Programmation pour cartes à puce
Cours 2 - Mise en oeuvre

Halim Djerroud

LISV
Laboratoire d'ingénierie
des systèmes de Versailles

UVSQ
université PARIS-SACLAY

révision : 0.1

Bibliographie

- Smart Card Handbook (Wolfgang Rankl, Wolfgang Effing)
- 7816 Part 4 : `http://www.ttfn.net/techno/smartcards/iso7816_4.html`

Ce cours est basé sur de nombreux supports et codes sources fournis par Philippe Guillot

Ont participé à l'élaboration de ce cours :

- Philippe Guillot
- Christelle OU
- Kévin CARRIER
- Mehdy Tounsi

LISV Laboratoire d'ingénierie des systèmes de Versailles | UVSQ université PARIS-SACLAY

Histoire de la carte à puce

- Première carte à puce (Carte avec une mémoire) : 1974
  - Breveté par un : Roland Moreno (français)
  - Au départ, c'était une carte à mémoire
  - Objectif : Principalement sécuriser les cabines téléphoniques au moyen de DES
- Première carte à puce intelligente *Smart Card* (+ processeur) : 1976
  - Michel Ugon (français) Employé chez Bull : ajoute un processeur donnant ainsi la faculté aux cartes à puces de traiter l'information
  - L'année 1976 correspond également à l'appel d'offres DES (Data Encryption Standard)1978, le premier algorithme de chiffrement à clé publique, RSA, est publié.
- Entrée des carte à puces dans le domaine publique : 1983
  - Télécartes (cartes à puce pour cabines téléphoniques)
  - Diminution du taux de fraude de 0.2% à 0.032%, c'est 80% de 0.2%
- Utilisation des cartes à puce dans le domaine bancaire : 1983

Histoire de la carte à puce (suite)

- Le marché de la carte à puce a failli disparaître : 1993 et 2000
  - durant cette période, la télévision à péage qui utilise les cartes à puce a subi une série de piratages qui entraîna une forte baisse du marché
  - Des rumeurs désignent la NSA comme suspect...
- La carte SIM a sauvé le marché de la carte à puce : 2000
  - Les cartes SIM (Subscriber Identity Module) représente plus de 75% du marché des cartes à puces
- De nos jours, les cartes à puces sont omniprésentes
  - Exemples : Carte vitale, pièce d'identité, permis de conduire, carte SIM, carte de transport (Navigo), carte bancaire, carte d'étudiant, télé à péage, etc.

Exercice :

- Comptez le nombre de cartes à puce que vous avez dans vos poches.

Marché des cartes à puces

- 2006 : 2.6 Milliards
- 2010 : 6.0 Milliards (88.6 millions de cartes bancaire en France)
- 2012 : 6.9 Milliards
- 2013 : 7.5 Milliards
- 2015 : 8.2 Milliards
- 2020 : 12 Milliards
- Marché en constante évolution

Conclusion

Il y a donc un travail important de cryptologie à effectuer autour de cette technologie

Architecture d'une carte à puce

- La carte à puce qu'on utilisera dans ce cours est basé sur le microcontrôleur ATMega 328, inspirée de la carte *FunCard ATMega163*
- C'est un processeur 8 bits qui utilise une architecture Harvard c'est-à-dire que la mémoire de données et la mémoire programme sont physiquement séparées.
- La mémoire de données est reliée à plusieurs périphériques : une mémoire volatile RAM (Random Access Memory) de 2 Ko, une mémoire non volatile EEPROM (Electrically Erasable Read-Only Memory) de 1 Ko, c'est-à-dire qu'il s'agit d'une mémoire programmable et effaçable de manière électronique, d'un périphérique compteur et d'une entrée/sortie branchée sur les contacts de la puce.

Architecture d'une carte à puce

Une carte à puce contient donc trois types de mémoire :

- une mémoire volatile RAM
- une mémoire non volatile EEPROM
- une mémoire programme non volatile FLASH (effaçable par page)

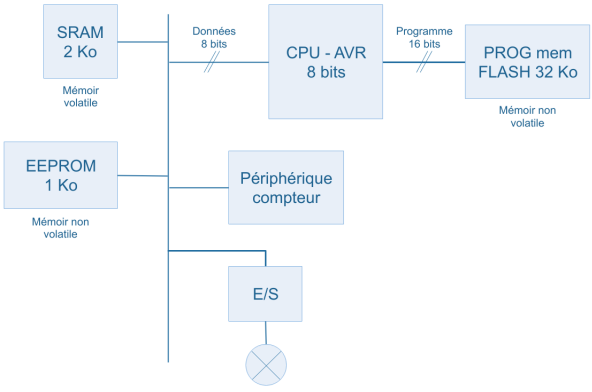
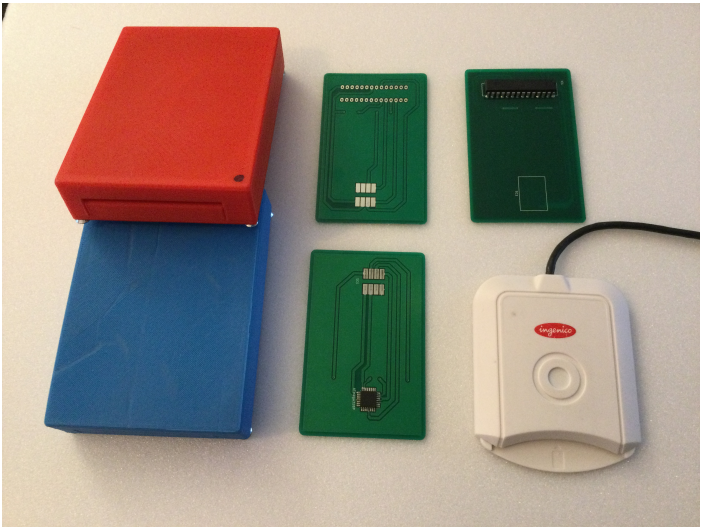


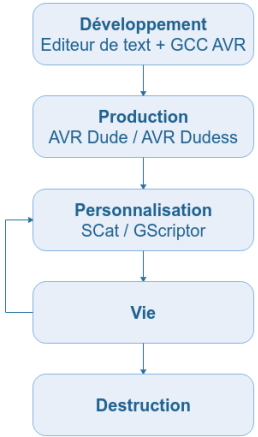
Figure – Architecture interne simplifiée

Carte à puce utilisé dans ce cours



Cycle de vie d'une carte à puce

1. **Développement** : C'est là que l'on imagine le programme en s'aidant de simulateurs ou en faisant des tests en programmation Flash
2. **Programmation / Production** : de la carte si la carte possède une mémoire programme Flash. Réalisation de la carte si cette mémoire est une ROM
3. **Personnalisation** : Cette étape consiste à intégrer de l'information dans l'EEPROM pour rendre une carte unique. Cela peut être un mot de passe, des identifiants, etc
4. **Vie** : La mémoire EPPROM peut être modifié au cours de cette vie
5. **Destruction**



Cartes utilisées dans ce cours

Dans ce cours, nous utiliserons des cartes reprogrammables, le programme réside dans la mémoire FLASH

1. Étape 1 : Nous développerons un code en C sur un IDE comme Emacs, CodeBock etc. Puis AVR-GCC pour compiler notre code
2. Étape 2 : Nous utiliserons le logiciel AVRDUDE (avec un programmateur à base d'arduino connecté par USB)
3. Étape 3 et 4 : Nous allons utilisé le logiciel **SCat**. Bien évidement, nous aurons aussi besoin d'un lecteur de cartes à puce