

88

88

87

# EMV Security - A UK Payment Industry perspective

*Presented by*

Colin Whittaker

Head of Security



# Outline

- Understanding the Language
- Cardholder Verification Methods (CVM)
- Card Authentication Methods (CAM)
- The Terminal & Key Management
- Conclusions



APACS

# Understanding our Language

- Cardholder Verification Methods (CVM)
  - ◇ How do we verify at point of sale that the owner of the card is presenting the card to pay?
    - ◇ Forensic Signature
    - ◇ Biometric
    - ◇ PIN
- Card Authentication Methods (CAM)
  - ◇ Is this a valid and authentic card that has been presented?
    - ◇ Static data Authentication
    - ◇ Dynamic Data Authentication
    - ◇ Branding, image, hologram



# Cardholder Verification Methods (CVM)

- Which method should we choose?
- What happens if the CVM fails or does not work?
  - ◇ Fallback and priority
- How do we protect the CVM data?
- How do we verify the CVM data?
  - ◇ On the card?
  - ◇ Off the card locally?
  - ◇ Off the card in distant back end CVM databases?



APACS

## Card Authentication Methods (CAM)

- Are we authorizing transactions predominately on-line or off-line?
- Where are the risks in using SDA in an off-line environment?
- How safe and secure is static data?

## The Protection of Static Data

- Is any static data safe from counterfeiting?
  - ◇ Music, video and Film and Luxury Products
  - ◇ Identity Credentials
  - ◇ Magnetic Stripe data
  - ◇ ..... smartcards?
- Can smartcards protect static data?
  - ◇ Integrity and Authenticity can in principle be preserved,
  - ◇ But SIM card and Satellite chip cards have all been attacked
    - there is a large body of technical knowledge.
  - ◇ Java cards are now readily available and easy to use.



APACS

# Smartcard Tools Are Available

smartcard : an inexpensive BASIC programmable smart card - program your own smartcard - Microsoft Internet Explorer

File Edit View Favorites Tools Help


Address http://www.basiccard.com/

- Home
- Overview
- NEWS
- Free Download
- Development Kit
- Hardware
- Cryptofunctions
- Order online
- Distributors
- Service
- Press/Release
- Reference


Mail us!

changed: 30-03-2003  
by: lintercast

---



**ZeitControl**  
card systems GmbH



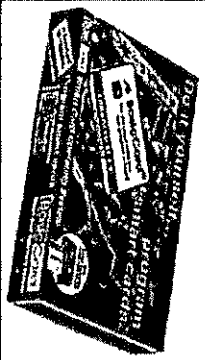
**BasicCard**  
Smart Card Operating System

Order Development Kit BasicCard®

**BasicCard® Development Kit**

Includes:

- 1x CyberMouse v1.050 Smartcard reader with a serial version
- 1x Balanced Reader
- 1x Software Development Kit (SDK) for Windows®
- 1x Documentation on CD-ROM
- 1x Technical manual (in printed form)
- 1x Enhanced BasicCard Z637 (2kByte EPROM)
- 2x Enhanced BasicCard Z639 (4kByte EPROM)



Price: 59,- € - plus shipping and postage (outside Europe)

Price: 59,- US\$ - plus shipping and postage (outside Europe)

View... | Previous | Next | Home | Search | 19:59



## Learning from the Experience of others

- In April 2001 The Carte Bancaire Scheme 320 bit Private Key was successfully factored and openly exposed on the Internet.
- This led to the production of fraudulent cards with valid data, but which for invalid accounts, signed by this compromised scheme private key; including the ability to say “yes” to any PIN
- By 1 Jan 2002 Carte Bancaire had successfully migrated all cards to a longer key length,
- But in Nov 2001 .....

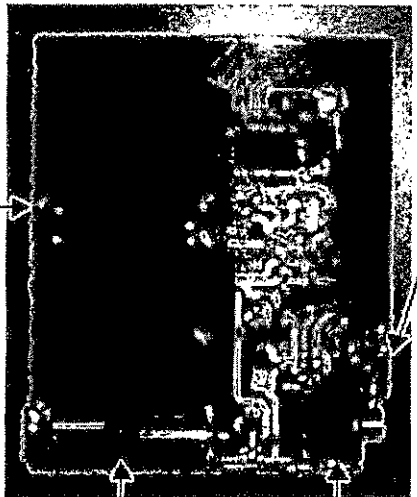


APACS

# Smart Card Copying Tool

## CLONEUR DE POCHE PAR MAX SIRIUS9

Connecteur de programmation du

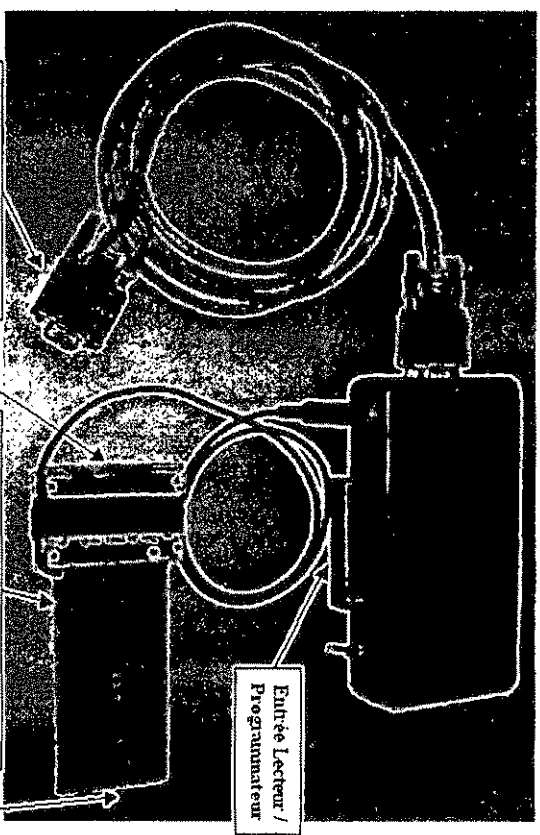


Connecteur de carte à puce

Prise PC

Ce petit appareil permet de recevoir ou envoyer toutes les zones d'une CB vers le PC via mon Box, de lire des CB, de programmer une YesCard avec toutes les zones d'une CB stockées dans sa mémoire. Les zones d'une CB

LECTEUR / PROGRAMMATEUR / LOGUEUR pour PC



Prise série DB9 pour PC

Entrée Lecteur / Programmeur

Dispositif pour Loger (enregistrer les communications entre une CB et un terminal de paiement).

Entrée de la CB pour le Log

Sortie vers le TPE pour le Log



APACS

# Terminal Requirements

- Smartcards require a terminal
  - ◇ The CAM and CVM requires an interaction between Card and terminal
- The terminal must be secure and not subject to compromise
  - ◇ UK PIN Entry Device Protection Profile for Point-of-Sale Applications
- Scheme Public Key distribution
  - ◇ Which public key should be used for what smartcard ?
  - ◇ How do you update or revoke them?

## Conclusions

- Risk management requires an understanding of the end-to-end process and the entirety of the scheme, card, key, terminal and user lifecycle
  - ◇ It is not just about a public key cryptography and smartcards
- Solutions must be tailored to need and be capable of surviving and evolving over time to new threats
  - ◇ On-line vs off-line; SDA vs DDA; key length
- These cards and terminals are in the public domain their perception is critical
  - ◇ Reputation and credibility are as important reasons to get it right as are overall security needs