Cetelem

A BNP PARIBAS company

Training

EMV

1/2

Functional Concepts & Technical Items

Q1 200

AGENDA

INTRODUCTION

GENERAL DEFINITIONS of EMV

Cetelem
A BNP PARIBAS company

INTRODUCTION

EMV ?

WHO is concerned by EMV

AIMS of EMV Technology

General Concepts of EMV

EMV Specifications

EMV Architecture

Cetelem
A BNP PARIBAS company

What is EMV ?

EMV, developed jointly by Europay, Visa & Mastercard is significant standard, which ensures global interoperability of chip payment transactions.

EMV is a "toolbox" which defines all the possible interactions between card and terminal.

An EMV terminal must support all possible EMV-defined interactions.

An EMV card, on the other hand, only needs to support a subset of the EMV standard (like M/Chip from Mastercard, Vis from Visa).

Cetelem
A BNP PARIBAS company

What is EMV ?

The toolbox for Chip Transaction and the domains concerned

DEBIT/CREDIT TRANSACTIONS

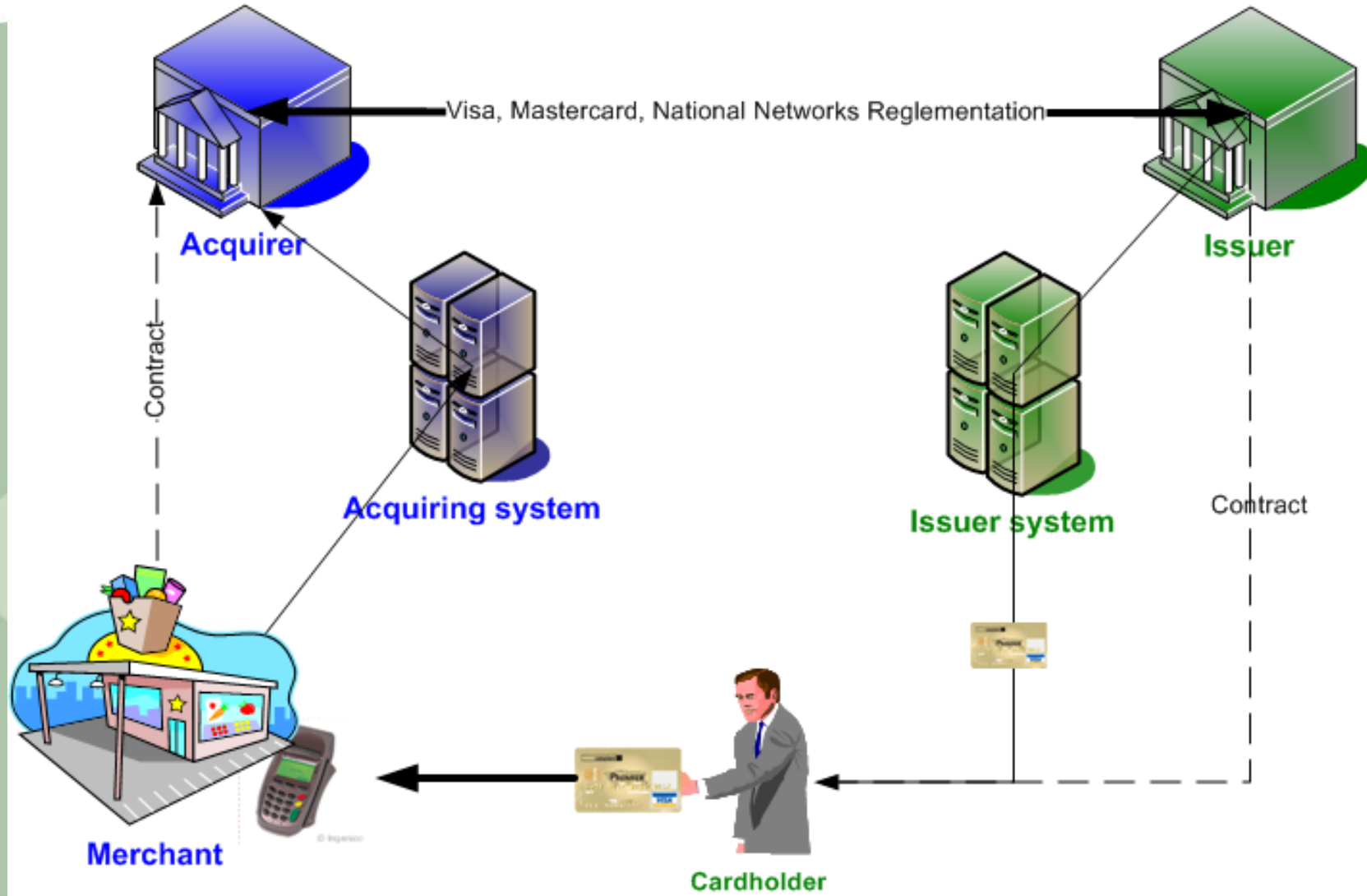
- Common Specification for international cards belonging to both networks (and more…)
- First diffusion: version 3.1.1 May 1998 : EMV96
- Version 4.1 since June 2004
- Project CPA (Common Payment Application :Specs v1.0 (Dec. 2005)

Functional Domains concerned

- Cards (components, mask, data),
- Cards Manufacturing and Personnalization
- Terminal (POS or ATM) merchants management
- Issuer (authorization systems, cardholders management)
- Clearing systems
- Security
- Systems Approvals and Agreements
- National and International Reglementation

Cetelem
A BNP PARIBAS company

ACTORS in EMV CHAIN



ADVANTAGES with EMV

INTEROPERABILITY

- At Issuing side, future EMV cards could be used anywhere, national or international
- At Acquiring side, every accepting system must treat all EMV cards in chip mode.

RISK MANAGEMENT

- Part of Issuer most important in cinematic of payment/withdrawal transaction at accepting point (floor limit, on-line/off line, card decision)

SECURITY

- Security improved in EMV environment. Dynamic authentication card-terminal, crossed authentication card-issuer.

MULTI-APPLICATION COMPLIANT ENVIRONMENT

- Another card application can be hosted on the chip with such EMV architecture

LIABILITY SHIFT

- The non-EMV component meets the cost of fraudulous transcaction if the other component is EMV

Cetelem
A BNP PARIBAS company

GENERAL CONCEPTS of EMV

EMV allows an off-line risk management with final decision commonly taken by card (Issuer) and terminal (Acquirer)

3 choices are available

- On-line completion, Off-line completion, Rejection

Issuer defines the rules allowing the card to take decisions during transaction

In on-line mode only Issuer can decide to accept or reject the transaction

EMV has been created by card Issuers

- Important impact on Card Risk Management

Cetelem
A BNP PARIBAS company

GENERAL CONCEPTS of EMV (example 1)

Transaction Off-Line

I want 80€ transaction off-line.

Do you accept ?

①

Yes, with approval certificate

②

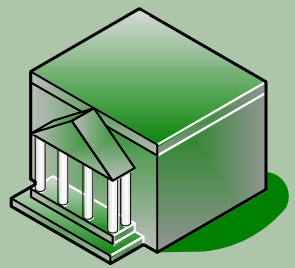
Terminal EMV

Card EMV

Risk management on_line :

- amount > 100 €
- every 3 transactions

GENERAL CONCEPTS of EMV (example 2)



Issuer

Do you accept this 180€ Transactions? With certif.

④ ③

Yes I do With certif.

Terminal EMV

I want 180€ transaction off-line.

Do you accept ?

①

No, ask to my bank

With certif. (180 € > 100€)

②

Your bank is ok

Give me your certif.

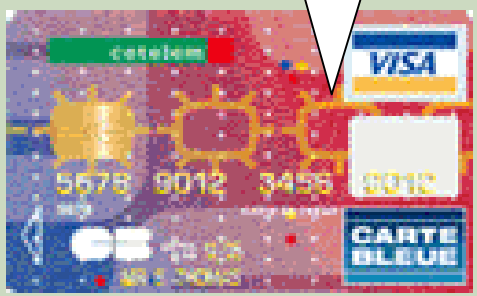
⑤

OK, here it is

⑥

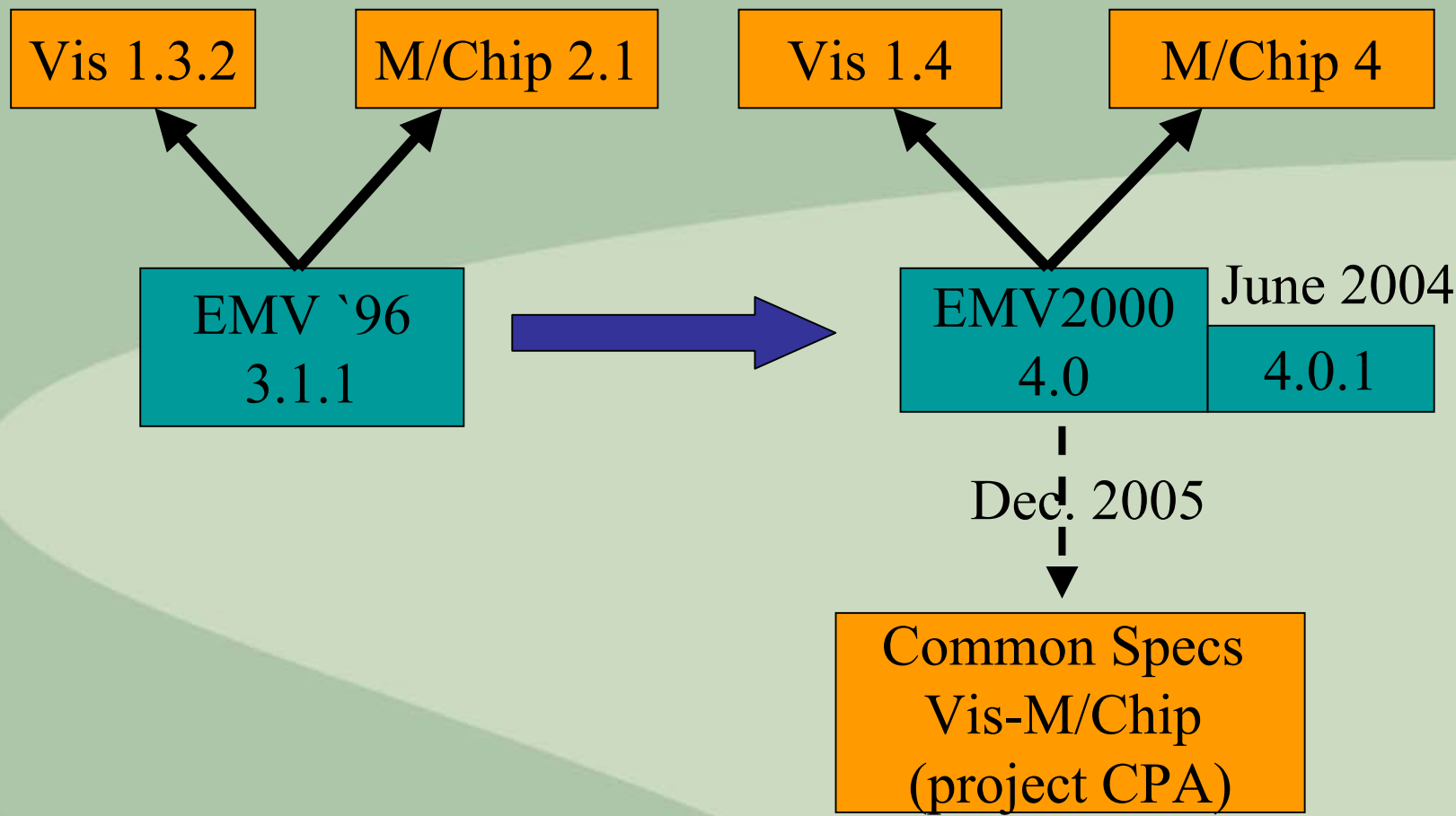
Risk management on_line :

- amount > 100 €
- every 3 transactions



Card EMV

EMV SPECIFICATIONS overview



Cetelem
A BNP PARIBAS company

EMV 2000 SPECIFICATIONS

Restructuration of specifications

- Book 1: Interface ICC-Terminal
- Book 2: Security and Key Management
- Book 3: Application Specification
- Book 4: Cardholder, Attendant, Acquirer Interface

Evolution EMV2000 (compared to EMV96)

- Physical Level: timing tolerance improvment
- Application Level: security improvment

Cetelem
A BNP PARIBAS company

ICC SPECIFICATIONS

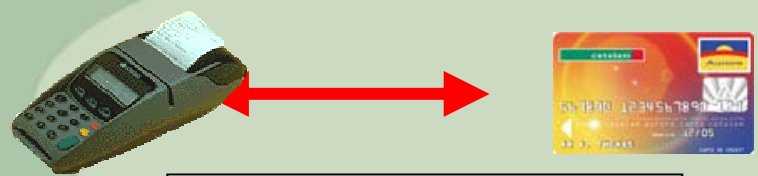
ISO 7816- 1/2/3

EMV Book 1

-Physical Characteristics

- Electrical Characteristics

- Communication Protocol



EMV Book 3

- Application Selection

ISO 7816-4

EMV Book 1

- Files Structure

- Data

- Set of commands

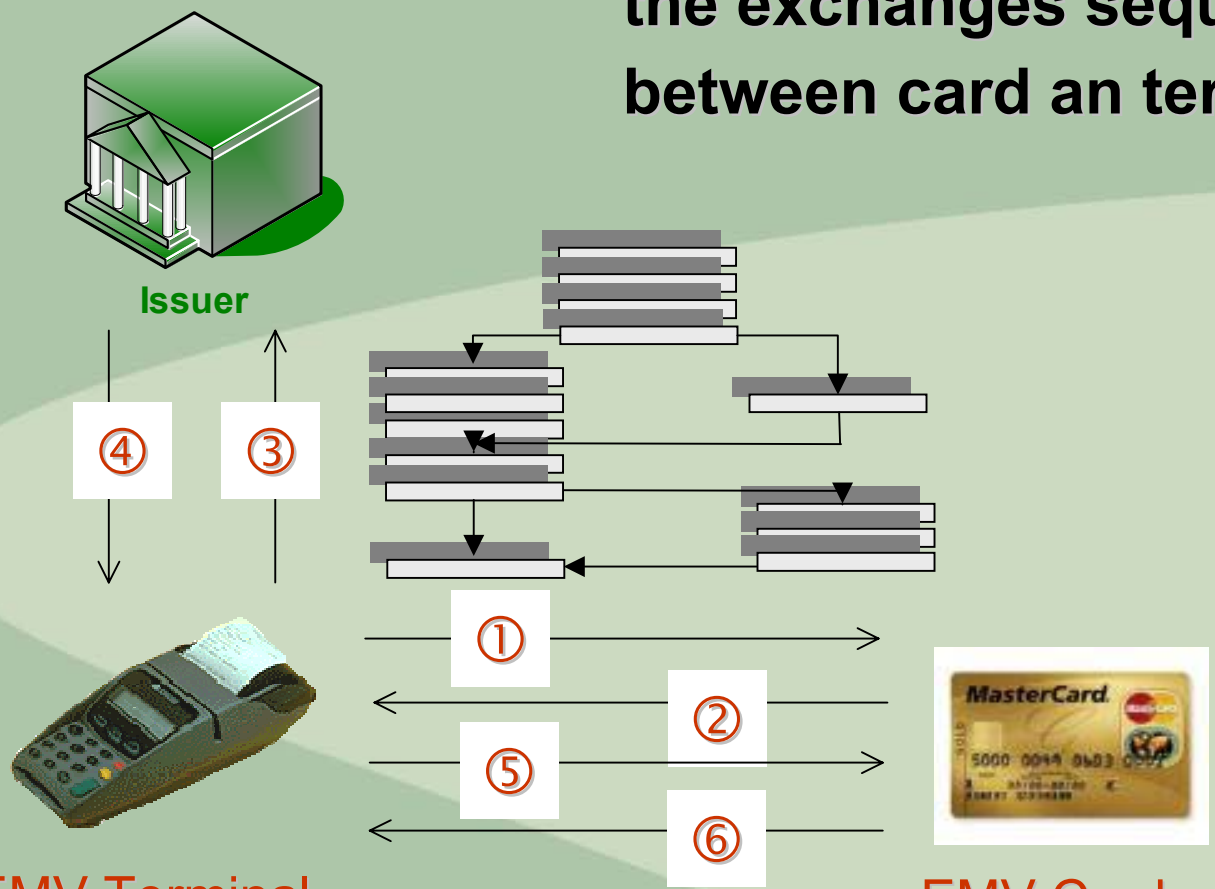
EMV Book 2

- Security Mechanisms

Cetelem
A BNP PARIBAS company

ICC APPLICATION SPECIFICATIONS – Book 3

– **Defines the card application and the exchanges sequencies between card an terminal**



Cetelem
A BNP PARIBAS company

ICC TERMINAL SPECIFICATIONS – Book 4

Type of Terminals

Functional Requirements

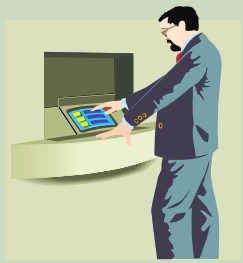
Physical Characteristics

Security Characteristics

Software Architecture

Interfaces

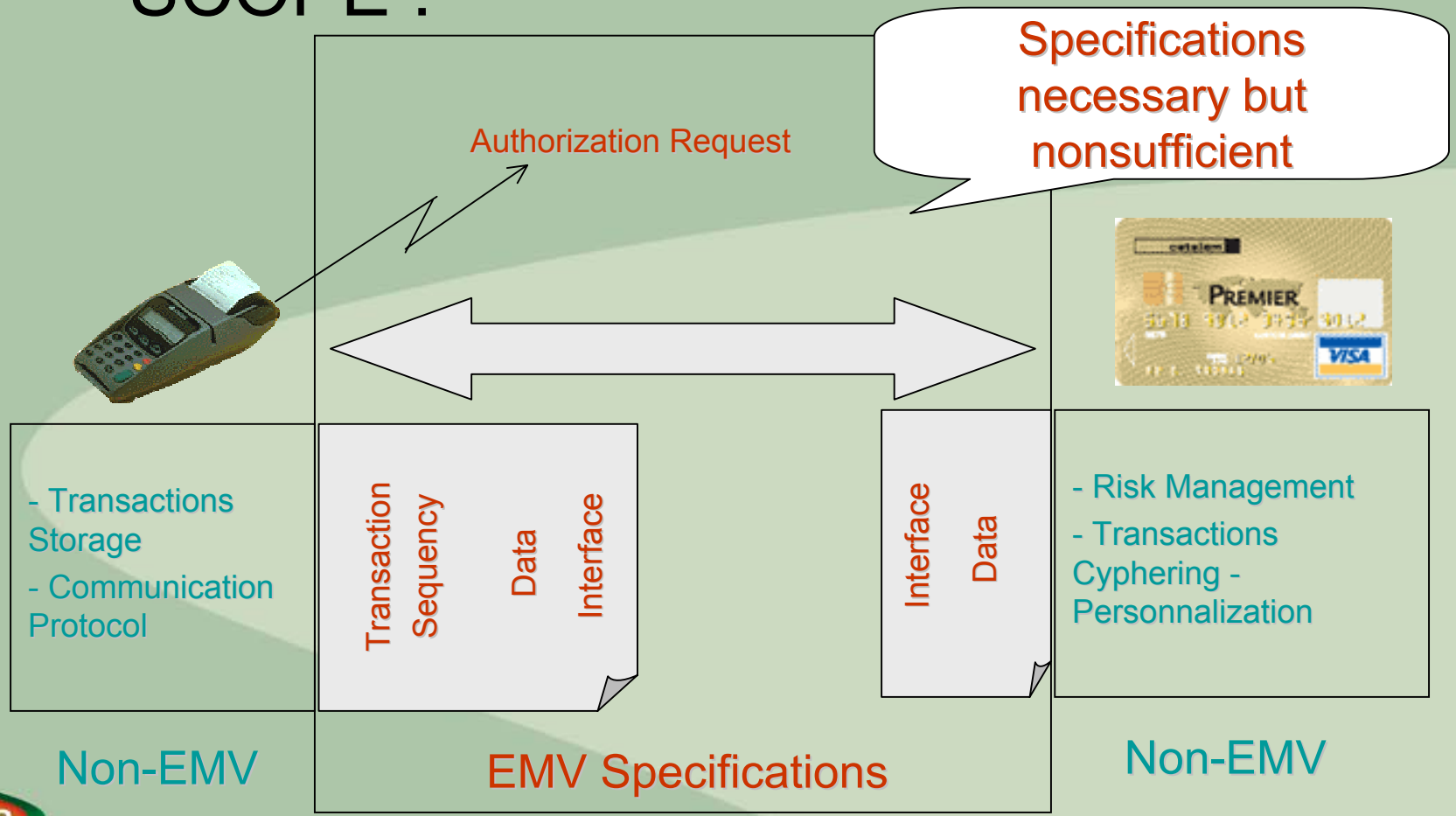
- Cardholder
- Attendant
- Acquirer



DAB

EMV SPECIFICATIONS

SCOPE :



APPLICATION OF EMV TERMINAL

Implementation Specification
Mastercard, Visa

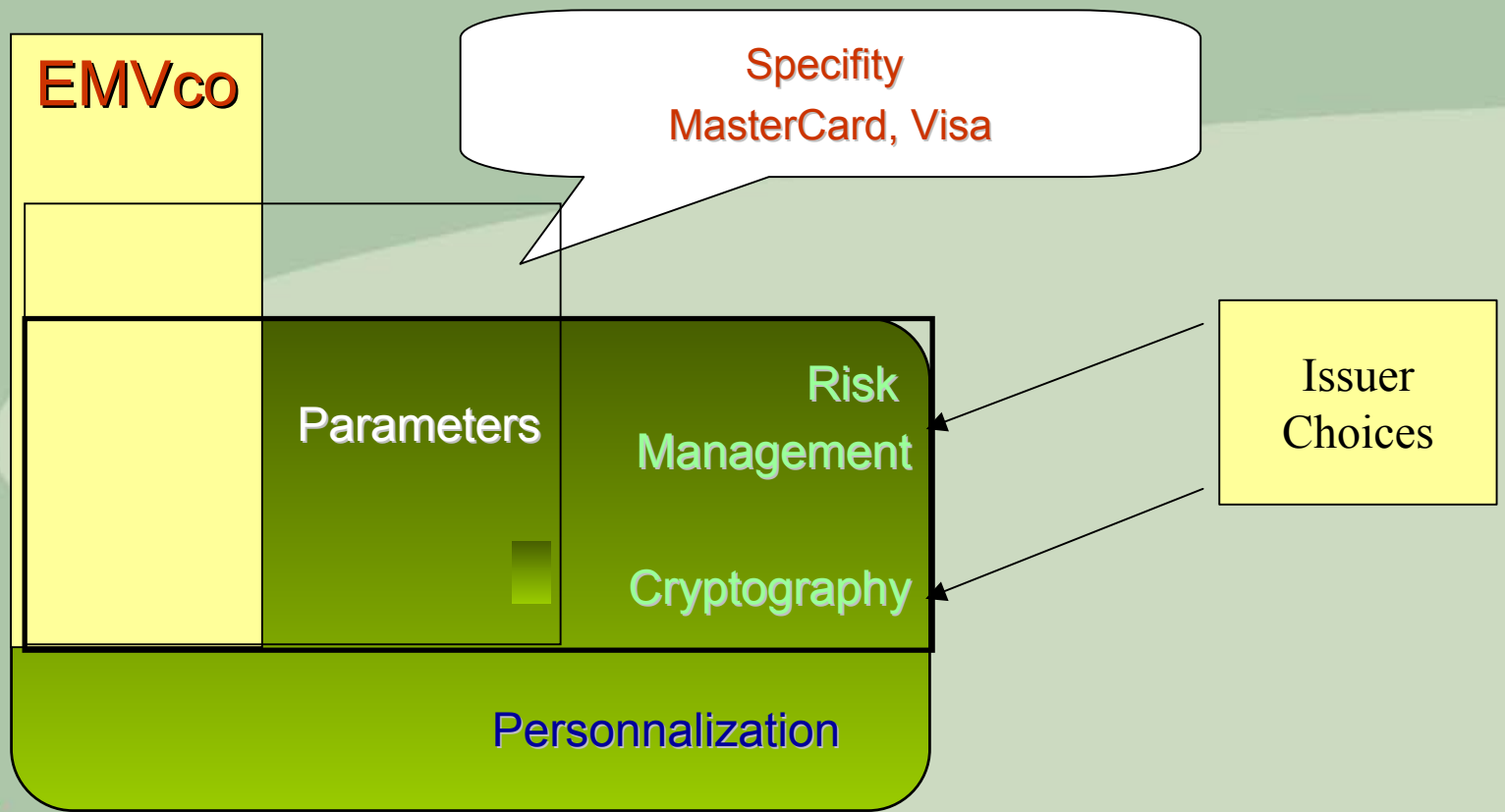
EMV

Application EMV terminal
Ex : MPEV5.2 for C.B. in France

Parameters Acquirer Protocol of communication Storage of transactions	- Parameters - Format of authorizations -Specific Functions	Sequency of transactions Interface

Cetelem
A BNP PARIBAS company

EMV CARD APPLICATION

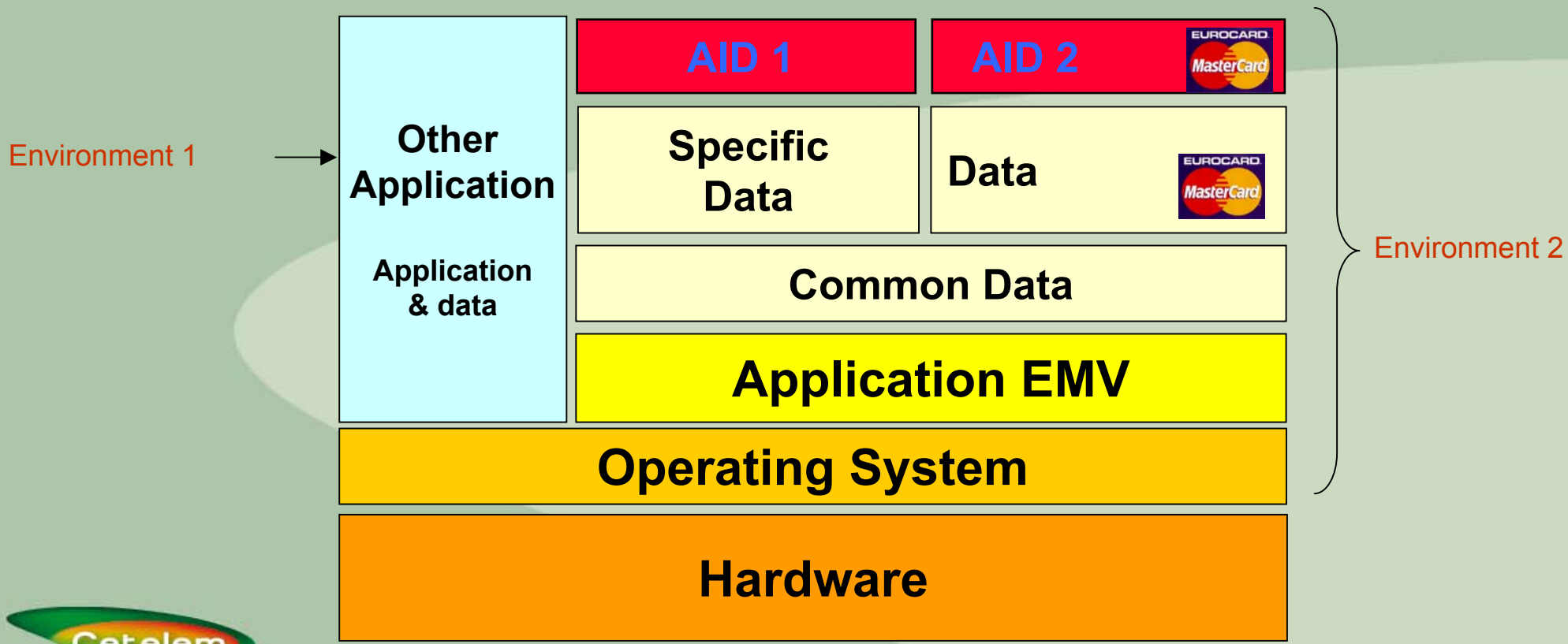


THE EMV CARD

ARCHITECTURE of EMV Card

EMV DUAL CARDS (coexistence of several independent environments)

- Examples MasterCard Card with national application, international application, other applications
- Characteristic : Operating system « close »



DATA MANAGEMENT

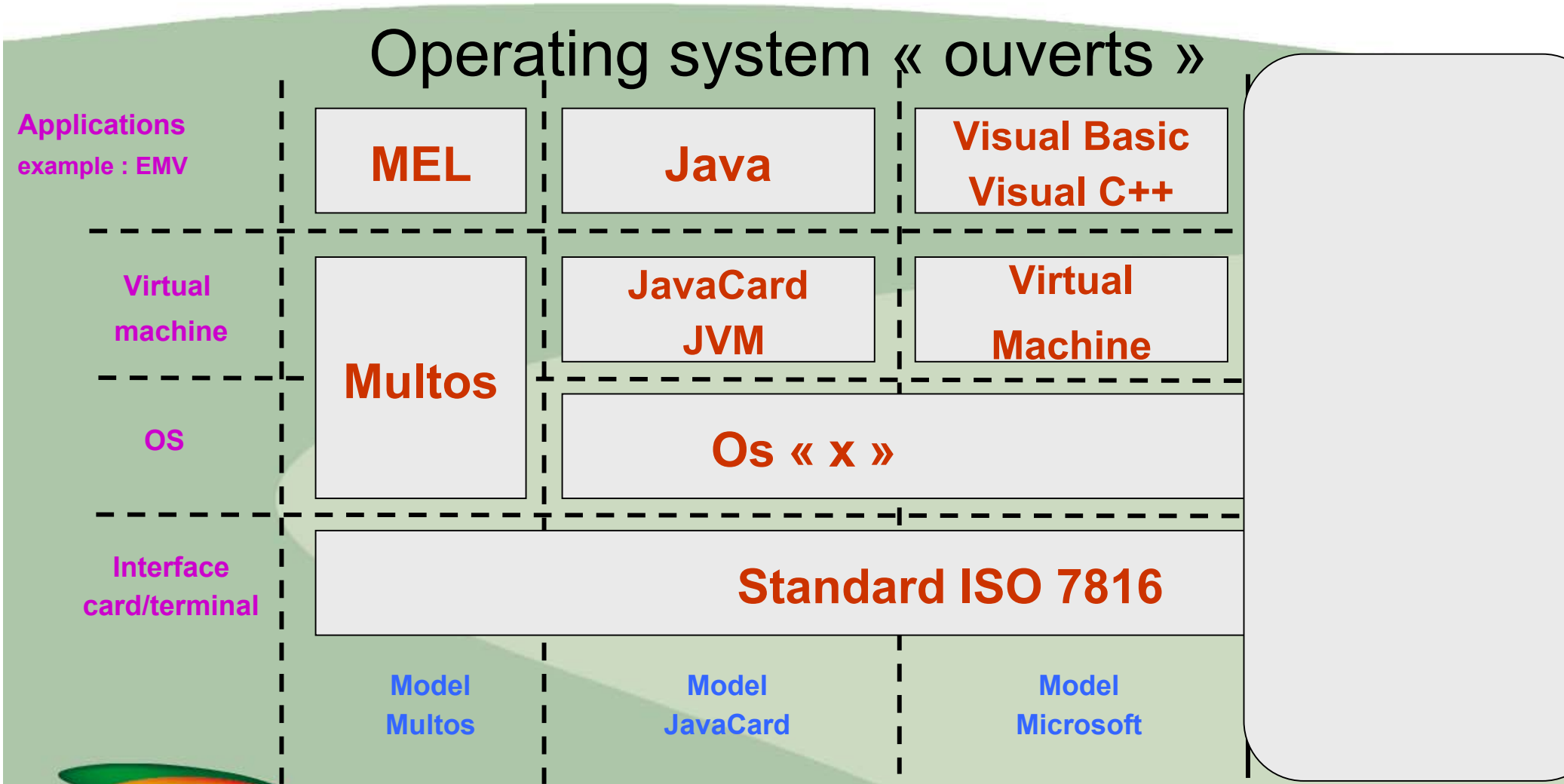
The management of data on card depends on implementation specifications of Issuer.

For example, CB Network specifications distinguish 3 types of data for payment/withdrawal applications

- Common EMV application data
- Data could be shared by all applications present on the card (chosen by Issuer)
- Specific data for each application

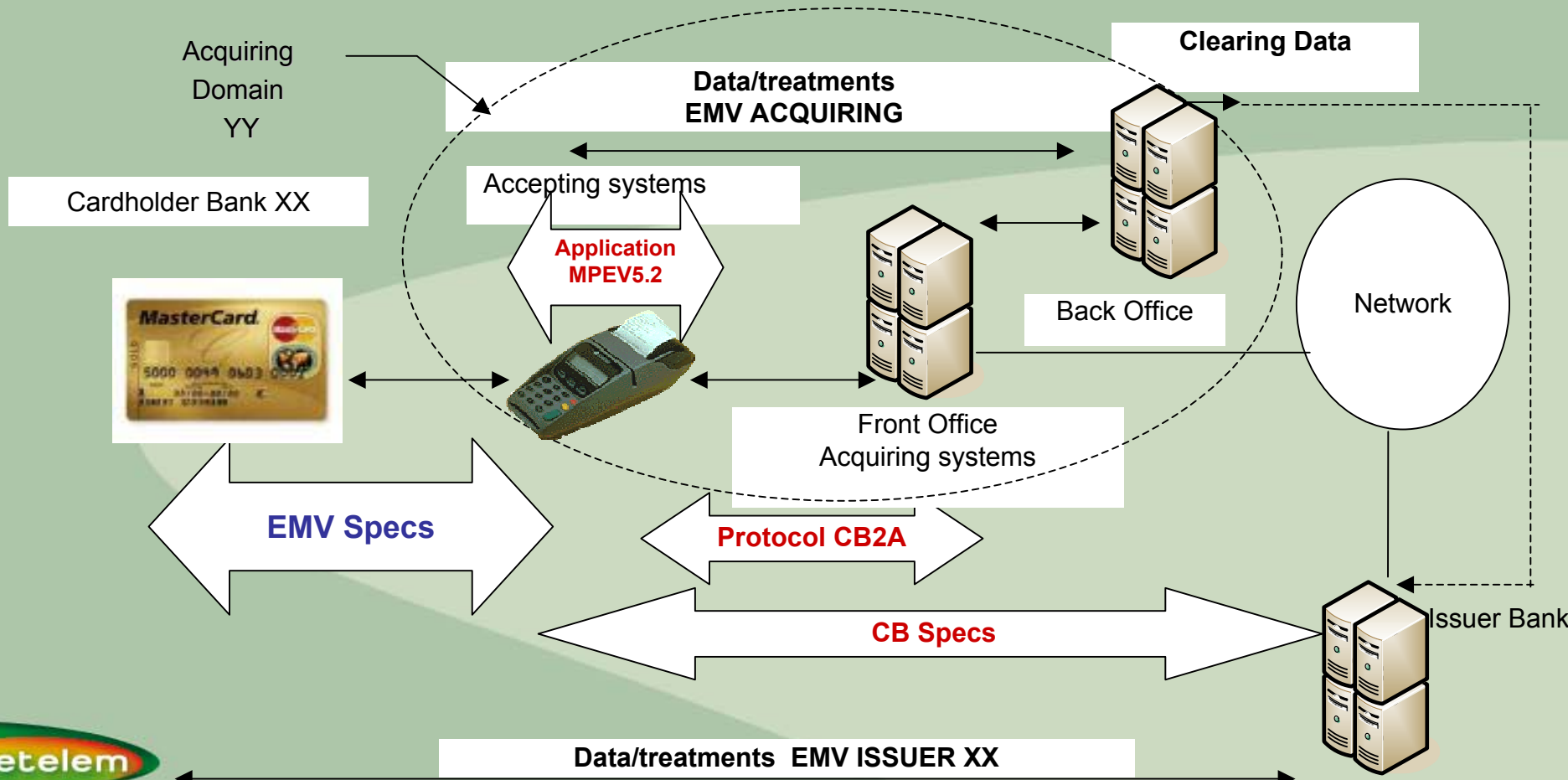
Cetelem
A BNP PARIBAS company

OPEN TECHNICAL ARCHITECTURE



ARCHITECTURE of EMV SYSTEM

Example of French Electronic Banking exchanges



END OF FIRST PART

Cetelem

A BNP PARIBAS company

Training

EMV

2/2

EMV Transaction

IMPACTS on IT Systems

Q1 2006

AGENDA

DELIVERING CARD to the CARDHOLDER

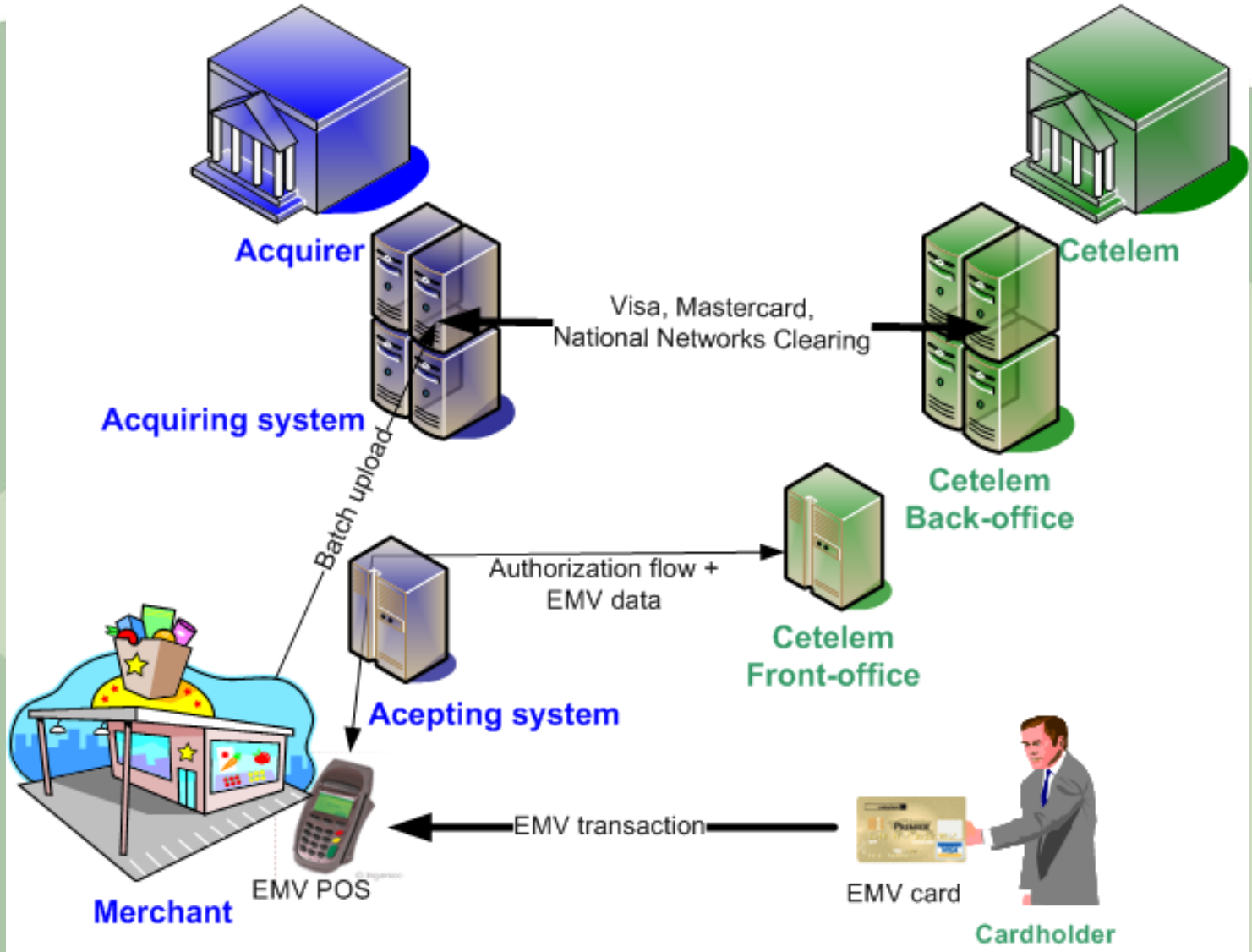
- Choice of Card Product
- Definition of EMV profile of the card
- Personnalization Set Up
- Agreements and Approvals

ACTIVATION and EXPLOITATION of the CARD

- Front-Office Domain
- Back-Office Domain

Cetelem
A BNP PARIBAS company

OVERVIEW of the SCOPE



CARD DELIVERING to CARDHOLDER

- **What we have to do to deliver an EMV card to our client?**

The subsidiary has to provide to the personalizer the files including data required to load the EMV application on the chip.

This data required constitutes the profile of the card which has to be defined previously by the project team.

The data must be transmitted by secure channel guarantying the integrity and the confidentiality.

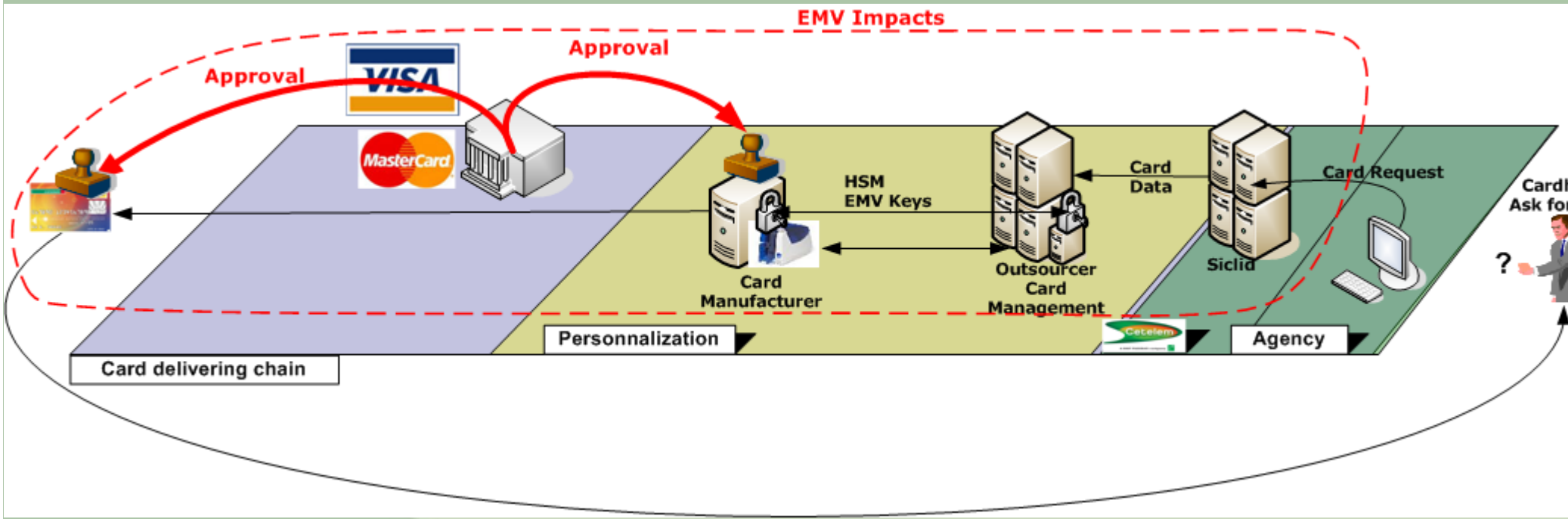
The network Authorities (Visa and Mastercard) have to certify all elements impacted by EMV (security, card profile, card manufacturers, etc…)

Cetelem
A BNP PARIBAS company

- Choice of Card Product
- Definition of EMV profile of the card
- Personnalization Set Up
- Agreements and Approvals

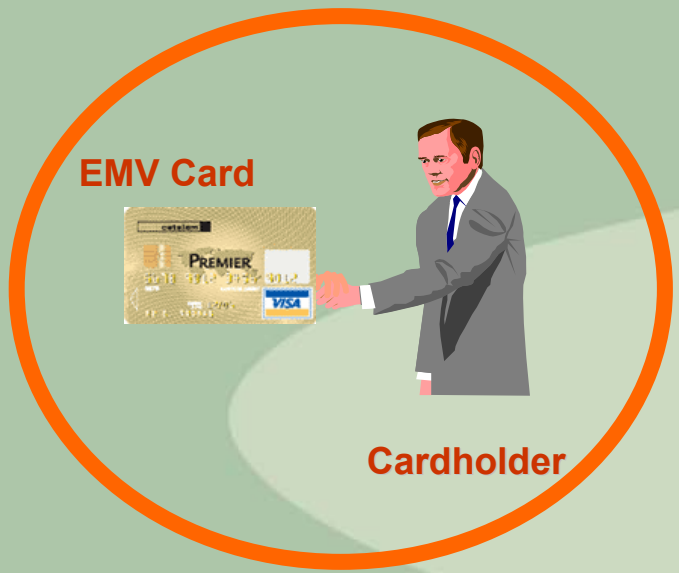
CARD DELIVERING

Impacts on Cetelem IT System delivering card to client



CARD DELIVERING

- **Impacts on Cetelem IT System delivering card to client**



- **Phase into 4 steps:**
  - Choice of card product
  - Definition of EMV profile of the card
  - Personnalization Set Up
  - Agreements and Approvals

Cetelem
A BNP PARIBAS company

CHOICE of CARD PRODUCT

What kind of card?

- Native card (static application in OS)
- Open-platform card (Multos)

There is two kinds of family card:

- Native card is the most widespread product on the chip card market, low cost but less progressive technology for innovative payment solution

- Open-platform card, chip and personalizing cost higher but able to host any EMV based application you want

CHOICE of CARD PRODUCT

Which application?

- Withdrawal, Payment, Full Authorization ?

⇨AID definition

Marketing needs determine which services the card carries. These services will define the AID (= Application Identification)

Services	Mastercard	Visa	Other National Authority
Payment & Withdrawal	Mastercard	Visa	Other
Withdrawal	Cirrus	Plus	Other
On-line	Maestro	Electron	Other
Other services	…	…	…

Cetelem
A BNP PARIBAS company

CHOICE of CARD PRODUCT

Which technology?

- Crypto processor (DDA/CDA)?
- Multi-application environment (other application) ?
- Archives Files?

The features of the chip will be precised depending of functionality which will be carried by the card.

Cryptoprocessor is required if the off-line authentication card-terminal is dynamic (to avoid SDA duplicated fraud)

Chip Memory space depends on number of application supported and storage needs

Cetelem
A BNP PARIBAS company

Definition of EMV Profile

Which EMV profile for the card application?

- Choice of « standard » profile

⇨ recommandations of MCD and Visa networks

Depending on the network(s) in which the card will be used, the profile is built following specifications and recommandations of Network Authorities (Visa, Mastercard or other national authoritity – SIBS, GCB, Banksys, so on…).

The master specification are Vis 1.4 and M/Chip 4. These guides will help to define the profile with “template profile” for each type of application as Marstercard, Maestro, Cirrus, Visa, Electron …

Definition of EMV Profile

- Choice of security data

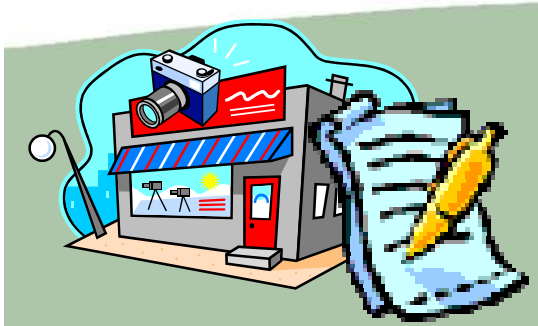
⇨ in collaboration with Risk Management team (IAC, floor limit CVM list, SDA data to be signed)

There is two domains of security to define for EMV profile.

First, the way to secure the card itself in the payment environment. It concerns the authentication of the card (SDA/DDA/CDA), the choice of cryptogram algorithms, the choice of Keys length.

Second, the Risk management of card using by the cardholder. It concerns the ADA (Visa) or CardIAC(MCD) for the decision of transaction completion, the way to identify the cardholder,or the floor limit of the card (amount, number of transactions off-line, online).

Definition of EMV Profile



- Choice of card services data

⇨ in collaboration with Marketing team (AUC: type of services matching with the card)

The EMV application could be used on all kind of terminal EMV compliant. But the marketing needs could be more selective.

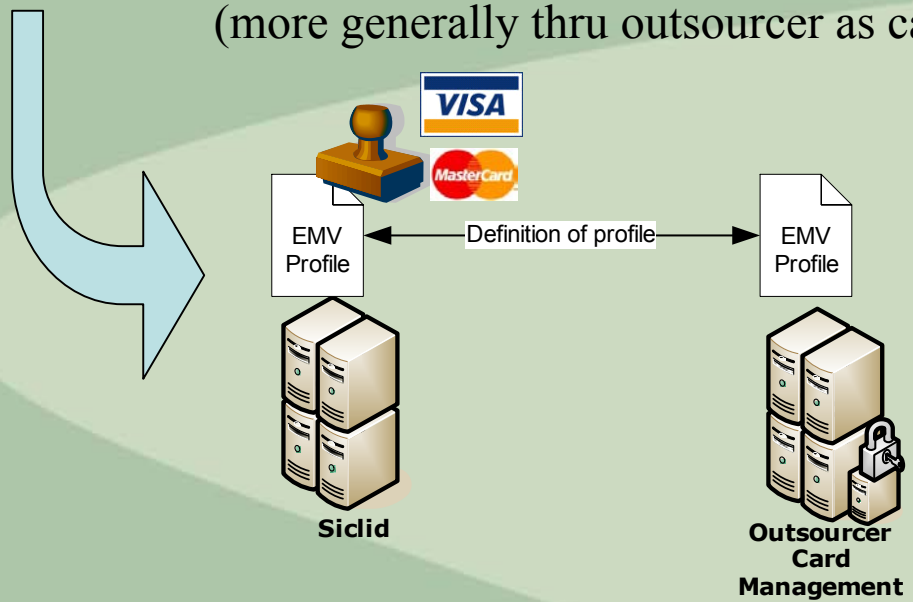
To do that, the definition of AUC (Application Usage Control) data allows to precise for which kind of transaction the card is authorized.

By example, ATM only, Domestic goods, Domestic cash advance, International Cashback allowed, etc..

Definition of EMV Profile

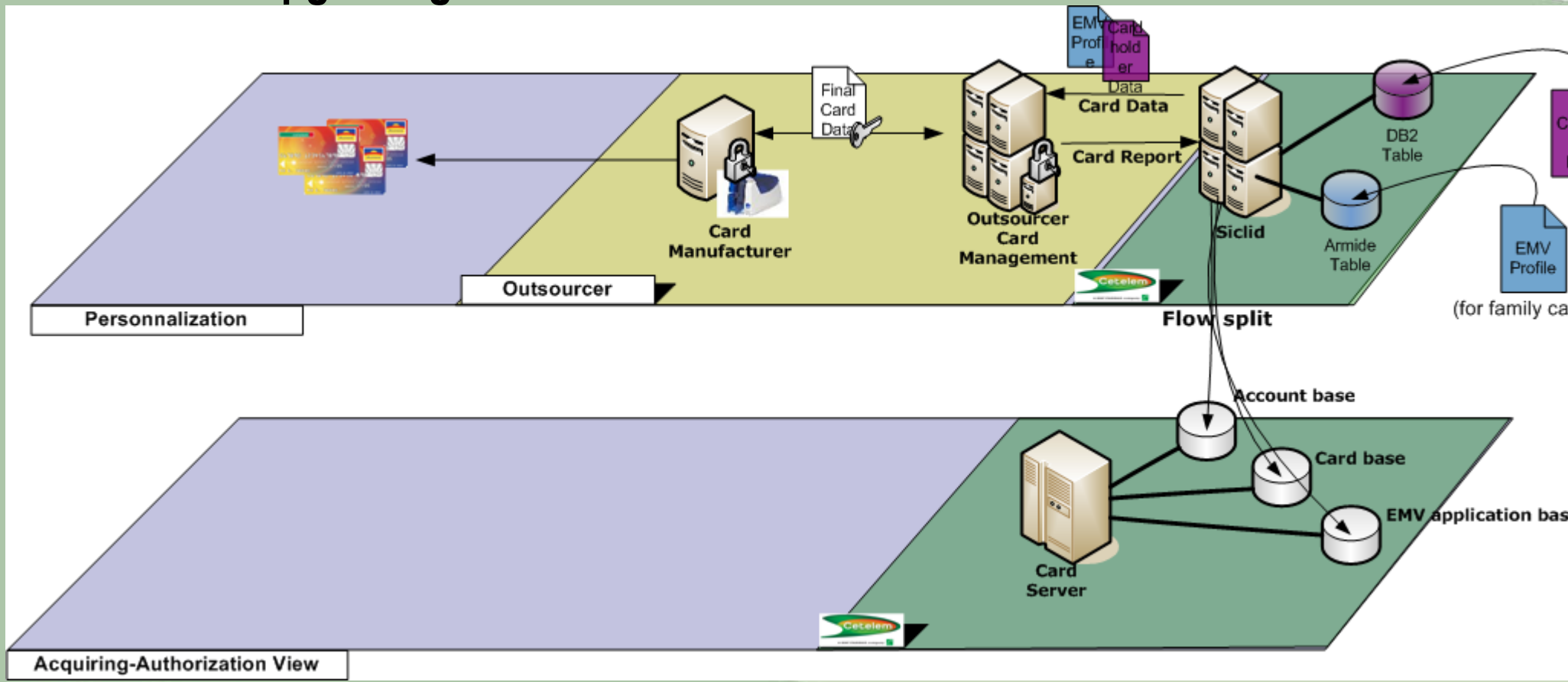
The complete profile is defined for each family card (Mastercard, Maestro, Visa…)

Once done and certified by Networks (Visa and Mastercard for the family card respectively) the profile could be exchanged with card manufacturer (more generally thru outsourcer as card management module)



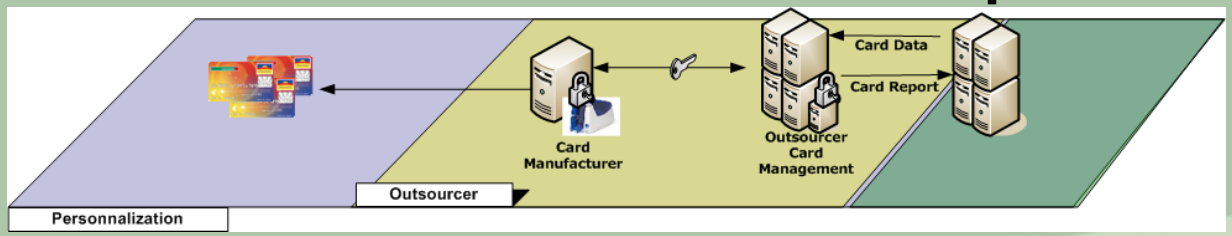
Set Up of Personalization

EMV Upgrading of the Personalization chain



Set Up of Personalization

Phase 1 of Personalization Set Up:

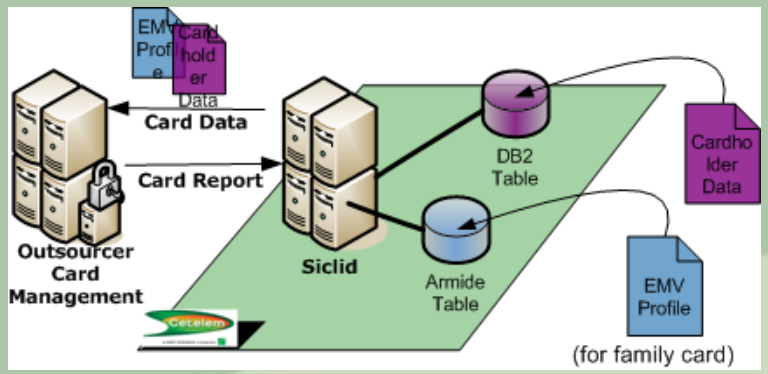


- Choice of outsourcer EMV certified by Visa & Mastercard and compliant with choice of card product (type of chip, memory size, ciphering processor)
- Interface between Siclid and outsourcer

  Specifications must be defined and developed to exchange personalization files

Set Up of Personalization

Phase 2 of Personalization Set Up:



- Implementation of EMV profile into Siclid

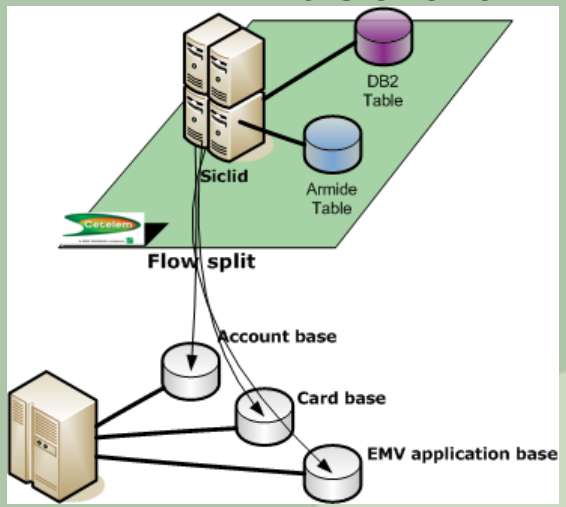
  The card family profile previously validated by Network Authority must be launched in Siclid (Armide table)

- Exchanges of EMV card family data (Armide table = profile pre-defined) and Cardholder data (DB2 table)

Cetelem
A BNP PARIBAS company

Set Up of Personalization

Phase 3 of Personalization Set Up:



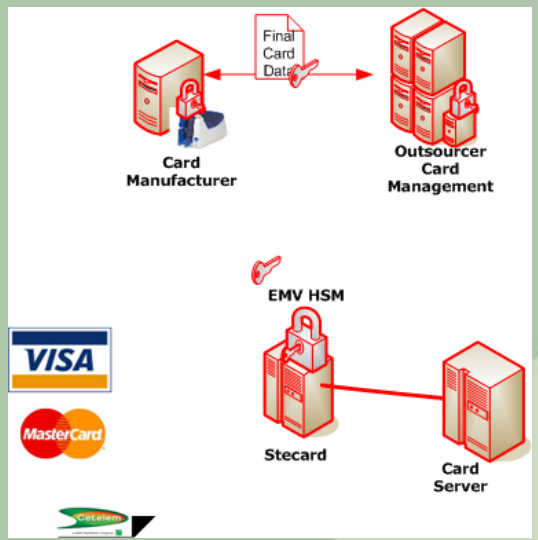
The card data creation (including EMV data) must be exchanged with Telematic Corporate Servers.

This is done by MQSeries into flow split (3 flows: account; card; EMV application)

This is a real time flow.

Set Up of Personalization

Phase 4 of Personalization Set Up – EMV keys:



The keys Kac, Ksm certified by Network Authorities (as well as matching keys using to personalize the card) must be loaded on the HSM of Stecard.

This is a pre-requisite of opening the online flow.

Agreement and Approval

- **EMV Project with Mastercard and Visa**
  - Each EMV project is matter of certification of Mastercard and Visa. The whole chain of Card Issuing must be approved, i.e. the chip, personalizer, profile of family card (BIN), specimen card and authorization systems.
    - ✓Open a EMV project
    - ✓Validation of EMV profiles
    - ✓Validation of Cards specimen
    - ✓Final agreement for project – end to end tests
  - Final agreement leads to open the flow (EMV data included) for the BIN certified

AGENDA

DELIVERING CARD to the CARDHOLDER

- Choice of Card Product
- Definition of EMV profile of the card
- Personnalization Set Up
- Agreements and Approvals

ACTIVATION and EXPLOITATION of the CARD

- Front-Office Domain
- Back-Office Domain

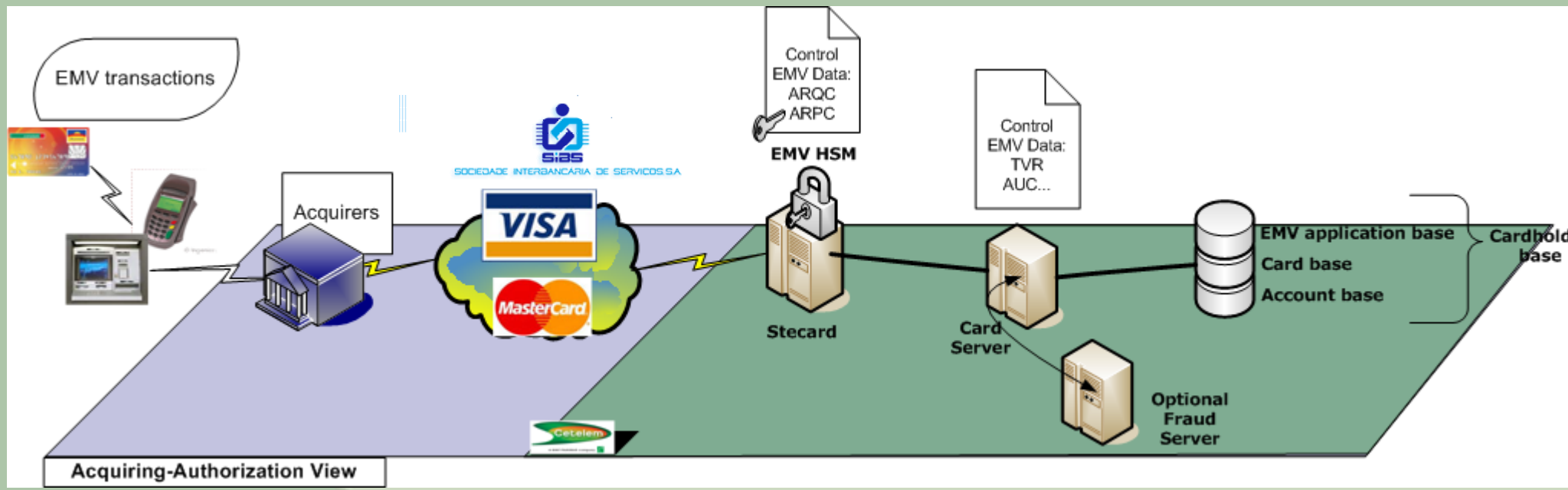
Cetelem
A BNP PARIBAS company

Exploitation of the Card

- **Using of EMV card in the Cetelem IT system**
  - As soon as the card is delivered to the cardholder, EMV data are transmitted thru several payments system. IT system must exploit them into front and back-offices. The following description takes into account the evolution:
    - ✓Front-office system – Stecard and Card Server
    - ✓Back-office system - Siclid

Exploitation of the Card

- **Authorization flow of EMV transaction – Stecard and Card Server**



Exploitation of the Card

- **EMV Evolution on Stecard and Card Server**
  - Stecard

  Entry point for online transactions, it assumes security control on EMV data (ARQC, I-CVV) and format control. EMV keys must be loaded into HSM linked to Stecard (K_{AC} and K_{SM}) as mentioned previously.

  Once security control done, Stecard sends the transaction to Card Server by indicating the results of control.

Exploitation of the Card

- **EMV Evolution on Stecard and Card Server**
  - Card Server

  It assumes control on EMV data about the context (AID, AUC, CVR, TVR) and about the elements of the transaction (amount, application, date, country). Then it gives the response to the request depending on the results of security controls sent by Stecard.

Script Processing

- **EMV functionality: script-processing execution**
  - Scripts EMV

EMV allows to modify some data on the chip after personalizing. This command (called post-modification) is sent in the response to the authorization. Card server prepare the command and the encryption is done by Stecard with special key (K_{SM}). The commands authorized are:

- ✓ Data update
- ✓ Card block
- ✓ Application block / unblock
- ✓ PIN unblock

Script Processing

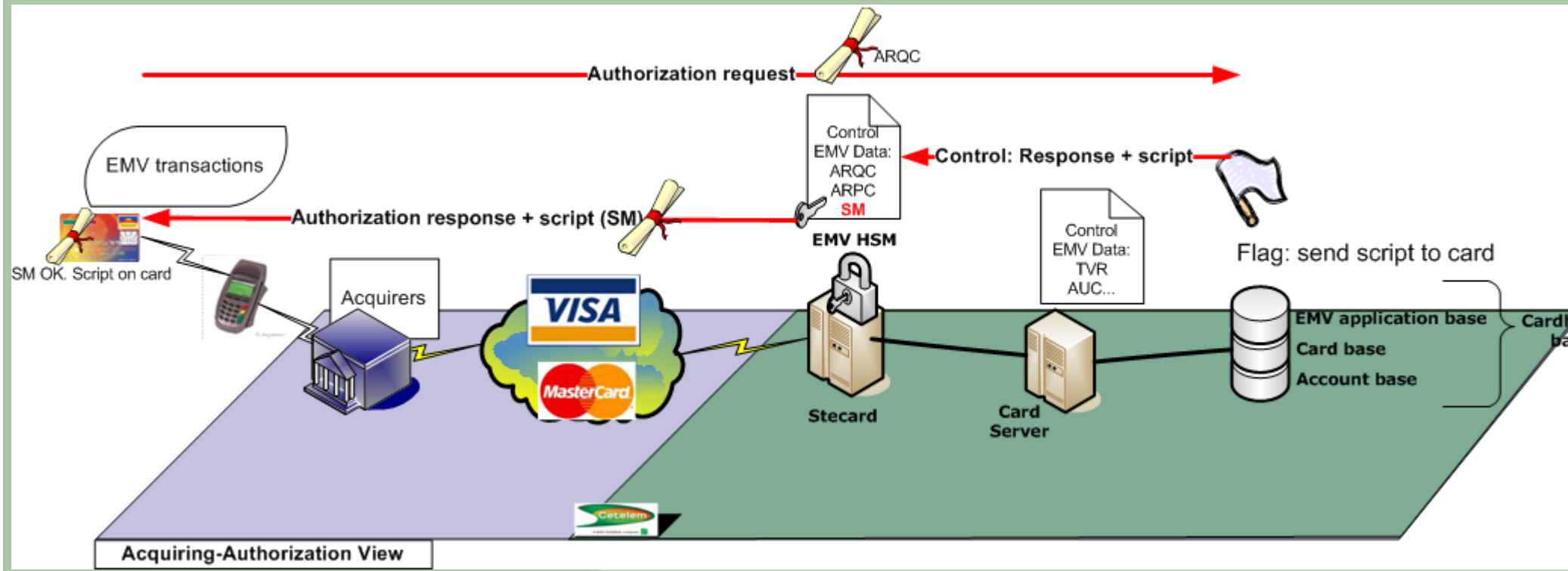
- **EMV functionality: script-processing execution**
  - Scripts EMV

The processing of sending a post-modification script to the card could be done in two ways:

- Automatically: rules on card server allow to send the script depending on certain data of transaction (ex: 3 pin false -> sending of Application Block script)
- Manually: Siclid informs card server (by MQSeries) that card must be blocked. A flag will indicate to card server to send the script as soon as on-line authorization is received.

Script Processing

- **EMV functionality: script-processing execution**



Clearing - Chargebacks

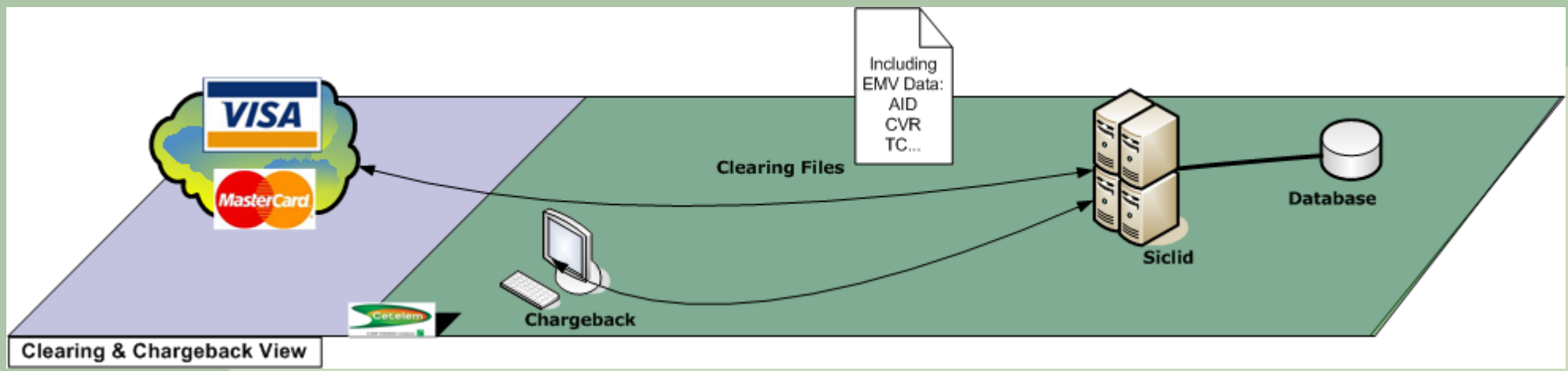
- **Implementation and exploitation of EMV Data**
  - EMV data exploitation

EMV data are transmitted into clearing files. Siclid has to receive and exploit them in case of chargebacks. To process it, system must control following data:

- ✓AID
- ✓AIP
- ✓ATC
- ✓IAD
- ✓Application cryptogram
- ✓CVR
- ✓TVR
- ✓Issuer script results (if present)

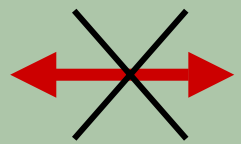
Clearing

- **Implementation and exploitation of EMV Data**



Liability Shift

Non EMV Terminal



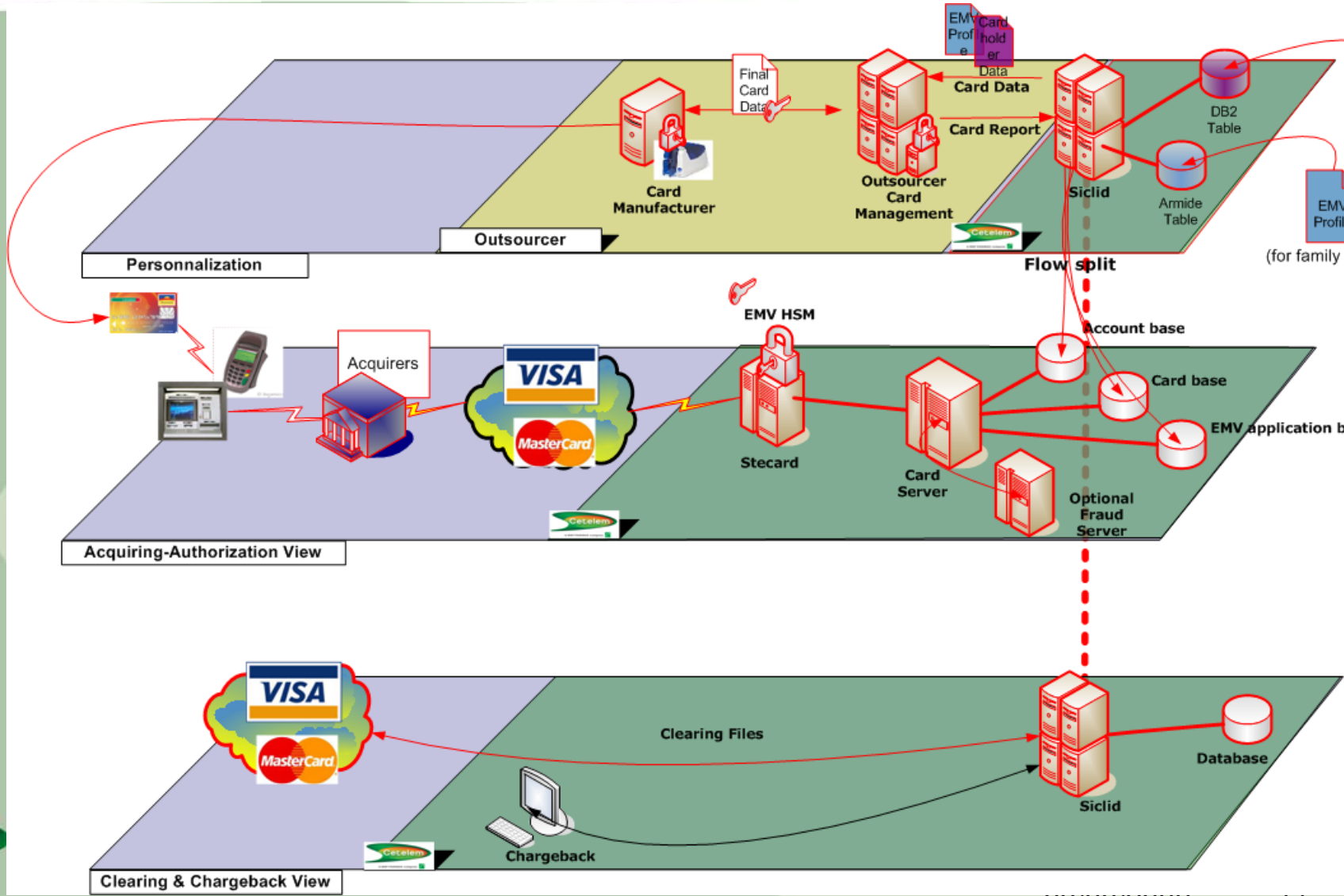
EMV Card

Fraudulous Transaction

- **Liability of Acquirer**
  - **If the terminal is non-EMV and the card EMV, in case of fraudulous transaction the Acquirer will support the fraud and no more the Issuer.**

Cetelem
A BNP PARIBAS company

EMV Sum Up – View of Modules Impacted



END OF SECOND PART

Cetelem
A BNP PARIBAS company