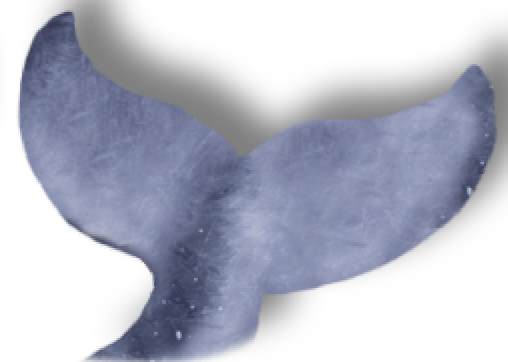


EMV

Europay MasterCard & Visa
Chip Cards

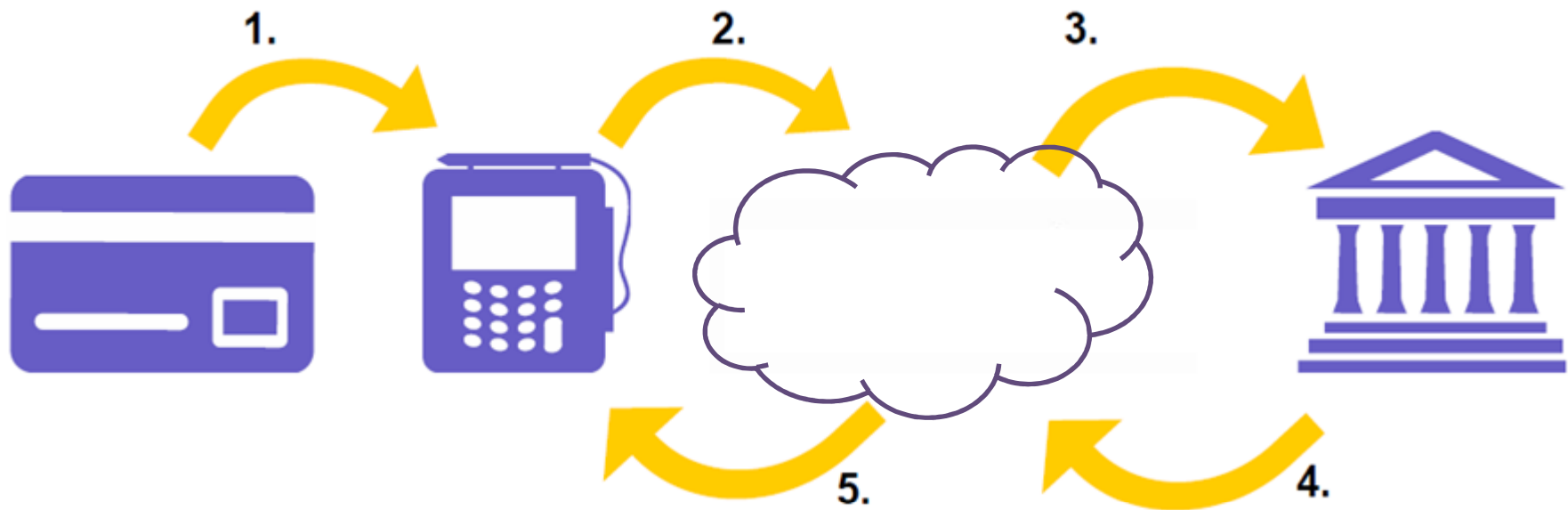


Fraud declined by 27% in the first five years after EMV was introduced in the UK.

In 2012, the U.S. accounted for 23.5% of payment card volume but 47.3% of payment card fraud.

Mag Stripe Card



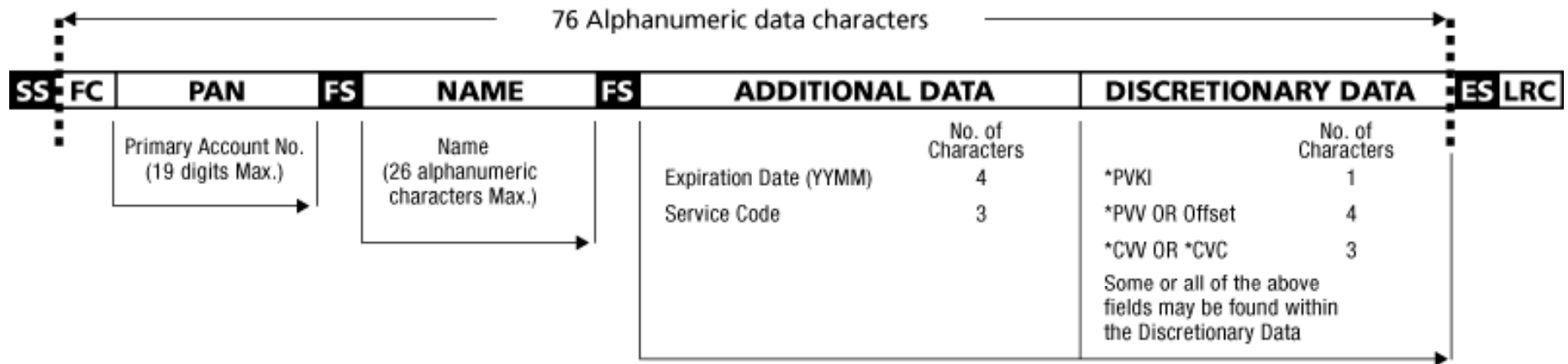


Terminal Magstripe Transaction Flow

1. Card is swiped through Terminal
2. Authorization Request from Terminal to Acquirer
3. Authorization Request from Acquirer to Issuer
4. Authorization Response from Issuer to Acquirer
5. Authorization Response from Acquirer to Terminal

Mag Stripe Card

Track 1:



Shaded area identifies control characters

SS Start Sentinel	%	FC Format Code
FS Field Separator	^	LRC Longitudinal Redundancy Check Character
ES End Sentinel	?	

*(PVKI) PIN Verification Key Indicator

*(PVV) PIN Verification Value

*(CVV) Card Verification Value

*(CVC) Card Validation Code

Track 2: Similar to track 1, no name section only 36 numeric characters

Track 3: 104 numeric characters, country code/currency code, not used widely



**For >\$500 you too can
have your own card
fraud kit**

[All](#)
 Cart (0) 0.0\$
 Balance: **0.0\$**
[Add money](#)
[Replace policy](#)
[Logout](#)

[All](#)

Cle

Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country	Bank	Base	Price
553891	 MASTERCARD	DEBIT	STANDARD	01/14	Yes	101	 United States, KS, WICHITA, 67209	FIFTH THIRD BANK	Tortuga-4 	24.7\$
553891	 MASTERCARD	DEBIT	STANDARD	10/14	Yes	101	 United States, KS, WICHITA, 67205	FIFTH THIRD BANK	Tortuga-4 	24.7\$
553891	 MASTERCARD	DEBIT	STANDARD	02/15	Yes	101	 United States, KS, WICHITA, 67226	FIFTH THIRD BANK	Tortuga-5 	24.7\$
553891	 MASTERCARD	DEBIT	STANDARD	10/14	Yes	101	 United States, KS, WICHITA, 67226	FIFTH THIRD BANK	Tortuga-5 	24.7\$
553891	 MASTERCARD	DEBIT	STANDARD	09/15	Yes	101	 United States, KS, WICHITA, 67205	FIFTH THIRD BANK	Tortuga-10 	26.6\$
553891	 MASTERCARD	DEBIT	STANDARD	10/15	Yes	101	 United States, KS, WICHITA, 67205	FIFTH THIRD BANK	Tortuga-12 	26.6\$
553891	 MASTERCARD	DEBIT	STANDARD	10/15	Yes	101	 United States, KS, WICHITA, 67205	FIFTH THIRD BANK	Tortuga-13 	26.6\$

EMV Card

Bank Name



1234 5678 9876 5432

1234

VALID THRU ▶ MONTH/YEAR
12/99

CARDHOLDER

Card Types





> Contact EMV



> Contactless EMV

> Contactless Mag Stripe Emulation



Combi

> Contact EMV

> Contactless EMV

> Contactless Mag Stripe Emulation



Transaction Types

Online

Offline

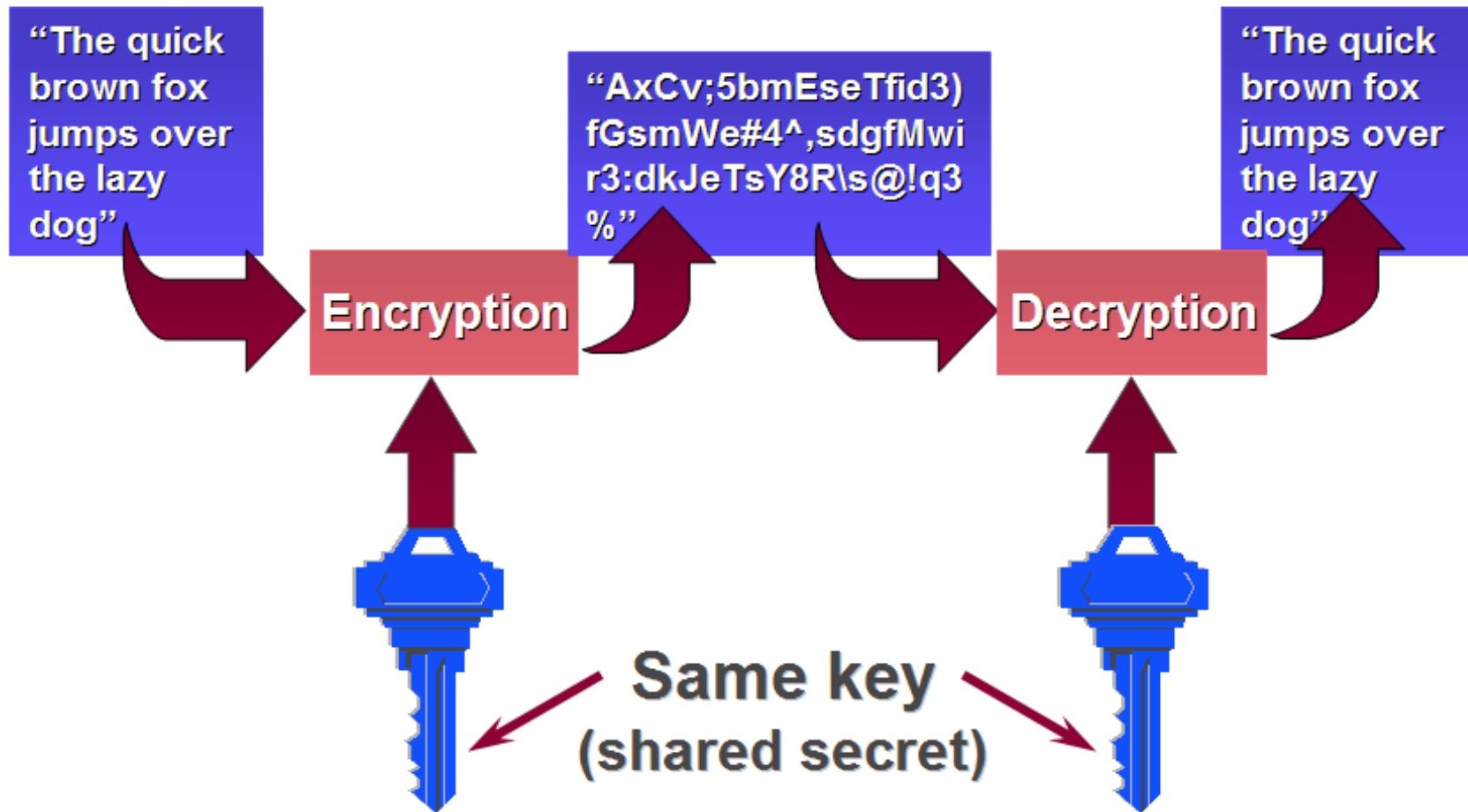
Online

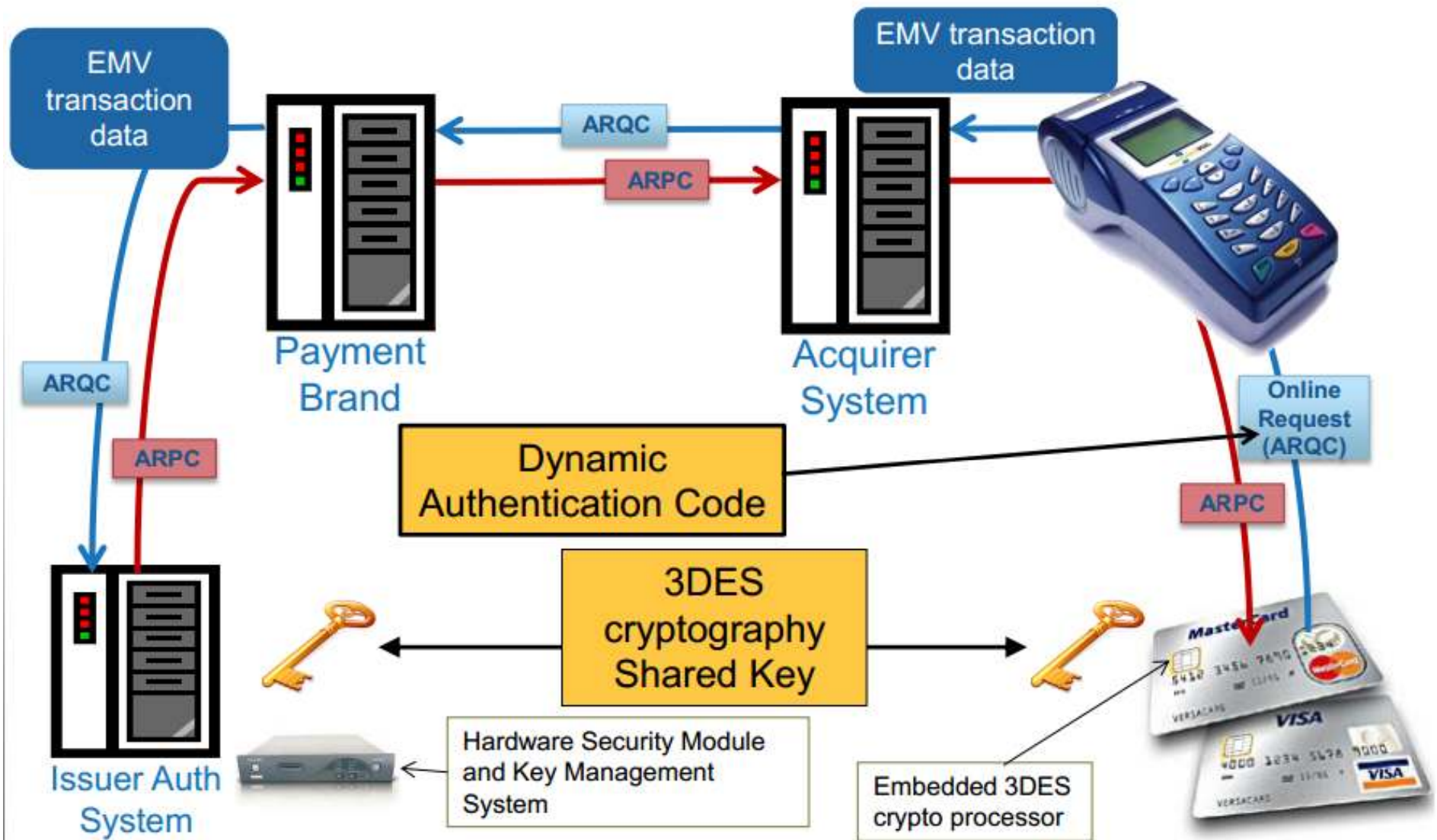
Relies on Symmetric Key Technology

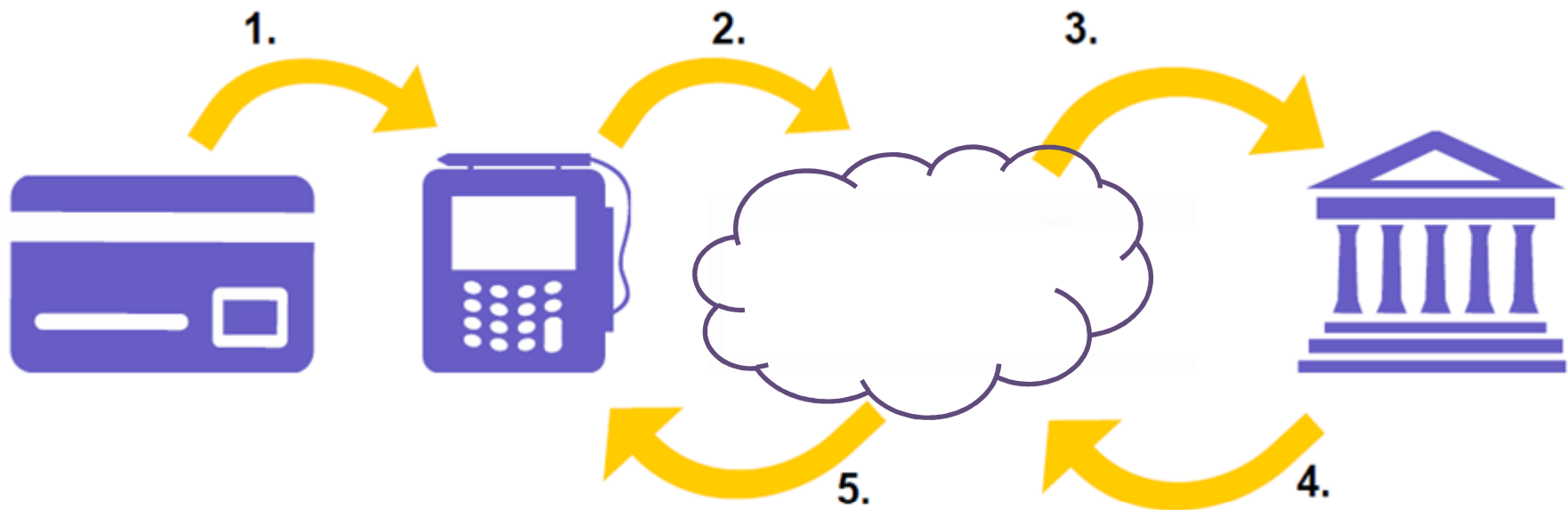
Plain-text input

Cipher-text

Plain-text output

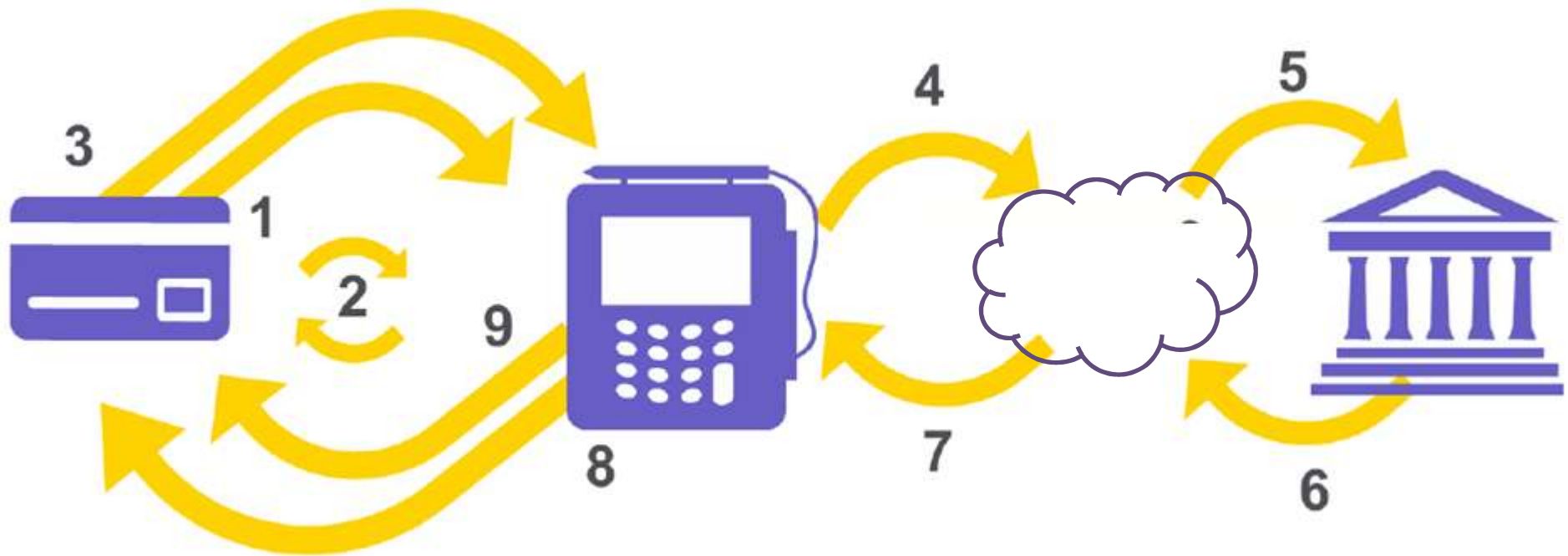






Terminal Magstripe Transaction Flow

1. Card is swiped through Terminal
2. Authorization Request from Terminal to Acquirer
3. Authorization Request from Acquirer to Issuer
4. Authorization Response from Issuer to Acquirer
5. Authorization Response from Acquirer to Terminal

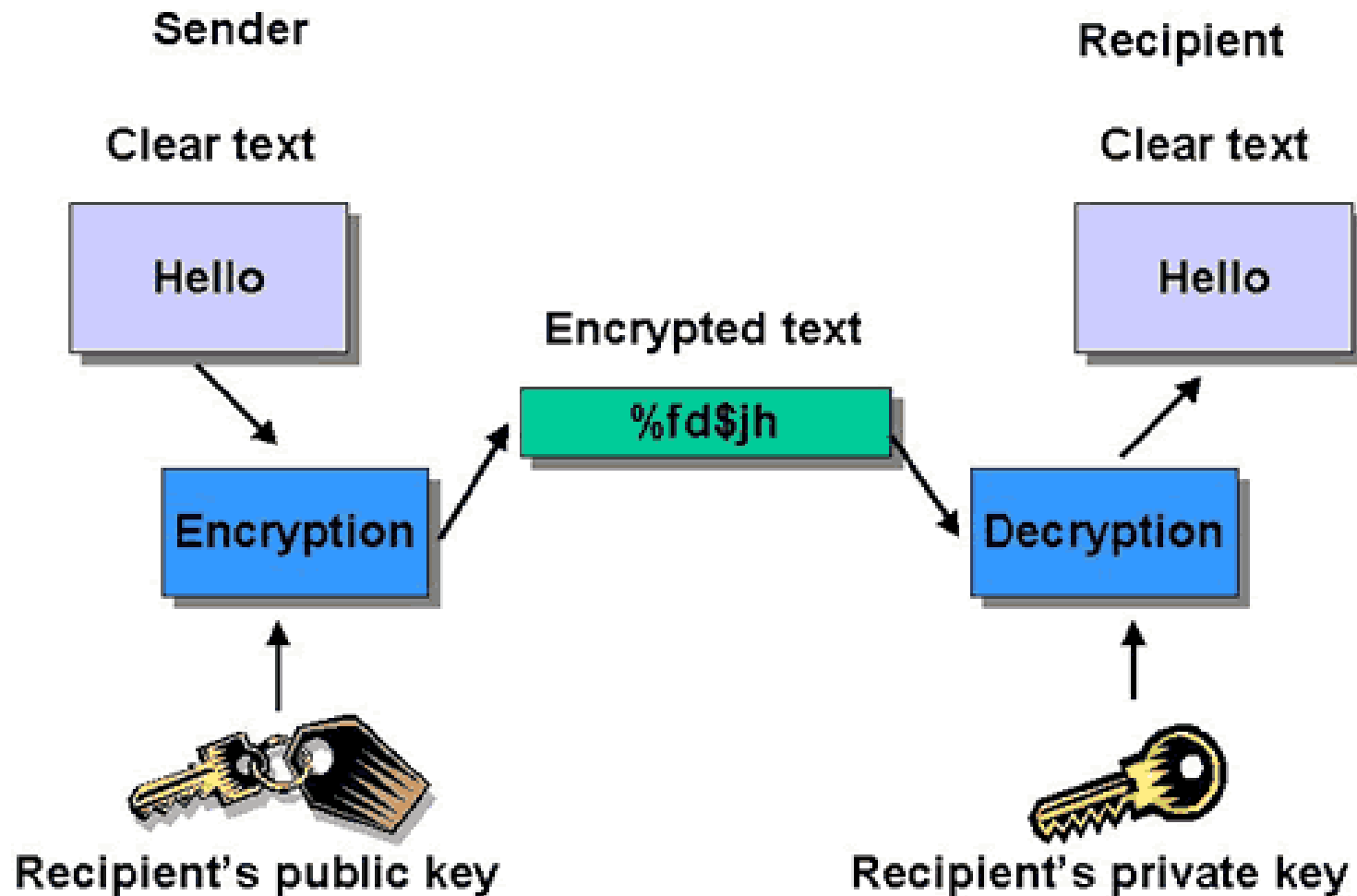


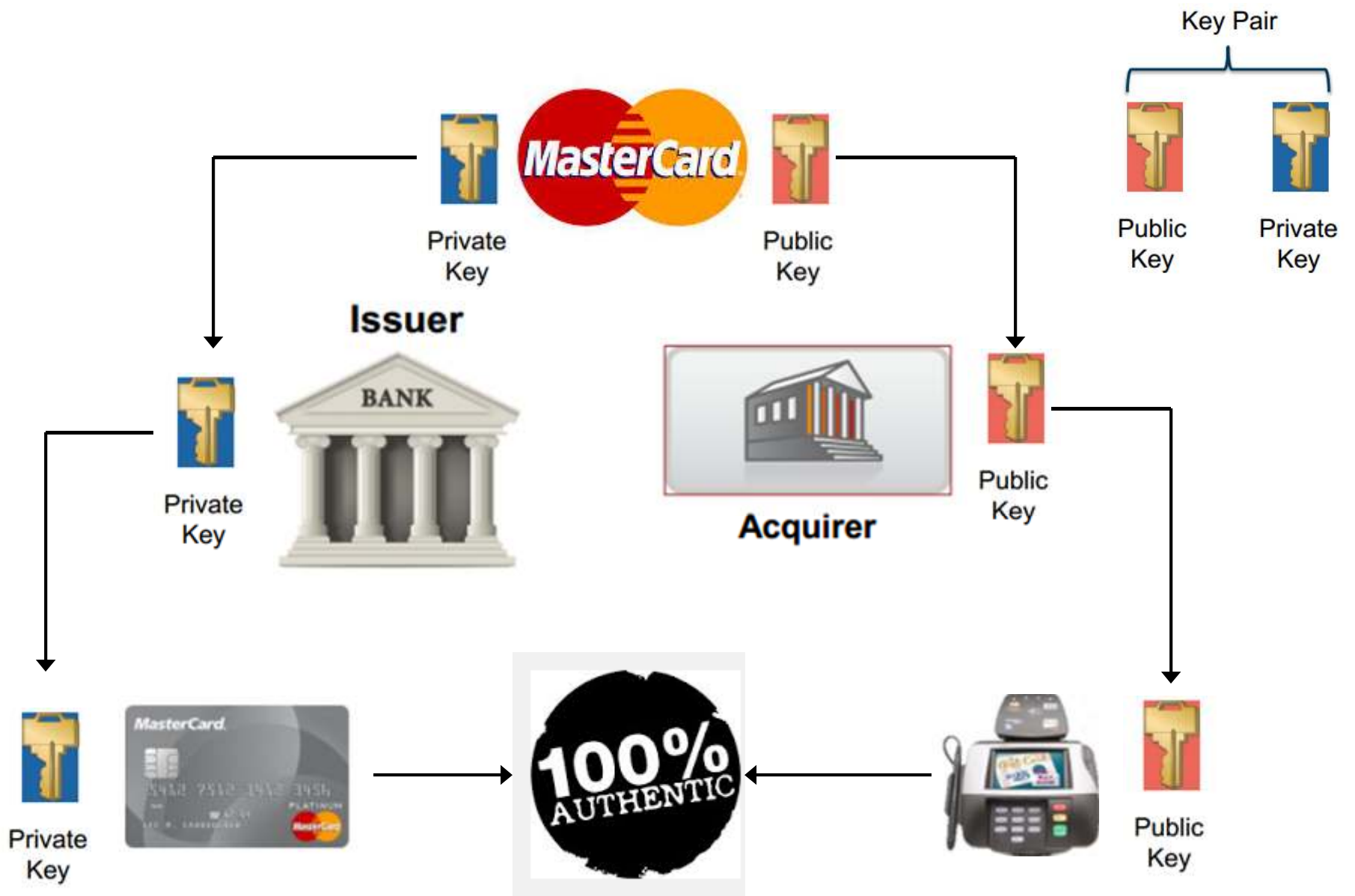
Terminal EMV Transaction Flow

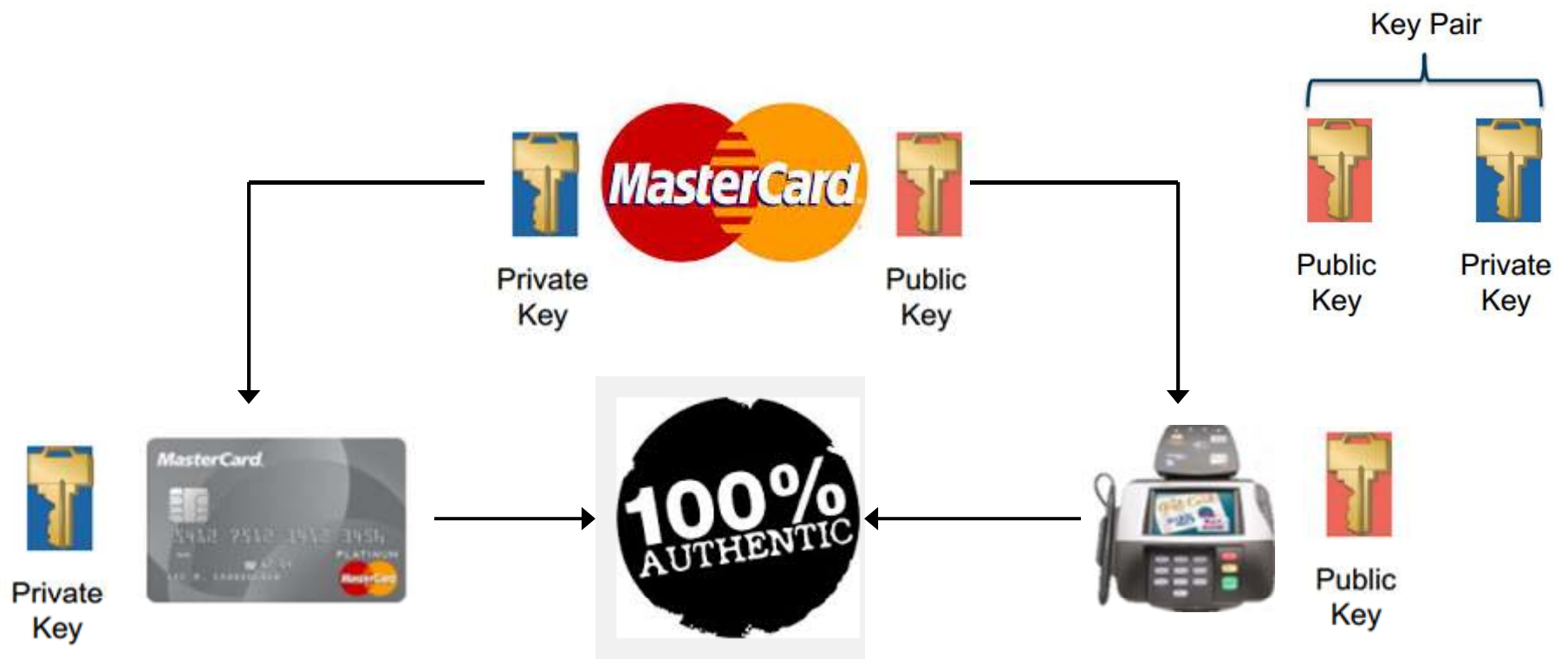
1. Card is inserted into EMV Terminal
2. First Half of EMV Transaction Protocol
 - A. Application Selection
 - B. Read Application Data
 - C. *Offline Data Authentication*
 - D. *Processing Restrictions*
 - E. *Cardholder Verification*
 - F. *Terminal Risk Management*
 - G. *Terminal Action Analysis*
 - H. *Card Action Analysis*
3. Online Authorization Request from Card to Terminal
4. Authorization Request from Terminal to processor
5. Authorization Request from processor to Issuer
6. Authorization Response from Issuer to processor
7. Authorization Response from processor to Terminal
8. Completion and script processing. If Issuer approved but card denied transaction a reversal is produced
9. Card is removed from EMV Terminal

Offline

Relies on Asymmetric Key Technology







- 1 – Terminal generates random number.
- 2 – Terminal hashes random number.
- 3 – Terminal encrypts hash with MasterCard's public key.
- 4 – Terminal passes off encrypted string to card.
- 5 – Card decrypts the string using MasterCard's private key.
- 6 – Card responds to terminal with decrypted hash value to prove that the card is authentic.
- 7 – If hashes match, card is authentic transaction continues. If hashes differ transaction should fail.

Offline Risk Management on the Chip

Consecutive Transaction Counter

Last Online Application Transaction Counter

Lower Consecutive Offline Counter

Upper Consecutive Offline Counter

Lower Consecutive Offline Amount

Upper Consecutive Offline Amount

PIN

PIN Try Limit

PIN Try Counter

Issuer Action Codes

Card Issuer Action Codes





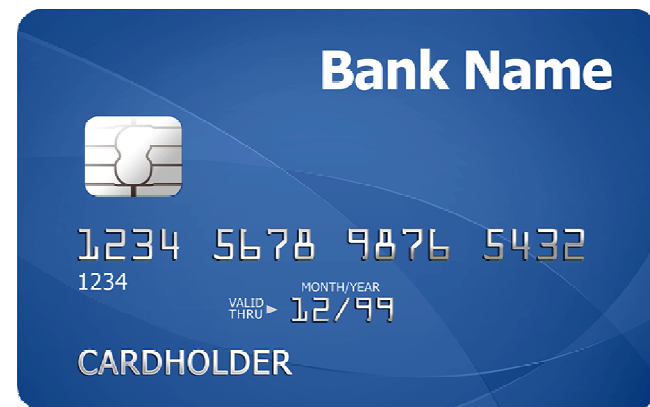
Cardholder Verification Methods



CVM Options

- No CVM
- Signature
- Online PIN at ATM
- Online PIN at POS
- Offline PIN plain-text.....
- Offline PIN enciphered





I accept:

Signature

Offline Pin

No "Online Pin"

Card CVM Priority:

P1 – Online PIN @ ATM

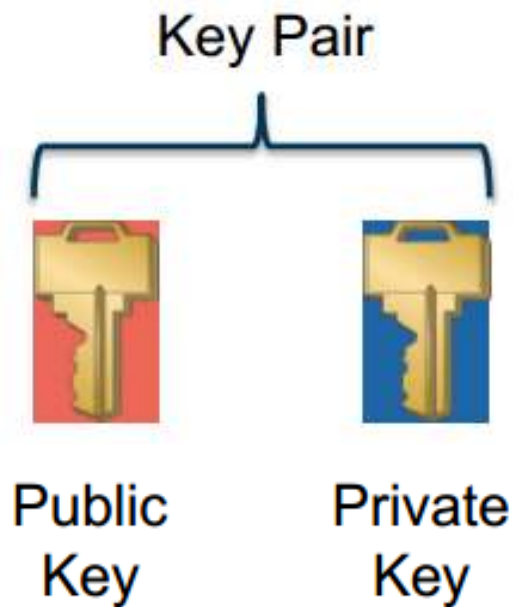
P2 – Online PIN at POS

P3 – Signature @ POS

P4 – No CVM at POS

Why Can't I Just Copy All of The EMV Chip?

The encryption keys on the card are placed in a protected area on the chip.

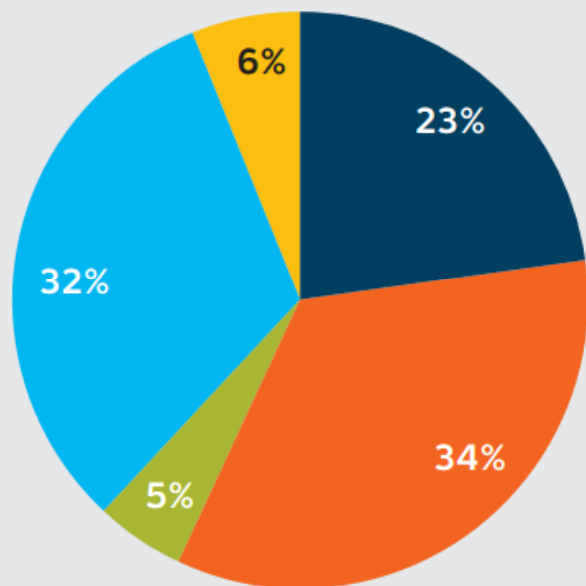


If tampering is detected, the card will self destruct.

ISSUES STILL UNRESOLVED

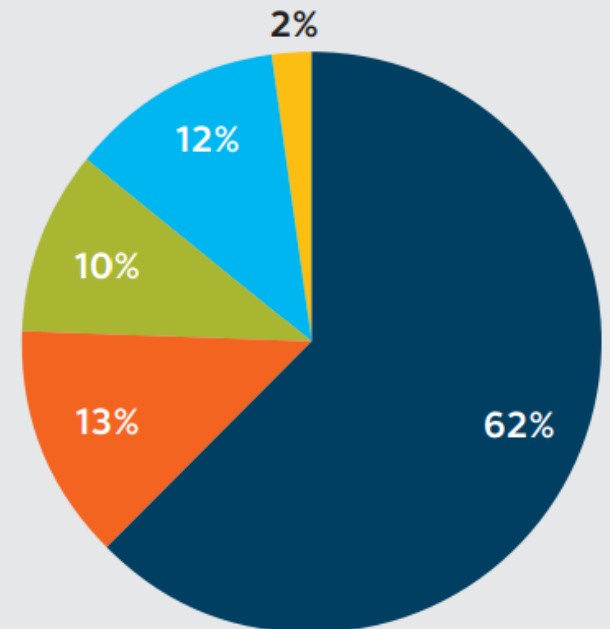
Card Fraud in The UK

2000



- Lost/stolen
- Mail non-receipt
- Card-not-present
- Counterfeit
- Card ID Theft

2010





- Data can be read off the card without entering a PIN.
- Terminals read all of the information off the card and then determine what type of CVM to use.

```
tag name
----|-----
4f Application Identifier (VISA)
5f2d Language Preference (itenfrde)
9f1f Track 1 Discretionary Data
57 Track 2 Equivalent Data
5f25 Application Effective Date
5f24 Application Expiration Date
5a Application PAN (credit card number)
8e Cardholder Verification Method (CVM) List
5f20 Cardholder Name
9f36 Application Transaction Counter (ATC)
9f17 PIN Try Counter
```

MiTM attack allows card CVM to be downgraded to plain text pin transaction

POINT-TO-POINT ENCRYPTION (P2PE) & END-TO-END ENCRYPTION (E2EE)















P2PE

- Card data is encrypted to the PCI compliant data center
- Unencrypted at data center and then routed to issuer

E2EE

- Card data is encrypted the entire way back to the issuer

“A true E2EE solution is not possible. The PAN and discretionary data must be decrypted at some point to be routed to the correct payment network and issuer.” – Smart Card Alliance

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expired	Track 1	Code	Country
<input checked="" type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	01/14	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	10/14	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	02/15	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	10/14	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	09/15	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	10/15	Yes	101	 United States WICHITA, 672
<input type="checkbox"/>	553891	 MASTERCARD	DEBIT	STANDARD	10/15	Yes	101	 United States WICHITA, 672

FUN 'FEATURES'

If a terminal fails to read a chip it will allow a mag stripe transaction to be performed.



EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 1 189 pages

Application Independent ICC to Terminal
Interface Requirements

Version 4.3
November 2011

EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 3 230 pages

Application Specification

Version 4.3
November 2011

EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 2 174 pages

Security and Key Management

Version 4.3
November 2011

EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 4 154 pages

Cardholder, Attendant, and Acquirer
Interface Requirements

Version 4.3
November 2011

Overall Thoughts



Travis Lowe
travis.ryan.lowe@gmail.com
@tloweict



Sources:

https://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions

http://www.smartcardalliance.org/resources/media/scap13_preconference/02.pdf - Fundamentals of EMV

<https://www.youtube.com/watch?v=Zv1DjtBwADg> – EMV 101: Fundamentals of EMV Chip Payment

<https://www.youtube.com/watch?v=JABJlvrZWbY> – Defcon 19: Chip & PIN is broken

<https://www.youtube.com/watch?v=qgobg1-HrfY> –A Rambling Walk Through an EMV Transaction

<http://www.emvco.com/specifications.aspx?id=223> – EMV Specification Books

http://www.creditcards.com/credit-card-news/feed_horn-scheme-curses-foiled-again-1282.php - Curses! Foiled Again!
FBI warns of tinfoil 'feed horn' scheme

<http://www.emv-connection.com/wp-content/uploads/2014/10/EMV-Tokenization-Encryption-WP-FINAL.pdf> -
Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization

<http://blog.saush.com/2006/09/08/getting-information-from-an-emv-chip-card/> - Getting Information From an EMV Chip Card With Java

<https://www.firstdata.com/emv/files/img/emv-infographic.jpg> - The ABC's of EMV