

Identification par radio fréquences

Les aspects technico-économiques

Xavier Lagorce

Mercredi 16 décembre 2009



Introduction

Dossier sur l'identification par radio fréquences.
Ensemble de 19 documents, regroupables en 3 grandes catégories

- Descriptions générales et fonctionnement (10)
- Applications industrielles (5)
- Sécurité (4)



Introduction

Dossier sur l'identification par radio fréquences.
Ensemble de 19 documents, regroupables en 3 grandes catégories

- Descriptions générales et fonctionnement (10)
- Applications industrielles (5)
- Sécurité (4)



Introduction

Dossier sur l'identification par radio fréquences.
Ensemble de 19 documents, regroupables en 3 grandes catégories

- Descriptions générales et fonctionnement (10)
- Applications industrielles (5)
- Sécurité (4)



Introduction

Dossier sur l'identification par radio fréquences.
Ensemble de 19 documents, regroupables en 3 grandes catégories

- Descriptions générales et fonctionnement (10)
- Applications industrielles (5)
- Sécurité (4)



1 Principes du RFID

- Définition et historique
- Fonctionnement
- En pratique

2 Exemples d'applications

- Des exemples qui sautent aux yeux
- Contrôle d'accès à la RATP
- Electronic Product Code
- Dans nos maisons

3 Risques et sécurité

- Une surveillance continue ?
- Des risques de sécurités ?
- Des sécurités matérielles cachées...



Sommaire

- 1 Principes du RFID
 - Définition et historique
 - Fonctionnement
 - En pratique
- 2 Exemples d'applications
- 3 Risques et sécurité



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



RFID tag ?

Un peu analogue aux cartes à puces, avec certaines différences :

- logique "intelligente" (μ C, ...)
- mémoire
- Alimentation par induction électromagnétique
- Données transmises sur le même principe

⇒ Radio Frequency IDentification



Historique

- **1940** : Britanniques – Identify : Friend or Foe
Principes fondateurs
- **1970** : Usage militaire pour le contrôle d'accès aux sites sensibles (centrales nucléaires)
- **1980** : Apparition des tags passifs – Identification du bétail
- **1990** : Début de la normalisation en vue de l'interopérabilité

Historique

- **1940** : Britanniques – Identify : Friend or Foe
Principes fondateurs
- 1970 : Usage militaire pour le contrôle d'accès aux sites sensibles (centrales nucléaires)
- 1980 : Apparition des tags passifs – Identification du bétail
- 1990 : Début de la normalisation en vue de l'interopérabilité

Historique

- **1940** : Britanniques – Identify : Friend or Foe
Principes fondateurs
- **1970** : Usage militaire pour le contrôle d'accès aux sites sensibles (centrales nucléaires)
- **1980** : Apparition des tags passifs – Identification du bétail
- **1990** : Début de la normalisation en vue de l'interopérabilité



Historique

- **1940** : Britanniques – Identify : Friend or Foe
Principes fondateurs
- **1970** : Usage militaire pour le contrôle d'accès aux sites sensibles (centrales nucléaires)
- **1980** : Apparition des tags passifs – Identification du bétail
- **1990** : Début de la normalisation en vue de l'interopérabilité

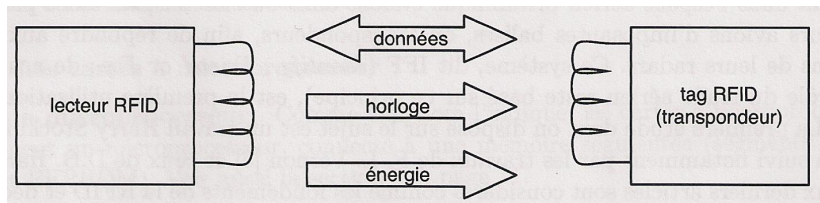


Historique

- **1940** : Britanniques – Identify : Friend or Foe
Principes fondateurs
- **1970** : Usage militaire pour le contrôle d'accès aux sites sensibles (centrales nucléaires)
- **1980** : Apparition des tags passifs – Identification du bétail
- **1990** : Début de la normalisation en vue de l'interopérabilité



Composition



Le tag

Tag, étiquette ou transpondeur

- une puce
- une mémoire
- une antenne bobinée

Souvent collé sur un film plastique ou moulé dans une carte



Le tag

Tag, étiquette ou transpondeur

- une puce
- une mémoire
- une antenne bobinée

Souvent collé sur un film plastique ou moulé dans une carte



Le tag

Tag, étiquette ou transpondeur

- une puce
- une mémoire
- une antenne bobinée

Souvent collé sur un film plastique ou moulé dans une carte



Le tag

Tag, étiquette ou transpondeur

- une puce
- une mémoire
- une antenne bobinée

Souvent collé sur un film plastique ou moulé dans une carte



Le tag

Tag, étiquette ou transpondeur

- une puce
- une mémoire
- une antenne bobinée

Souvent collé sur un film plastique ou moulé dans une carte



Le lecteur

- Peut lire ou écrire sur la carte (selon la technologie)
- Émet des ondes radio et des champs magnétiques...
- ... puis écoute les réponses des *tags*



Le lecteur

- Peut lire ou écrire sur la carte (selon la technologie)
- Émet des ondes radio et des champs magnétiques...
- ... puis écoute les réponses des *tags*



Le lecteur

- Peut lire ou écrire sur la carte (selon la technologie)
- Émet des ondes radio et des champs magnétiques...
- ... puis écoute les réponses des *tags*



Communication

- **Close coupling systems** : portée jusqu'à 1 cm. Champs électromagnétiques jusqu'à 30 Mhz. Grande énergie disponible.
- **Remote coupling systems** : portée jusqu'à 1 m. 90% des systèmes vendus actuellement. En général 135 kHz et 13.56 MHz.
- **Long-range systems** : portée de plus d'1 m. Transpondeurs actifs. 868 MHz (Europe), 915 MHz (USA), 1.5 GHz et 5.8 GHz.



Communication

- **Close coupling systems** : portée jusqu'à 1 cm. Champs électromagnétiques jusqu'à 30 Mhz. Grande énergie disponible.
- **Remote coupling systems** : portée jusqu'à 1 m. 90% des systèmes vendus actuellement. En général 135 kHz et 13.56 MHz.
- **Long-range systems** : portée de plus d'1 m.
Transpondeurs actifs. 868 MHz (Europe), 915 MHz (USA), 1.5 GHz et 5.8 GHz.



Communication

- **Close coupling systems** : portée jusqu'à 1 cm. Champs électromagnétiques jusqu'à 30 Mhz. Grande énergie disponible.
- **Remote coupling systems** : portée jusqu'à 1 m. 90% des systèmes vendus actuellement. En général 135 kHz et 13.56 MHz.
- **Long-range systems** : portée de plus d'1 m. Transpondeurs actifs. 868 MHz (Europe), 915 MHz (USA), 1.5 GHz et 5.8 GHz.



Différents types de *tags*

- Bobinage sur auto-collants
 - Cartes
 - Boutons
 - Capsules



Différents types de *tags*

- Bobinage sur auto-collants
- Cartes
- Boutons
- Capsules



Différents types de *tags*

- Bobinage sur auto-collants
- Cartes
- Boutons
- Capsules



Différents types de *tags*

- Bobinage sur auto-collants
- Cartes
- Boutons
- Capsules



Sommaire

- 1 Principes du RFID
- 2 Exemples d'applications
 - Des exemples qui sautent aux yeux
 - Contrôle d'accès à la RATP
 - Electronic Product Code
 - Dans nos maisons
- 3 Risques et sécurité

Bibliothèques

- Gestion facilitée de l'inventaire
- Vatican : 50000 parmi 120000 des ouvrages disponibles à la lecture sont pucés.



Bibliothèques

- Gestion facilitée de l'inventaire
- Vatican : 50000 parmi 120000 des ouvrages disponibles à la lecture sont pucés.



Autres exemples

- **Blanchisseries**
- Accès des véhicules dans un parking
- Limiter la contrefaçon de billets de banque
- Traçabilité des bêtes dans les élevages...
- ... ou pour les animaux domestiques

Autres exemples

- Blanchisseries
- Accès des véhicules dans un parking
- Limiter la contrefaçon de billets de banque
- Traçabilité des bêtes dans les élevages...
- ... ou pour les animaux domestiques

Autres exemples

- Blanchisseries
- Accès des véhicules dans un parking
- Limiter la contrefaçon de billets de banque
- Traçabilité des bêtes dans les élevages...
- ... ou pour les animaux domestiques



Autres exemples

- Blanchisseries
- Accès des véhicules dans un parking
- Limiter la contrefaçon de billets de banque
- Traçabilité des bêtes dans les élevages...
- ... ou pour les animaux domestiques



Autres exemples

- Blanchisseries
- Accès des véhicules dans un parking
- Limiter la contrefaçon de billets de banque
- Traçabilité des bêtes dans les élevages...
- ... ou pour les animaux domestiques



Des puces pour sauver des vies

- Joseph Krull porte sur lui une puce passive
- Puce qui contient son dossier médical
- Allergies graves à 2 médicaments
- En cas d'urgence, pas d'erreur si lecture de la puce



Des puces pour sauver des vies

- Joseph Krull porte sur lui une puce passive
- Puce qui contient son dossier médical
- Allergies graves à 2 médicaments
- En cas d'urgence, pas d'erreur si lecture de la puce



Des puces pour sauver des vies

- Joseph Krull porte sur lui une puce passive
- Puce qui contient son dossier médical
- Allergies graves à 2 médicaments
- En cas d'urgence, pas d'erreur si lecture de la puce



Des puces pour sauver des vies

- Joseph Krull porte sur lui une puce passive
- Puce qui contient son dossier médical
- Allergies graves à 2 médicaments
- En cas d'urgence, pas d'erreur si lecture de la puce



Introduction

- Développement d'un système de contrôle d'accès
 - Système global sur tout le parc
 - Gestion centralisée
 - Utilisé depuis plus de 10 ans



Introduction

- Développement d'un système de contrôle d'accès
- Système global sur tout le parc
- Gestion centralisée
- Utilisé depuis plus de 10 ans



Introduction

- Développement d'un système de contrôle d'accès
- Système global sur tout le parc
- Gestion centralisée
- Utilisé depuis plus de 10 ans



Introduction

- Développement d'un système de contrôle d'accès
- Système global sur tout le parc
- Gestion centralisée
- Utilisé depuis plus de 10 ans



Fonctionnalités

- Fonctions d'accès
- Fonctions de supervision
- Fonctions de commande



Fonctionnalités

- Fonctions d'accès
- Fonctions de supervision
- Fonctions de commande



Fonctionnalités

- Fonctions d'accès
- Fonctions de supervision
- Fonctions de commande



Architecture

- Un badge « Passe sans contact »
- Un lecteur de badges
- Un coffret contrôleur d'accès
- Un dispositif commandé
- Un système de gestion

Architecture

- Un badge « Passe sans contact »
- Un lecteur de badges
- Un coffret contrôleur d'accès
- Un dispositif commandé
- Un système de gestion



Architecture

- Un badge « Passe sans contact »
- Un lecteur de badges
- Un coffret contrôleur d'accès
- Un dispositif commandé
- Un système de gestion



Architecture

- Un badge « Passe sans contact »
- Un lecteur de badges
- Un coffret contrôleur d'accès
- Un dispositif commandé
- Un système de gestion



Architecture

- Un badge « Passe sans contact »
- Un lecteur de badges
- Un coffret contrôleur d'accès
- Un dispositif commandé
- Un système de gestion

Navigo

- Utilisation du savoir-faire « Sans contact »
 - Contrôle des abonnements et des accès voyageurs
 - Possibilité de traçage des voyages



Navigo

- Utilisation du savoir-faire « Sans contact »
- Contrôle des abonnements et des accès voyageurs
- Possibilité de traçage des voyages



Navigo

- Utilisation du savoir-faire « Sans contact »
- Contrôle des abonnements et des accès voyageurs
- Possibilité de traçage des voyages



2 types de badges

- Intégrale ou Imagin'R' : traçable
- Passe « Découverte » : non-traçable

2 types de badges

- Intégrale ou Imagin'R' : traçable
- Passe « Découverte » : non-traçable

Introduction

- **Sorte de fantôme ultime**
 - Attribution d'un code individuel à chaque objet
 - EPC : norme visant à tout étiqueter
 - Permet virtuellement de numérotter tous les objets de la planète



Introduction

- Sorte de fantôme ultime
- Attribution d'un code individuel à chaque objet
- EPC : norme visant à tout étiqueter
- Permet virtuellement de numéroter tous les objets de la planète



Introduction

- Sorte de fantôme ultime
- Attribution d'un code individuel à chaque objet
- EPC : norme visant à tout étiqueter
- Permet virtuellement de numéroter tous les objets de la planète



Introduction

- Sorte de fantôme ultime
- Attribution d'un code individuel à chaque objet
- EPC : norme visant à tout étiqueter
- Permet virtuellement de numérotter tous les objets de la planète



But

- Anticiper la demande
- Réduire les stocks
- Prévoir les pénuries

⇒ Énormes perspectives économiques



But

- Anticiper la demande
- Réduire les stocks
- Prévoir les pénuries

⇒ Énormes perspectives économiques



But

- Anticiper la demande
- Réduire les stocks
- Prévoir les pénuries

⇒ Énormes perspectives économiques



But

- Anticiper la demande
 - Réduire les stocks
 - Prévoir les pénuries
- ⇒ Énormes perspectives économiques

Des habitudes modifiées

- Plus de caisses
- Des lecteurs RFID...
- ... qui débitent automatiquement nos CB



Des habitudes modifiées

- Plus de caisses
- Des lecteurs RFID...
- ... qui débitent automatiquement nos CB



Des habitudes modifiées

- Plus de caisses
- Des lecteurs RFID...
- ... qui débitent automatiquement nos CB



Une démocratisation accrue

- le RFID débarque aussi chez les amateurs
- ID-Innovation : puces « tout intégré »
- Lecteurs USB



Une démocratisation accrue

- le RFID débarque aussi chez les amateurs
- ID-Innovation : puces « tout intégré »
- Lecteurs USB



Une démocratisation accrue

- le RFID débarque aussi chez les amateurs
- ID-Innovation : puces « tout intégré »
- Lecteurs USB



Sommaire

- 1 Principes du RFID
- 2 Exemples d'applications
- 3 Risques et sécurité**
 - Une surveillance continue ?
 - Des risques de sécurités ?
 - Des sécurités matérielles cachées...



« Dans le passé, aucun gouvernement n'avait eu le pouvoir de maintenir ses citoyens sous une surveillance constante. Maintenant, la Police de la pensée surveillait tout le monde, constamment »

George Orwell, 1984



Internet des objets

- **Etiquettes RFID sur tous les objets**
- Transports et accès régis par des badges RFID
- Possibilité de tracer nos habitudes et nos comportements



Internet des objets

- Etiquettes RFID sur tous les objets
- Transports et accès régis par des badges RFID
- Possibilité de tracer nos habitudes et nos comportements



Internet des objets

- Etiquettes RFID sur tous les objets
- Transports et accès régis par des badges RFID
- Possibilité de tracer nos habitudes et nos comportements



Interrogation Éthique

- Risques de susciter certaines convoitises
- Autorités de surveillance : CNIL, Caspian
- Nécessité d'une certaine vigilance sur les informations collectées



Interrogation Éthique

- Risques de susciter certaines convoitises
- Autorités de surveillance : CNIL, Caspian
- Nécessité d'une certaine vigilance sur les informations collectées

Interrogation Éthique

- Risques de susciter certaines convoitises
- Autorités de surveillance : CNIL, Caspian
- Nécessité d'une certaine vigilance sur les informations collectées



Exemple du passeport numérique

- Code cryptographique anti-copie
 - Il suffit de retirer la mention de cette clé dans l'index de la puce
 - Simple signalement du problème par la borne de validation
 - Très forte probabilité que l'incident soit ignoré par le douanier

Exemple du passeport numérique

- Code cryptographique anti-copie
- Il suffit de retirer la mention de cette clé dans l'index de la puce
- Simple signalement du problème par la borne de validation
- Très forte probabilité que l'incident soit ignoré par le douanier



Exemple du passeport numérique

- Code cryptographique anti-copie
- Il suffit de retirer la mention de cette clé dans l'index de la puce
- Simple signalement du problème par la borne de validation
- Très forte probabilité que l'incident soit ignoré par le douanier



Exemple du passeport numérique

- Code cryptographique anti-copie
- Il suffit de retirer la mention de cette clé dans l'index de la puce
- Simple signalement du problème par la borne de validation
- Très forte probabilité que l'incident soit ignoré par le douanier



Des failles intrinsèques ?

- ePassports ⇒ nombreuses failles découvertes
- Standard trop laxiste...
- ... car laisse en option les systèmes s'authentification poussés



Des failles intrinsèques ?

- ePassports ⇒ nombreuses failles découvertes
- Standard trop laxiste...
- ... car laisse en option les systèmes s'authentification poussés



Des failles intrinsèques ?

- ePassports \Rightarrow nombreuses failles découvertes
- Standard trop laxiste...
- ... car laisse en option les systèmes s'authentification poussés



Attaque « Man in the middle »

- Exemple : clé de voiture
- Relais du challenge de la voiture vers le propriétaire
- Envoi de la réponse du propriétaire à la voiture
- Ouverture du véhicule !

Attaque « Man in the middle »

- Exemple : clé de voiture
- Relais du challenge de la voiture vers le propriétaire
- Envoi de la réponse du propriétaire à la voiture
- Ouverture du véhicule !



Attaque « Man in the middle »

- Exemple : clé de voiture
- Relais du challenge de la voiture vers le propriétaire
- Envoi de la réponse du propriétaire à la voiture
- Ouverture du véhicule !



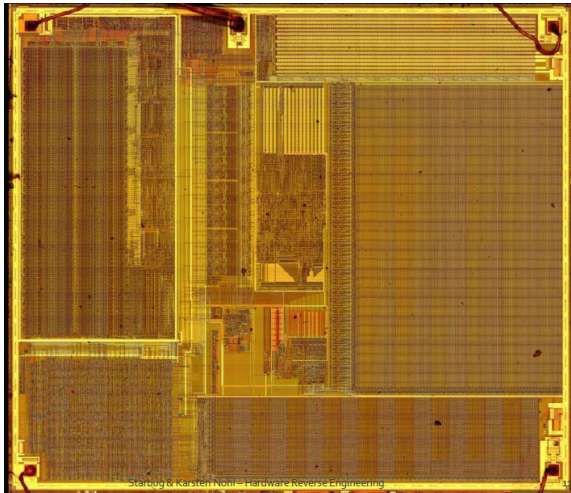
Attaque « Man in the middle »

- Exemple : clé de voiture
- Relais du challenge de la voiture vers le propriétaire
- Envoi de la réponse du propriétaire à la voiture
- Ouverture du véhicule !

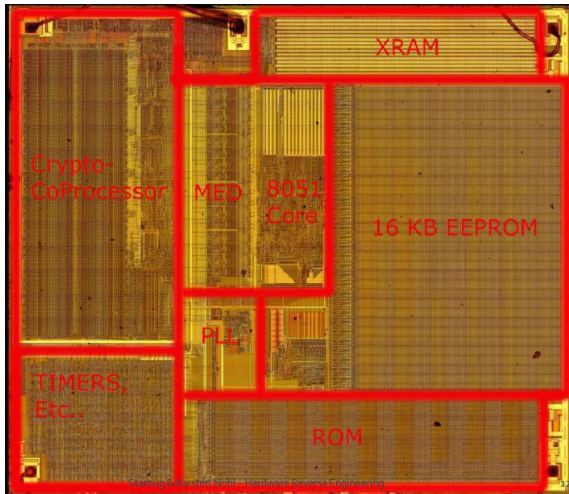
Des sécurités inutiles ?



La sécurité par l'obscurantisme ?



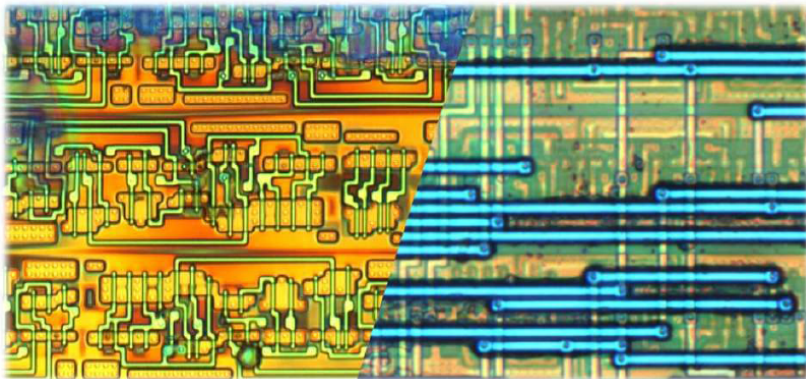
La sécurité par l'obscurantisme ?



Une fausse sécurité...



... qui ne peut espérer durer



Conclusion

Identification par radio fréquences :

- Une technologie en plein expansion
- Une technologie qui envahit de plus en plus notre quotidien
- Une technologie qui peut nous surveiller
- Une technologie qu'il faut correctement sécuriser



Conclusion

Identification par radio fréquences :

- Une technologie en plein expansion
- Une technologie qui envahit de plus en plus notre quotidien
- Une technologie qui peut nous surveiller
- Une technologie qu'il faut correctement sécuriser



Conclusion

Identification par radio fréquences :

- Une technologie en plein expansion
- Une technologie qui envahit de plus en plus notre quotidien
- Une technologie qui peut nous surveiller
- Une technologie qu'il faut correctement sécuriser



Conclusion

Identification par radio fréquences :

- Une technologie en plein expansion
- Une technologie qui envahit de plus en plus notre quotidien
- Une technologie qui peut nous surveiller
- Une technologie qu'il faut correctement sécuriser



Conclusion

Questions

