# Managing Smart Card Field Returns

## A Joint Presentation from:

GEMPLUS

Oberthur Card Systems
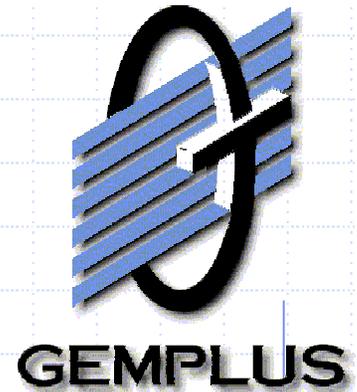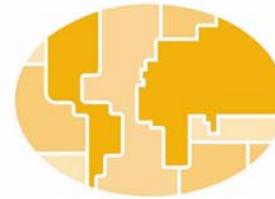
Schlumberger

# Perfection is not of this World

◆ Smart Card systems are subject to the laws of physics and need to be monitored (mainly during the first years) in order to guarantee a good quality of service to end users

- Passwords may be forgotten
- Cards may fail
- Terminals may go crazy
- Application software may have errors
- Card personalization may be incomplete or incorrect
- Users may not know what they are doing wrong

*Got a **BUG**?*

◆ Smart cards consist of an integrated circuit component embedded into a piece of plastic but may also have embossing, a magnetic stripe, or other features. When one element fails, the whole card may need to be replaced
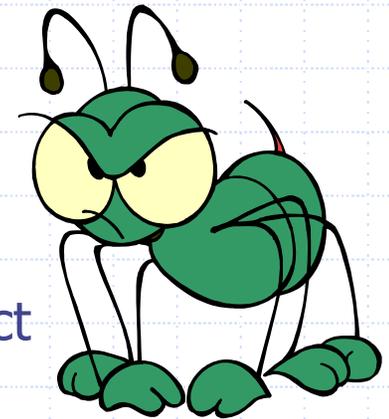
# Monitoring is Important
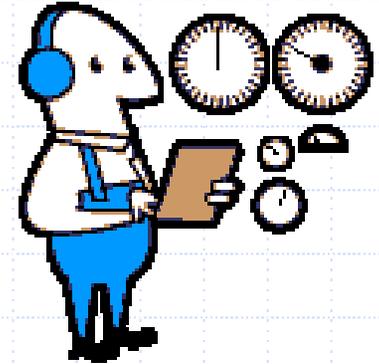
◆ Faulty terminals may stress chips in cards, shortening their lives.

◆ Cards with weakened components may stress terminals and alter their characteristics

◆ Cards combining multiple technologies may have one technology generating problems for the others

◆ Components from different vendors may not be identical and could behave differently when used at the limits of their specifications (mainly true for non micro-processors cards and contactless interfaces).

# Acknowledgments & Caveats

- All numbers in this presentation come from European applications using > 1 million cards.

- Nothing is specific to any given chip or card manufacturer.

- Not all applications used micro processor chips. Micro processor chips do have a much higher resistance to failure than simple memory chips.

- Most numbers were collected between 1998 and 2001. Unless specified, they have not been updated to present as most of these applications have now reached stability and no longer require close monitoring.

# Life is Tough !
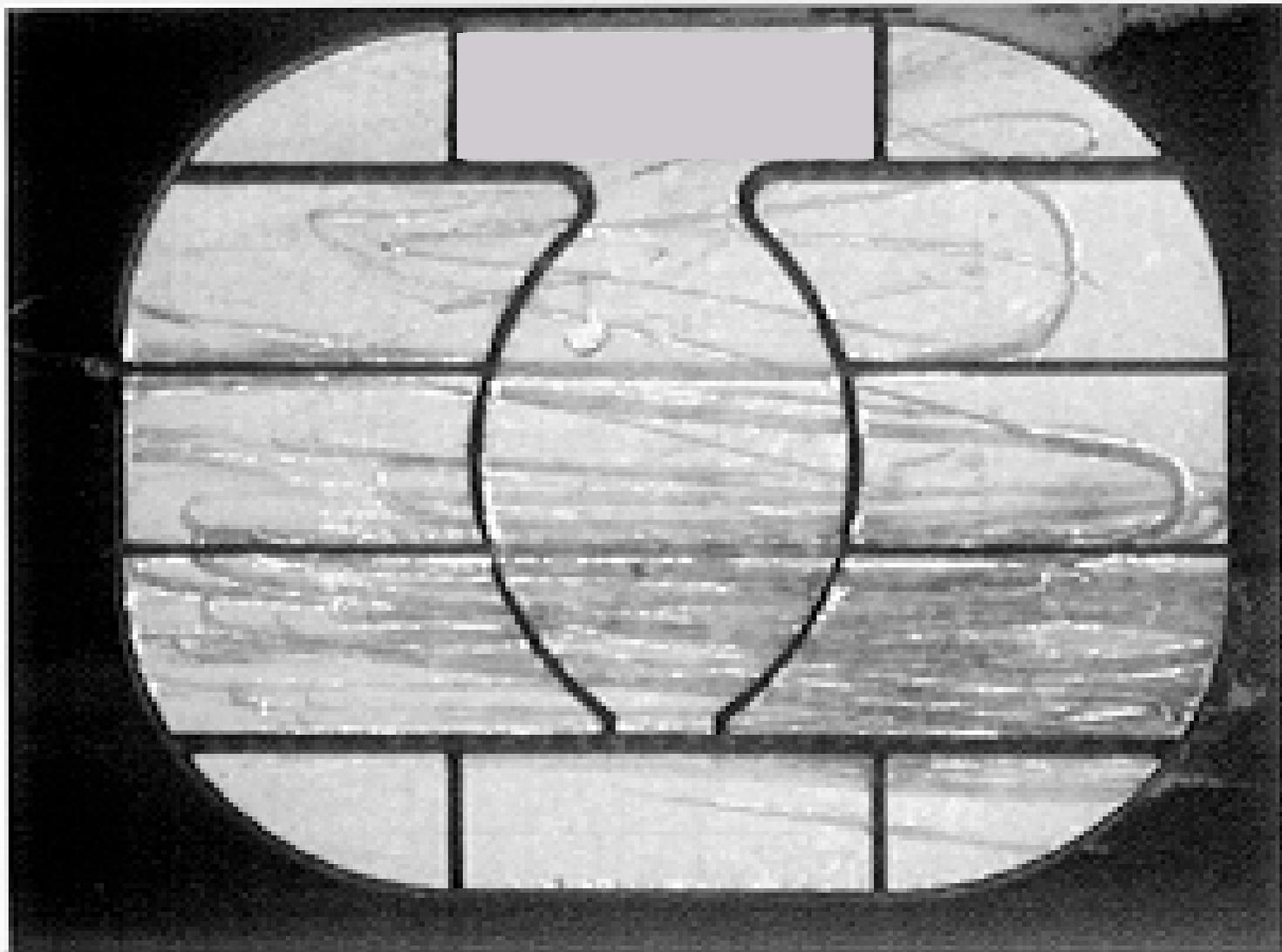
# Give me a break !
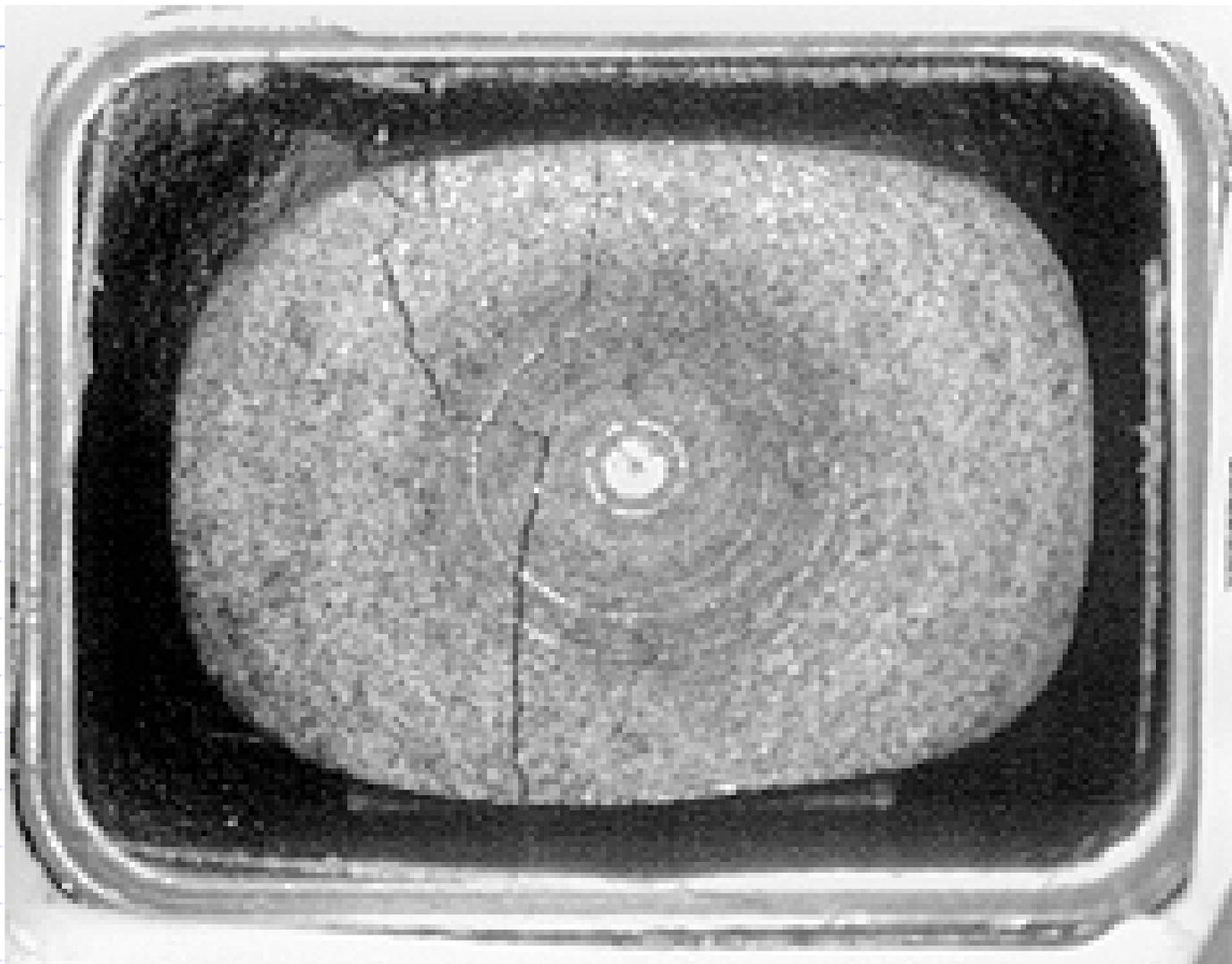
# A broken relationship !
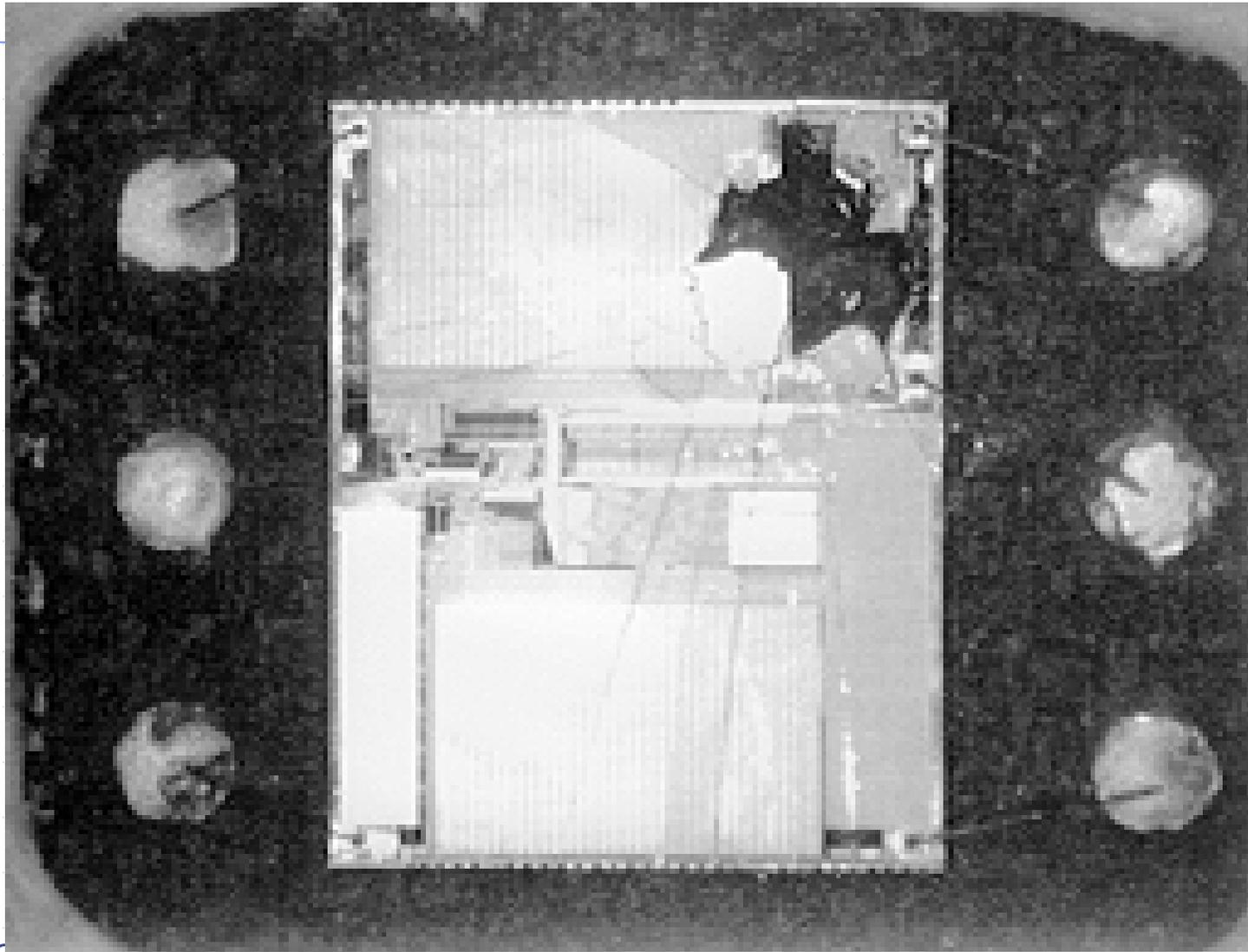
# Banking Application (1/2)



Legend: IC Functional | Pin Locked on card | Other Logical Error | Physical Abnomalies
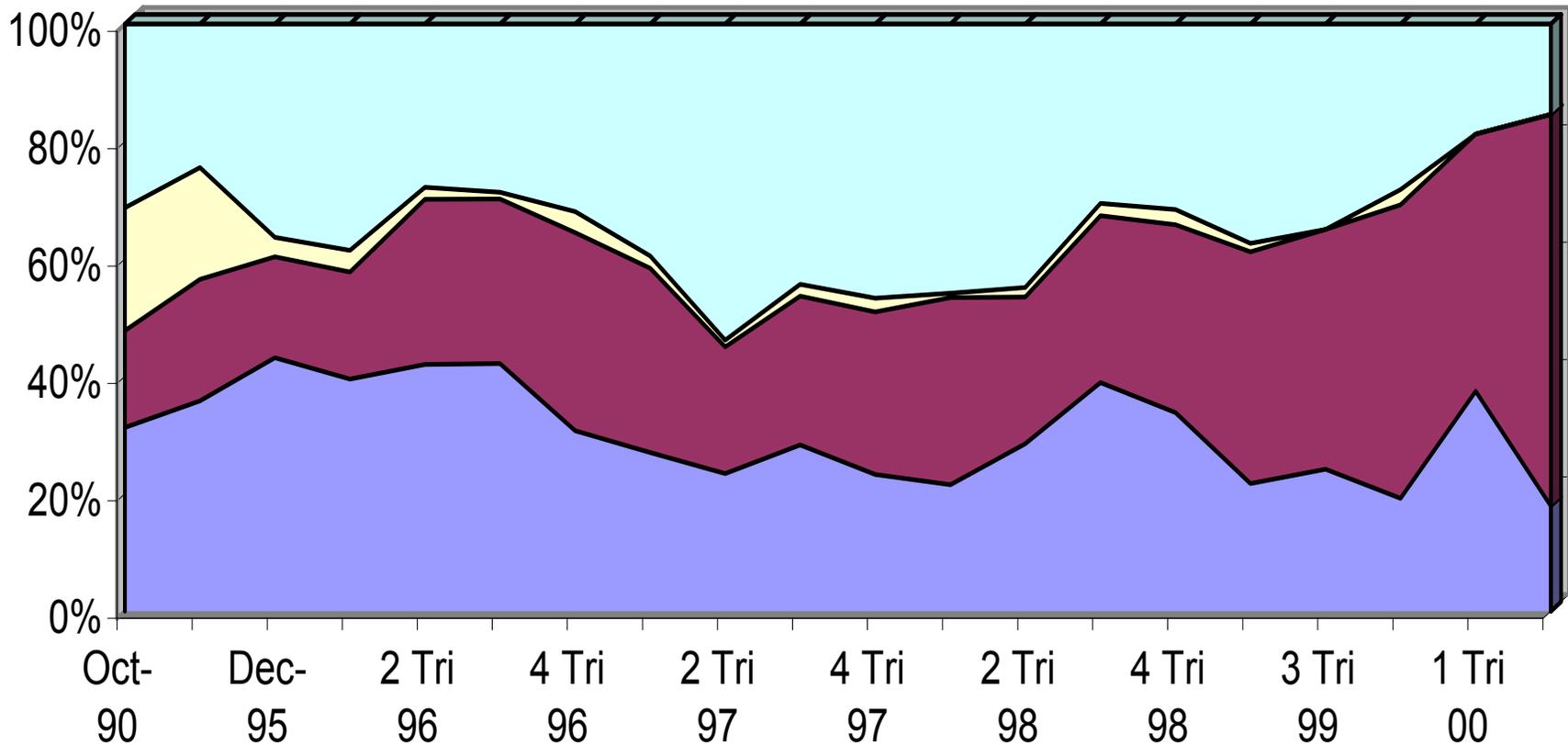
# Banking Application (2/2)

- Cards are issued for two years

- They have a microprocessor chip, a magnetic stripe and are embossed

- About 30% of the cards returned as failed are fully functional

- About 40% of the cards are locked because of PIN presentation errors (3 consecutive errors locks the card)

# Cellular Phones - GSM (1/2)

**GSM SIM cards**

Quantity Delivered

PPM

Field Return PPM row: 0 0 0 17 10 13 21 25 23 21 20 27 31 28 25 25 27 28 28 28 26 25 23 22 21

Values: 0 5 0 2 7 2 1 3 1 14 9 0 0 2 8 2 3 0 2 1 0 0 0

0 0 0 1 2 4 0 0 1 2 2 0 0 4 1 2 3 1 0 0 0 0 0

0 5 5 8 17 23 24 27 29 45 56 56 56 62 71 75 81 82 84 85 85 85 85 5

0 5 0 3 9 6 1 3 2 16 11 0 0 6 9 4 6 1 2 1 0 0 0

Legend: Quantity delivered — Field Return in PPM

Months: S O N D J F M A M J J A S O N D J F M A M J J A S
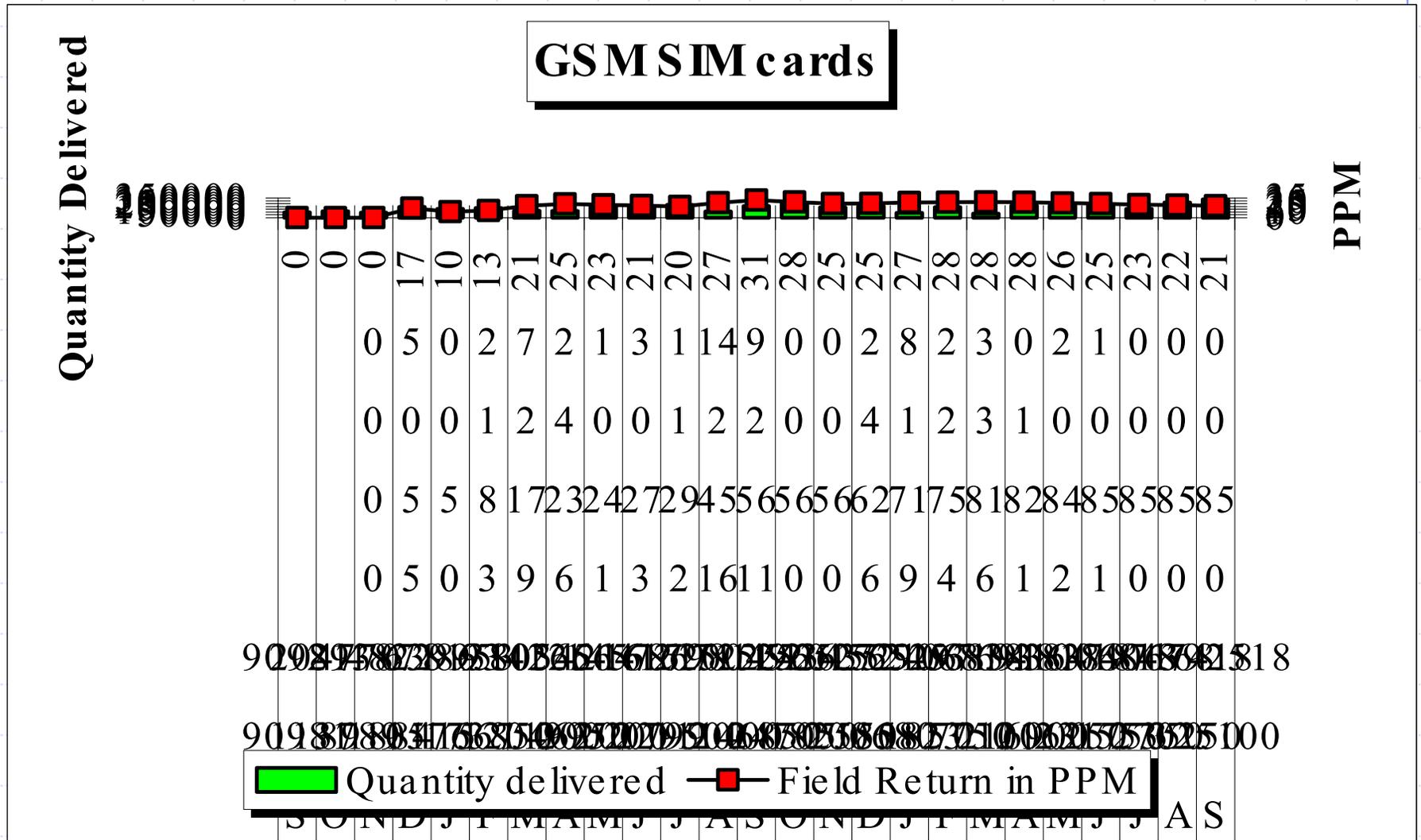
# Cellular Phones - GSM (2/2)

- Card stays most of the time in the same phone (no mechanical stress by insertion)

  - Low return rate (less than 35 PPM)

- Quite high memory update activity

  - EEPROM memory cells were not guaranteed by the IC manufacturers over 100K updates in early products

- As in most Smart Card applications, returns start to happen about three months after the cards have been delivered.

# Microprocessor cards 1/2



**Type of defect (in %) for 1999 for Microprocessor Products**

Legend: GSM, Other Micro

Categories: PIN/Password lock, Memory Pb (9240), Broken chip (Customer/perso), Use (Dirt,,,), Defect not found, Assembly defect, Good card, Application error (soft), Component defect, Visual G+, Grinding, Virgin memory
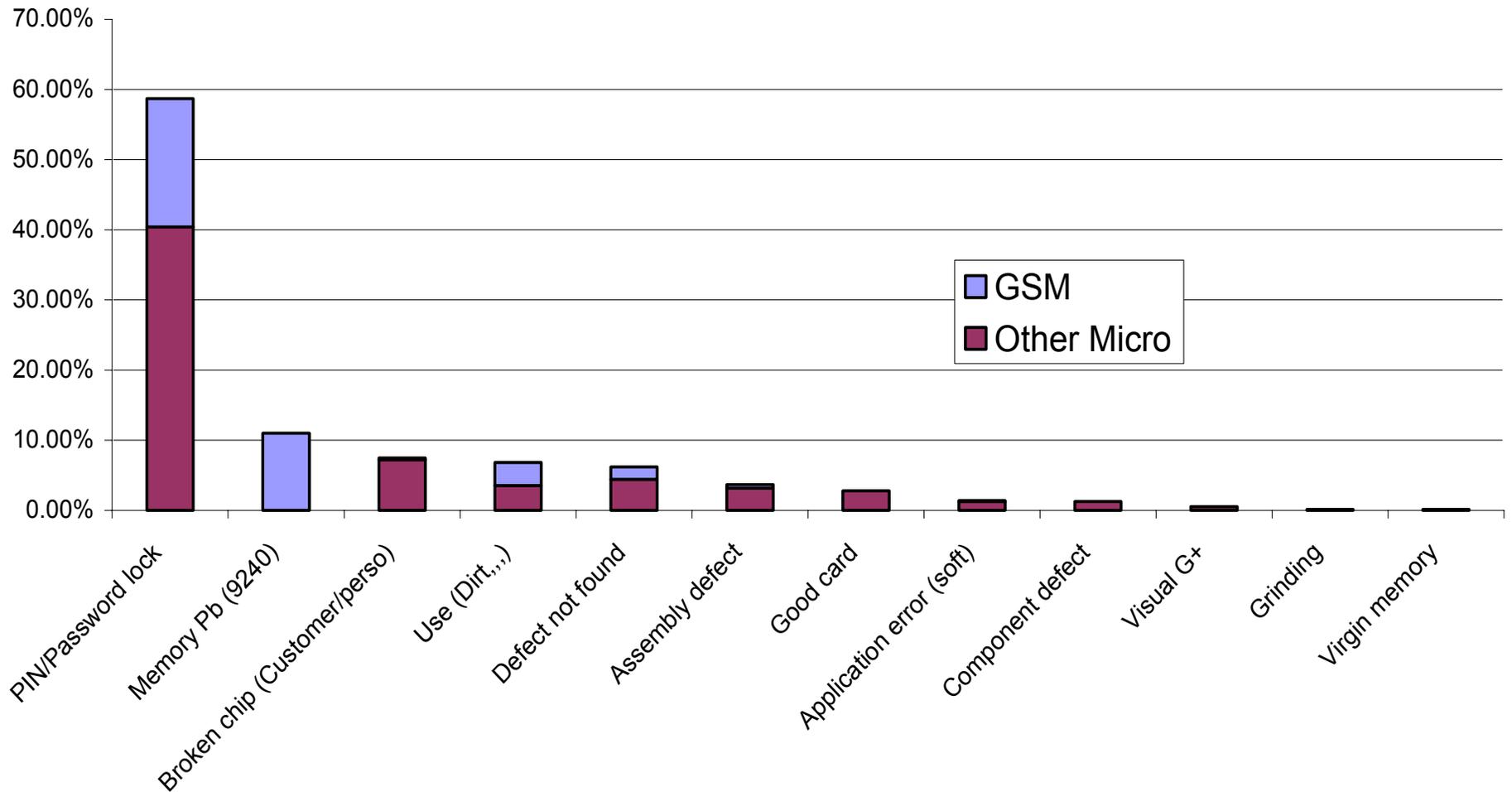
# Microprocessor cards 2/2

◆ Security locked is the main reason for cards to be returned (PIN or Password locked)

◆ Applications with high memory update activity required a specific memory management with early EEPROM technologies

◆ The third main reason for failure is mechanical (chip broken) and improves with customer education

# Payphones - Multiple suppliers

**Payphone Field Return Rate in PPM by suppliers**

Defectives components affect all card manufacturers at the same time but impact may depend on the card embedding process

7878

2059  3146  2588  3938  48

316  314  210

320  716  603  1208  1789  1472  1424  766  598  1599  657  59

503  786  427  744  857  606  588  404  281  642  219  2

289  466  292  442  467  362  328  241  181  420  159  2

61  380  159  369  215  271  415  285  204  468  108  1

8000

6000

4000  ppm

2000

0

Dec-99  Nov-99  Oct-99  Sep-99  Aug-99  Jul-99  Jun-99  May-99  Apr-99  Mar-99  Feb-99  Jan-99

# Payphone Cards

◆ Synchronous cards are much more sensitive to their environment (terminal) than microprocessor cards

◆ Getting the terminals and the PLA* chip to work correctly is not trivial and sometimes requires serious mods to the terminal software and some chip re-design

◆ Having multiple suppliers of chips and cards allows pinpointing of the issues coming either from the chip manufacturing or from the chip embedding process

*** PLA = Programmable Logic Array**

# Loyalty Application

Percentages by
type of failure



Chart categories:
- **Pin code Locked**
- **Application error**
- **No defect detected**
- **User errors**
- **Broken wires**
- **ESD (*)**
- **Chip broken**

Y-axis values: 60.00%, 50.00%, 40.00%, 30.00%, 20.00%, 10.00%, 0.00%
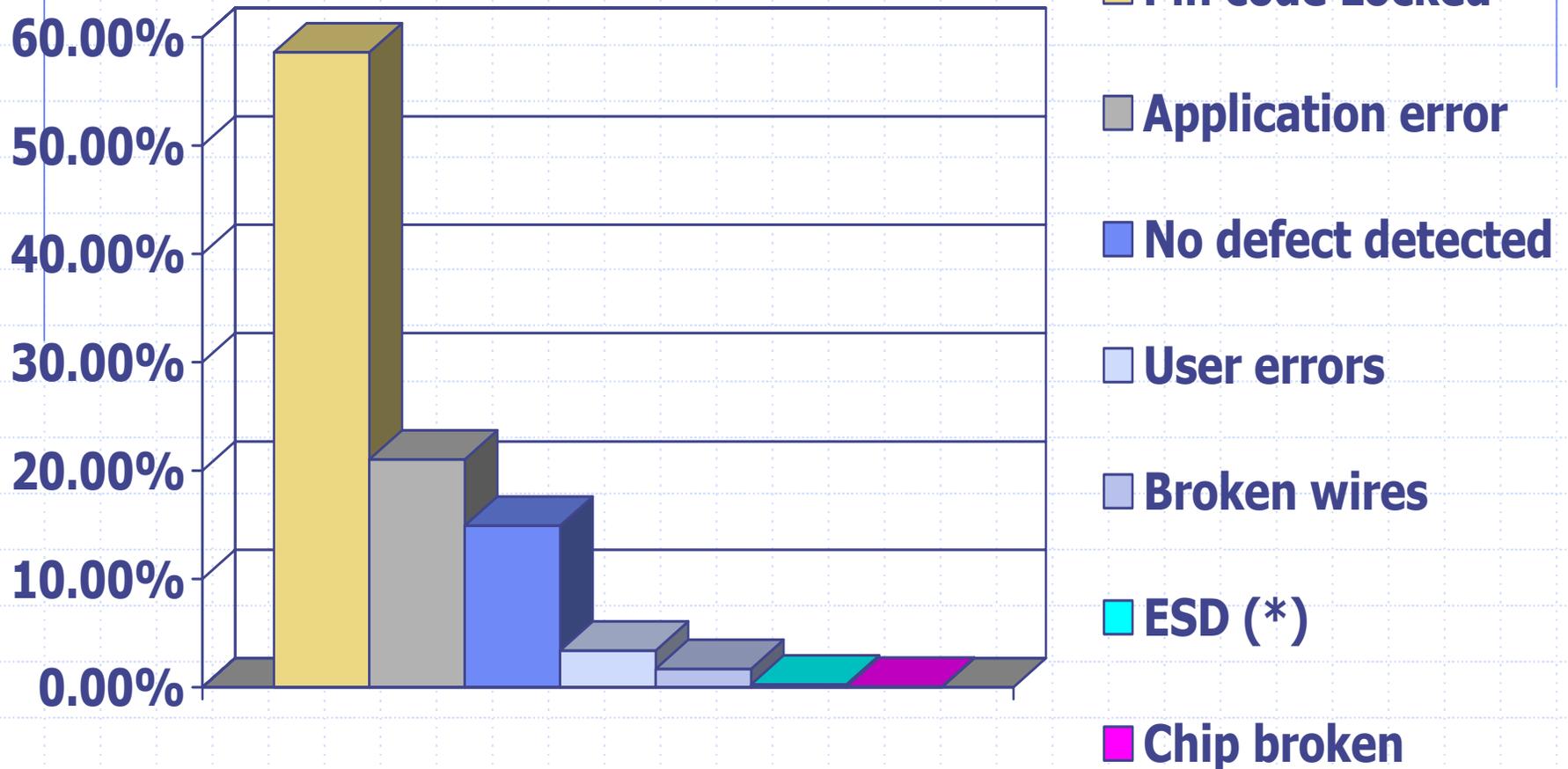
*(*) ESD = Electro-Static Discharge*

7/22/2003

16

# CAC - Fort Bragg Analysis

- **136 randomly sampled cards were monitored during four months in 2002**
  - Lamination damage observed (25%)
  - PIN unknown or forgotten (20%)
  - Printing wear signs
  - Incorrect use or abuse of card (e.g. chewed corners)
  - Repeated use of mag-stripe increases wearing
  - Some ICCs with visual corrosion signs
  - Lack of training/awareness of ICC use/protection
- **No terminal analysis even though some could be the reason for card damage**
- **No detailed reason analyzed at this point for non-functional cards (chip functions)**

*At the time of the study, there were 1.1 million CAC cards issued*
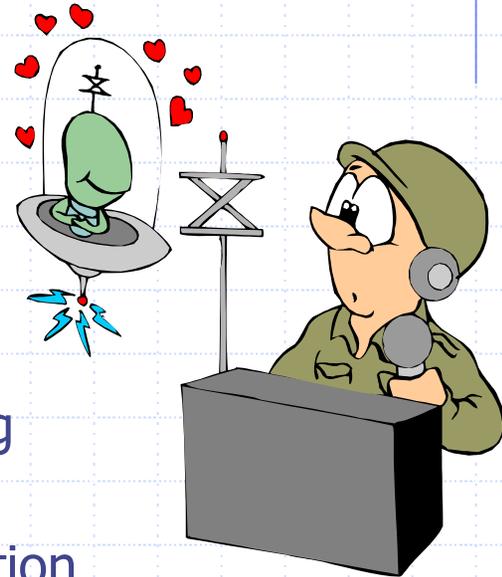
# Contactless Cards Type of defect



Legend:
- Out of Specification
- Good cards
- Die or Wire broken
- Bad Personalization
- Defect unknown
- Antenna issue
- Application error
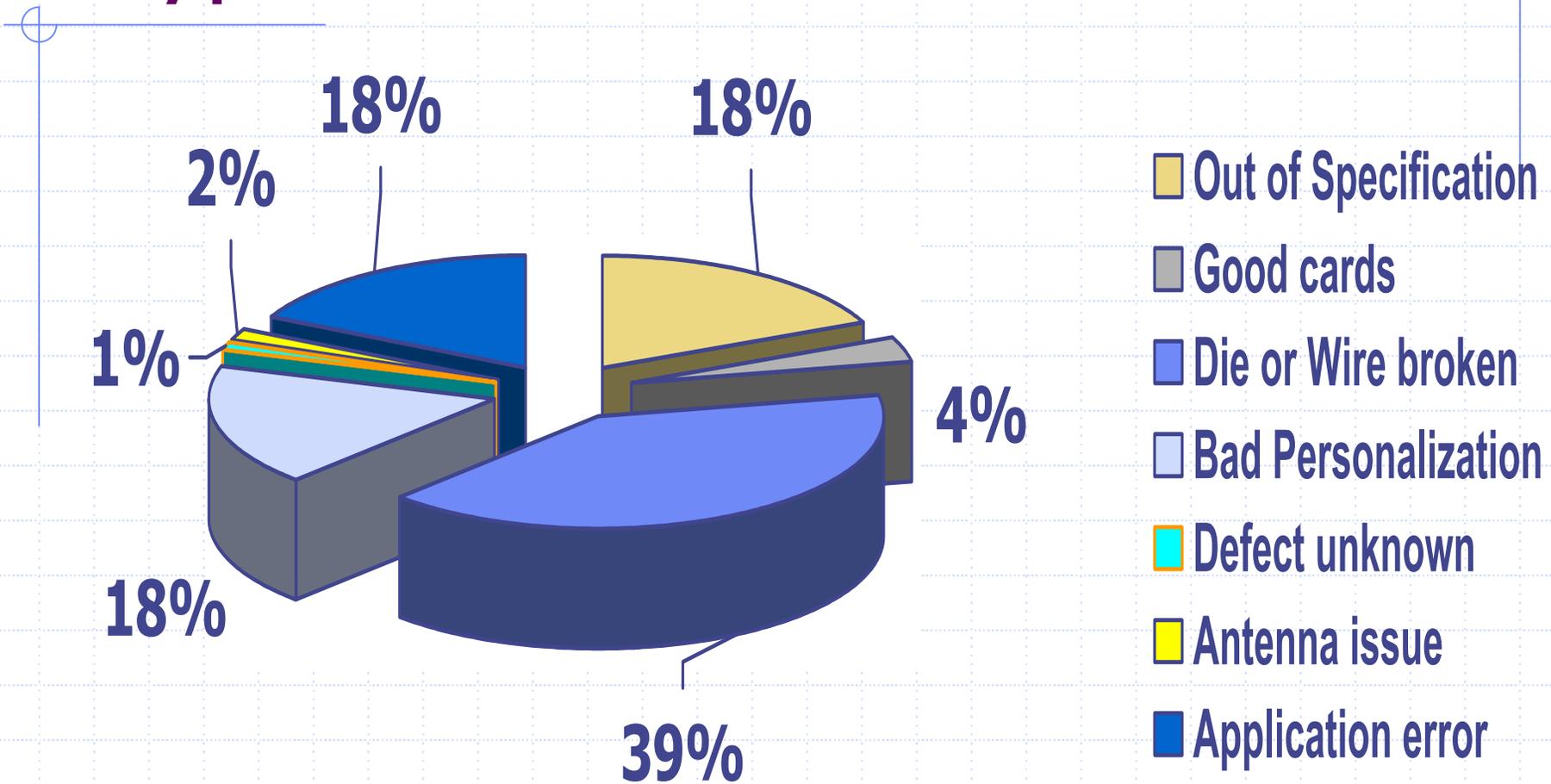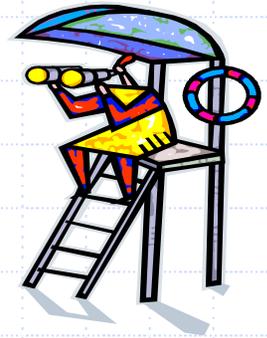
# Standard Warranty

◈ Today, for cellular phone cards as well as financial cards, the standard warranty from card manufacturers is:

***Up to 500 cards failing per million sold over a period of three years and used in normal conditions will be replaced by the card vendor.***

Above this rate is considered abnormal and a joint study by suppliers and application providers will generally be initiated.

# Why should card returns be monitored:

◆ Increases end-user confidence (they have a process for recourse)

◆ Allows retention of manufacturers with high quality products

◆ Increases the security of the application (non-functional cards are collected and accounted for)

◆ Allows faster detection of the nature of the problem

- IC failures (process error, batch issue, passivation, etc.)

- Packaging failure (glue, plastic, epoxy resin, etc.)

- Operating System or Application error

- Security vs. Convenience balance (PIN locks)

- User error (training issue)

- User abuse (training issue)

- Terminal error (incorrect electrical signals, glitches, etc.)

- Terminal context (heat, external signals, etc.)

- Use of one technology creating a hazard for another one on the card (e.g. mag-stripe readers breaking the chips)
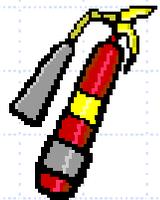
# Conclusions
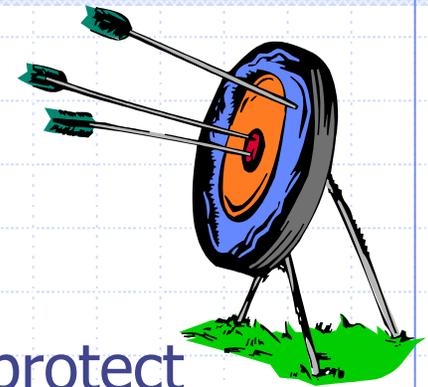
- All applications using a PIN or password to protect a smart card must be prepared for high return rates

- Using the card to scrap ice off windshields or hammering the chip will break the silicon component

- The more often the card is inserted into a terminal the faster it ages. Mechanical stress, power-on/power off, password presentation, memory updates

- Cards with a high number of updates on the same data do require a specific memory management in the OS

- ESD has never been seen on the radar screen as a problem - for contact smart cards

- Frequent changing of suppliers may lead to failures

# Contact Information

**Gilles Lisimaque** - Senior Vice President
**Gemplus Corporation**
Gilles.Lisimaque@Gemplus.com
http://www.Gemplus.com
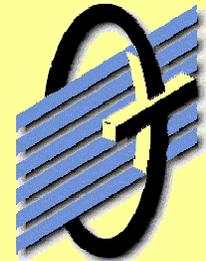
**GEMPLUS**

**Christophe Goyet** *Director Program Management*
**Oberthur Card Systems**
Christophe.Goyet@oberthurusa.com
http://www.oberthurusa.com

*Oberthur* Card Systems

**Craig Diffie** - Marketing Manager
Schlumberger - Smart Cards
cdiffie@slb.com
http://www.slb.com

**Schlumberger**