IEEE Key Management Summit 2010

Incline Village, NV, 03 – 05, May 2010

# Practices and difficulties of key management in the credit card market

Fabian Martins

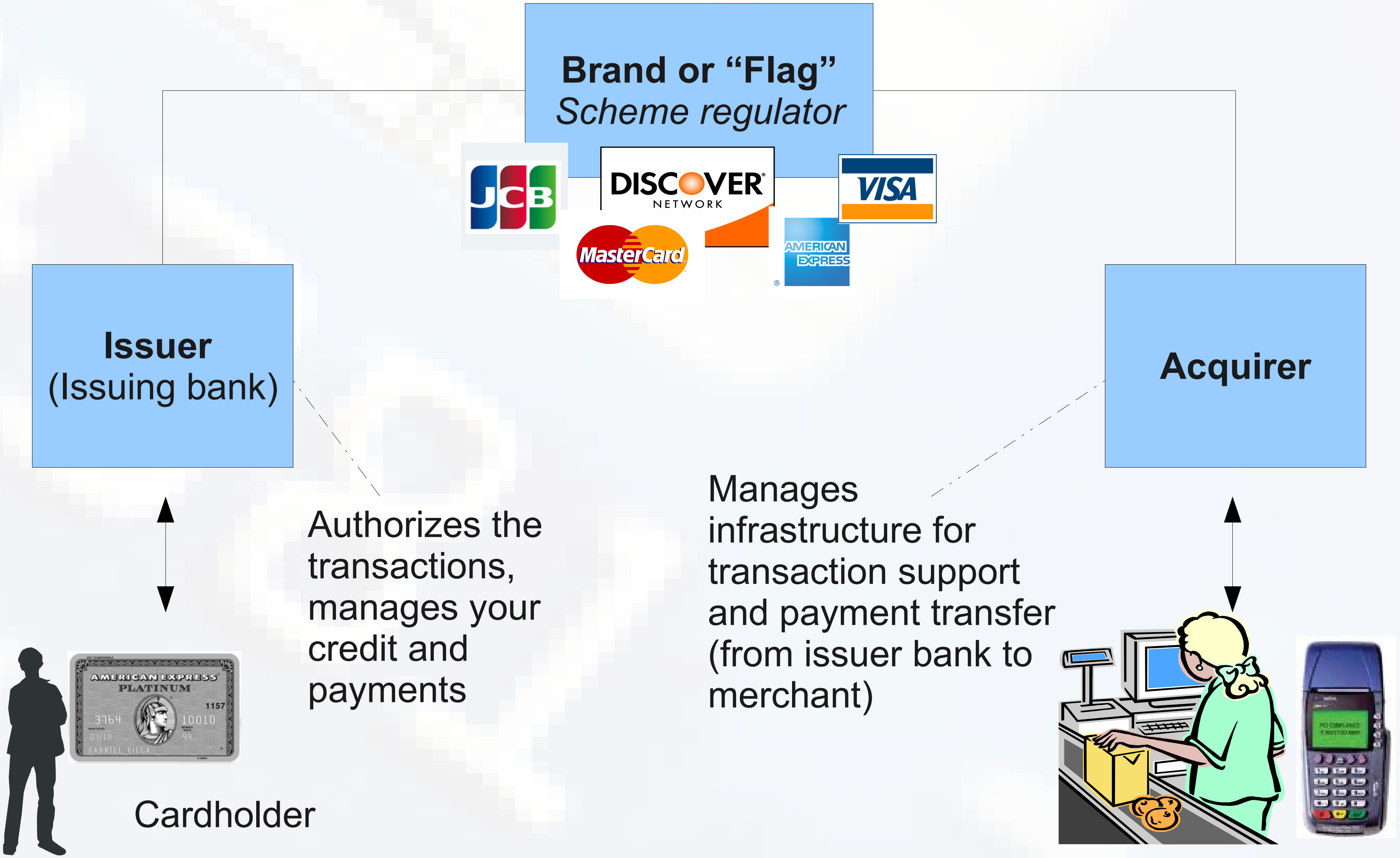
Crosscut Consulting
www.crosscut.com.br

FIAP University
www.fiap.com.br
(Singularity University Partner)

# Agenda

1. The players on the credit card market
2. Where keys are used
3. Infrastructure and processes for symmetric key distribution
4. What are the difficulties
5. What we have found
6. Solutions under construction
7. Solutions we are looking for

# The players on the credit card market (*branded model*)



**Brand or "Flag"**
*Scheme regulator*

**Issuer**
(Issuing bank)

**Acquirer**

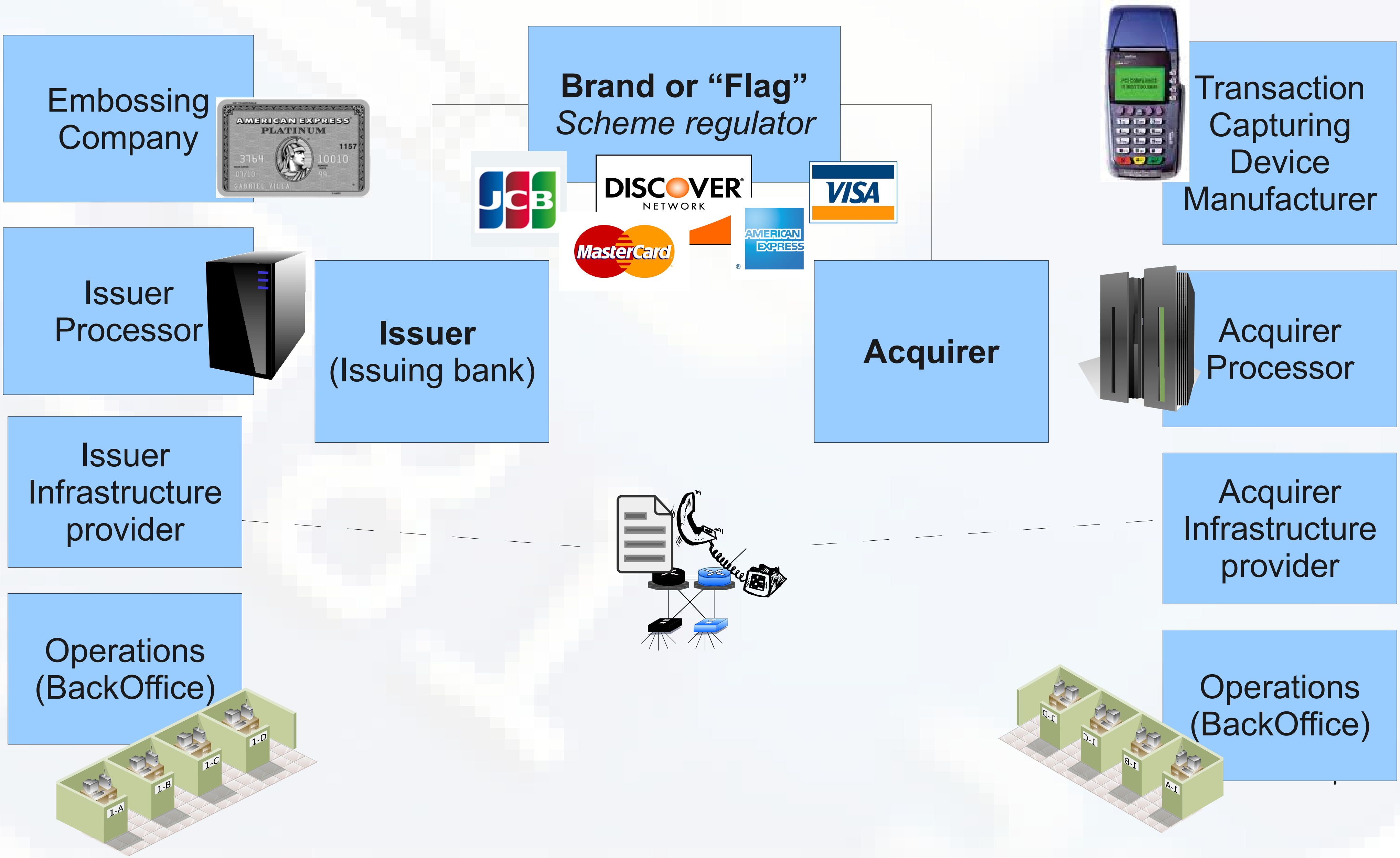
Authorizes the transactions, manages your credit and payments

Manages infrastructure for transaction support and payment transfer (from issuer bank to merchant)

Cardholder

Merchant

# The players at the credit card market (*services view*)



Embossing Company

Issuer Processor

Issuer Infrastructure provider

Operations (BackOffice)

**Brand or "Flag"**
*Scheme regulator*

**Issuer**
(Issuing bank)

**Acquirer**

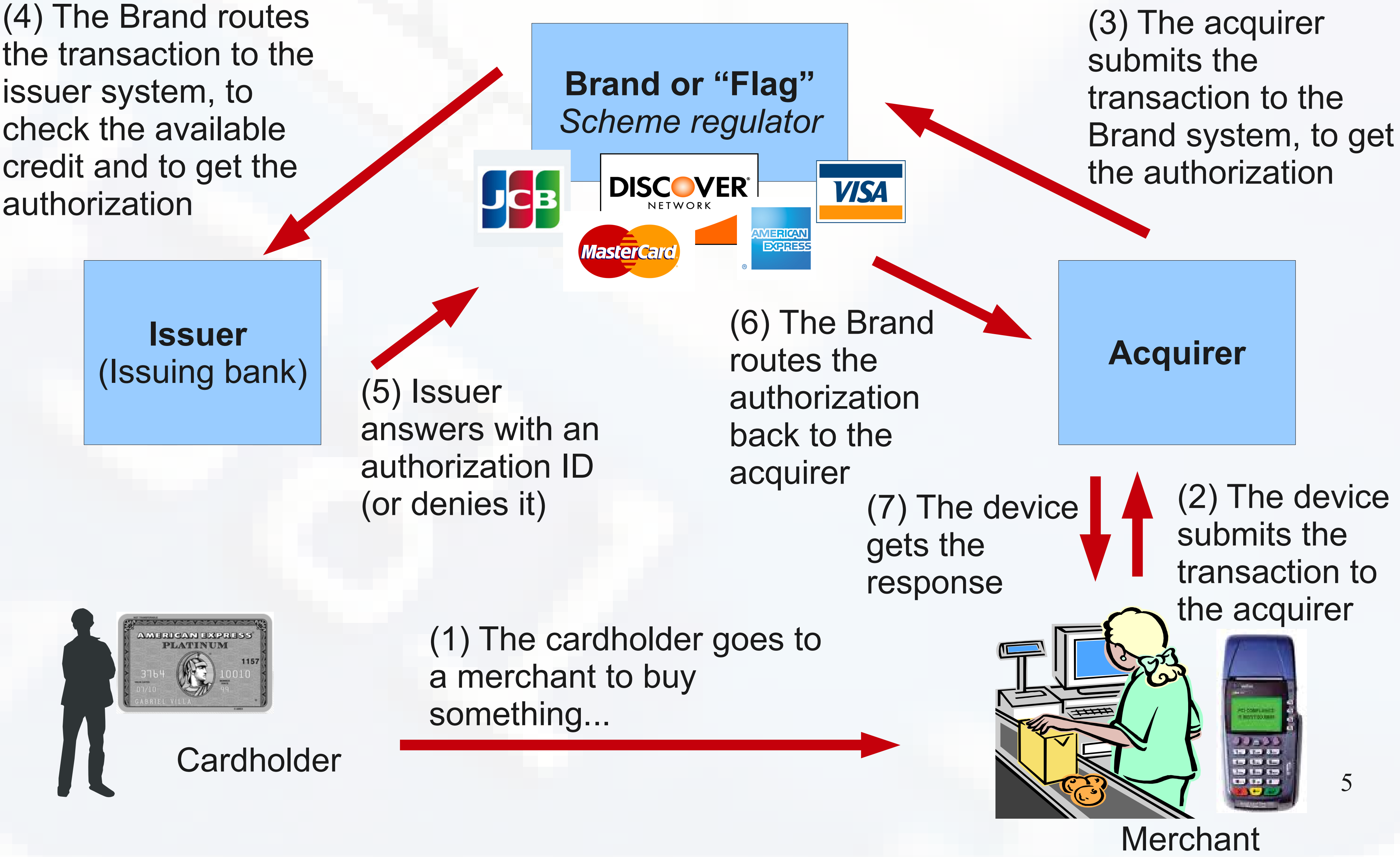
Transaction Capturing Device Manufacturer

Acquirer Processor

Acquirer Infrastructure provider

Operations (BackOffice)

# The players at the credit card market (*The transaction flow*)



(1) The cardholder goes to a merchant to buy something...

(2) The device submits the transaction to the acquirer

(3) The acquirer submits the transaction to the Brand system, to get the authorization

(4) The Brand routes the transaction to the issuer system, to check the available credit and to get the authorization

(5) Issuer answers with an authorization ID (or denies it)

(6) The Brand routes the authorization back to the acquirer

(7) The device gets the response

**Brand or "Flag"**
*Scheme regulator*

**Issuer**
(Issuing bank)

**Acquirer**

Cardholder

Merchant

# The need for keys

**For transaction security**

- Lots of “gateways” between acquirers and issuers (transportation of PIN, magnetic stripe/chip data);

**For issuers needs**

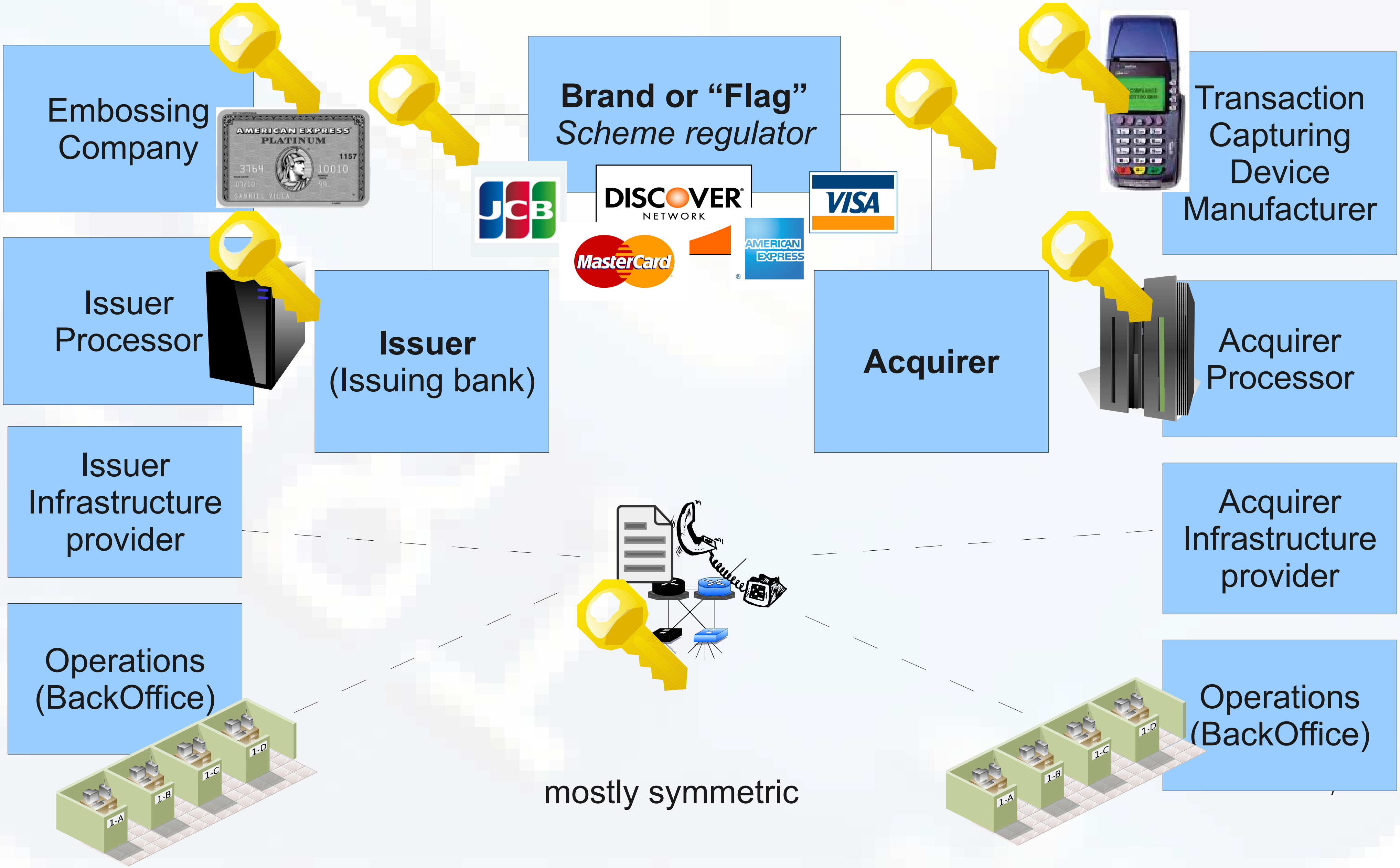
- To send confidential data to the embossing company in order to produce cards;
- Exchange confidential information with card processing/backoffice companies;

**For acquirers needs**

- To send confidential data to POS manufacturer, to deploy transaction authorization and capturing software;
- Exchange confidential information with acquirer processors/backoffice companies (transaction data);

**PCI Standards** (for data processing and PIN Pads)

# Where keys are used



Embossing Company

Issuer Processor

Issuer Infrastructure provider

Operations (BackOffice)

**Brand or “Flag”**
*Scheme regulator*

**Issuer**
(Issuing bank)

**Acquirer**

Transaction Capturing Device Manufacturer

Acquirer Processor

Acquirer Infrastructure provider

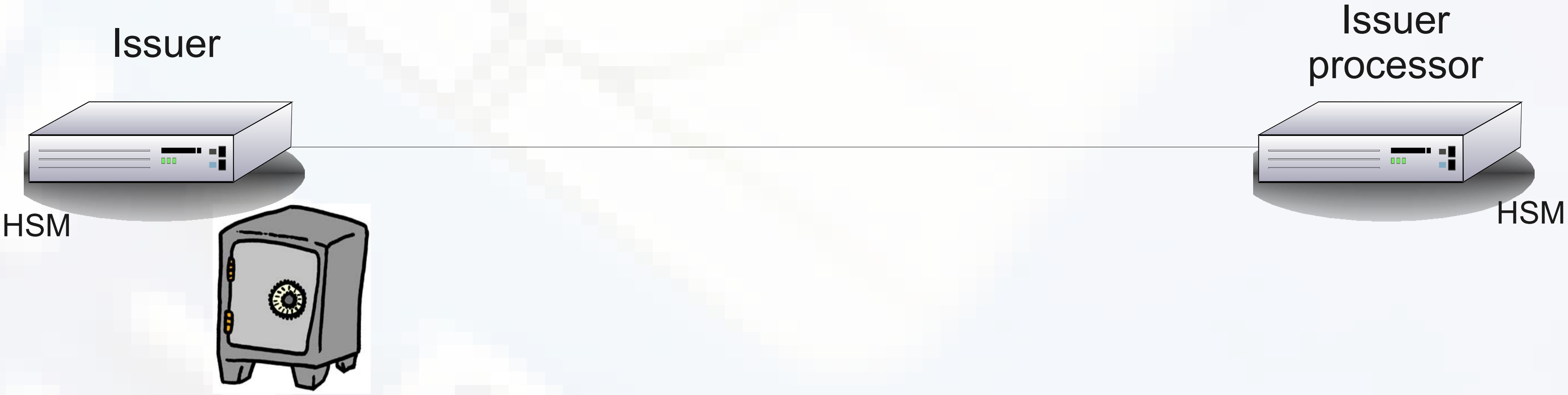
Operations (BackOffice)

mostly symmetric

# Where keys are used
# inside the card

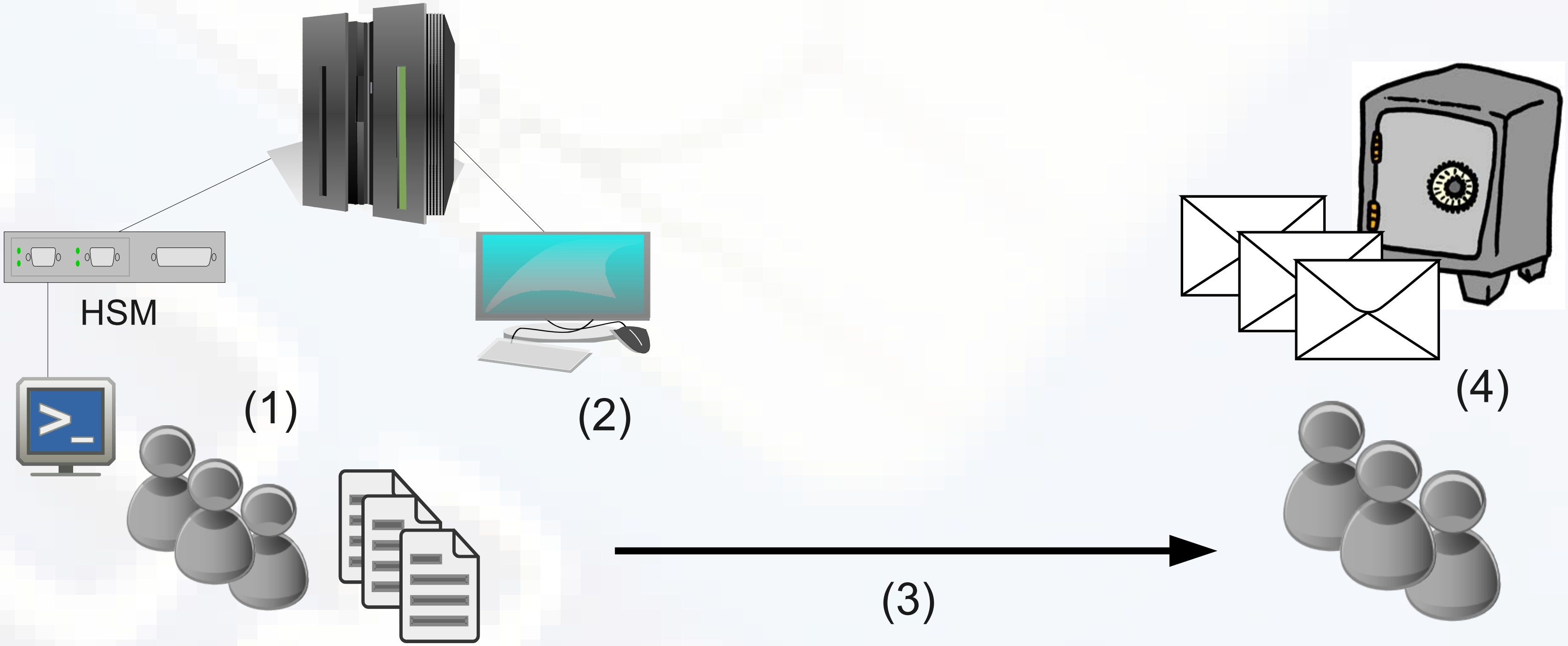
- Different kinds of cards may require different sets of keys;
- Magnetic-stripe cards do not store keys (but use them at the POS equipment);
- Chip-based cards store keys for:
    - PIN encryption and validation;
    - Application (software) integrity validation;
    - Application specific data encryption;
    - Message authentication (MAC keys);
    - Securing the communication between the target part (for multi-purpose/multi-branded cards);
- Contact less cards are similar to chip-based cards, but also includes keys for ciphering the information transfered to the terminal;

# Infrastructure for symmetric key distribution



- Keys are in general created by one part or the generation can be shared (each one generates one component);
- The parts share keys for supporting secure links (ZMKs);
- The parts must have HSMs;
- Working keys are exchanged through the secure link;
- Some keys are physically transported and deployed on the other part (that happens with ZMKs)
- Issuers banks store physical components inside safes;

# Usual processes for symmetric key distribution ( *the "ceremony"* )



The ceremony is a controlled and audited event where the keys are handled (created or transported).

For key generation:

(1) HSM generates the key and the custodians, one each time, take notes about the generated components
(2) The components are inserted into the mainframe system (e.g, issuer system).
(3) The components are securely (physically) transported;
(4) The components are stored inside the safe;

For key sharing, take the reverse way, including one step for taking the keys back into the safe.

# Where are the difficulties

- Despite NIST SP 800-57 has described requirements for key security, including key accountability (section 9, part 1) and key policy structure (section 3, part 2) there are no recommended controls as it happens on SP 800-53 (more specifically, on SP 800-53A);
- Banks are more “stimulated” to implement proper management and controls when there are strong international or market norms that explicitly requires them to;

# What we have found

- Very generic policies;
- Very poor controls;
- Lack of knowledge of key management requirements;
- Absence of proper information about the keys:
  - What is the purpose of that key?
  - If a state change (even a unauthorized disclosure) happens to the key?
    - What assets will be in danger in that case?
    - What products has been affected?
    - Where is the source of the effect?
    - Who will be impacted by the change?

# What we have found

This correspond to a sample of an auditing process in an issuing bank:

- More than 400 envelopes, some dating from the beginning of 90's;
- Unidentified custodians;
- In clear components sharing a same locker;
- Absent or unidentified components;
- Unspecified key size and components quantity;
- Multiple copies of the same key;
- Unnamed keys;
- Non specified: in clear or ciphered?
- In-clear sharing of non KEK/ZMK keys;

# What we have found

- Sharing of keys between Brands, between products;
- Multiple keys into the same envelope;
- Key hash codes stored inside the envelope;
- Absence of key backups;
- Key management roles distributed across the organization without proper alignment:
  - Key generation and sharing is managed by distinct business areas;
  - Product Manager does not know all the keys it needs for their products;
  - IT/Development people does not know what the key is for; only knows its label;
  - IT/Production people only knows the hash and label;

# Solutions under construction

- Issuing bank is developing a computer-based system for key management purposes, with focus on the accountability;
- Role-based access control;
- Plans to store key components into secure chip-cards;

| **Product Manager** | **Information Security / Internal Audit** | **IT/Development Team** | **IT/Production** |
|---|---|---|---|
| Product;<br>Function;<br>Key ID supporting each function;<br>Key Label<br>Key check value (KCV);<br>Entities sharing the key;<br>Ceremony control;<br>Key state; | Auditing information.<br><br>Will be capable of consulting all the information available | Product;<br>Key ID;<br>Key Label;<br>KCV;<br>Key purpose; | KCV;<br>Key Label;<br>Key state; |

# Solutions we are looking for

- Reference controls for key management procedures, accounting and auditing;
  - Required controls across all the organization;
  - Test procedures;
- Integrated systems (software) for key information storing and management (accountability and auditing) possibly integrated to HSM;

# Conclusions

- Issuing banks have more difficulties with key management;
- Acquirers and service providers have more detailed policies and controls in place. Most are already using DUKPT (*Derivated Unique Key Per Transaction*, ANSI X9.24);
- None of the evaluated sites had an integrated computer-based system for key management (mostly managed through books or computer-based spreadsheets);
- The PCI/DSS has enhanced the key controls and auditing procedures at the credit card market players, but the specific controls for key management are generic;
- There are no strong enough reference controls for key management (what to do; how to evaluate polices and procedures);

# Thank you !!!

Send questions... keep in touch...

Fabian Martins

fabian.martins@gmail.com
crosscut@crosscut.com.br
www.linkedin.com/in/fabianmartinssilva