

# Composants pour carte a puce

Solutions et évolutions pour l'identification électronique



**Laurent SOURGEN**

*Microcontroller, Memories & Smartcard Group*

---

**STMicroelectronics**

OCOVA Forum, 13 Septembre 2007 - Gap - France

# Marchés & Besoins

- ❑ Des marchés très variés, faible standardisation
  - Identification / authentification simple
  - Identification a haute sécurité (passeport...)
  - Des application jointes
  - Des solutions multi applicatives
  - ...
  - Des volumes faibles a moyens
  
- ❑ Des constantes pour ces composants
  - Communications avec et/ou sans contact
  - Une capacité de traitement embarquée
  - De la mémoire non volatile programmable
  - Un moteur cryptographique performant (haut de gamme)
  - Une certification sécuritaire forte (haut de gamme)
  - Des couts abordables (flexibilité)



# Plateformes Actuelles

- ❑ Une gamme de 8 a 128KOctet de mémoire programmable
- ❑ Bâtie autour d'un processeur 8bit cadencé a 20Mhz
- ❑ Interface sans contact (ISO 14443) jusqu'à 848Kb/s
- ❑ Coprocesseur cryptographique
  - Algorithmes a clé publique (RSA & courbes elliptiques)
  - Fonctionnement compatible avec la téléalimentation
- ❑ Certification sécuritaire Critères Commun EAL5+
- ❑ Technologie silicium EEPROM 0.15 $\mu$  et 0.13 $\mu$
- ❑ *ST19NR66 composant pour passeport électronique*
  - *Interopérabilité démontrée sur de nombreux lecteurs*



# Evolutions

- ❑ Pilotées par plusieurs besoins
  - Une interopérabilité et une flexibilité accrue,
    - Nécessite des couches logicielles plus nombreuses
  - De véritables solutions multiplicatives
  - Des temps de transaction raccourcis
  - Une sécurité améliorée
- ❑ Les plateformes
  - Processeurs plus performants (8/16/32bits)
  - Capacité mémoire augmentée
  - Moteurs cryptographiques plus rapides
    - Nouveaux algorithmes, protocole plus complexes, clés plus longues
  - Interface (contact / sans contact) plus rapide (<1Mb/s → 3-5Mb/s)
  - Sécurité renforcé et évolution des certifications
- ❑ La technologie semi-conducteur
  - Faible intérêt de descendre en dessous de  $\sim 0.1\mu$
  - Effort sur la simplification et la réduction des couts

