

I. Généralité

NFC = Near Field Communication

Technologie sans fil

Courte portée (20cm max)

Débits de communication : 106, 212 ou 424 kbps

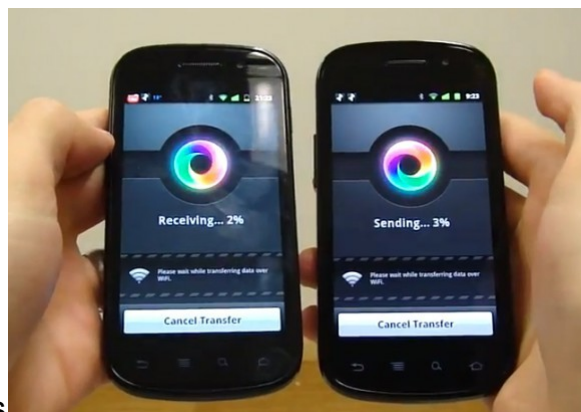
Haute fréquence (13,56MHz)

Extension de la norme ISO/CEI 14443



I. 1. Quelques usages de la NFC

- Paiement
- Achat, validation de titre de transport
- Couponing
- Accès et démarrage d'un véhicule
- Contrôle d'accès à des locaux
- Lecture d'informations produits
- Récupération de la clef Wifi d'un point d'accès



I. 2. Développement de la technologie

Promesse à un avenir certain

Forum NFC :

- Sony (carte NFC FeliCa)
- NXP Semiconductors (carte Mifare)
- Samsung, Apple,...

Normes liées à la NFC :

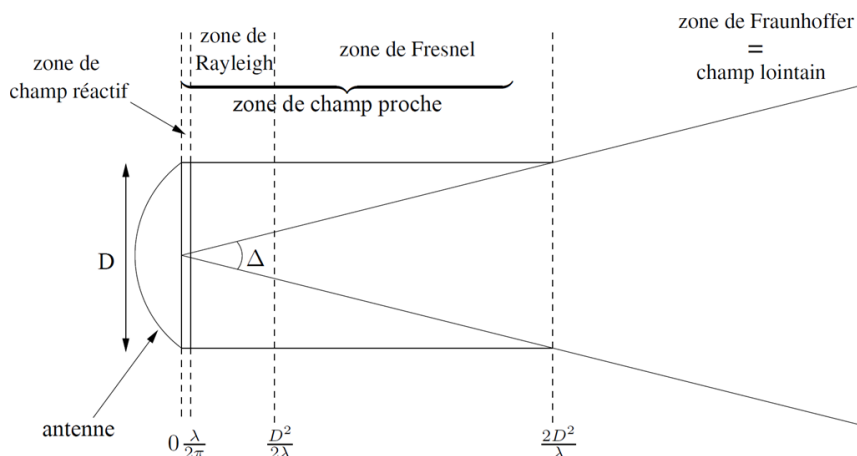
- NFCIP-1
- ISO/CEI 14443-1 à 14443-4
- NDEF



I. 3. Un peu de physique

Champ proche → couplage magnétique

Champ lointain → propagation d'ondes



I. 4. NFC et réglementations

Distances de fonctionnement réduites

Voir réglementation ERC 7003 et ETSI 300 330

→ environ 20 cm max

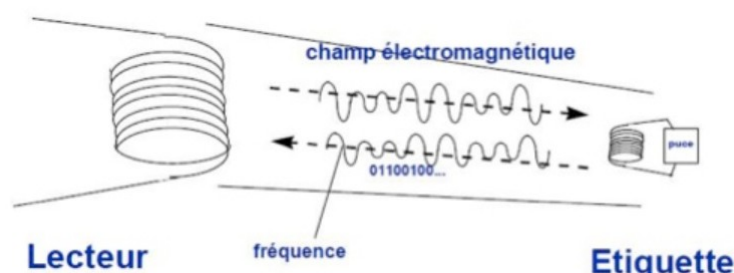
Au niveau applicatif : entre 3 et 5 cm



	Frequency Band	Power / Magnetic Field
a	6765-6795 kHz	42 dBμA/m at 10m
b	13.553-13.567 MHz	42 dBμA/m at 10m

II. Généralités sur le fonctionnement

La NFC définit des protocoles. Elle s'appuie sur la technologie RFID (Radio Frequency IDentification). Le champ électromagnétique créé sert de support au transport de l'information.



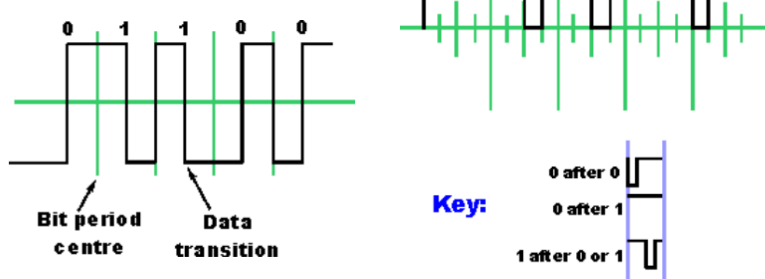
II. 1. Modulation, codages

Modulation d'amplitude

Porteuse : 13,56 MHz

2 systèmes de codage

- Manchester
- Miller modifié

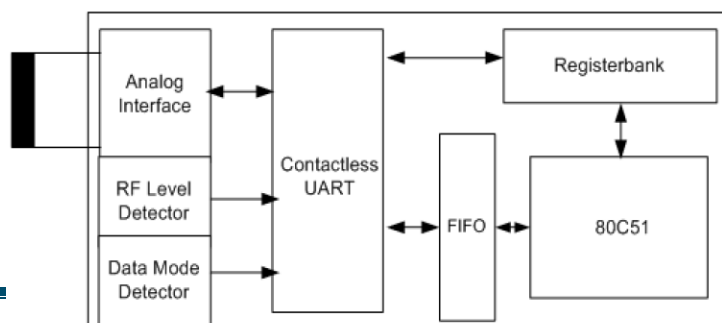


DATA RATE KBPS	ACTIVE DEVICE	PASSIVE DEVICE
106	Modified Miller, 100%, ASK	Manchester, 10%, ASK
212	Manchester, 10%, ASK	Manchester, 10%, ASK
424	Manchester, 10%, ASK	Manchester, 10%, ASK

III. Modes de fonctionnement

Un équipement doté de la NFC peut être utilisé :

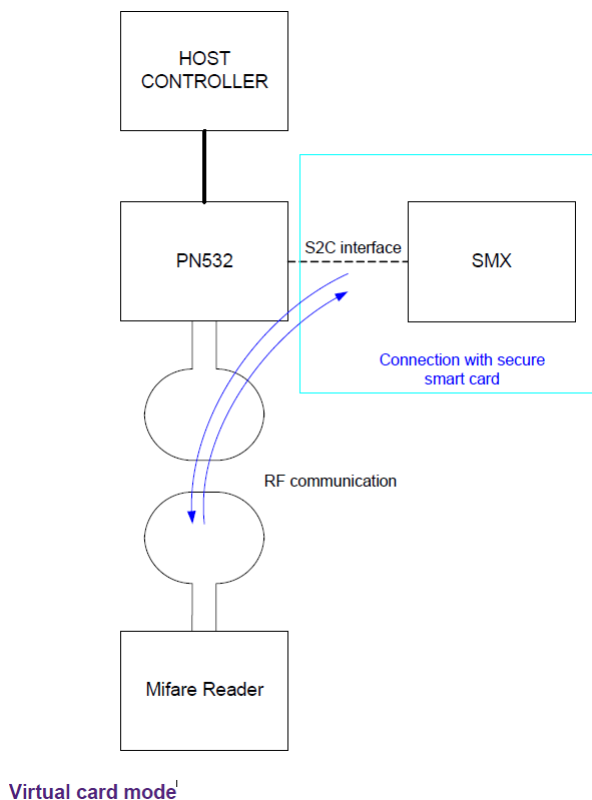
- en émulateur de cartes (NFC Target)
- en lecteur de cartes (NFC Initiator)



Deux équipements dotés de la NFC peuvent effectuer des échanges en mode peer-to-peer. Ces trois modes sont permis grâce à un contrôleur de communication NFC (ex : le PN532)

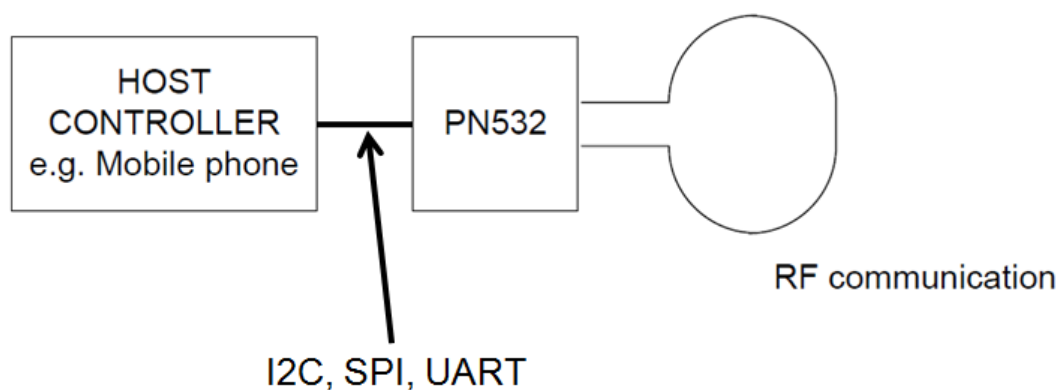
III. 1. Mode émulation de carte

Le contrôleur NFC joue le rôle de passerelle entre une carte à puce sécurisée et un lecteur



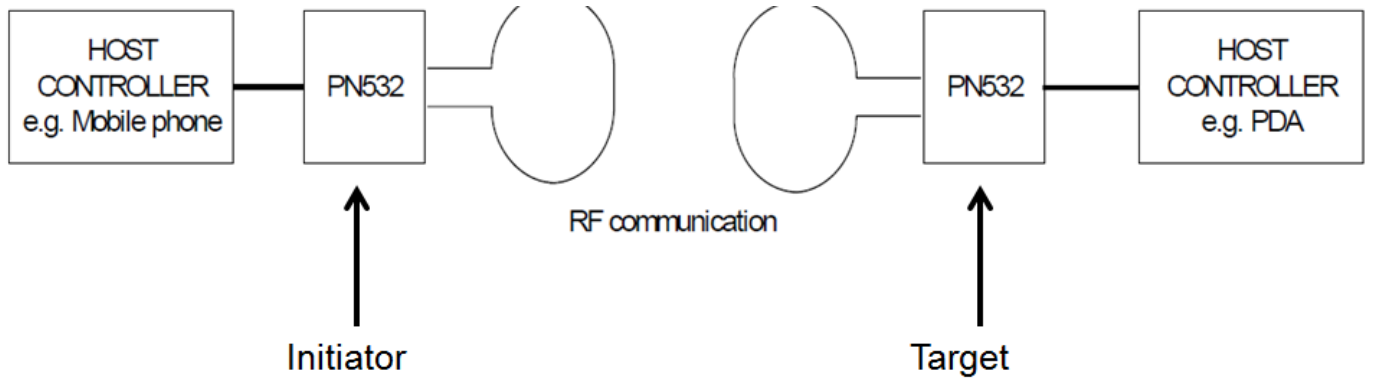
III. 2. Mode lecteur

Le contrôleur NFC est l'initiateur de l'échange de données. La communication est dite passive car seul le contrôleur NFC génère le champ RF.



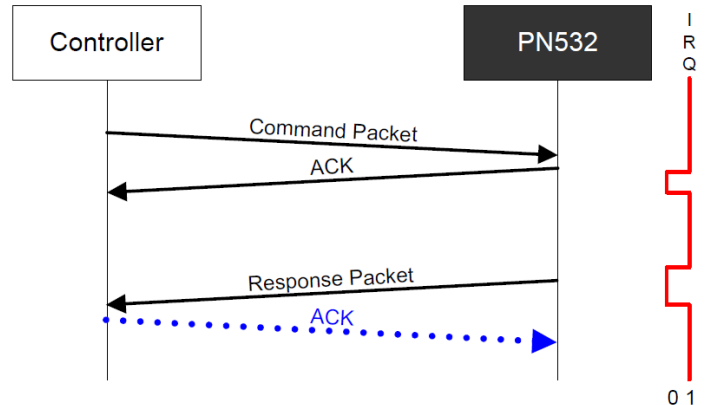
III. 3. NFC en mode P2P

L'un des deux contrôleurs NFC prend le rôle d'initiateur, l'autre le rôle de cible. La communication peut être passive ou active. Dans ce cas, chaque contrôleur génère son champ RF lorsqu'il émet des données



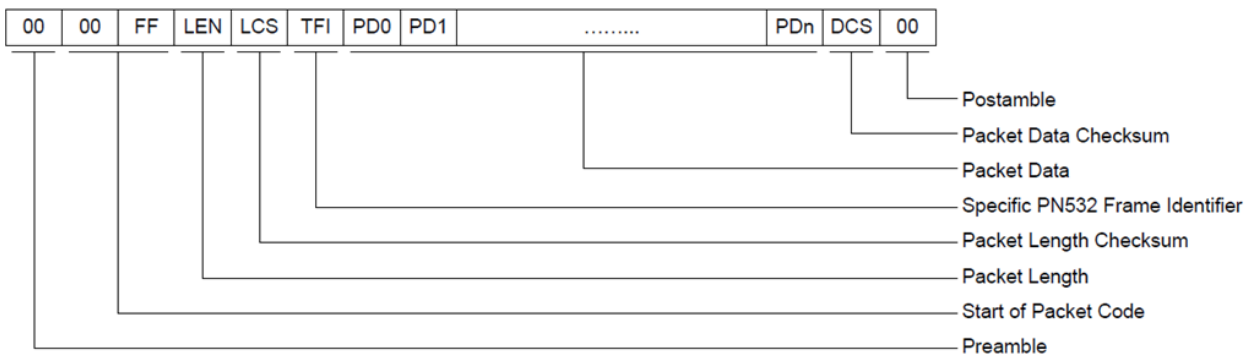
IV. Quelques caractéristiques liées au protocole

Communication de type Half Duplex
 Détection de collisions : oui
 Acquitement entre "host" et contrôleur NFC

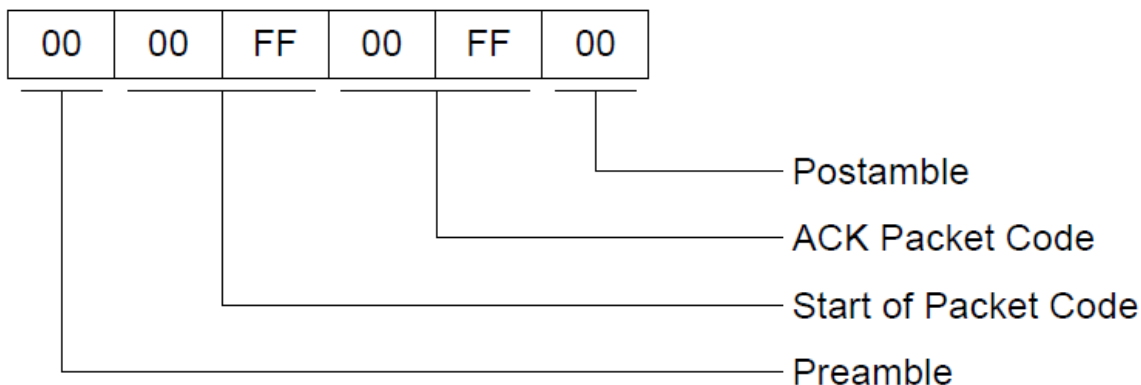


Normal exchange between host controller and the PN532

a) Structure des trames de commande et de réponse



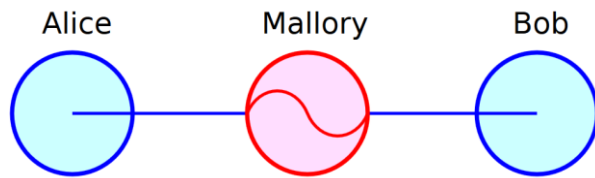
b) Structure d'une trame d'acquitement



V. NFC et sécurité

V. 1. Sources de vulnérabilité

- L'écoute (Eavesdropping)
- La corruption de données
- La modification des données
- L'attaque de l'homme du milieu (HDM) * ou en anglais, MITM (man in the middle)



V. 2. Protection

- courte portée
- surveillance du niveau d'énergie magnétique
- mode de communication actif-passif
- canal sécurisé (chiffrement des données)
- sécurité physique : Secured Element (SE)

VI. Intérêts de la NFC

- Facilité de mise en œuvre
- Prix moyen d'un tag NFC : 10cts
- Établissement rapide de la connexion
- Mode passif → low energy

