bits de données doit être 56
    - La longueur minimum de la partie 1 doit être 16 bits
    - La longueur maximum de la partie 1 doit être de 55 bits : En conséquence la partie 2 a une longueur minimum de 1 bit et maximum de 40 bits.

Protocole Lecteur-carte



PCD : Proximity Coupling Device : Lecteur

PICC : Proximity Integrated Circuit Card : Carte

Les états de la carte

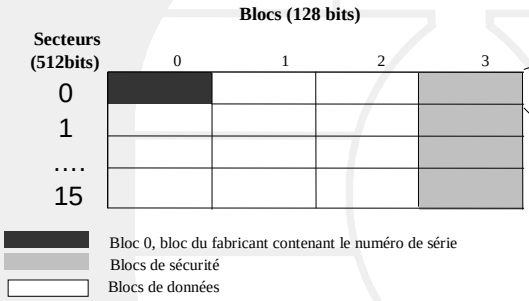
- Les états suivants sont définis pour les cartes qui suivent la spécification A et le protocole associé pour l'anticollision
  - **Etat Power-off** : La carte n'est pas alimentée et n'émet pas de sous porteuse
  - **Etat Idle (Attente)** : La carte est alimentée. Elle est capable de reconnaître des commandes de lecteur comme REQA et WAKE-UP. Etat qui suit un Reset.
  - **Etat Ready** : Etat suite à réception d'une commande valide REQA et WAKE-UP. La carte est sélectionnée avec son UID (Byte number of Unique Identification). La méthode anti-collision peut être appliquée.
  - **Etat Active** : Etat correspondant à la sélection de la carte avec son UID complet
  - **Etat Halt** : La carte est muette. Suite à une commande Halt, la carte peut devenir inactive. Une carte dans cet état requiert un Reset pour retourner dans l'état IDLE

Les commandes utilisées par le lecteur pour gérer la communication multicartes

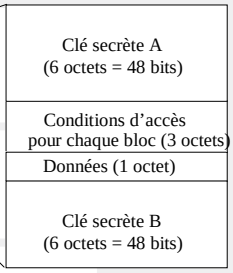
- REQA : les cartes concernées répondent avec ATQA (codage de type anticollision applicable sur 2 octets). Le lecteur réalise un OU logique entre les réponses ATQA.
- WAKE-UP
- ANTICOLLISION
- SELECT
- HALT

ORGANISATION MEMOIRE DE LA CARTE SANS CONTACT

Organisation de la mémoire EEPROM 8kbits



Organisation de la mémoire EEPROM en 16 secteurs



Organisation du bloc sécurité

Définitions

- Taille de la mémoire : 1 kilo-octets
- La carte est divisée en 16 secteurs
  - 1 secteur = 4 blocs de données = 64 octets (512 bits)
  - 1 bloc de données = 16 octets (128 bits)
- **Le bloc est le plus petit élément adressable**

Les Secteurs

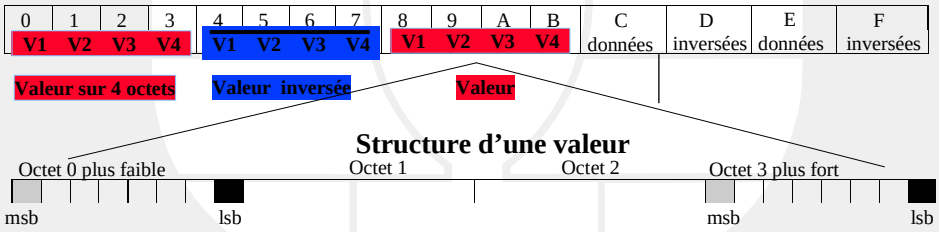
- Chaque secteur est divisé en 4 blocs
  - 3 blocs de données (Blocs 0 à 2)
  - 1 bloc de sécurité (Bloc 3)
    - Les clés et les conditions d'accès sont propres à chaque secteur
- **Les conditions d'accès sont définies bloc par bloc et stockées dans le bloc sécurité**

Les blocs de données

- **Blocs transparents**
  - Les données lues ou écrites ne sont pas interprétées par la carte
- **Blocs valeurs**
  - Format spécial de codage dédié aux fonctions de porte monnaie électronique

Les blocs de valeur

- Le champ valeur est codé sur 4 octets
  - Stocké 2 fois en codage classique et une fois en inversé.
  - Ordre des octets inversé
- Le champ données (un octet) n'est pas interprêté par la carte



Exemple de blocs de valeur

Exemple : Le bloc suivant contient la valeur 1 et l'octet de données 01 en hexadécimal

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
01	00	00	00	FF	FF	FF	FF	01	00	00	00	données	données	données	données

Exemple : Le bloc suivant contient la valeur 12 34 56 78

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
78	56	34	12	87	A9	CB	ED	78	56	34	12	données	données	données	données

Le bloc 0 (16 octets) : bloc fabricant

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Numéro de série				Lrc	Données circuit				Numéro de lot			Date de production			

- Numéro de série sur 4 octets. (CSN Chip Serial Number)
- Longitudinal Redundancy Check : Checksum sur le numéro série
- Données circuit. Ex 08 : 8 kbits, 04 00 : type de circuit, 43 : version.
- Les octets 00 à 08 sont envoyés à l'extérieur de la carte lors de la réponse au Reset.

Gestion de la sécurité

Sécurité

- **Chaque secteur est protégé indépendamment**
- Chaque bloc dans un secteur a ses propres conditions d'accès
- L'authentification par secteur implique les dispositions suivantes :
  - 2 clés (A et B) stockées dans chaque secteur
  - 2 clés (A et B) stockées dans le lecteur pour chaque secteur
  - Calcul d' un cryptogramme utilisé pour prouver que le lecteur et la carte détienne le même secret.
- **Echanges chiffrés :**
  - La communication entre la carte et le lecteur est cryptée par la clé de session générée après l'authentification

Bloc de sécurité (Bloc 3 du secteur)

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Clé secrète A						Conditions Accès				Clé secrète B					

- **Le bloc de sécurité de chaque secteur contient :**
  - La clé secrète A sur 6 octets (48 bits)
  - Les conditions d'accès sur 3 octets
  - 1 octet de données
  - La clé secrète B sur 48 bits
- **Les conditions d'accès sont définies pour chaque bloc**

Définition des conditions d'accès

- Les conditions d'accès sont définies pour chaque bloc
- Pour chaque bloc, elles sont stockées dans le secteur de sécurité
- Les conditions d'accès sont définies :
  - Par bloc de données (transparent ou valeur)
  - Pour le bloc de sécurité lui-même
- Huit jeux de conditions d'accès sont disponibles pour les 4 commandes Read/Write/Add/Substract (Pour les blocs valeurs seulement)

Conditions d'accès pour les blocs de données

BxACn **x : numéro du bloc (0 <= x <= 3)** **n : numéro du bit (1 <= n <= 3)**

N°AC	BxAC1 (0<=x<=2)	BxAC2	BxAC3	Lecture	Ecriture	Addition transf./sauveg	Soustraction transf./sauveg
0	0	0	0	A ou B	A ou B	A ou B	A ou B
1	0	0	1	A ou B	jamais	jamais	A ou B
2	0	1	0	A ou B	jamais	jamais	jamais
3	0	1	1	B	B	jamais	jamais
4	1	0	0	A ou B	B	jamais	jamais
5	1	0	1	B	jamais	jamais	jamais
6	1	1	0	A ou B	B	B	A ou B
7	1	1	1	jamais	jamais	jamais	jamais

Conditions d'accès pour les blocs de sécurité

Clef secrète A (octets 0 à 5)		Conditions d'accès (octet 6 à 8) + octet 9		Clef secrète B (octet 10 à 15)		Valeur des bits de condition d'accès		
lecture	écriture	lecture	écriture	lecture	écriture	B3AC1	B3AC2	B3AC3
jamais	A ou B	A ou B	jamais	A ou B	A ou B	0	0	0
jamais	A ou B	A ou B	A ou B	A ou B	A ou B	0	0	1
jamais	jamais	A ou B	jamais	A ou B	jamais	0	1	0
jamais	B	A ou B	B	jamais	B	0	1	1
jamais	B	A ou B	jamais	jamais	B	1	0	0
jamais	jamais	A ou B	B	jamais	jamais	1	0	1
jamais	jamais	A ou B	jamais	jamais	jamais	1	1	0
jamais	jamais	A ou B	jamais	jamais	jamais	1	1	1

Exemple de conditions d'accès (p11)

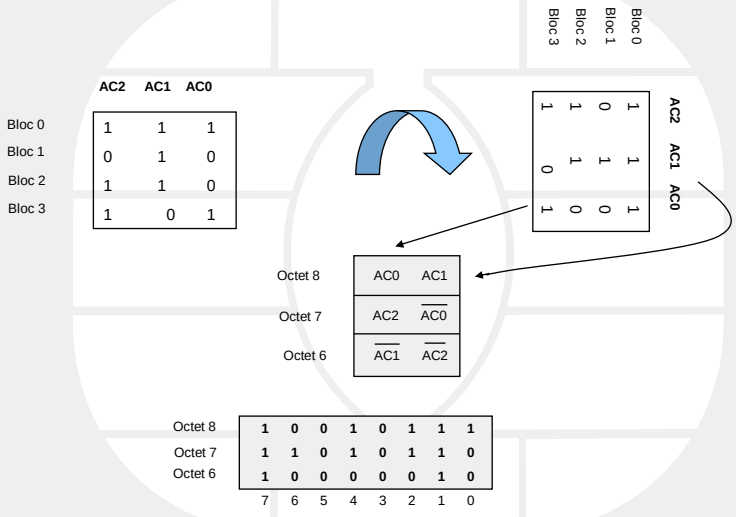
- Conditions d'accès lors du transport :
  - **AC1,AC2,AC3 = (0,0,0) pour les blocs mémoire**
  - Accès aux blocs mémoire pour toutes les fonctions
  - **AC1,AC2,AC3 = (0,0,1) pour le bloc de sécurité**
  - Accès à la clef A en écriture
  - Accès au reste du bloc de sécurité en lecture et écriture

Octet	Bits	Bloc 3	Bloc 2	Bloc 1	Bloc 0
6	de 3 à 0	1	1	1	1
	de 7 à 4	1	1	1	1
7	de 3 à 0	**0**	**1**	**1**	**1**
	de 7 à 4	0	0	0	0
8	de 3 à 0	**0**	**0**	**0**	**0**
	de 7 à 4	**1**	**0**	**0**	**0**

Octets 6,7, 8

FF 07 80

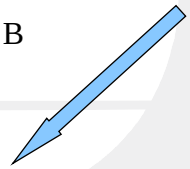
Calcul des conditions d'accès



Conditions d'accès pour le transport au niveau carte

- Pour tous les blocs de données (0 à 2)
  - Condition d'accès n°0
    - Toutes opérations protégées par clé A ou B
- Pour tous les blocs de sécurité (bloc 3)
  - Condition d'accès n°1
    - Toutes opérations protégées par clé A ou B
- Mêmes clés pour tous secteurs

	AC2	AC1	AC0
Bloc 0	0	0	0
Bloc 1	0	0	0
Bloc 2	0	0	0
Bloc 3	0	0	1



Octets 6, 7 et 8 : FF 07 80

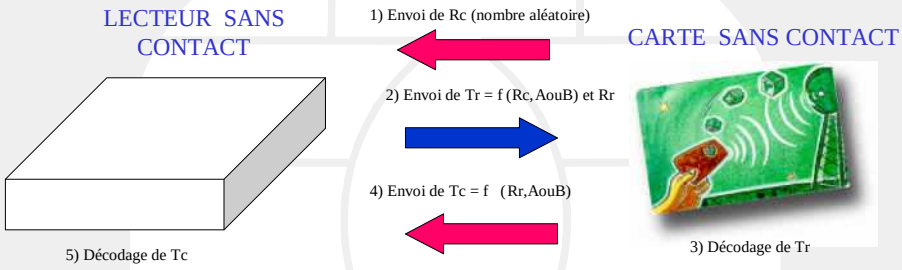
La procédure d'authentification

- **Nécessaire pour accéder à un secteur**
- Permet de prouver la possession d'une clé (Dans la carte et dans le lecteur)
- L'authentification se fait en trois passes (ISO 9798-2)
- Les clés secrètes ont une taille de 48 bits
- Utilisation de nombres aléatoires
- Etablissement d'une clé de session (clé de chiffrement de la communication)

Schéma d'authentification

- **COMMANDE**
  - 1 Authenticate (Secteur, clé)
  - 3 Calcul de ResR1 = F (Rc,clé) Envoi de ResR1 et RandomRr
  - 6 Calcul ResR2 = F(Rr,clé), Test si ResR2 = ResC2
  - 7 Génération de la clé de session de chiffrement = CF (Rc,Rr,clé)
- **REPONSE DE LA CARTE**
  - 2 Génération de RandomRc
  - 4 Calcul ResC1 =F(Rc,clé),Test si ResR1 = ResC1
  - 5 Calcul de ResC2 = F (Rr,clé) et envoi
  - 8 Génération de la clé de session de chiffrement = CF (Rc,Rr,clé)

L'authentification mutuelle carte-lecteur



1) La carte envoie sur demande un nombre aléatoire Rc au lecteur
2) Le lecteur encrypte à l'aide d'une clé (A ou B) ce nombre Rc . Le jeton (token) obtenu Tr est envoyé à la carte avec Rr.
3) La carte vérifie qu'on lui a bien envoyé le Rc initial.
4) La carte encrypte à l'aide d'une clé (A ou B) le nombre aléatoire Rr et l'envoie au lecteur
5) Le lecteur vérifie qu'il est capable de retrouver le nombre aléatoire utilisé. L'authentification est alors considérée comme réussie !

Durée de l'opération : 3 ms

L'authentification se fait secteur par secteur.

Avantages de la procédure d'authentification mutuelle

- Deux nombres aléatoires sont encryptés simultanément. Ceci permet d'empêcher de procéder à la transformation inverse utilisant Rc pour obtenir le cryptogramme 1 dans le but de calculer la clé secrète.
- L'usage strict de nombres aléatoires provenant de sources indépendantes (lecteur et carte) signifie que l'enregistrement d'une séquence d'authentification pour la rejouer plus tard est vouée à l 'échec
- Une clé de session (aléatoire) peut être calculée à partir des nombres aléatoires générés pour sécuriser par chiffrement la transmission.

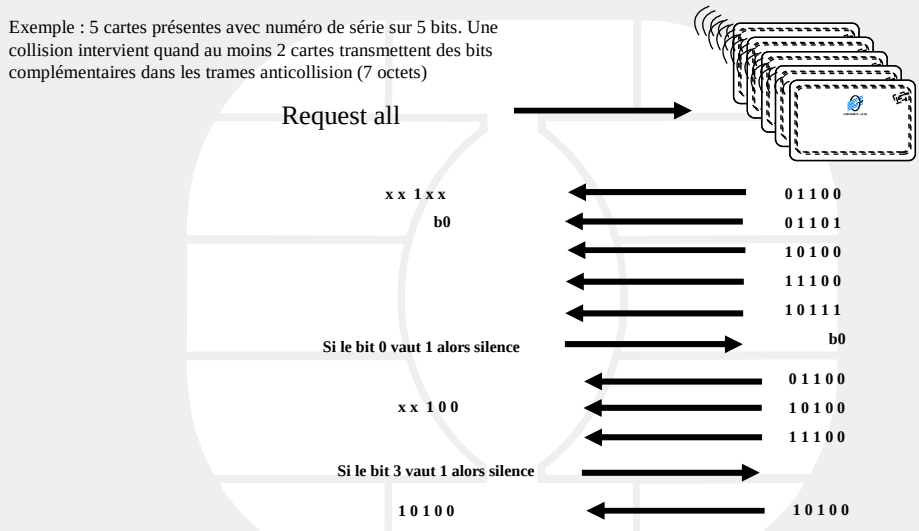
Caractéristiques particulières de la carte sans contact

Présence de plusieurs cartes

- Algorithme d'anti-collision
  - Gestion de plusieurs cartes en même temps
  - Inhibition des lectures ou écritures accidentelles
  - Lecture-écriture dynamique (Carte entrante ou sortante du champ)

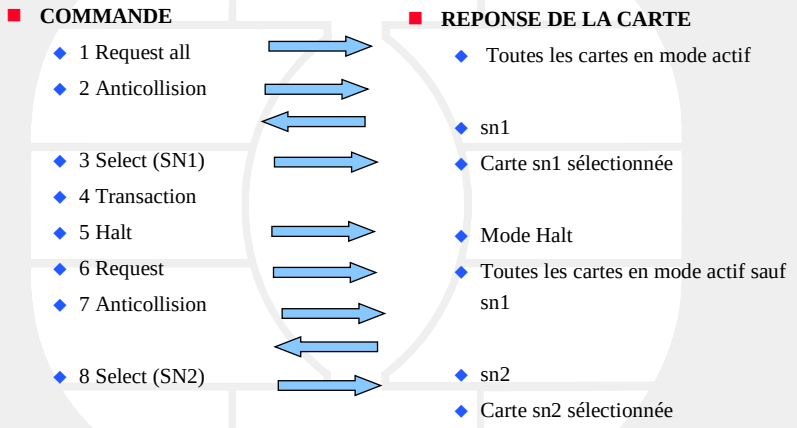
Mécanisme d'anti-collision

Exemple : 5 cartes présentes avec numéro de série sur 5 bits. Une collision intervient quand au moins 2 cartes transmettent des bits complémentaires dans les trames anticollision (7 octets)



Une seule carte répond : elle est sélectionnée

Protocole en présence de plusieurs cartes

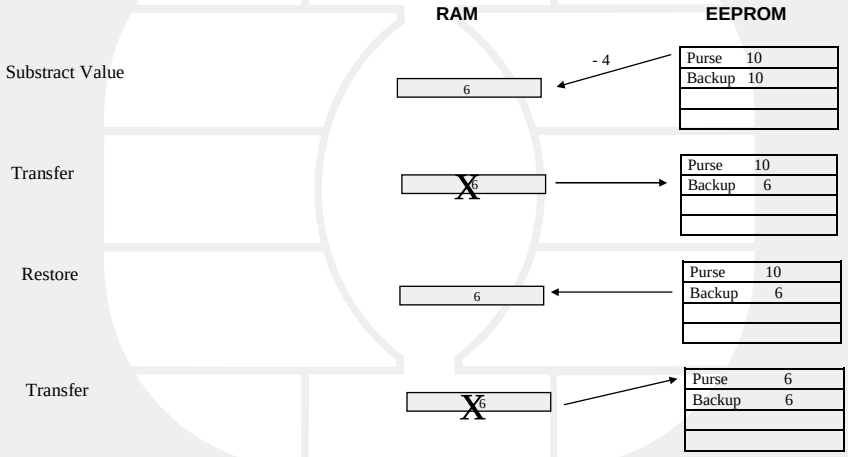


Fonctions Blocs valeurs

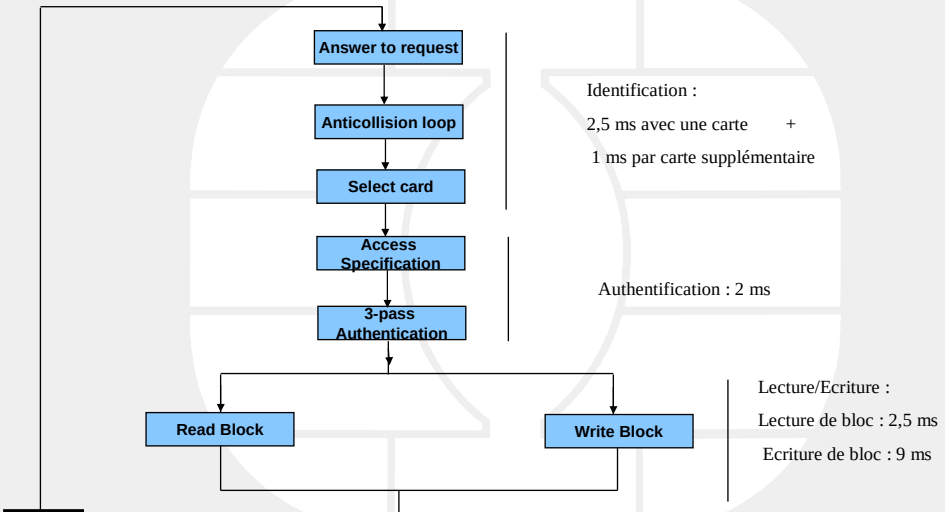
- **Substract Value et Add Value**
  - Ajoute ou soustrait la valeur spécifiée à la valeur mémoire destination
  - Le résultat est stocké dans le registre RAM de la carte
  - Le bloc mémoire destination n'est pas affecté
- **Transfer**
  - Place la valeur du registre RAM dans le bloc mémoire EEPROM spécifié
- **Restore**
  - Place la valeur issue du bloc mémoire EEPROM spécifié en RAM

Procédure de sauvegarde (Back up)

- Exemple : Valeur de départ : 10 Soustrait 4



Séquencement et temps d'une transaction

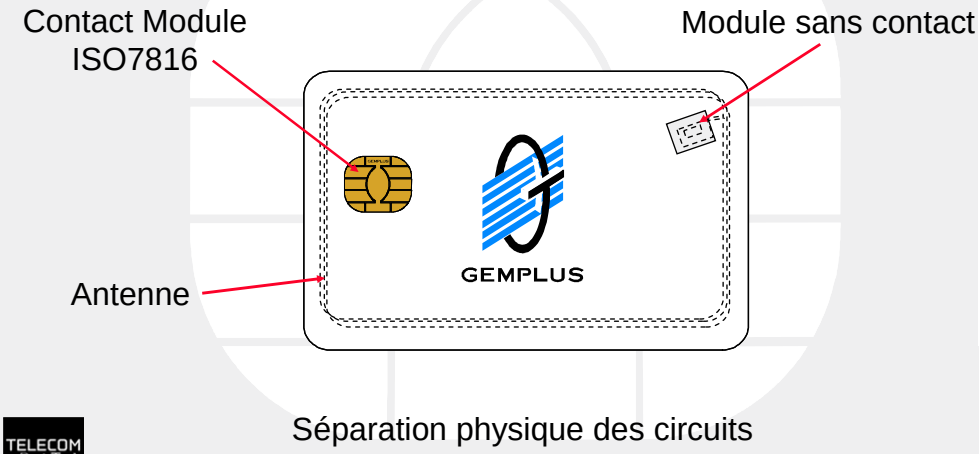


Temps de transaction

- Request, Anticollision, Select 3 ms
- Authentication 2 ms
- Read Block 2.5 ms
- Write Block + verify 9 ms

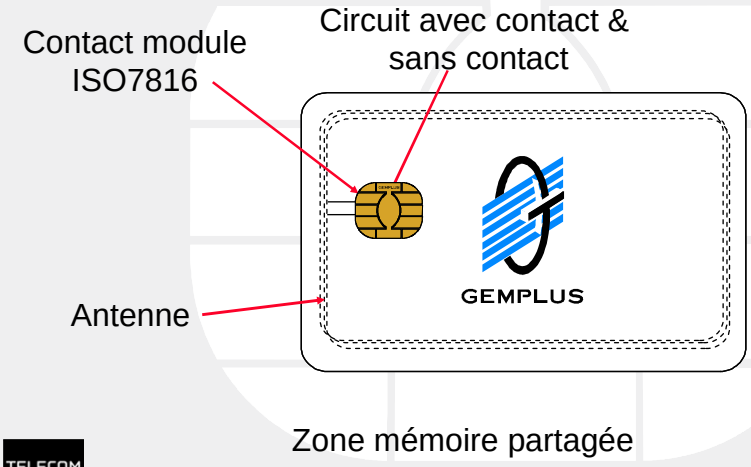
Ces temps n'incluent pas la communication et les traitements du terminal.

GemTwin (cartes hybrides)



Séparation physique des circuits

GemCombi



Evolution de la technologie Combi

Mifare+

- Premier circuit **Combi** disponible sur le marché :
  Deux mémoires séparées :
  - Une privée pour contact
  - Une partagée pour contact & sans contact
  - Bon compromis entre sécurité & vitesse

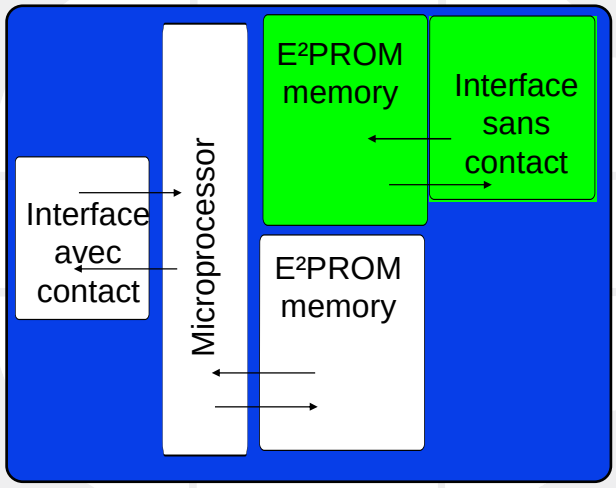
Moto, ST, Mifare Pro, ...

- Tous les circuits **Combi** suivants

  Mémoire unique toujours accessible via le µprocesseur

  - Niveau de sécurité ajustable au prix de la rapidité de la transaction

MIFARE + (Combi 1G)

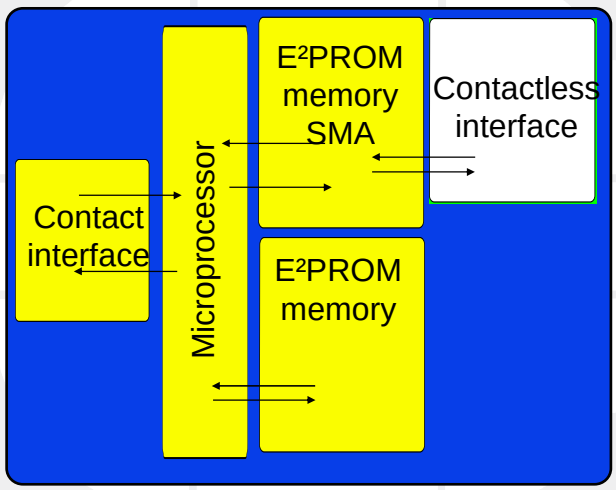


Compatible

ISO 7816

ISO 14443 - A
Compatible avec les cartes Mifare : Gamme GemEasy

MIFARE + type 1 (Combi 1G)



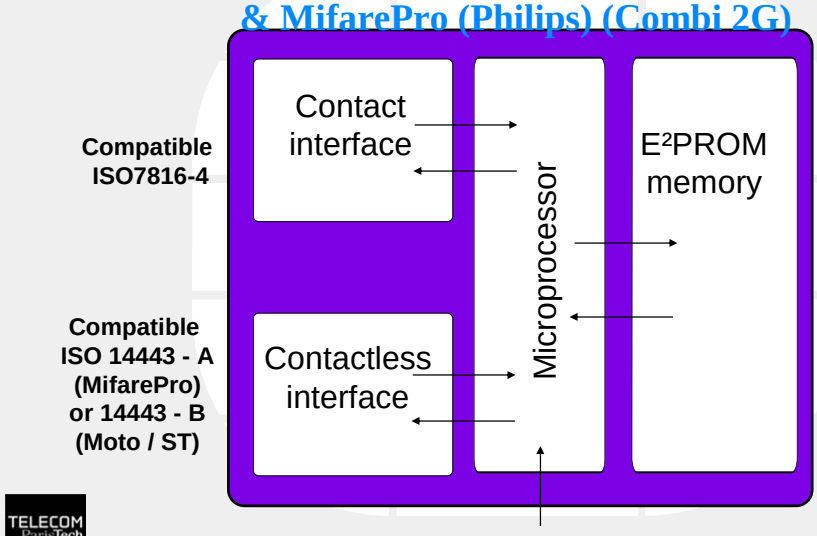
Compatible

ISO 7816

ISO 14443 - A
Compatible avec les cartes Mifare : Gamme GemEasy

icroprocesseur Siemens 8051 pour l'interface contact. Interface sans contact géré par une logique câblée

Mirage (Moto), ST16RFXX(SGS-Thomson) & MifarePro (Philips) (Combi 2G)



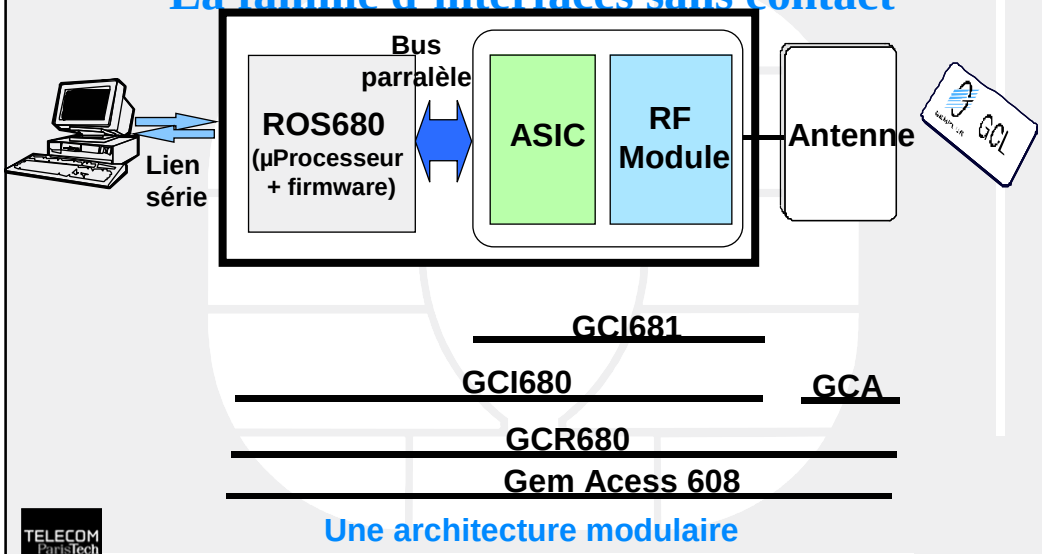
Compatible ISO7816-4

Compatible ISO 14443 - A (MifarePro) or 14443 - B (Moto / ST)

ISO 14443 - B Compatible avec les cartes Mifare : Gamme GemEasy

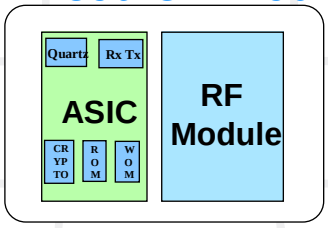
Architecture du lecteur

La famille d'interfaces sans contact



Une architecture modulaire

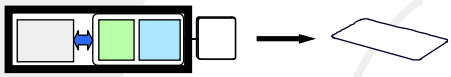
ASIC - Module RF du lecteur



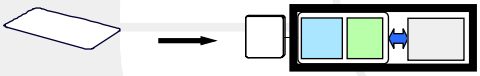
- **ASIC**
  - Oscillateur à Quartz à 13,56 Mhz
  - Module Emetteur Récepteur avec lien série avec le module RF
  - Unité cryptographique (authentification et cryptage)
  - ROM (Read Only Memory)
  - WOM (Write Only Memory)
- **Module Radio Fréquence**
  - Transmetteur pour l'énergie et la transmission de données
    - Fréquence de la porteuse 13,56 MHZ
    - Utilisée pour transmettre énergie, données et horloge
  - Récepteur pour recevoir les réponses de la carte

Interface Radio Fréquence

Modulation OOK (On Off Keying) du lecteur vers la carte



Modulation de charge de la carte vers le lecteur



Compatible avec le standard ISO 14443 type A

Fréquence de la porteuse : 13,56 Mhz

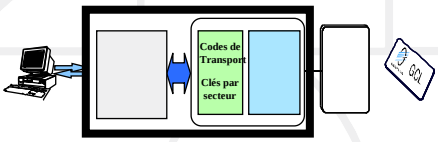
Protocole de communication

- Contrôlé par le circuit ASIC du lecteur
  - Protocole de communication à l'alternat (half duplex)
  - Utilise un mécanisme de poignée de main
    - mécanismes de contrôle utilisé :
      - CRC 16
      - Analyse du flux de données (Bit de parité)
      - Monitoring de la séquence protocole (Compteur de bits)
  - Vitesse de transmission des échanges de données par voie Radio fréquence : 106 kilobits/s

GCR 680 Firmware

- Protocole de type Bloc Gemplus
- Basé sur le noyau OROS
- ROS 680
  - Commandes au niveau carte (Read, Add-value)
  - Commandes combinées (haut niveau) : C-write
    - Pour s'adapter à la vitesse de transmission de l'interface
    - Pour faciliter la programmation d'applications
  - Commandes au format APDU : Request, Select

Gestion de la sécurité : codes de transport lecteur



ASIC

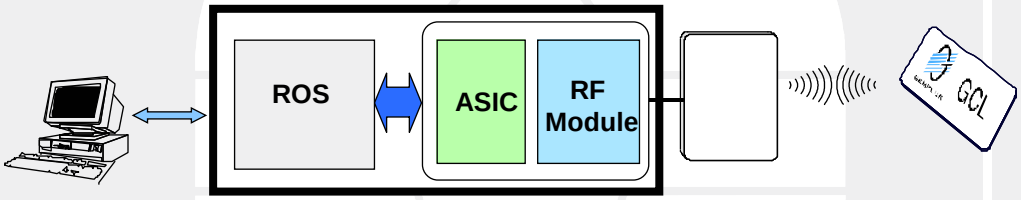
- Les clés sont stockées dans la mémoire WOM de l'ASIC
- Protégées par des clés de transport avant le chargement des clés
  - **Une clé de transport par secteur**
  - Les clés de transport sont stockées dans la ROM de l'ASIC
  - Les clé de transport et les clés doivent être présentées ensemble pour charger les clés dans la WOM
- Tous les lecteurs ont les mêmes codes de transport
- Une valeur de code de transport par secteur : 16 valeurs
- Exemple pour le secteur 0 : BD DE 6F 37 83 83

Stockage des Jeux de clés

- **ROM** : Jeu fixé de 16 codes de transport
  - Non accessible de l'extérieur de l'ASIC
  - 1 code de transport par secteur
  - Les codes de transport sont requis pour charger les clés en WOM
- **WOM :** (Write Only Memory) pour le stockage des clés
  - 16 jeux de 3 paires de clés
  - Les données WOM sont volatiles. Elles requièrent des piles dans le lecteur.
- paires de clés A ou B par secteur
- Peut être utilisé pour avoir différentes versions de clés
  - Prototype
  - Test
  - Application finale

Jeu de commandes

Les échanges



Echange d'APDU
Commandes haut niveau

Contrôle de la communication entre le lecteur et la carte

Commandes bas niveau

TYPE DE COMMANDES

Commandes de configuration du lecteur	Commandes de l'interface ASIC	Commandes APDU Elémentaires (Pas d'authentification)	Commandes APDU Combinées (Authentification en option)
Configure SIO RF On RF Off RF Switch	Reset Get Card Get FirstCard Request Request all Anticollision Select RequestAll&Select Halt Exchange APDU Load Key	Authenticate Transfer Restore AddValue SubstractValue Read Write	C_Read C_Write C_ReadValue C_CopyValue C_AddValue C_SubstractValue C_CreateValue

Mode d'adressage pour les commandes

■ Secteur 0	Bloc 0	(16 octets)	Adresse 0
	Bloc 1	(16 octets)	Adresse 1
	Bloc 2		Adresse 2
	Bloc 3	Sécurité	Adresse 3
■ Secteur 1	Bloc 0		Adresse 4
	Bloc 1		Adresse 5
	Bloc 2		
	Bloc 3	Sécurité	
■ Secteur 15	Bloc 0		
	Bloc 1		
	Bloc 2		Adresse 62
	Bloc 3	Sécurité	Adresse 63

Commandes de configuration du lecteur

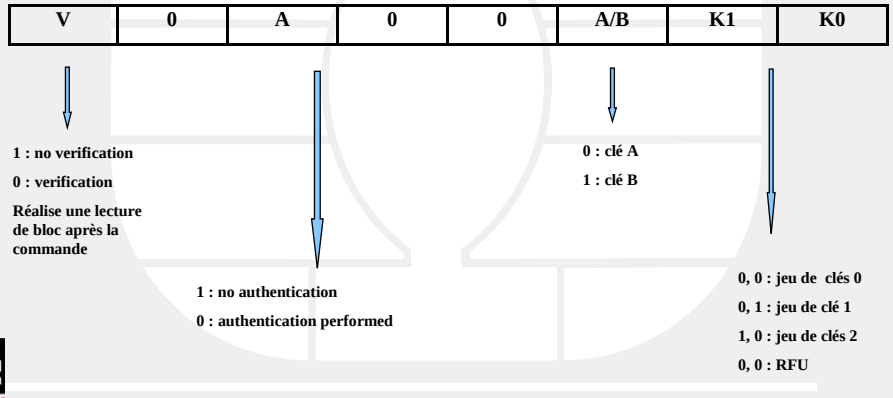
- **Configure SIO** : Spécifie la vitesse du lien série entre le terminal et le lecteur.
- **RF On** : Met en marche l'émetteur RF
- **RF off** : Met hors service l'émetteur RF
- **RF Switch** : Pour piloter deux antennes

Commande de l'interface (I)

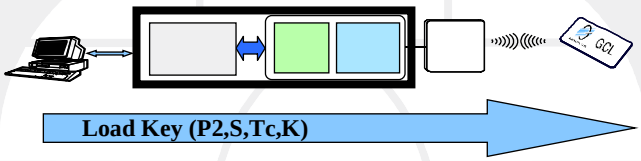
- Echange APDU : Sert à envoyer une commande d'interface à une carte et à recevoir une réponse : (Ex Select)
  - Format utilisé : Application Protocol Data Unit
  - Compatible avec le standard ISO 7816-4
- Load Key : Charge une clé secrète dans la mémoire WOM de l'ASIC

Authentication Mode Control Byte (S)

- Cet Octet S de commande du mode d'authentification est utilisé dans toutes les commandes qui comprennent une authentification



Load Key



Charge une clé secrète à partir de l'application dans la mémoire WOM de l 'ASIC du GCR 680.
Chargement de la clé secrète K et du code de transport correspondant

P2 : Adresse du bloc protégé par la clé à charger.
S : Octet
Données : contiennent K et TC (Chacune sur 6 octets).

Syntaxe :

CLA	INS	P1	P2	LC	Data
90	D8	00	P2	13	S TC K

Commande de l'interface (II)

- **Reset**
- **GetFirstCard**
  - (Reset, Requestall, Anticollision, Select)
- **GetCard**
  - (Halt, Request, Anticollision, Select)

Commande de l'interface (III)

- **Request all :** Place toutes les cartes en mode actif et reçoit leur numéro de série
- **Request :** Place en mode actif toutes les cartes qui ne sont pas en mode HALT et reçoit leur numéro de série
- **Anticollision :** Isole un numéro de série parmi les cartes activées
- **Select :** Sélectionne une carte en fonction de son numéro de série
- **Halt :** Place les cartes en mode arrêt

Commandes au niveau Carte

Commandes au niveau carte (1/2)

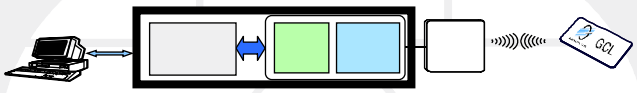
- **Authenticate :** Réalise une authentification mutuelle dynamique
- **Read :** Lit les données stockées dans un bloc
- **Write :** Ecrit les données dans un bloc

Commandes au niveau carte (2/2)

- **Transfer :** Envoie le contenu d'un registre RAM dans un bloc mémoire EEPROM
- **Restore :** Copie un bloc mémoire EEPROM dans un registre RAM
- **AddValue :** Ajoute la valeur du contenu d'un bloc mémoire EEPROM et écrit le résultat dans un registre RAM
- **SubstractValue :** Soustrait la valeur du contenu d'un bloc mémoire EEPROM et écrit le résultat dans un registre RAM

Voir T55

Authenticate



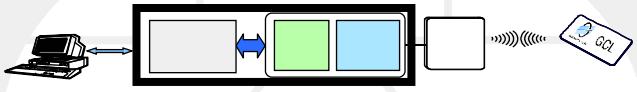
Authenticate (P2,S)

Produit une authentification mutuelle entre la carte et le lecteur.
P2 correspond à l 'adresse du bloc à authentifier. S est l 'octet de commande du mode d'authentification

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	26	00	P2	01	S

Transfer



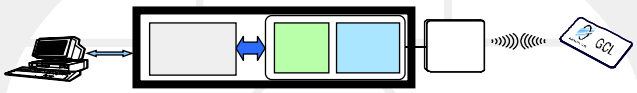
Transfer (P2)

Transfère le contenu de la RAM dans l 'EEPROM à l'adresse spécifiée.
La valeur est effacée de la RAM

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	DA	00	P2	01	00

Restore



Restore (P2)

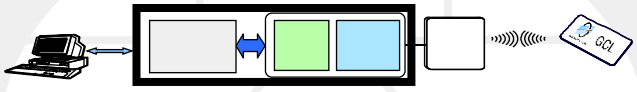
Copie le contenu d'un bloc de l'EEPROM à l'adresse spécifiée. vers la RAM. P2 adresse du bloc à restaurer**.**

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	8A	00	P2	01	00

J. Leroux Les Jardins (leroux@enst.fr)

AddValue



AddValue (P2,Count)

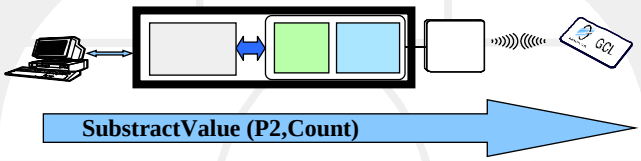
Lit la valeur de l'EEPROM à l'adresse spécifiée dans la RAM. Additionne Count à la valeur lue. Ecrit le résultat dans le registre RAM. Note : la valeur stockée en EEPROM n'est pas modifiée.
P2 : Adresse du bloc contenant la valeur.
Count : Montant à additionner.

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	36	00	P2	04	Count

J. Leroux Les Jardins (leroux@enst.fr)

SubstractValue



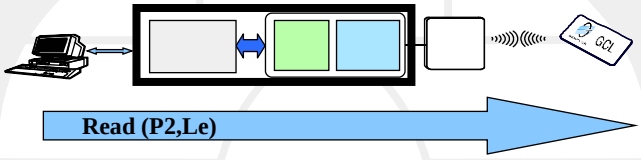
SubstractValue (P2,Count)

Lit la valeur de l'EEPROM à l'adresse spécifiée dans la RAM.
Soustrait Count à la valeur lue. Ecrit le résultat dans le registre RAM.
Note : la valeur stockée en EEPROM n'est pas modifiée.
P2 : Adresse du bloc contenant la valeur.
Count : Montant à soustraire.

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	34	00	P2	04	Count

Read



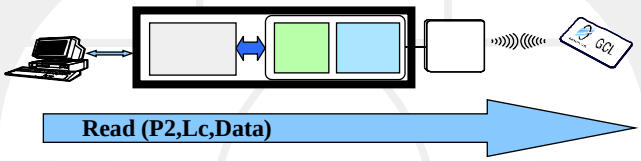
Read (P2,Le)

Lit la valeur de l'EEPROM à l'adresse spécifiée dans la RAM.
Lecture d 'un bloc
P2 : Adresse du bloc contenant la valeur.

Syntaxe :

CLA	INS	P1	P2	LE
94	34	00	P2	16

Write



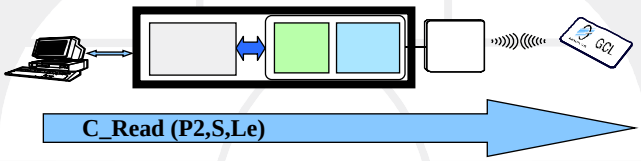
Ecrit la donnée à l'adresse spécifiée.
Ecriture d'un bloc.
P2 : Adresse du bloc destination.
Data : Données à écrire

Syntaxe :

CLA	INS	P1	P2	LC	Data
94	D8	00	P2	16	Data

Commandes combinées au niveau carte

C_Read (Authenticate, Read Block)

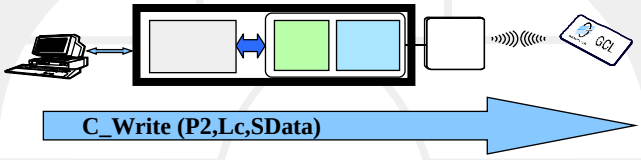


Produit une authentification mutuelle entre la carte et le lecteur.
Lit la valeur en EEPROM à l'adresse spécifiée.
Note : Lit à l'intérieur d'un secteur (De 1 à 4 blocs). Les conditions d'accès en lecture doivent être remplies pour tous les blocs.
P2 correspond à l 'adresse du premier bloc contenant la valeur.
S est l'octet de commande du mode d'authentification.
Le : Nombre d'octets à lire (De 1 à 64)

Syntaxe :

CLA	INS	P1	P2	LC	Data	LE
84	B8	00	P2	01	S	Le

C_Write (Authenticate, Write Block)



Produit une authentification mutuelle entre la carte et le lecteur.
Ecrit la valeur en EEPROM à l'adresse spécifiée.
Note : Ecrit à l'intérieur d'un secteur (De 1 à 4 blocs). Les conditions d'accès en écriture doivent être remplies pour tous les blocs.
P2 correspond à l'adresse du premier bloc contenant la valeur.
S est l'octet de commande du mode d'authentification.
Le : Nombre d'octets à lire (De 1 à 64)
Data : Données à écrire

Syntaxe :

CLA	INS	P1	P2	LC	Data
84	D8	00	P2	Lc	S Data

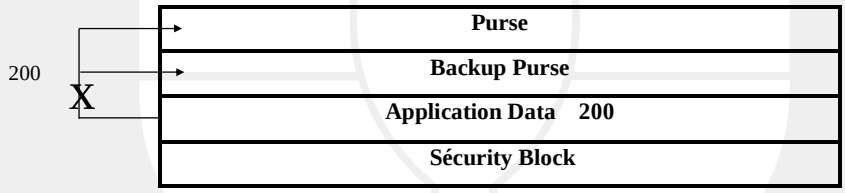
CONFIGURATION D'UNE APPLICATION PORTE-MONNAIE

Spécifications du porte-monnaie

- **Principaux points à prendre en compte :**
- DEBIT : Opération rapide, peu sensible à la fraude
  - Une clé dédiée au débit pour toutes les cartes
  - Utilisation de la clé A
- CREDIT : Sensible à la fraude
  - Clé B diversifiée par la valeur du numéro de série (CSN)
- Protection du montant (Purse backup) : Assurer l'intégrité du montant
  - Utilisation d'un bloc valeur

Gestion des données

Les données de l'application doivent être protégées en sauvegarde et transfert pour éviter les fraudes avec la valeur du porte monnaie :



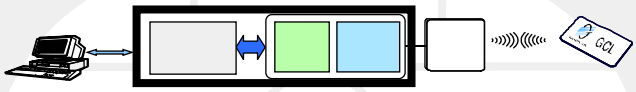
Configuration du porte monnaie

Conditions d'accès

	Read	Write	Add/Transfer/Restore	Substract/Transfer/Restore
Purse	A	B	B	A
Backup Purse	A	B	B	A
Application Data	A	B	N	N
Clé A **40 FF 0B** **Clé B**			Conditions verrouillées	

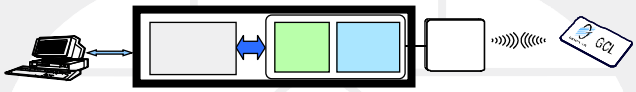
Les données applicatives sont stockées dans un bloc de données transparent

Opération de crédit du porte-monnaie



- **COMMANDE**
  - 1 Get Card
  - 2
  - 3 Key B = F (KBm, CSN)
  - 4 Load in ASIC (Transport Code + KeyB)
  - 5 Authenticate (Calcul de cryptogrammes)
  - 6 Credit Purse : C_addvalue to Backup
  - 7 C_CopyBackup to Active
- **REPONSE DE LA CARTE**
  - Numéro de série (CSN)
  - Cryptogrammes

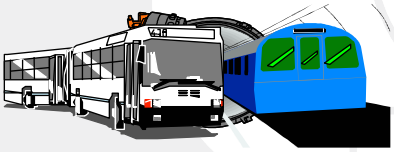
Opération de débit du porte-monnaie



- **COMMANDE**
  - 1 Load once in ASIC (Transport code + clé A)
  - 2 Get Card
  - 3
  - 4 Authenticate (Calcul de cryptogrammes)
  - 5 Débit Purse : C_Substract_value to Backup
  - 6 C_CopyBackup to Active
- **REPONSE DE LA CARTE**
  - Numéro de série (CSN)
  - Cryptogrammes

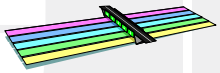
Les Applications du sans contact

- Télébilletique (Ticketing) dans le domaine du transport
- Porte monnaie électronique pour les paiements de faibles montants
- Services divers comme des programmes de fidélité (loyalty)



Transport de masse

Parking - Contrôle d'accès



Péage

Technologie sans contact NFC (1/4)

- Technologie de communication en champ proche
- Promue par Philips et Sony
- Consortium rejoint par Nokia, Samsung, Panasonic, Microsoft
- Réalisée grâce à des circuits dits NFC implantés dans des dispositifs mobiles de grande consommation (PDAs, téléphones mobiles, etc …)
- Téléchargement de fichiers et échanges de données entre terminaux

Usages des NFC (2/4)

- Mode émulation de carte à puce sans contact pour un terminal mobile
- Mode lecteur de cartes ou de tags passifs (étiquettes électroniques sur affiches, colis, cartes de visite…)
- Mode peer to peer : Deux terminaux mobiles échangent des données
- Réalisée grâce à des circuits dits NFC implantés dans des dispositifs mobiles de grande consommation (PDAs, téléphones mobiles, etc …)
- Téléchargement de fichiers et échanges de données entre terminaux

Technologie sans contact NFC (3/4)

- Acronyme NFC signifie Near Field Communication
- Porteuse à 13,56 Mhz
- Conçue pour être inter opérable avec les protocoles Mifare et FeliCa
- Débit allant jusqu'à 1 Mégabits/s
- Distance de transaction : jusqu'à 20 cm
- Standardisée ISO 18092

Applications NFC en préparation (4/4)

- Achat du droit d'écoute et transfert de musique entre un PDA et une affiche intelligente (smart poster)
- Télébillettique. Achat par téléphone mobile près d'une borne NFC
- Voyage : Réservation et achat de droits