Fundamentals of Smart Cards for Payment

Welcome – Rori Ferensic
Director of Education and Professional Development, ETA

The Smart Card Payments Application Series
November 18, 2008

Introductions

Randy Vanderhoof
Executive Director, Smart Card Alliance

Webinar Topics

Smart Cards and Payments: Technology, Standards & Transactions

- Gilles Lisimaque, Partner, Identification Technology Partners, Inc.

Smart Cards and Payments: Transaction Processing and Business Applications

- Roger Musfeldt, Director, Mobile Commerce Solutions, First Data Corporation

Conclusions and Q&A

- Randy Vanderhoof, Executive Director, Smart Card Alliance

Smart Card Alliance

Smart Card Alliance mission

To stimulate the understanding, adoption, use and widespread application of smart card technology through educational programs, market analysis, advocacy, and industry relations . . . .

Over 170 members, including participants from financial, retail, government, corporate, and transit industries and technology providers to those users

Major activities

- **Industry and Technology Councils**
  - **Contactless and Mobile Payments Council**
  - **Healthcare Council**
  - **Identity Council**
  - **Physical Access Council**
  - **Transportation Council**
- **Conferences, symposia, web seminars and educational workshops**
- **Web-based resources and email newsletters**

Contactless and Mobile Payments Council

Mission: ***Facilitate the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers***

Over 48 active member organizations, including financial industry representatives and technology suppliers

Resources

- **Merchant and Issuer Advisory Groups**
- **Educational publications on contactless and mobile payments**
  - *Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives*
  - *Merchant ROI Model & Implementation Guide*
  - *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*
  - *Contactless Payments: Frequently Asked Questions*
  - *The What, Who and Why of Contactless Payments*
- **Contactless and mobile payments resources and news**
- **Payments industry web seminars**

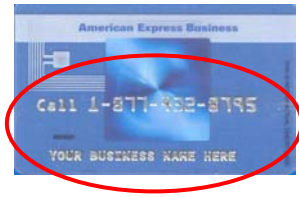
Smart Cards & Payments: Technology, Standards and Transactions

Gilles Lisimaque
Partner, Identification Technology Partners

Financial Payment Devices

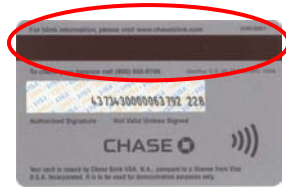
Embossing

- Used by humans and imprinting machines
  - PAN - Expiration date - Name - Discretionary



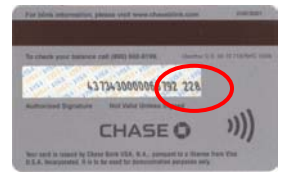
Magnetic stripe

- Used by point of sale terminals and ATMs
  - PAN - Expiration date - Name - Service Code - Discretionary information



Printed information

- Used for payment over the internet by owner
  - 3 or 4 digit numbers printed (front or back)



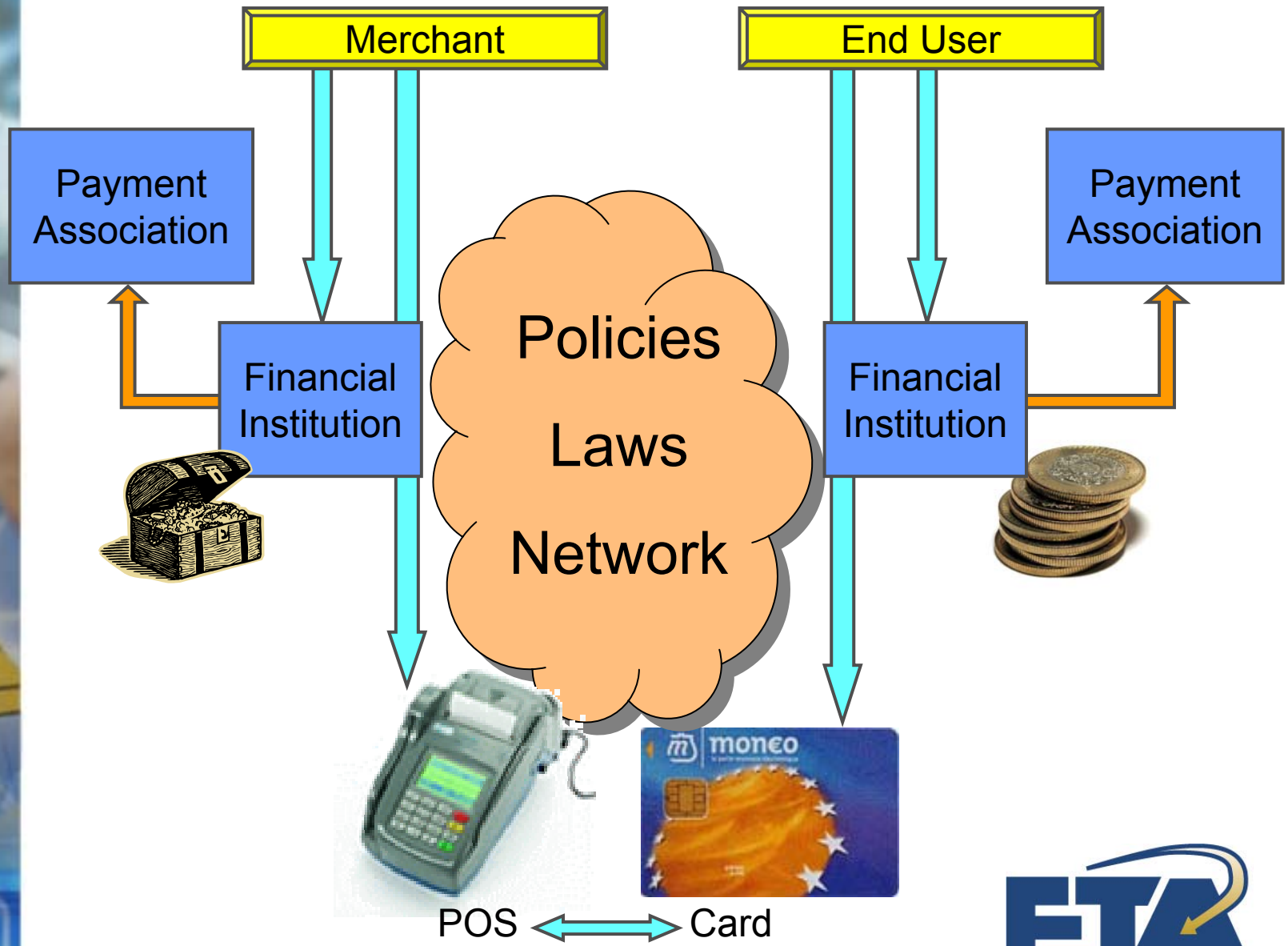
Smart chip (contact or contactless)

- Used by smart banking terminals
  - Allows active communication with the terminal for active authentications and unique transaction codes

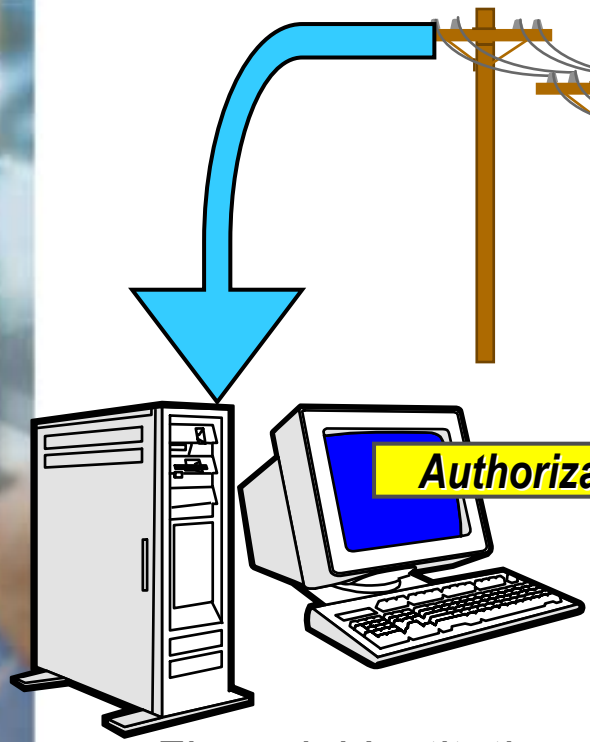
"Other" payment devices

- Contactless devices such as key-fobs, tags, NFC enabled cellular phones
  - Protocols similar to contactless smart cards

The Card is the Tip of the Iceberg



Classic Card Payment



Financial Institution
Authorization Server

Authorization Number

Transaction Data

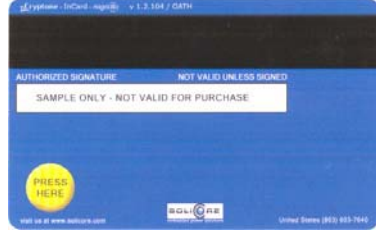
$ Amount
Merchant ID
Date
Time

Signature or PIN

PAN
Expiration Date
Name
CVV

All information coming from the card is static and can be copied in the process

Magnetic Stripe Information on Financial Cards



Track 1 210 bits /in. 79 characters Alpha Numeric

%B	Primary Acct. # up to 16 Char.	^	Name 2 to 26 Char.	^	Exp. date YY MM	Service Code	Discretionary

Track 2 75 bits /in. 40 characters Numeric

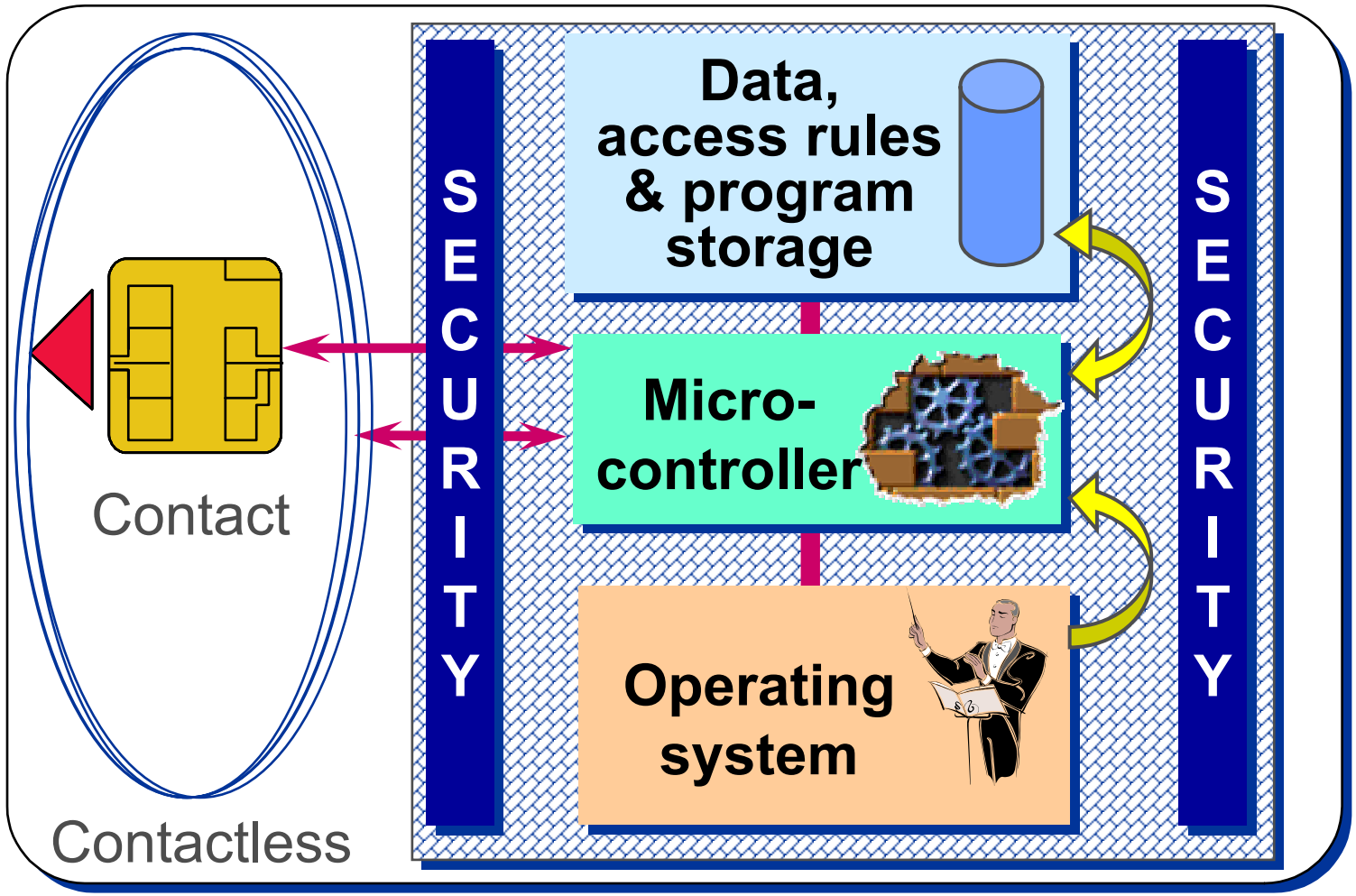
:	Primary Acct. # up to 16 Char.	=	Exp. date YY MM	Service Code	Discretionary

Track 3 210 bits /in. 107 characters Numeric

Not used in most applications

Tracks 1 & 2 are read only tracks and should match the embossing

What Is a Smart Card?

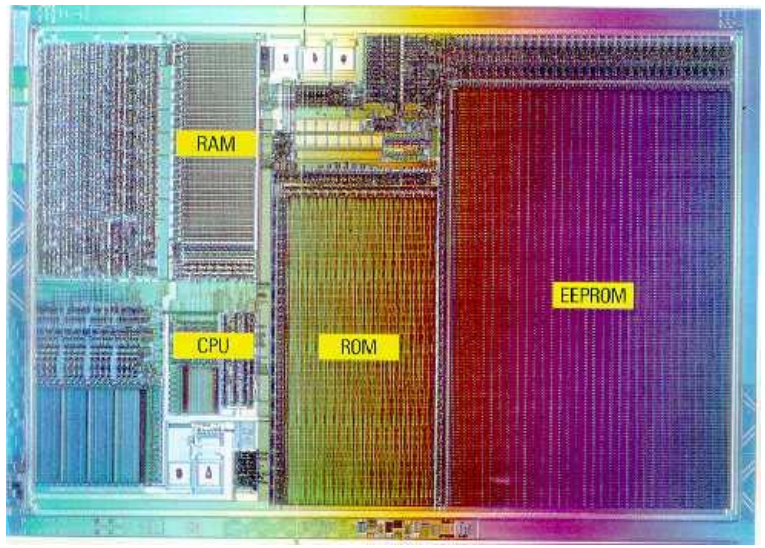


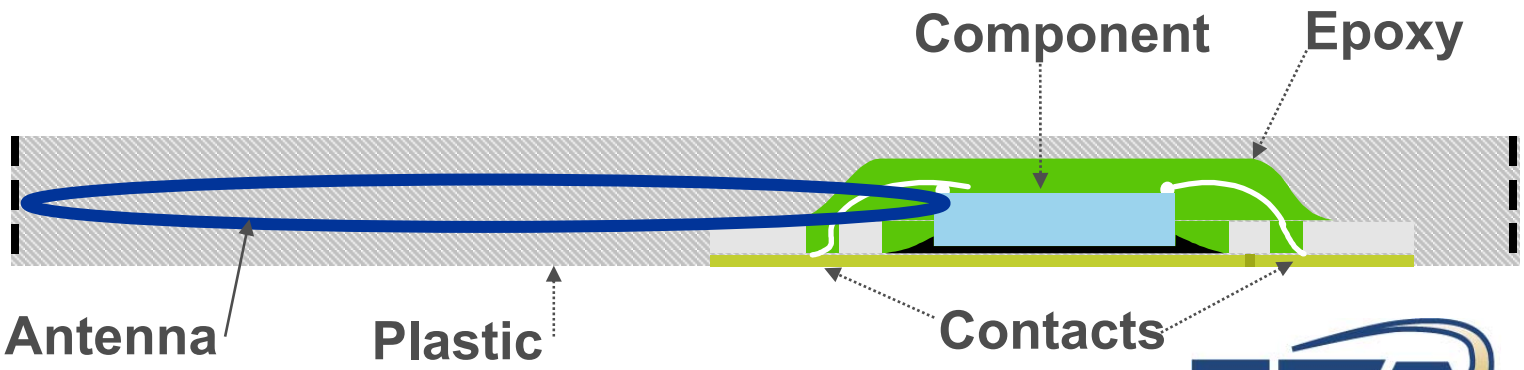
The card operating system controls the input/output lines, any access to the memory and the cryptographic processes such as digital signatures

Behind the Contacts : A Secure Component

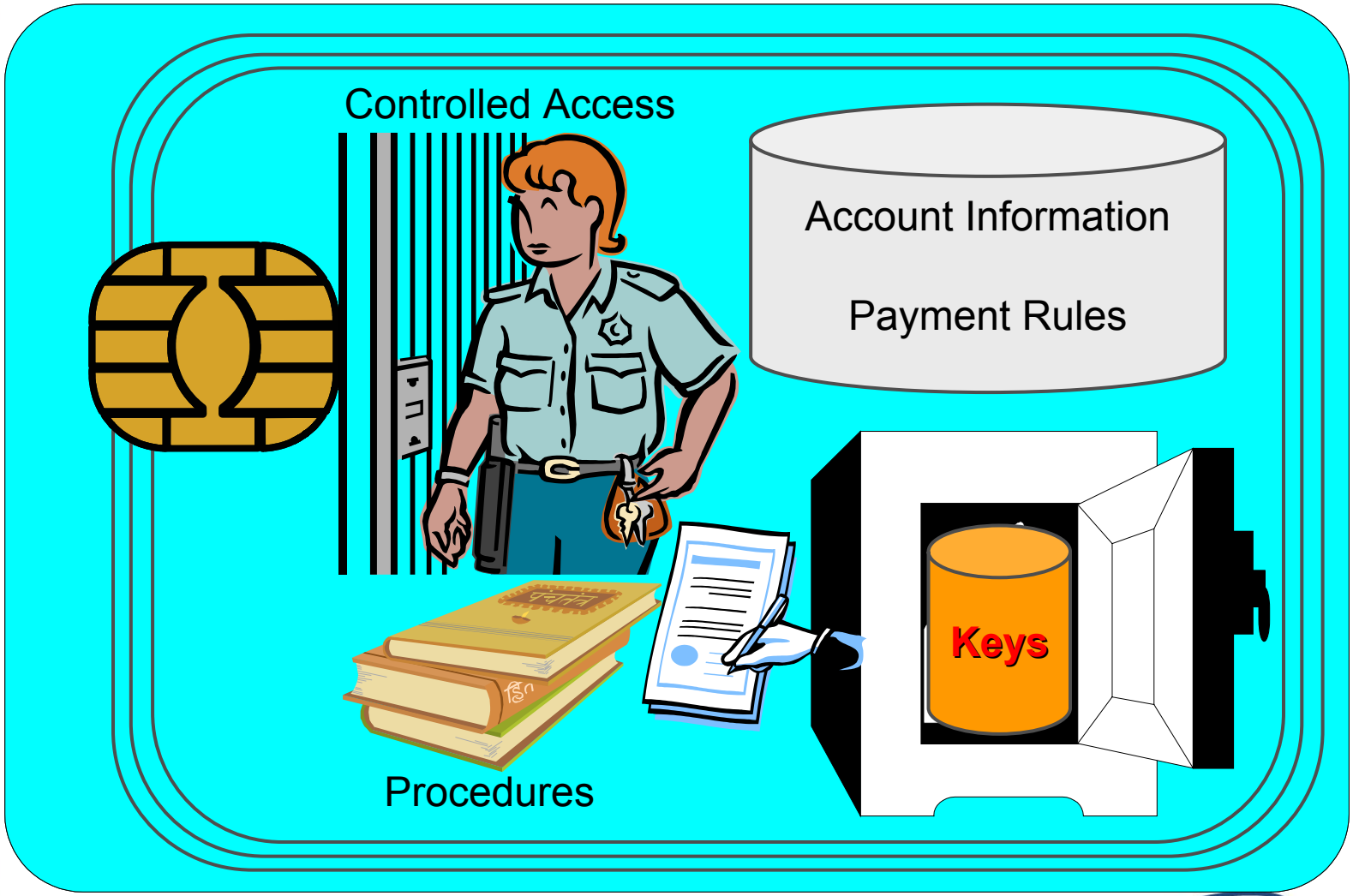
A smart card component monitors its environment to detect hackers.

Not only must it work within its specifications, but it must prevent a security breach to happen when used outside of these specifications.

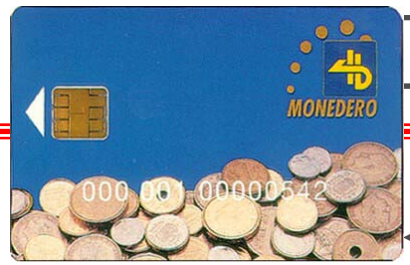




Inside the Card: A Vault



Smart Card Authentication
(very simplified example)



PAN

CVV

Passive PAN Authentication

PIN Code

PIN Code

User Authentication Achieved

Random Number

Cipher Random with Card Secret Key

Ciphered result

Calculate Dk from Master Key Mk & PAN

The card locks the process after "x" false attempts

Active Card Authentication Achieved

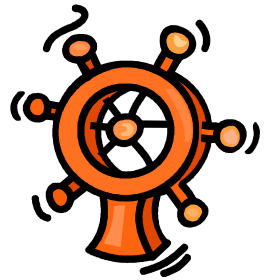
Payment Card Related Standards

Plastic Financial Cards	Card format	ISO/IEC 7810
	Magnetic stripe	ISO/IEC 7811
	Identification of issuers	ISO/IEC 7812
	Magnetic stripe data	ISO/IEC 7813
Network	Exchange of information	ISO/IEC 8583
Card & Devices Communication Protocols	Smart card contact	ISO/IEC 7816
	Smart card contactless	ISO/IEC 14443
	Near Field Communication	ISO/IEC 18092
Intelligent Card Application Commands	Smart card commands	ISO/IEC 7816

Payment Related Specifications

EMV (Europay, Mastercard, Visa and recently JCB)

- Interoperability of card acceptance, security and payment functions.
  Three levels of flexibility and compliance
  1. Different payment association affiliation
  2. Same payment association affiliation
  3. Same financial institution
- Require EMV compliant financial network
  - The network must allow rather complex bi-directional exchanges



AmEx ExpressPay, MC PayPass and Visa payWave

- Simplified EMV-compatible or EMV-like payment feature allowing existing mag-stripe networks to use the enhanced security of smart cards
- 14443 standard (contactless) providing cardholders with a simpler way to pay by tapping a payment card or other payment device, such as a phone or key fob, on a point-of-sale terminal reader rather than swiping or inserting a card.

EMV Specifications

MasterCard Worldwide, Visa, Inc. and JCB International worked jointly over the last few years to develop specifications that define a set of requirements to ensure interoperability between chip cards and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is used.

EMV 4.2 Specifications (June 2008) consist of four books:

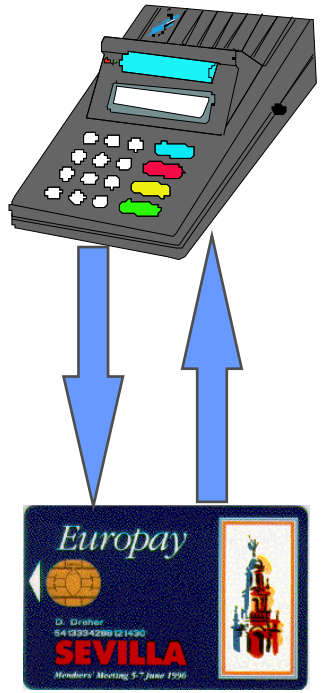
- Book 1 - Application Independent ICC to Terminal Interface Requirements
- Book 2 - Security and Key Management
- Book 3 - Application Specification
- Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements

http:// www.EMVco.com

EMV - Built for Off-line Decisions

The terminal

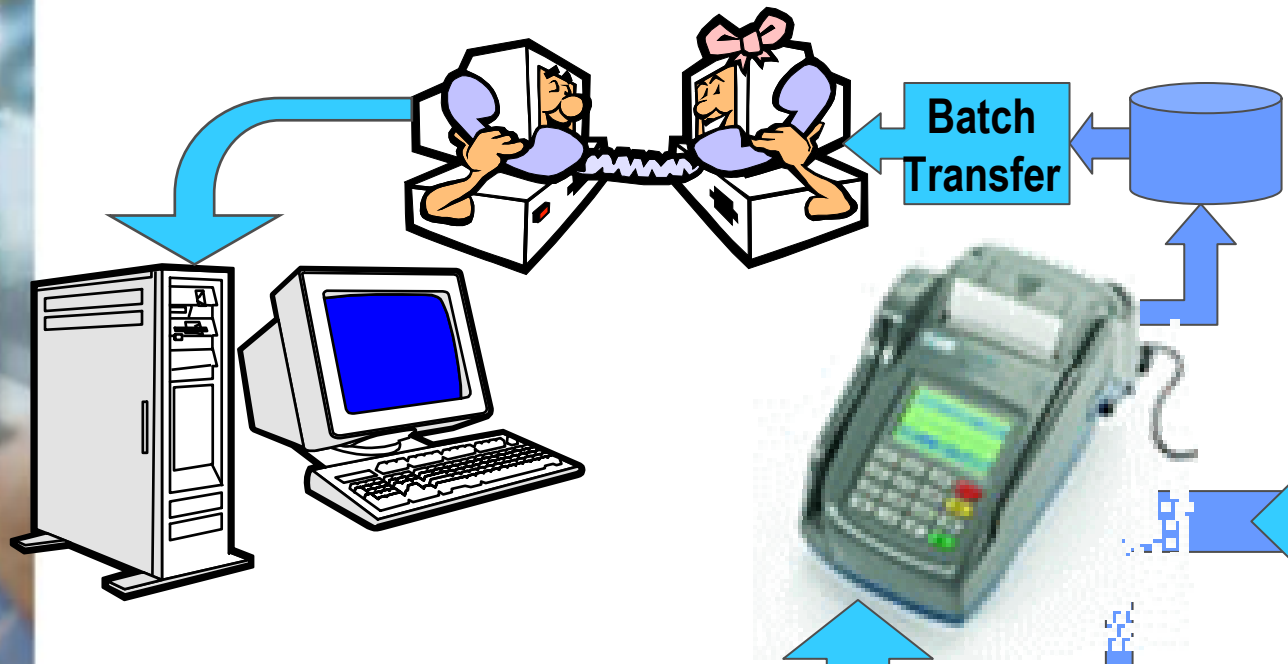
- contains the ***risk management of the merchant financial institution***
- is based on the terminal EMV specification



The card

- contains the ***risk management of the card issuing financial institution***
- contains the ***risk management and international rules of the payment association***
- is based on the card EMV specification and tailored to the specific need of the issuing financial institution

EMV Credit/Debit Semi Off-line



$ Amount
Merchant ID
Date
Time

PAN
Expiration Date
Name
Transaction Signature

PIN

The smart card, when authorized by its user, generates a unique cryptographic signature of the transaction (DDA = dynamic data authentication)

Smart Card EMV Payment Protocol

POS Terminal

Contact activation - ISO 7816

Identification according to ISO 7816

Smart Card

Select payment application (EMV)

Present PIN to the card

PIN accepted - Card ready

PAN

Send static account information

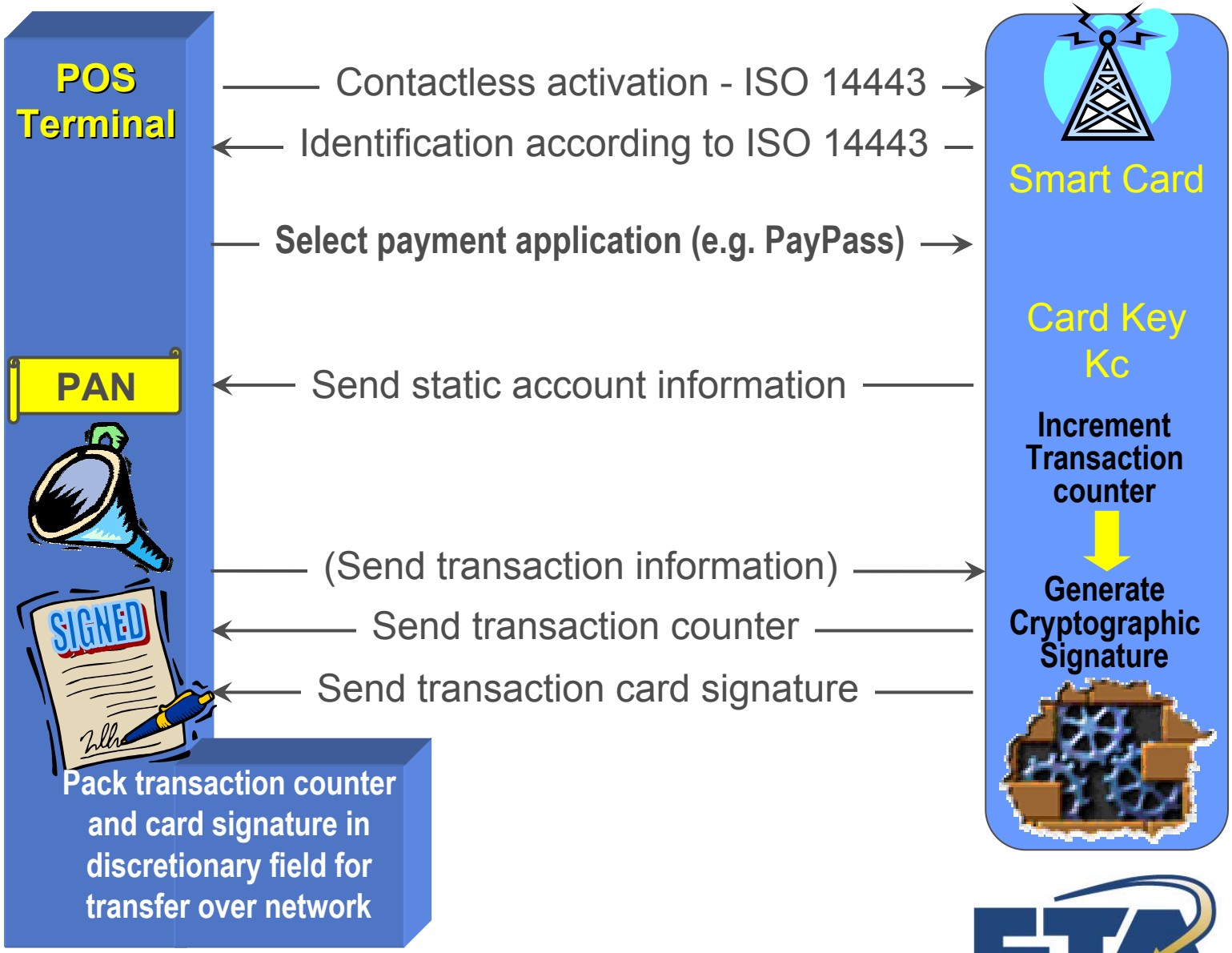
Card Key Kc

Provide transaction information

Generate Cryptographic Signature

Send transaction signature

Smart Card Contactless Payment



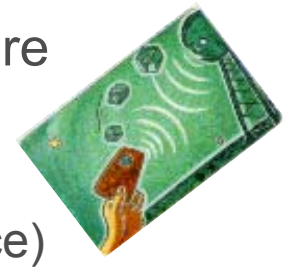
What Contactless Payment Brings

Fast, convenient payment

- Wave and be done for the customer
- Little terminal space on merchant counter
- No mechanical wearing of terminal or card
- Flexible form factor for payment device

Added security

- The card generation of a cryptographic signature based on information changing for each payment protects against:
  - Replay attacks (no transaction can be done twice)
  - Card cloning or skimming (the card key never leaves the protection of the smart card memory)



Simple integration

- The simplified contactless protocol allows use of existing networks for electronic payment

Smart Cards & Payments: Transaction Processing and Business Applications

Roger Musfeldt
Director, Mobile Commerce Solutions, First Data

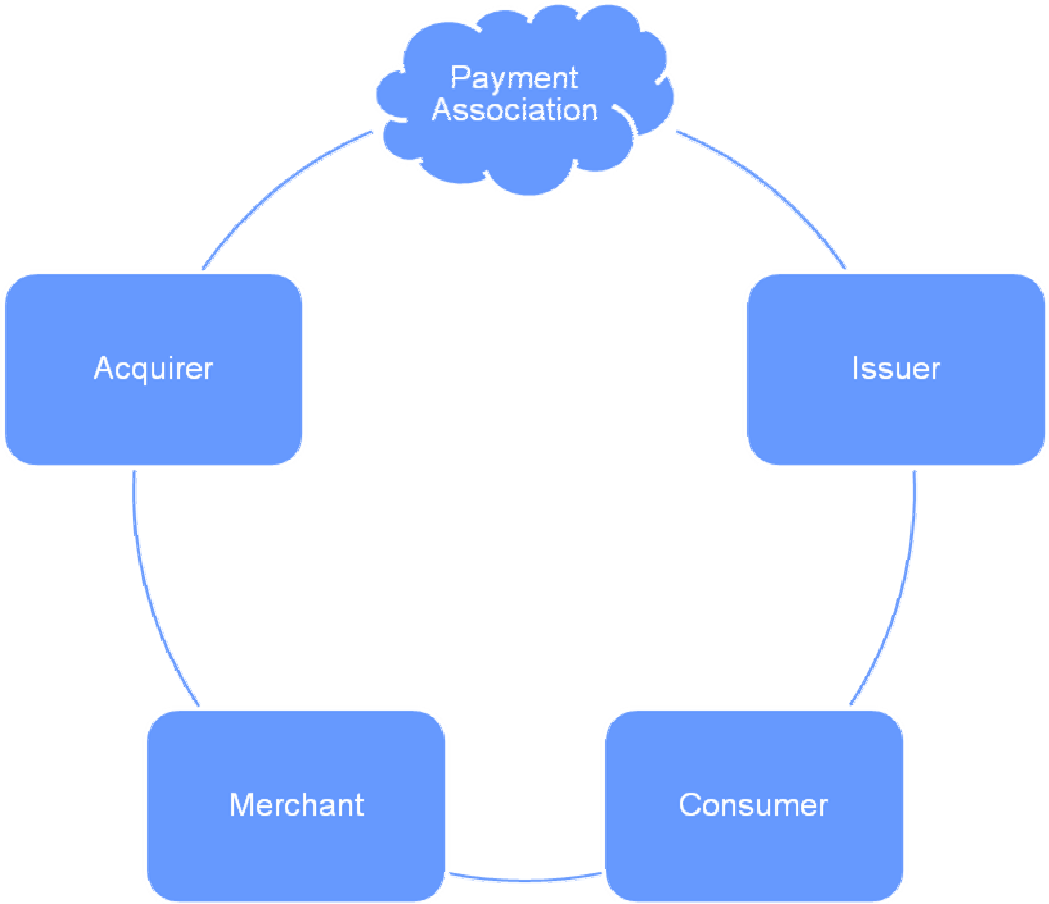
First Data

ETA

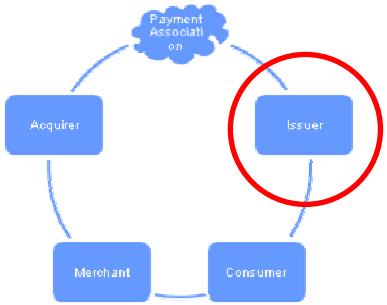
Discussion Topics

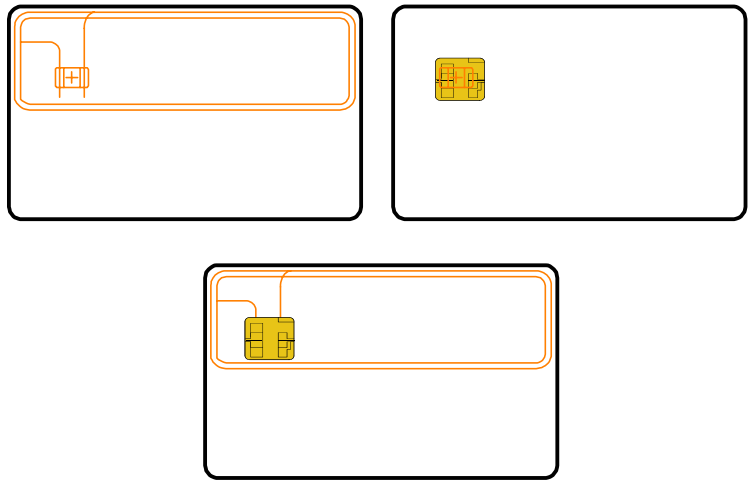
- The Players
- Presentation Instruments
- Acceptance Devices
- Multi-Application Smart Cards
- Payment Specifications
- Offline EMV Payment
- Online Payment
- Acquirers / Merchants: Steps to Smart Card Payment
- Issuers: Steps to Smart Card Payment

The Players



Presentation Instruments



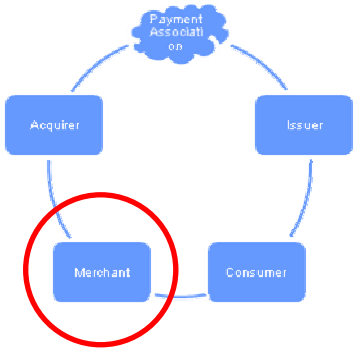


MAG STRIPE CARDS

Contact and Contactless Smart Cards

Contactless or NFC capable devices

Acceptance Devices

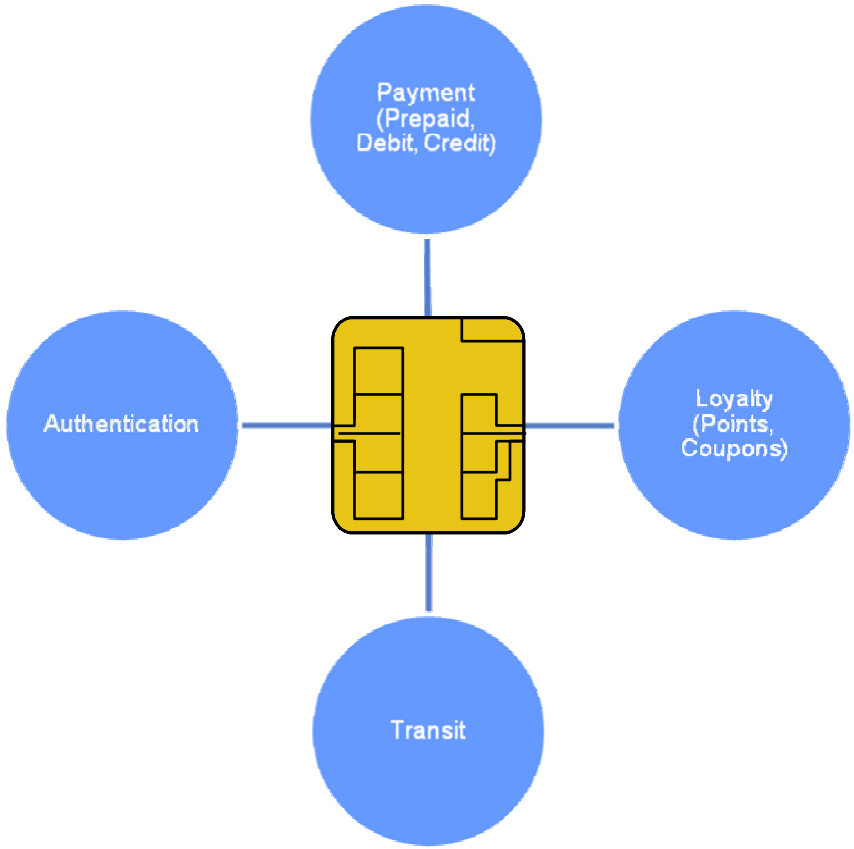


Contact Smart Card Readers

Contactless Smart Card Readers

NFC Capable Handsets

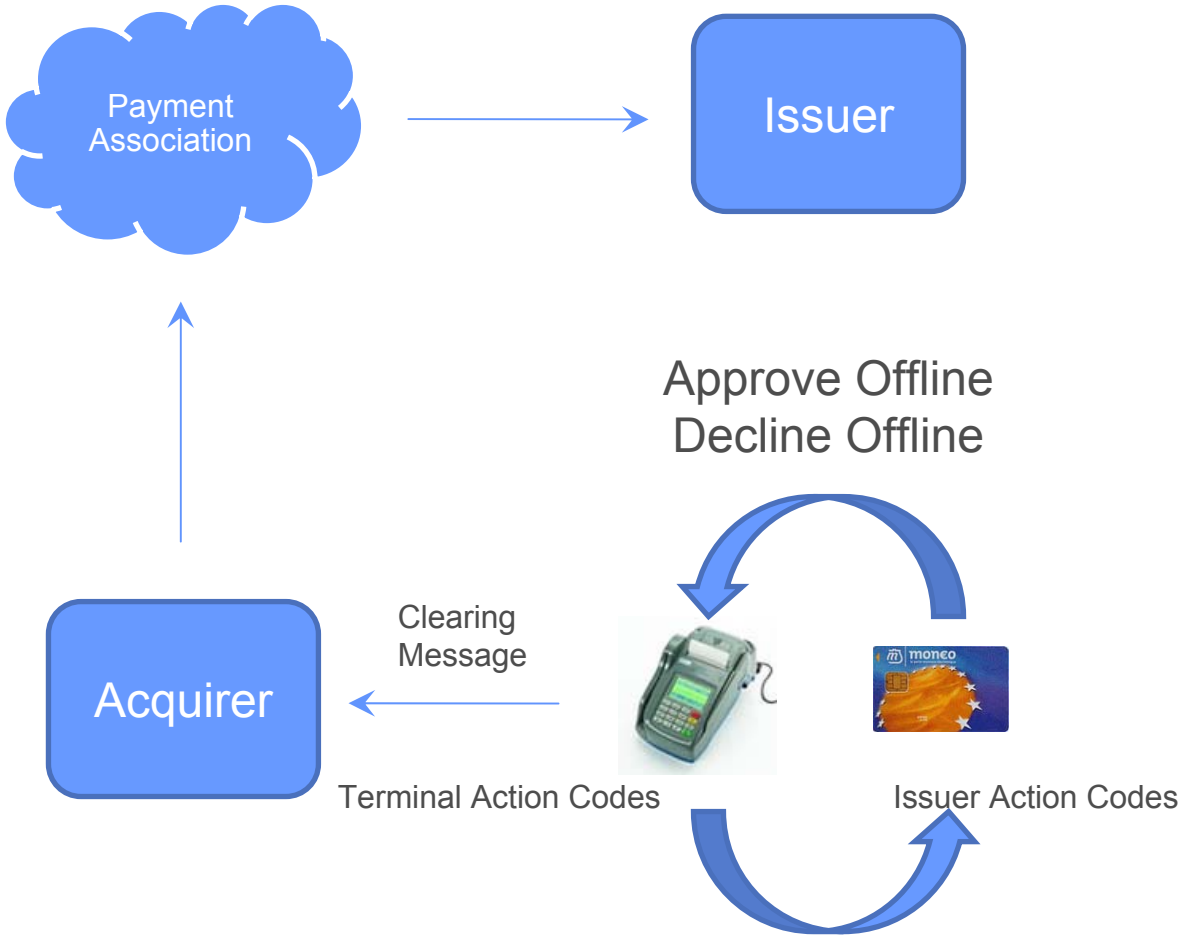
Multi-Application Smart Card



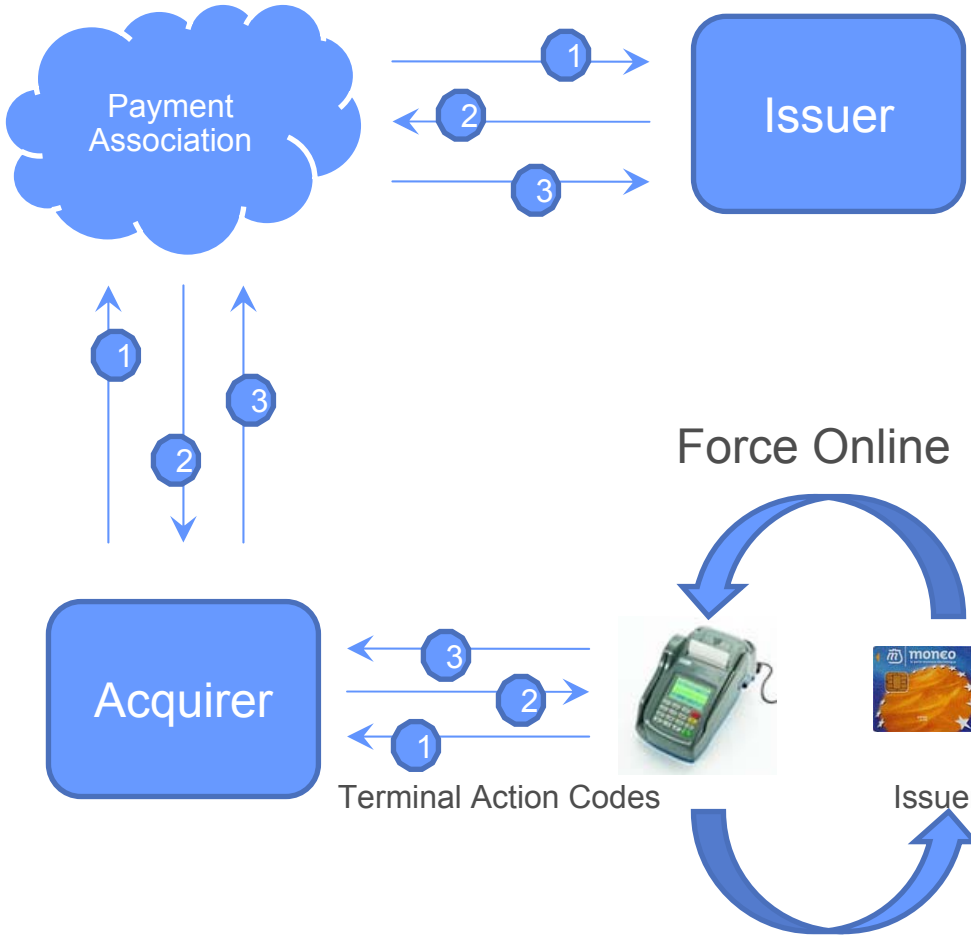
Payment Specifications

- **Contact EMV**
  - Chip & PIN
  - Highest Security Level
  - Online and Offline Transactions
  - Online Card Authentication (CAM)
  - Issuer Authentication
  - Issuer Scripting
- **Contactless EMV**
  - Online Transactions Only
  - Online Card Authentication (CAM)
- **Contactless Magnetic Stripe**
  - Online Transactions Only
  - USA-centric
  - Magnetic Stripe Environment

Offline EMV Payment

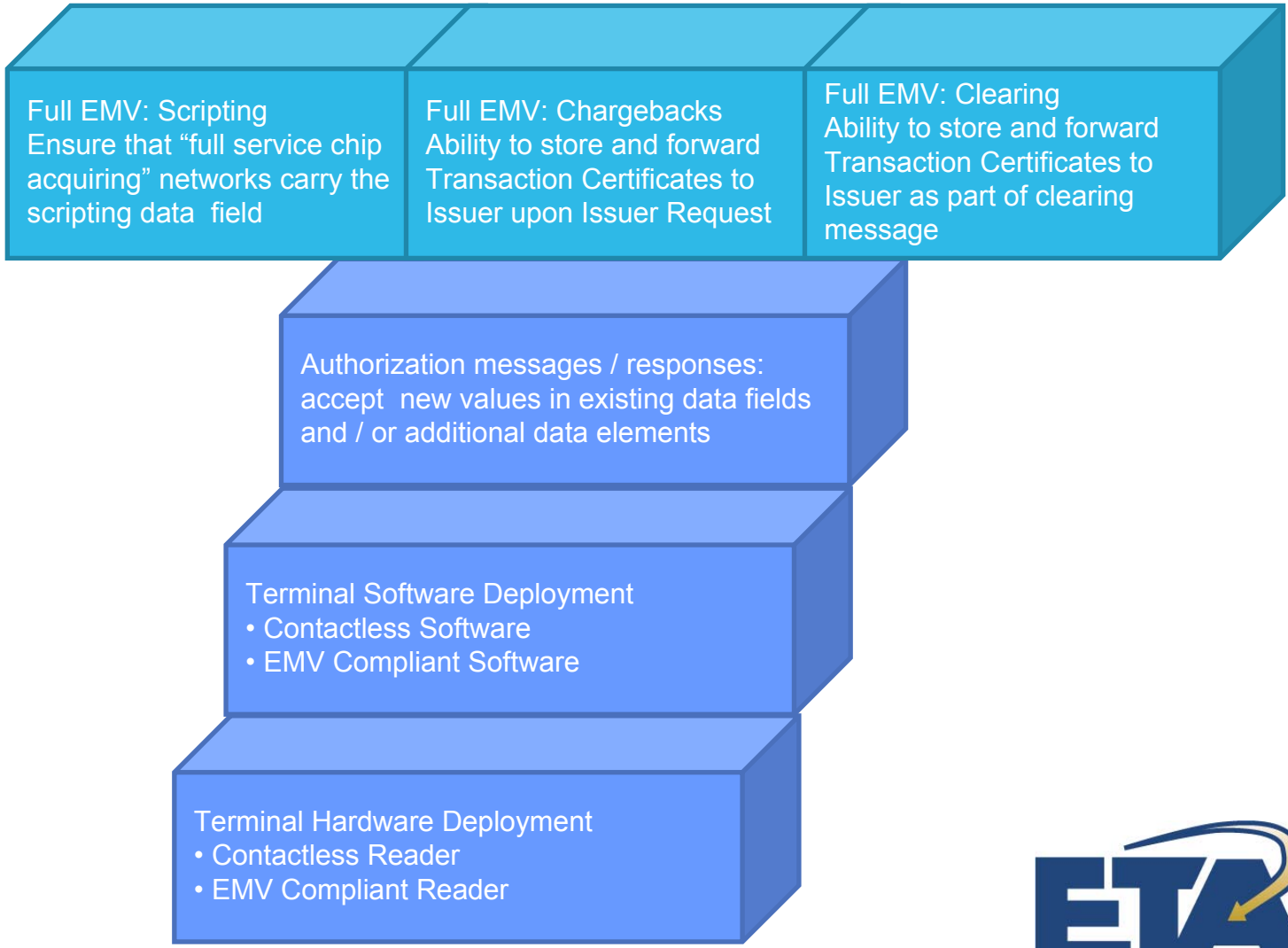


Online Payment
Contact and Contactless

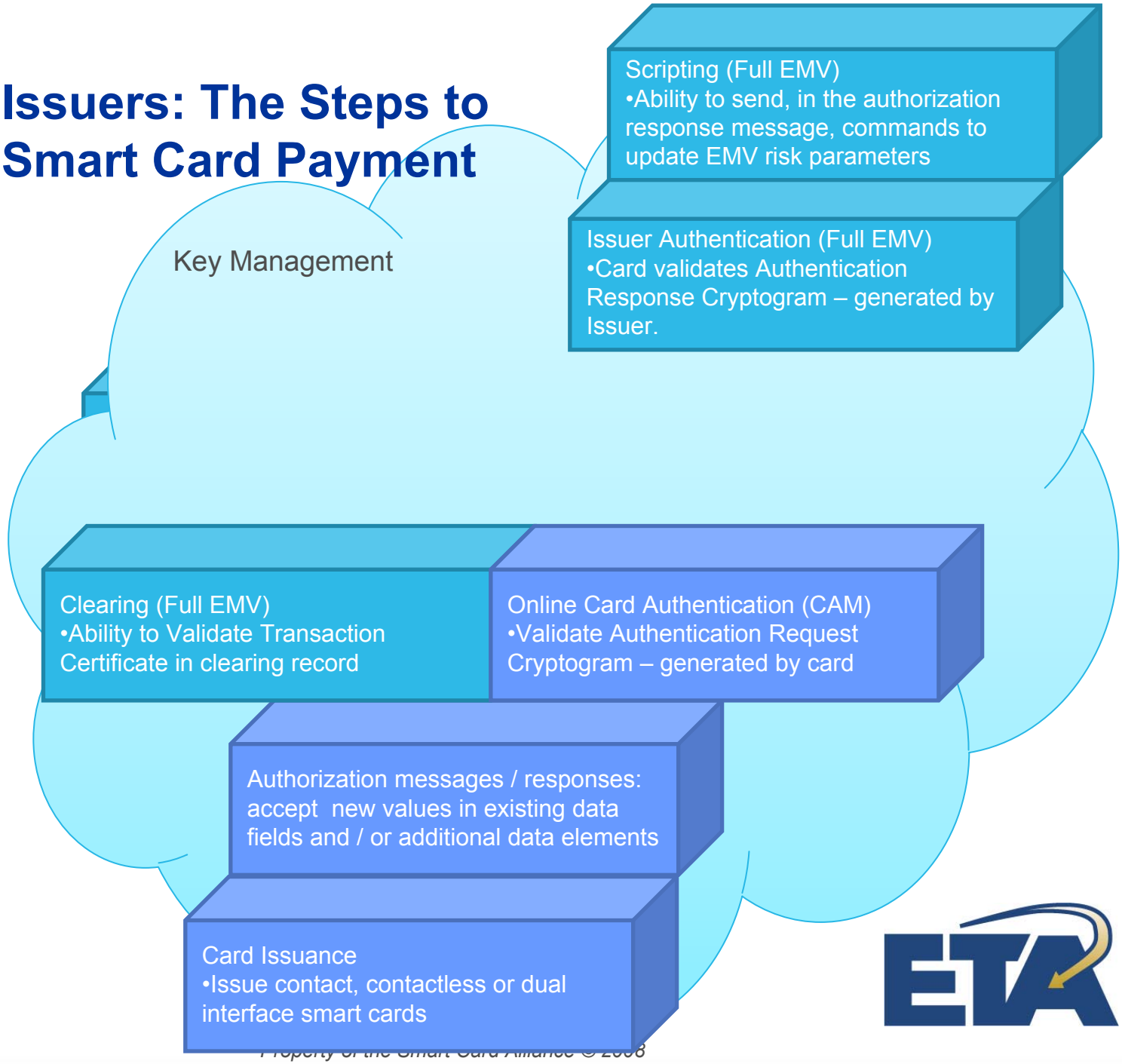


1. Authorization Request
2. Authorization Response
3. Clearing Message

Acquirers / Merchants
The Steps to Smart Card Payment



Issuers: The Steps to Smart Card Payment



Conclusions & Wrap Up

Randy Vanderhoof
Executive Director, Smart Card Alliance

Summary

- Smart cards in payment build on the fundamental elements of mag stripe and add layers of security across the payments network
- Offline and online payments are enabled and secured using PIN and encryption techniques to authenticate the cardholder and the POS terminal
- Merchant acquirers and card issuers have well-defined steps in place to manage the move to smart card payments

Questions & Answers

Moderated by: Randy Vanderhoof, Smart Card Alliance

Electronic Transactions Association
http://www.electran.org

Rori Ferensic, Electronic Transactions Association, rferensic@electran.org

Smart Card Alliance
http://www.smartcardalliance.org

Randy Vanderhoof, Smart Card Alliance
rvanderhoof@smartcardalliance.org

Gilles Lisimaque, IDTP
glisimaque@idtp.com

Roger Musfeldt, First Data
roger.musfeldt@firstdata.com

ETA & Smart Card Alliance Web Seminar Series

Smart Card Implementation

- January 13, 2009, 1:00 pm ET

Smart Cards and Payment Security

- February 3, 2009, 1:00 pm ET