SSTIC

1-3 juin 2005 à Rennes

Symposium sur la Sécurité des Technologies de l'Information et des Communications

Les cartes mémoire SD™ :

tout ce qu'on ne vous a pas dit

(et pour cause !)

Rump Sessions SSTIC'05

Bruno KEROUANTON

RSSI & « hardwarologue » occasionnel

Cartes SD - Introduction

- Au commencement, Ils inventèrent la mémoire Flash.
- Le deuxième jour, Ils conçurent la Multimedia Card (MMC).
- Le troisième jour, Ils répandirent la SD-Card, elle était belle et sans défauts, nous disait-on :
  - Moins épaisse
  - Protection en écriture par loquet
  - Résistance à l'électricité statique accrue

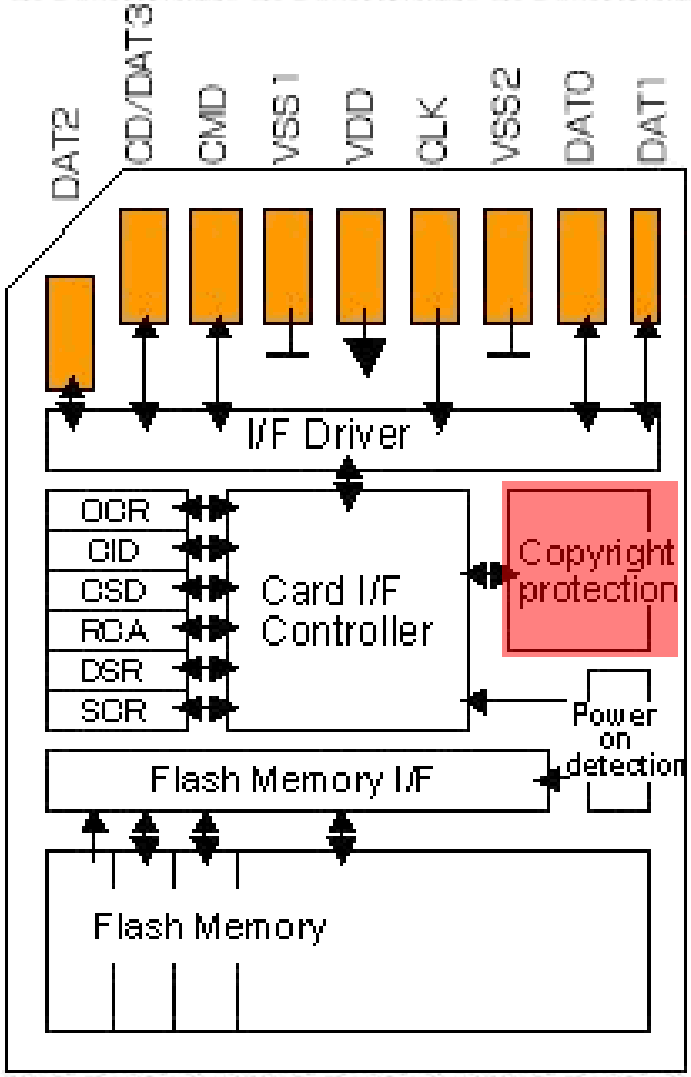
Mais, au fait…

- pourquoi est-elle donc plus chère que les autres formats de Flash ?
- et pourquoi diable dit-on « **Secure** Digital » ?

Cartes SD - Démontage

Contenu d'une carte SD :

- Plus complexe que les cartes traditionnelles.
- Possède un module de « protection du copyright »



… le fameux « Secure » !

Cartes SD – Le « Secure » version marketing

(ou comment prendre les gens pour des…)

Explication officielle du terme « Secure » :

« La carte SD Memory (…) est équipée d'une sécurité compatible SDMI, ce qui signifie que vous pouvez acheter et télécharger de la musique via internet en toute sécurité. »

(*source : fr.computers.toshiba-europe.com*)

Cartes SD – Le « Secure » version technique

Chaque SD Card contient :

- Module de chiffrement et de gestion de certificats
- Générateur de nombres aléatoires
- Zones mémoires chiffrées et/ou secrètes (usage interne)
- Implémentation de CPRM et de SDMI

CPRM – Content Protection for Recordable Media

Développé par le Consortium 4C : IBM, Intel, Matsushita et Toshiba

SDMI – Secure Digital Music Initiative

Forum créé en 1988, plus de 200 adhérents (électronique, informatique, sécurité, industrie du disque, etc.). Inactif depuis 2001.

Cartes SD – Spécifications CPRM

- Algorithme « Cryptomeria Cipher » (C2)
  ➔ blocksize 64 bits – clefs de 56 bits - réseaux de Feistel (10 rounds) - modes C-CBC, ECB et hachage.

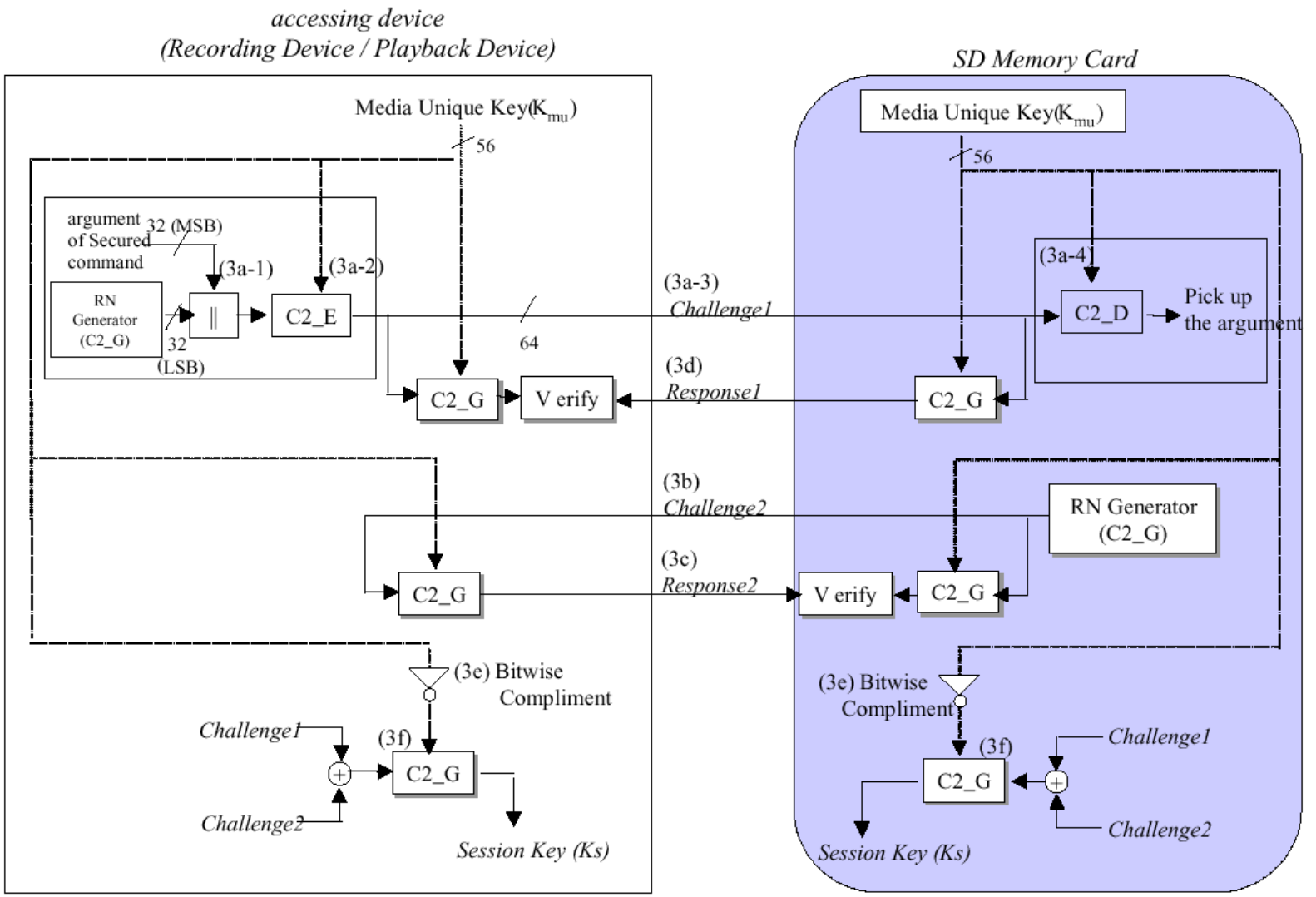
- Identifiant unique pour chaque périphérique de lecture / enregistrement, et pour chaque carte SD.

- 16 clefs secrètes embarquées dans chaque périphérique, et dans chaque carte SD.

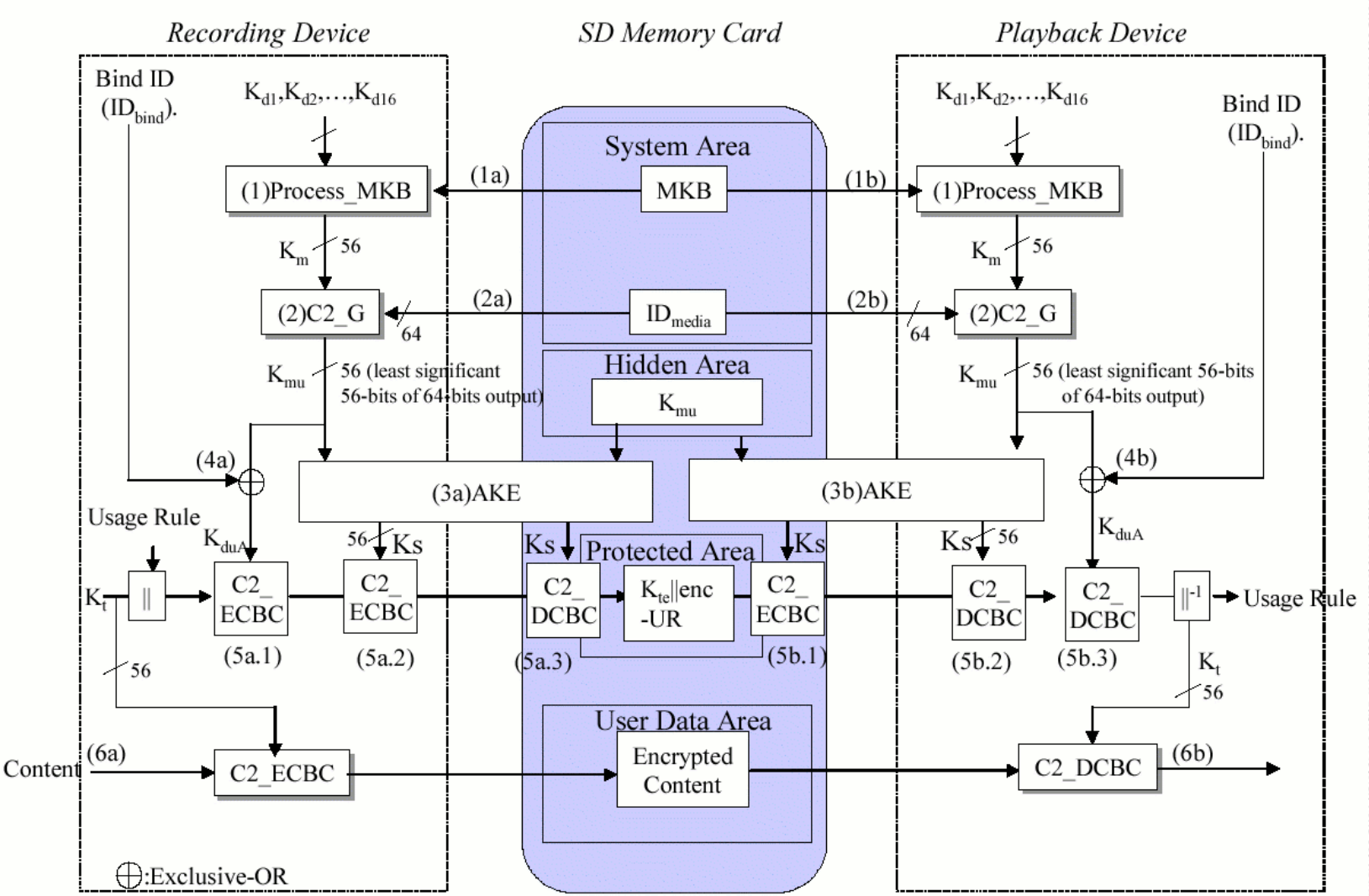
- Mécanisme d'authentification sécurisé et d'échange de clefs entre carte SD et périphérique ou PC.

- Mécanisme de révocation d'un périphérique piraté au niveau de la carte SD (Media Key Block) par upgrade des clefs invalides (!)

Cartes SD – Echange de clefs



Cartes SD – Lecture / écriture



Une vraie stratégie de dissimulation

Non Disclosure Agreements (NDA) nécessaires auprès de 4C et de SDcard Association, très peu d'informations disponibles librement.

Différents CPRM pour différents média…

« CPRM Specifications for SD Memory Card »

(SD-Audio, SD-Sound, SD-ePublish, SD-Image, SD-Video, SD-Binding)

➔ Différents formats de données = différentes méthodes de protection

« CPRM Specifications for recordable media DVD »

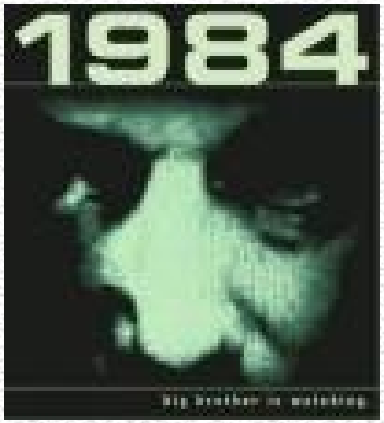
➔Implémenté sur tous les lecteurs, enregistreurs et DVD vierges

« CPRM Specification for portable ATA storage »

➔A priori abandonné lorsque le public a appris cela (ouf !)

Le 4C nous dévoile ses plans… inquiétants ?

« La protection conçue par le consortium 4C a été largement implémentée dans les PC et les périphériques CE. La carte SD est un succès phénoménal. La vente des enregistreurs DVD embarquant CPRM augmente. »



« Chaque DVD vierge (ou média protégé) possède un code média de 64 bits indélébile embossé dans une zone caché, et un numéro de série unique de 40 bits. »

« 4C réfléchit maintenant à la protection des livres audio, des jeux interactifs, et des données personnelles telles que les fichiers médicaux (…) afin de fournir le cadre de protection visant l'utilisateur domestique. »

« 4C et les autres organismes de protection seraient avisés de commencer à éduquer les consommateurs sur les libertés et restrictions qu'ils découvriront progressivement dans leurs foyers […] »

(*source : www.intel.com/standards/case/case_cp.htm*)

CPSA (Content Protection System Architecture)

Quelques autres protections matérielles implémentées :

CPRM ➔ Supports réinscriptibles ⇔ DVD-R, Cartes SD

DTCP ➔ Transfert digital ⇔bus IEEE1394 (Firewire) et USB

HDCP ➔ Transfert vidéo ⇔ signaux DVI (v2) et HDMI

… et oui, nos écrans savent déjà faire de la PKI !

Cartes SD - Ressources sur Internet

Sites internet :

- Association SD : www.sdcard.org
- Consortium 4C : www.4centity.com

White papers et databooks :

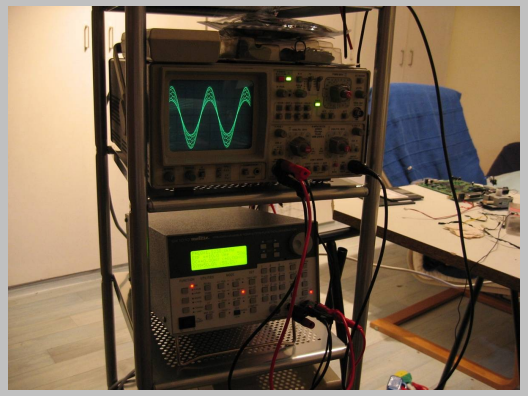
- Understanding SDIO Performance in Systems and Cards
  www.codetelligence.com/CodetSDIOPerf.pdf
- *SD Card Specification (simplified version of part E1)*
- *CPRM Specification, Cryptomeria Cipher (C2) Specification, etc.*
  www.4centity.com/docs/versions.html

Demandez-les moi !

« L'avenir ~~nous~~ appartient ! »

leur

Invitation : Mon labo hardware ➔ est à votre dispo (Paris) si vous voulez creuser la sécurité électronique ! (*je n'ai plus le temps*)



Merci de votre attention

Contact : bruno@kerouanton.net