OmniPayments

The Smarts Behind Smart Cards

Yash Kapadia
CEO, OmniPayments Inc.
HP NonStop Technical Bootcamp
November, 2014
Yash@OmniPayments.com

The Smarts Behind Smart Cards
Agenda

1. What Is a Smart Card?
2. The Structure of a Smart Card
3. Processing Flow – Preliminary Processing
4. Processing Flow – Online Processing
5. Processing Flow – Offline Processing
6. Smart Card Protections
7. Summary

What Is a Smart Card?

What Is a Smart Card?

- A smart card provides security via an embedded computer chip.

- Specifications developed by Europay, MasterCard, and Visa (EMV).

- Also known as an EMV card or a chip-and-PIN card.

What Is a Smart Card?

The Benefits of Smart Cards

- **Secure – Cards cannot be cloned or counterfeited.**

- **Secure – Lost or stolen cards cannot be used.**
- **Secure – All data in flight to POS terminal and issuer is encrypted.**
- **Issuer takes responsibility for fraudulent transactions rather than the merchant.**
- **Merchant does not have to do PCI audit (though PCI DSS must still be followed).**

What Is a Smart Card?
A Problem With Smart Cards

- Smart cards have been adopted worldwide:
  - everywhere but in the U.S.

- Magnetic-stripe cards are often not accepted by foreign merchants.

- Magnetic-stripe cards are often not accepted at foreign
  - kiosks (train stations).
  - gasoline pumps.
  - ATMs.

- U.S. travelers to Europe are often left with no payment-card options if they do not carry a smart card.

What Is a Smart Card?

A Problem With Smart Cards

- **Percentage of POS terminals that are EMV enabled:**
  - **Europe 99.9%**
  - **Canada, Latin America 84.7%**
  - **Africa, Middle East 86.3%**
  - **Asia Pacific 71.7%**
  - **United States migrating**

- **Many of these terminals no longer accept magnetic-stripe cards.**

What Is a Smart Card?
U.S. EMV Mandate

- U.S. payment industry has mandated that merchants be EMV-capable by October 2015 (gas stations 2017).

- If a merchant makes 75% of its transactions via EMV-enabled terminals, it can avoid:
  - liability for fraudulent or contested transactions.
  - PCI audit requirements.

What Is a Smart Card?

How Are Cards Read?

- **EMV cards may be:**
  - **contact – must be inserted into an EMV POS terminal.**
  - **contactless – must be placed near an EMV POS terminal.**
  - **mobile – displayed on a smart phone or tablet.**

- **Most EMV POS terminals today read cards by contact.**

The Structure of a Smart Card

The Structure of a Smart Card

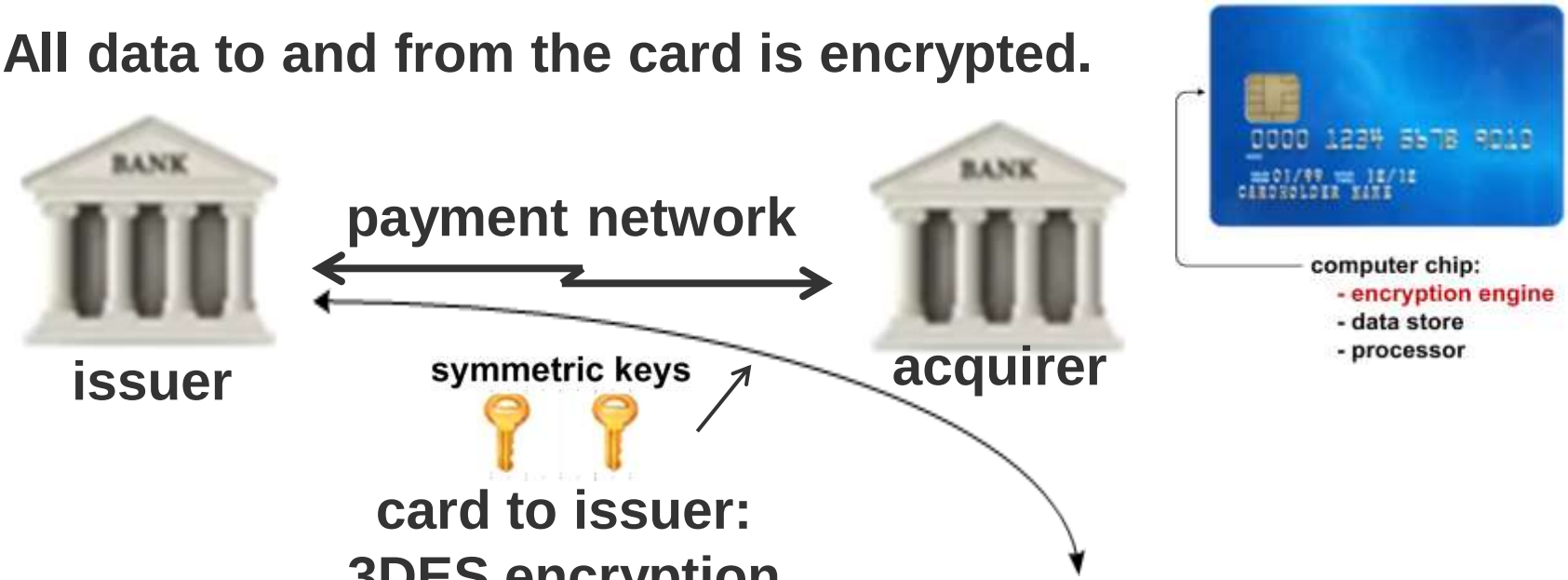
magnetic stripe
(back, optional)

embossing area

computer chip:
- encryption engine
- data store
- processor

The Structure of a Smart Card
Encryption

All data to and from the card is encrypted.



- **Card 3DES key is unique to each card:**
  - **card number encrypted with the issuer's symmetric key.**

The Structure of a Smart Card
The Data Stored on the Card

Card data includes static data, dynamic data, and secret data.

- **Static Data:**
  - card number
  - cardholder name
  - card effective date
  - card expiration date
  - card public key
  - issuer name
  - issuer public key
  - issuer applications*
  - Cardholder Verification Method (CVM)*
  - Signed Static Data*

*discussed later

No personal data is stored other than that stored on a magnetic stripe.

The Structure of a Smart Card
The Data Stored on the Card

Card data includes static data, dynamic data, and secret data.

- **Dynamic Data (risk parameters):**
  - card amount limit
  - transactions/day limit
  - transaction counter
  - lower floor limit
  - upper floor limit
  - max. offline limit
  - offline tx counter

- **Secret Data (will be erased if an access attempt is made):**
  - card PIN
  - card private key
  - issuer symmetric key

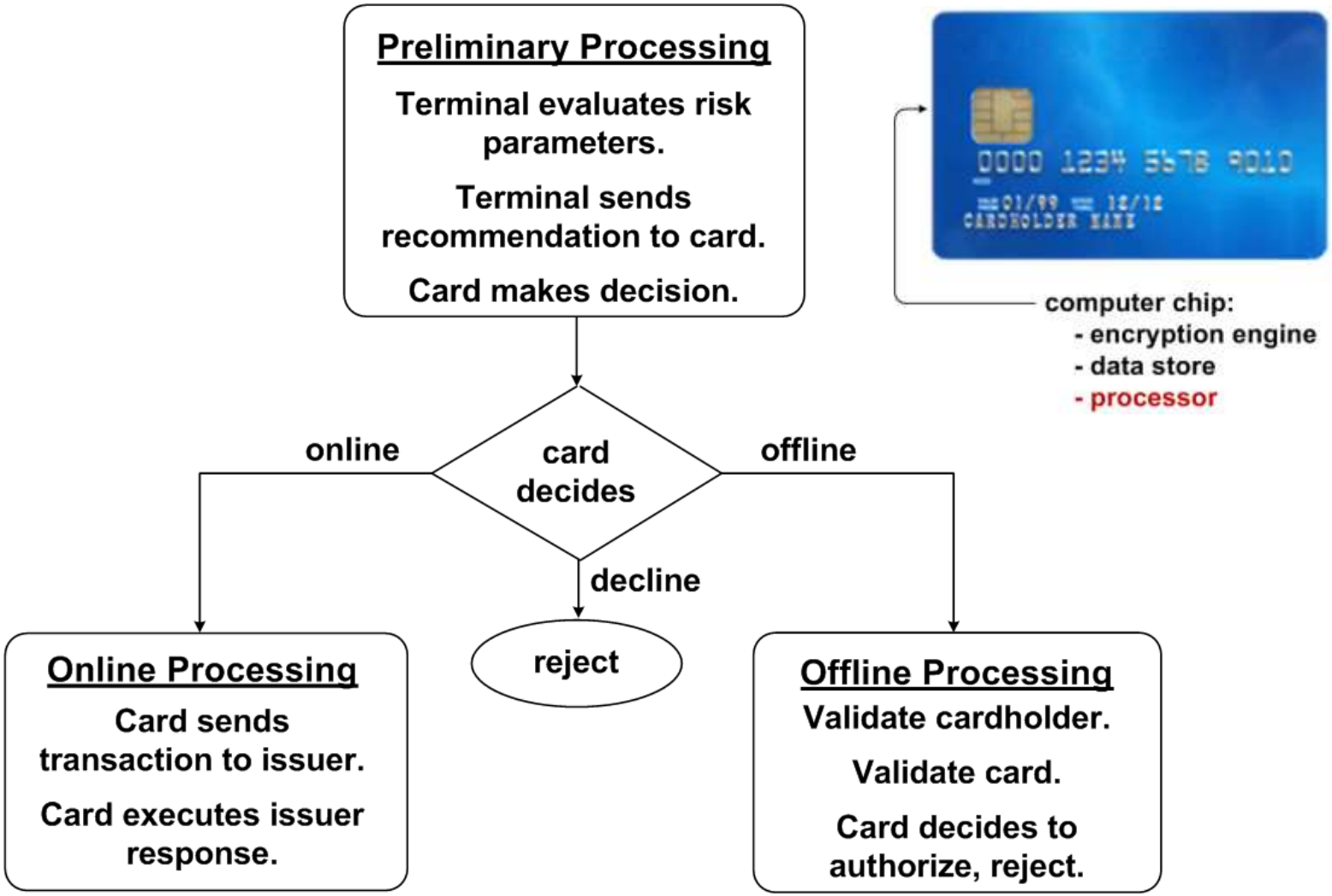
The Structure of a Smart Card

The Data Stored on the Card

- Card data is never read directly by the POS terminal.
- The terminal asks the card for data.
- The card encrypts the requested data with its private key.
- The terminal decrypts it with the card's public key.
- Likewise, all data transfer from the terminal to the card is encrypted with the card's public key.
- All data transfer between the card and the terminal is encrypted.

The Structure of a Smart Card

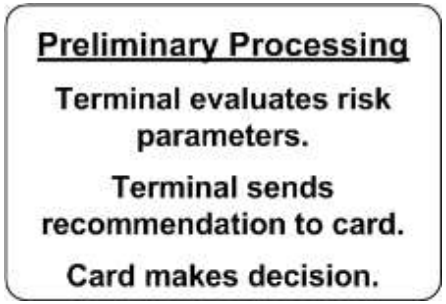
Processing Flow



Processing Flow:
Preliminary Processing

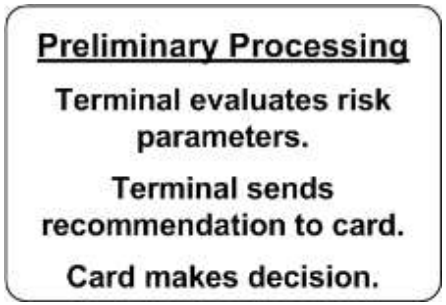
Preliminary Processing

- Terminal gets card's public key from card.
- Terminal gets static and dynamic data (risk parameters) from card.
- Terminal selects supported applications from card:
  - These are issuer rules for processing transactions.
  - Terminal matches card applications to those supported by terminal.
  - More than one?
    - Ask cardholder to select one (e.g., debit or credit).
- Terminal analyzes transaction against risk parameters.



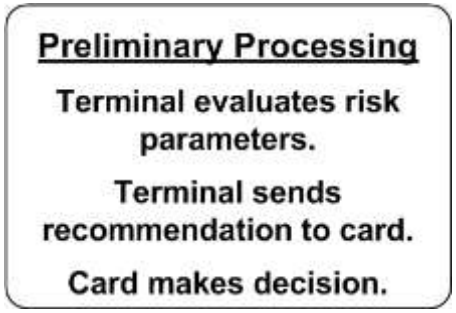
Preliminary Processing

- **Terminal recommends online, offline, reject to card.**
- **Card matches terminal recommendation to risk parameters.**
- **Card makes its own decision:**
  - **May be different than terminal recommendation, e.g.:**
    - **Issuer may want to authorize a tx from an expired card.**
    - **Issuer may want to authorize a tx over the card limit.**



Preliminary Processing

- **Card sends online, offline, reject decision to terminal:**
  - **online – Card will send transaction to issuer for authorization.**
  - **offline – Process transaction without issuer involvement.**
  - **reject – Reject transaction.**



Processing Flow:
Online Processing

The Structure of a Smart Card

The Data Stored on the Card

Online Processing

Card sends transaction to issuer.

Card executes issuer response.

- **Static Data:**
  - card number
  - cardholder name
  - card effective date
  - card expiration date
  - card public key
  - issuer name
  - issuer public key
  - issuer applications*
  - Cardholder Verification Method (CVM)*
  - Signed Static Data*

*discussed later

The Structure of a Smart Card
Cardholder Verification Method (CVM)

- The CVM specifies how a cardholder is to be verified:
  - online PIN – entered via PIN pad and sent to issuer.
  - offline PIN – entered via PIN pad and verified by card.
  - signature
  - no verification

- Methods to use are defined by issuer application.

- Examples:
  - ATMs require online PIN.
  - Offline kiosks (rail stations) require offline PIN.
  - POS terminals require online PIN and signature.
  - Small transactions require no verification.

Online Processing

- Request PIN from cardholder if required by CVM.

- Card sends encrypted transaction data to issuer:
  - card number
  - PIN
  - transaction amount
  - transaction counter

- Card receives encrypted response from issuer.

- Issuer Declines – Card informs terminal to reject transaction.

- Issuer Authorizes – Card informs terminal to accept transaction:
  - Request signature if required by CVM.

Online Processing

Card sends transaction to issuer.

Card executes issuer response.

Online Processing

Online Processing

Card sends transaction to issuer.

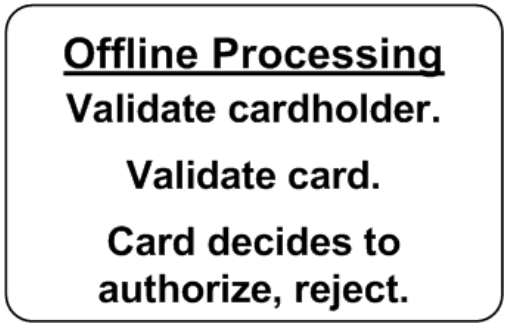
Card executes issuer response.

- Accept data updates, if any, from issuer:
  - new PIN, changed card limit, block card, etc.
- Card can reverse an issuer's authorization:
  - Response from host is suspicious.
  - Card is removed from terminal prematurely.
- A reversing transaction will be sent to the issuer.

Processing Flow:
Offline Processing

Offline Processing

When is Offline Processing Used?



- **Offline processing is used if:**
  - **There is no communication link (POS terminal on airline).**
  - **The communication link has failed.**
  - **The transaction amount is very small.**

Offline Processing
Risk Parameters

- Offline processing is controlled by the issuer's risk parameters:
  - lower floor limit – maximum amount of an offline transaction.
  - upper floor limit – maximum amount of offline transaction if communication has been lost.
    - allows merchant to continue in business.
  - maximum amount of consecutive offline transactions.
  - maximum number of consecutive offline transactions.

- Offline transactions are randomly selected for online authorization.

Offline Processing
Card Validation

Offline Processing
Validate cardholder.
Validate card.
Card decides to authorize, reject.

- **Offline processing must ensure that the card is neither cloned nor counterfeited.**

- **There are three methods to verify offline that a card is valid:**
  - **Static Data Authentication (SDA)**
  - **Dynamic Data Authentication (DDA)**
  - **Combined DDA/Application Cryptogram (CDA)**

The Structure of a Smart Card
Static Data Authentication

- **Static Data:**
  - card number
  - cardholder name
  - card effective date
  - card expiration date
  - card public key
  - issuer name
  - issuer public key
  - issuer applications*
  - Cardholder Verification Method (CVM)*
  - **Signed Static Data***

*discussed later

Offline Processing
SDA – Static Data Authentication

- SDA validates that the card is a valid card prepared by the issuer.
- The terminal reads the Signed Static Data from the card.
- This is the static data originally written to the card:
  - It is encrypted with the issuer's private key.
- The terminal decrypts the Signed Static Data with the issuer's public key.
- The terminal compares this to the static data on the card.
- If they match, the card is the original card (or a clone).

Offline Processing
DDA – Dynamic Data Authentication

- SDA guarantees that the card is not counterfeit.
- SDA does not protect against card cloning:
  - The signed static data will match the static data on the card.
- DDA encrypts the dynamic data on the card with the card's private key and sends the cryptogram to the terminal.

Dynamic Data (risk parameters):

card amount limit	lower floor limit
transactions/day limit	upper floor limit
transaction counter	max. offline limit
	offline tx counter

Offline Processing
DDA – Dynamic Data Authentication

- The terminal decrypts the cryptogram with the card's public key.

- If the dynamic data matches, the card has not been cloned:
  - The attacker could not have known the card's private key.

- The attacker cannot substitute its own key pair:
  - The public key will be rejected by the Certificate Authority.

Offline Processing
CDA – Combined DDA/Application Cryptogram

- SDA and DDA do not protect against a "wedge attack":
  - A man-in-the-middle attack.
  - Insert a real EMV card into the terminal to get a validation.
  - Then insert a device to emulate the card and authorize the transaction.

- CDA adds the card's application cryptogram:
  - The card's initial decision to process the transaction online, offline, or to reject it.

- The attacker cannot generate a valid application cryptogram:
  - It does not know the card's private key.

Offline Processing
Processing Flow

- Verify cardholder via CVM as mandated by application.
- Validate card via SDA, DDA, CDA as mandated by application.
- Terminal performs offline risk management.
- Terminal recommends accept/reject to card.

Offline Processing

Validate cardholder.

Validate card.

Card decides to authorize, reject.

Offline Processing
Processing Flow

- If card decides to reject offline authorization:
  - Reverts to online authorization.
  - Sends encrypted transaction to issuer.

- If card decides to authorize transaction:
  - Card tells terminal to accept transaction.

- Transaction data is batched for later transmission to issuer.

Offline Processing

Validate cardholder.

Validate card.

Card decides to authorize, reject.

Smart-Card Protections

Smart-Card Protections
Cloning and Counterfeiting

- **Smart-card cloning:**
  - **Making a copy of a smart card.**
  - **Data cannot be read by an attacker.**
    - **All data transfers between the card and the terminal are encrypted.**
  - **If an attempt is made to read secret data, it is erased.**

- **Smart-card counterfeiting:**
  - **Creating new smart cards.**
  - **Attacker can't write blank cards.**
  - **Every batch of blank cards is protected by a unique symmetric key known only to the issuer.**

Smart Card Protections
Cloning and Counterfeiting

- **Even if cloned or counterfeited cards were made:**
  - **The transaction counters in the dynamic data will be out of sync.**
  - **The issuer will block all such cards.**

- **Magnetic-stripe cloning:**
  - **Even if data could be read, card does not contain the magnetic-stripe CVC (Card Verification Code).**

Smart Card Protections
Card-Not-Present Fraud

- Internet purchases.
- Private card reader may be required by some merchants.

- They cost about $25 U.S.
- Generates a one-time passcode that is entered with order information.
- Passcode is verified by issuer.
- 30 million Europeans are using these passcode generators.

Smart Card Protections
Lost or Stolen Cards

- Lost or stolen cards cannot be used by others.

- Protected by CVM:
  - PIN known only to the cardholder.
    - Number of PIN attempts limited before blocking.
    - Issuer option not to require PIN.
  - Signature – hopefully the merchant checks.
  - Offline purchases with no CVM:
    - Limited by amount, number of transactions.
    - Issuer can block card if offline limits are exceeded.

Smart Card Protections
Using Smart Cards at Dumb Terminals

- A continuing vulnerability.
- Magnetic stripe can be cloned.
- Cloned magnetic-stripe cards can be used at other dumb terminals (just like now).
- Threat goes away when magnetic stripes are discontinued.

Smart Card Protections
Chip-and-Signature Cards

- Another vulnerability.

- U.S. Issuers are not issuing chip-and-PIN credit cards.
  - Only a signature is required.
  - Competitive reasons – cards easier to use.

- A lost or stolen card can be used by others.
  - Issuer takes loss, not merchant.

- Not accepted often outside of the U.S.
  - PIN needed.
  - Request PIN from issuer.

Summary

Summary

- If you go to Europe, carry a smart card.
- Security implemented via embedded computer chip.
- All data in flight to terminal or issuer is encrypted.
- Smart cards will eliminate the Target syndrome:
  - can't be skimmed.
  - can't be cloned
  - can't be counterfeited.
- Transactions can be authorized even if the network is down.
- U.S. merchants to be compliant by October, 2015, to obtain:
  - liability shift from merchant to issuer.
  - relief from PCI audit requirements.

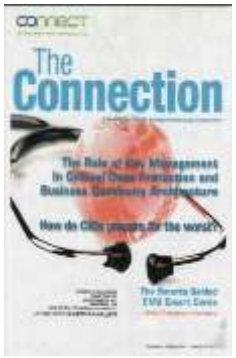
Summary

The Big Question -

- Are the hackers smarter than us?
- Smart cards have not been compromised in over a decade.
- But only time will tell.

Questions?

Thanks for Coming



The material in this presentation has been published in The Connection in much greater detail:

“ The Smarts Behind EMV Smart Cards:

“Part 1 – Online Transaction Processing” Sept/Oct 2014

“Part 2 – Offline Transaction Processing” Nov/Dec 2014

Visit www.omnipayments.com to learn about the OmniPayments EMV-compatible financial transaction switch.