



# Fraudes em meios de pagamentos

Aqui não, queridinha!



# Janaína centini



**Fraudes em  
meios de  
pagamentos**

# Janaína centini

Pós-graduada em Cybersecurity

Certificações: eWPT, eJPT, CASE Java

Experiência de 14 anos em Cybersecutiry

Desde 2017 trabalhando como AppSec

LinkedIn /jcentini  
@yabadabada

Fraudes em  
meios de  
pagamentos





grand  
theft  
auto  
**V**

# AGENDA

Pagamentos  
Online

Cartão EMV  
(chip)

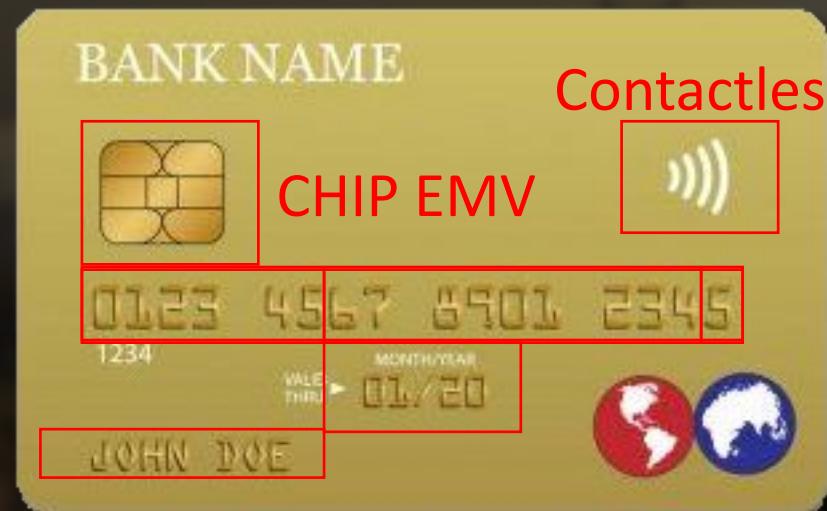


Pagamentos  
Pix

Cartão  
EMV  
(contactles  
s)

# Fraudes em Cartões EMV (Introdução)

Decifrando um cartão EMV:



BANDEIRA – Bandeira do país de emissão do cartão

Tarja Magnética



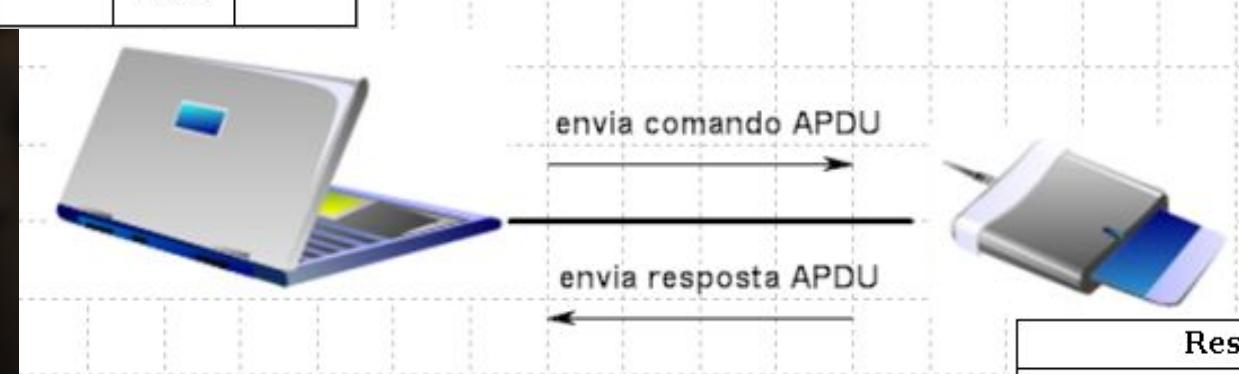
CVV – Card Verification Value

# Fraudes em Cartões EMV (Introdução)

Normas e padrões:

O protocolo APDU é o protocolo utilizado para transmissões entre cartões EMV e leitores (definido pela ISO/IEC 7816-3):

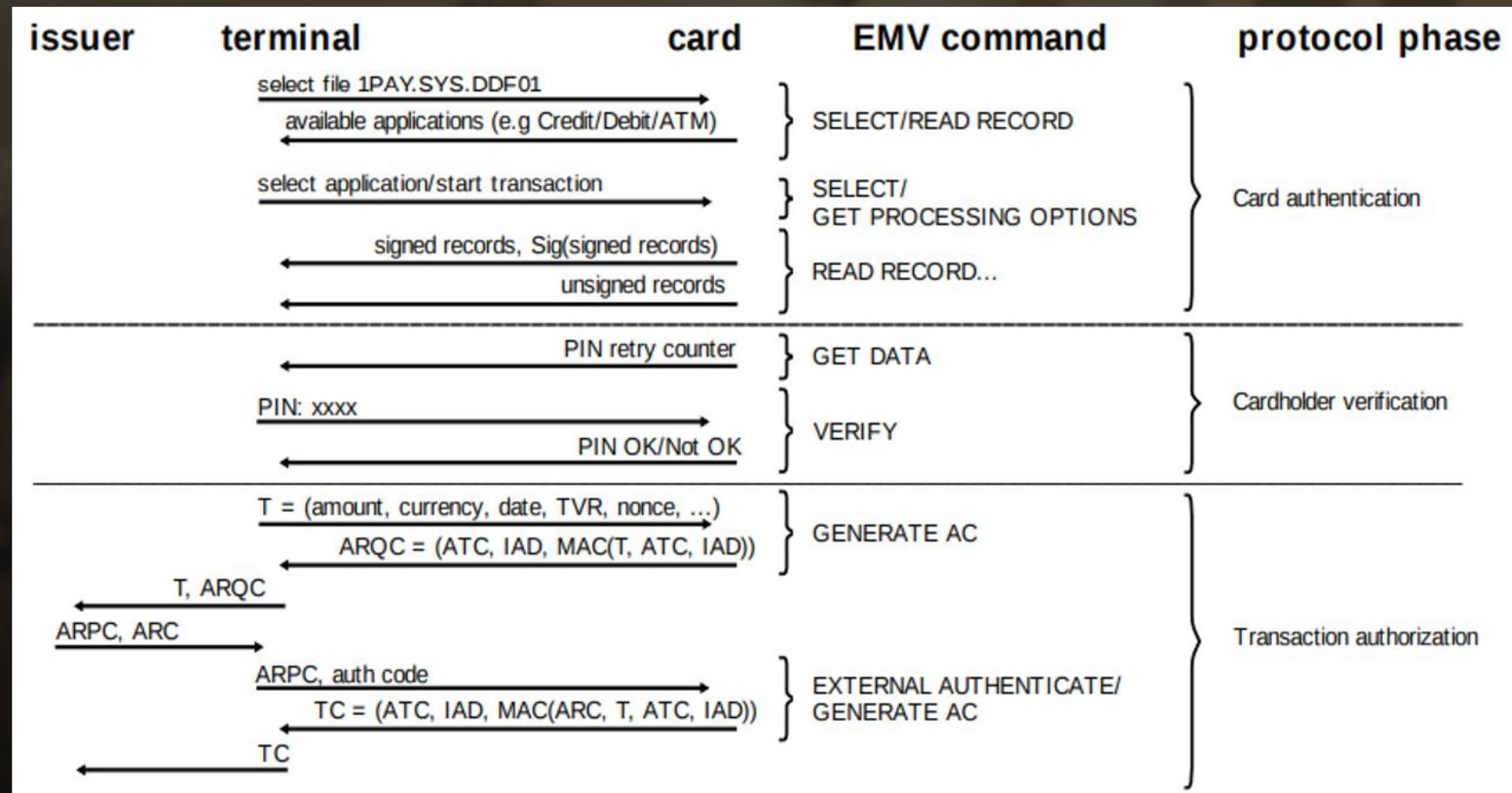
Command APDU						
Header (required)				Body (optional)		
CLA	INS	P1	P2	Lc	Data Field	Le



Response APDU		
Body (optional)	Trailer (required)	
Data Field	SW1	SW2

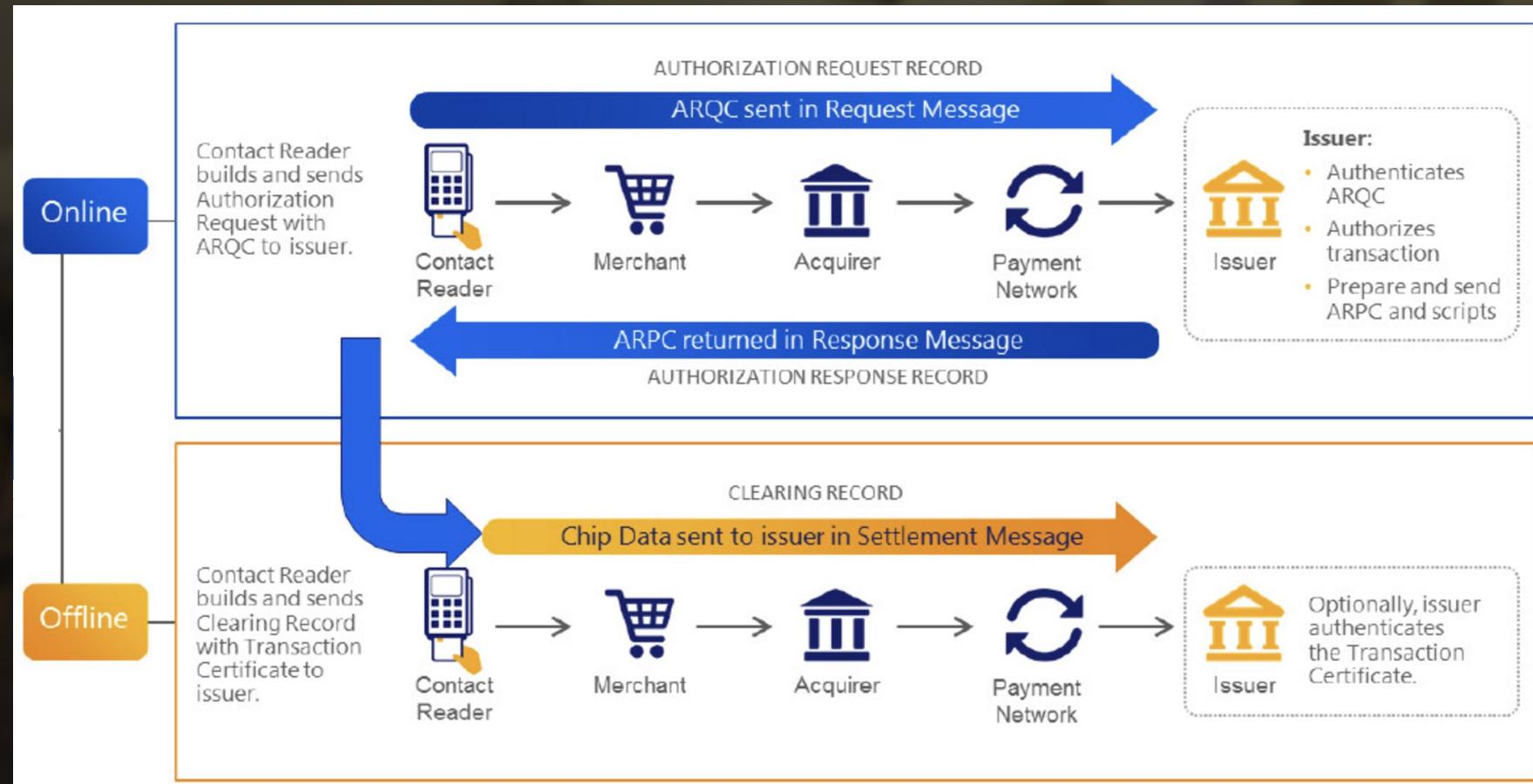
# Fraudes em Cartões EMV (pagamento presencial usando chip)

Overview de uma transação via comandos APDU:



# Fraudes em Cartões EMV (pagamento presencial usando chip)

Overview de uma transação:



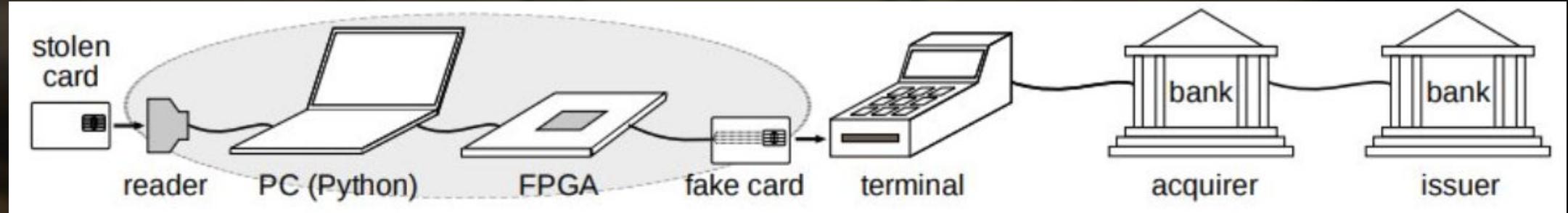
# Fraudes em Cartões EMV (pagamento presencial usando chip)

Pontos de entrada:



# Fraudes em Cartões EMV (pagamento presencial usando chip)

Ataque MiTM



# Fraudes em Cartões EMV (pagamento presencial usando chip)

Ataque MiTM – Bypass de senha

Response APDU					
Body (optional)	Trailer (required)				
Data Field	SW1	SW2			
			63 C0	W	Verify fail, no try left.
			63 C1	W	Verify fail, 1 try left.
			63 C2	W	Verify fail, 2 tries left.
			63 C3	W	Verify fail, 3 tries left.
			90 00	I	Command successfully executed (OK).
			90 04	W	PIN not successfully verified, 3 or more PIN tries left

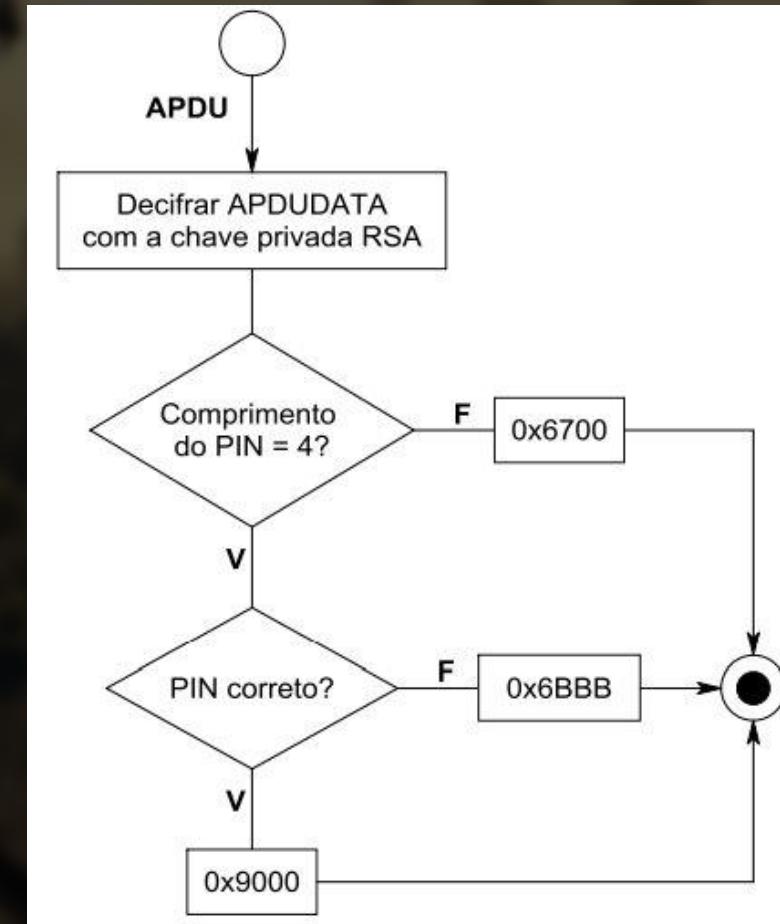
**Validação do Pin falhou**

**Pin validado com sucesso**

# Fraudes em Cartões EMV (pagamento presencial usando chip)

Ataque MiTM – Bypass de senha

```
if VERIFY_PRE and command[0:4] == "0020":  
    debug("Spoofing VERIFY response")  
    return binascii.a2b_hex("9000")
```



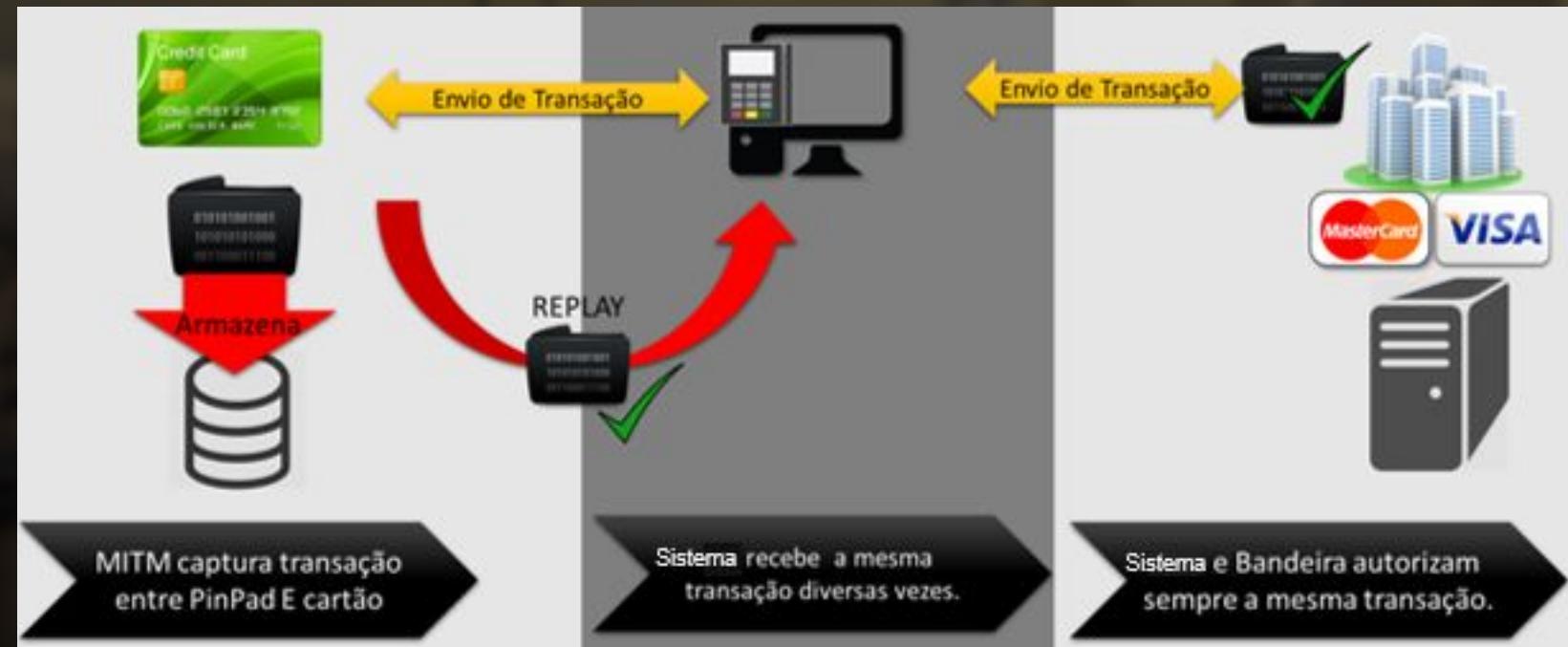
# Fraudes em Cartões EMV (pagamento presencial usando chip)

## Ataque MiTM – Bypass de senha

T → C	80 ca 9f 17 00	Get Data (PIN try counter)
C → T	9f 17 01 03 90 00	Remaining PIN tries = 3
	PIN	
T → M	00 20 00 80 08 24 00 00 <b>ffff ffff ffff</b>	Verify PIN “0000”
M → T	<b>90 00</b>	PIN correct
T → C	80 ae 80 00 1d xx xx xx xx xx xx 00 00 00 00 00 - 00 08 26 00 80 00 80 00 08 26 xx 11 09 00 xx xx - xx xx	Generate AC (ARQC)
C → T	80 12 80 xxxx xx xx xx xx xx xx xx 06 01 0a - 03 a0 00 10 90 00	ARQC
T → C	00 82 00 00 0a xx xx xx xx xx xx xx xx 30 30	External Authenticate
C → T	90 00	External authenticate successful
T → C	80 ae 40 00 1f 30 30 xx xx xx xx xx xx 00 00 00 - 00 00 00 08 26 00 80 00 80 00 08 26 xx 11 09 00 - xx xx xx xx	Generate AC (TC)
C → T	80 12 40 xxxx xx xx xx xx xx xx xx xx 06 01 0a - 03 60 00 10 90 00	TC

# Fraudes em Cartões EMV (pagamento presencial usando chip)

## Ataque MiTM – Replay



# Fraudes em Cartões EMV (pagamento presencial usando chip)

## Transação Original

```
<ID>37</ID>
<APDU>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 00 00 00 00 00 00 00 09 86 16 01 12
00 52 32 47 12 14 4B 75 00 00 00</APDU>
<CARD>61 2B</CARD>
</HANDSHAKE>
<HANDSHAKE>
<ID>38</ID>
<APDU>00 C0 00 00 2B</APDU>
<CARD>C0 77 29 9F 27 01 80 9F 36 02 00 25 9F 26 08 AE 36 62 1C 23 B0 90 76 9F
10 12 01 14 A0 00 03 22 00 00 4B 75 00 00 00 00 00 00 FF 90 00</CARD>
```

## Transação Clonada

```
<ID>37</ID>
<APDU>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 00 00 00 00 00 00 00 09 86 16 01 12
00 52 32 47 12 14 4B 75 00 00 00</APDU>
<CARD>61 2B</CARD>
</HANDSHAKE>
<HANDSHAKE>
<ID>38</ID>
<APDU>00 C0 00 00 2B</APDU>
<CARD>C0 77 29 9F 27 01 80 9F 36 02 00 26 9F 26 08 C4 25 B2 AE 85 AD E6 26 9F
10 12 01 14 A0 00 03 22 00 00 4B 75 00 00 00 00 00 00 FF 90 00</CARD>
<CARD-X>C0 77 29 9F 27 01 80 9F 36 02 00 25 9F 26 08 AE 36 62 1C 23 B0 90 76 9F
10 12 01 14 A0 00 03 22 00 00 4B 75 00 00 00 00 00 00 FF 90 00</CARD-X>
```

# Fraudes em Cartões EMV (pagamento presencial usando chip)

## Ataque MiTM – Replay

Transação Original

REDE DE AGENCIAS  
RECIBO DE  
SAQUE COM CARTAO EM CONTA CORRENTE  
12/01/2016 12:08:46 DATA CONTABIL:12/01/2016  
LOCAL:  
TRANSAÇÃO: 0000011 TERMINAL: 0000001  
JULIANA MARTINS CARTAO: 2672  
BANCO: AGENCIA: 0720 CONTA: 1  
  
VALOR DO SAQUE 1,00  
  
SBR 1330 001 12012016 0002 1,00P 2001

Transação Clonada/Replay

REDE DE AGENCIAS  
RECIBO DE  
SAQUE COM CARTAO EM CONTA CORRENTE  
12/01/2016 12:18:41 DATA CONTABIL:12/01/2016  
LOCAL:  
TRANSAÇÃO: 0000013 TERMINAL: 0000001  
JULIANA MARTINS CARTAO: 2672  
BANCO: AGENCIA: 0720 CONTA: 1  
  
VALOR DO SAQUE 1,00  
  
SBR 1330 001 12012016 0003 1,00P 2001

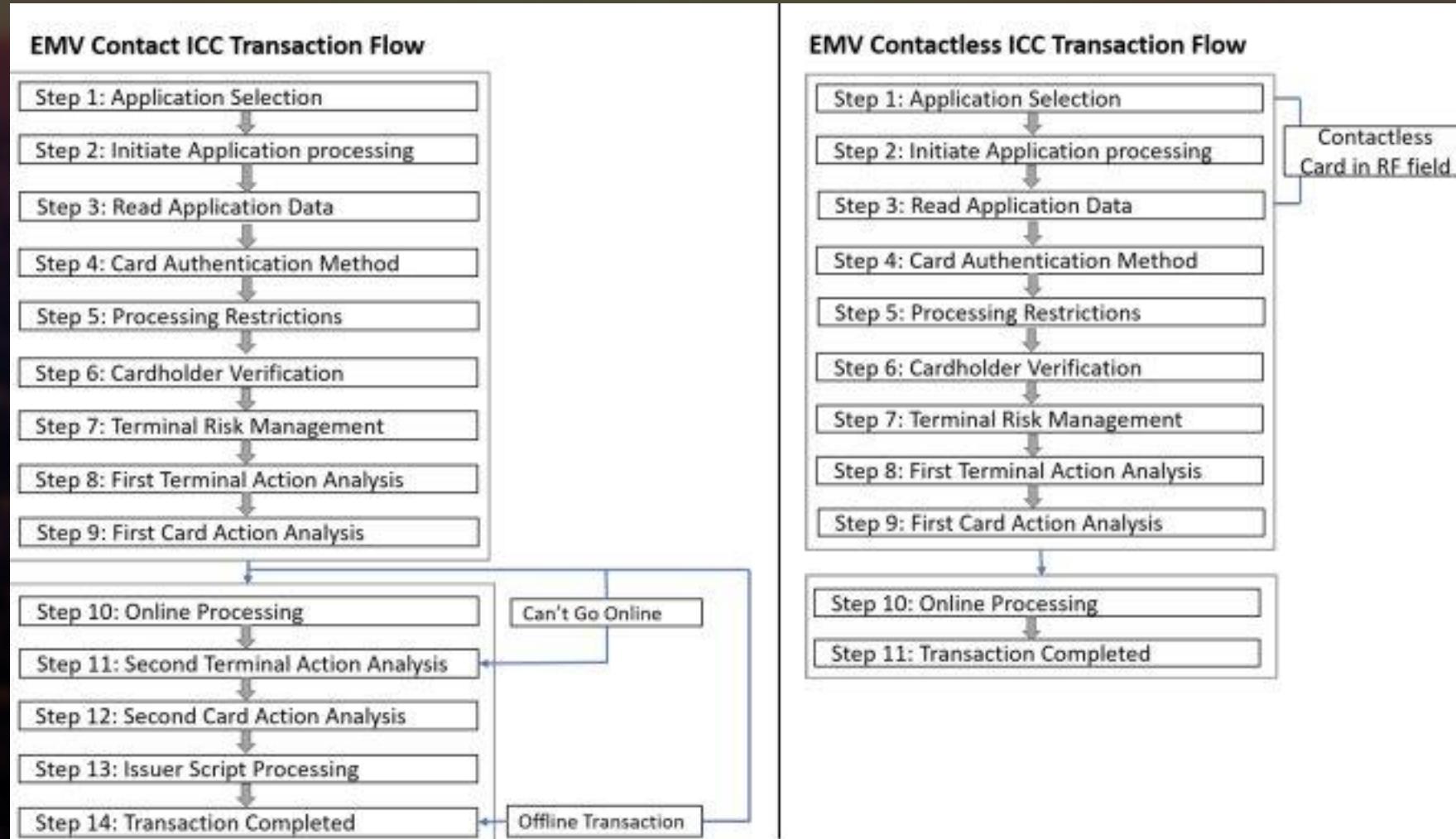
# Fraudes em Cartões EMV (pagamento presencial usando chip)

Mitigação:

- Evitar pagamentos em modo offline
- Efetuar a validação do criptograma e outros elementos do cartão
- Não utilizar chip SDA
- Se possível optar pelo conceito NO-ODA (No Offline Data Authentication)

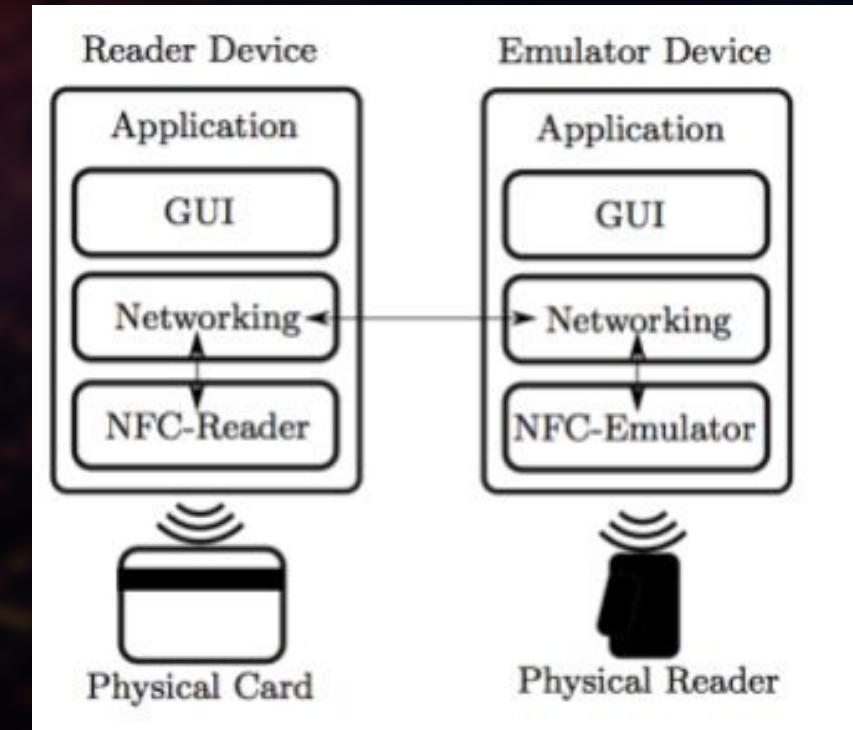
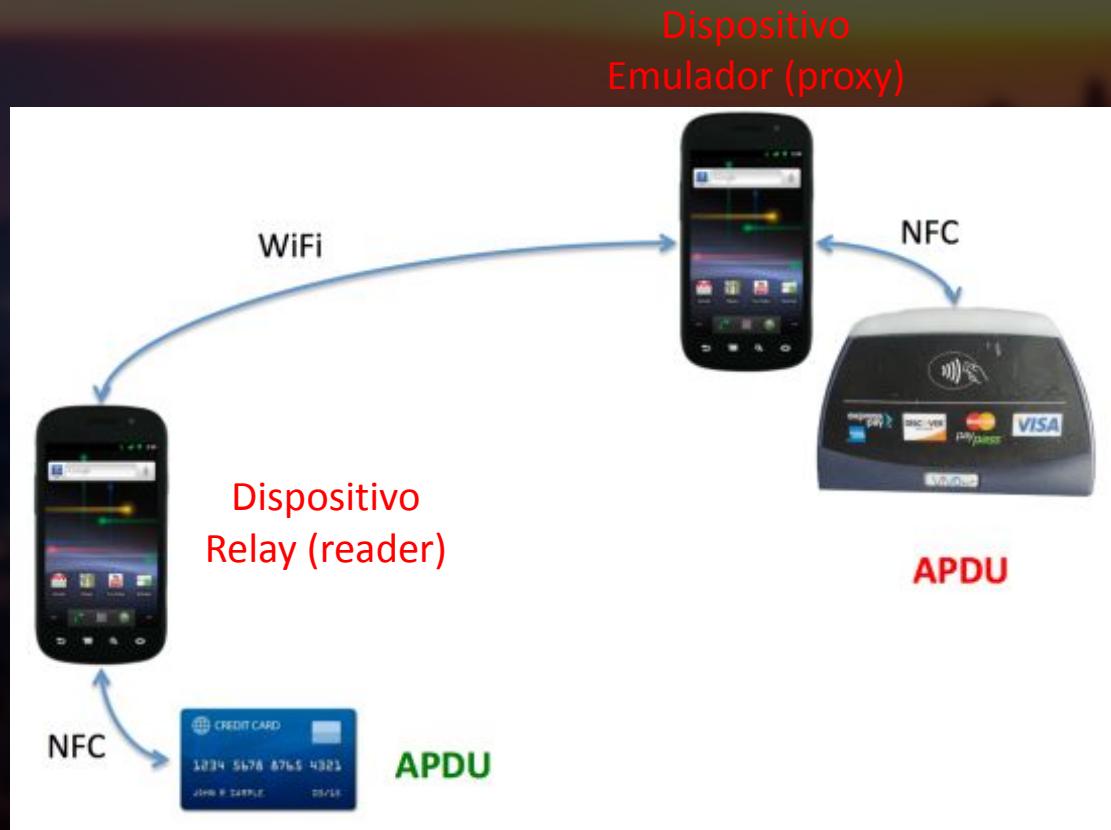
# Fraudes em Cartões EMV (pagamento presencial contactless)

Overview de uma transação:



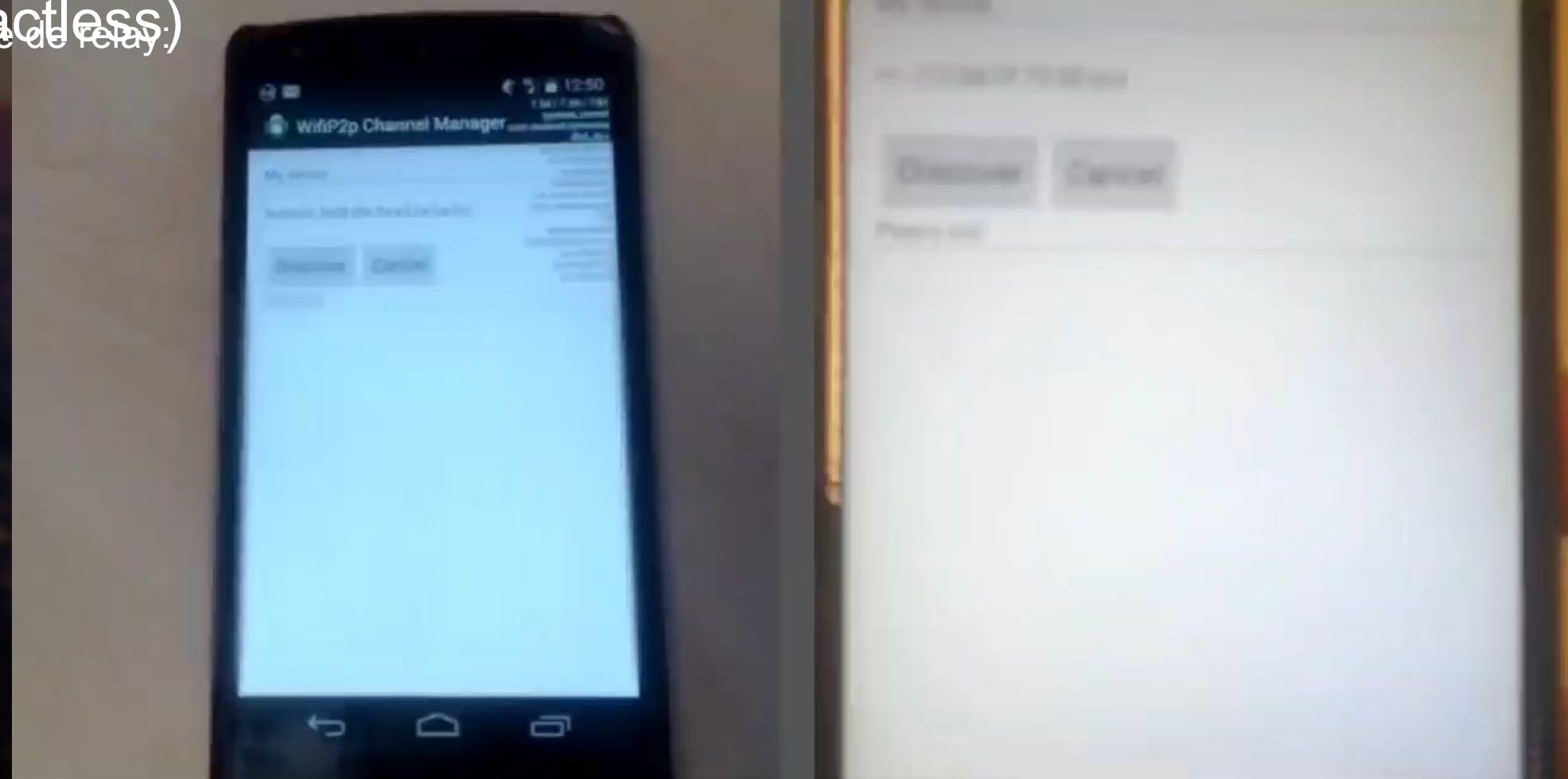
# Fraudes em Cartões EMV (pagamento presencial contactless)

Ataque de relay



# Fraudes em Cartões EMV (pagamento presencial contactless)

Ataque de relay



Mole

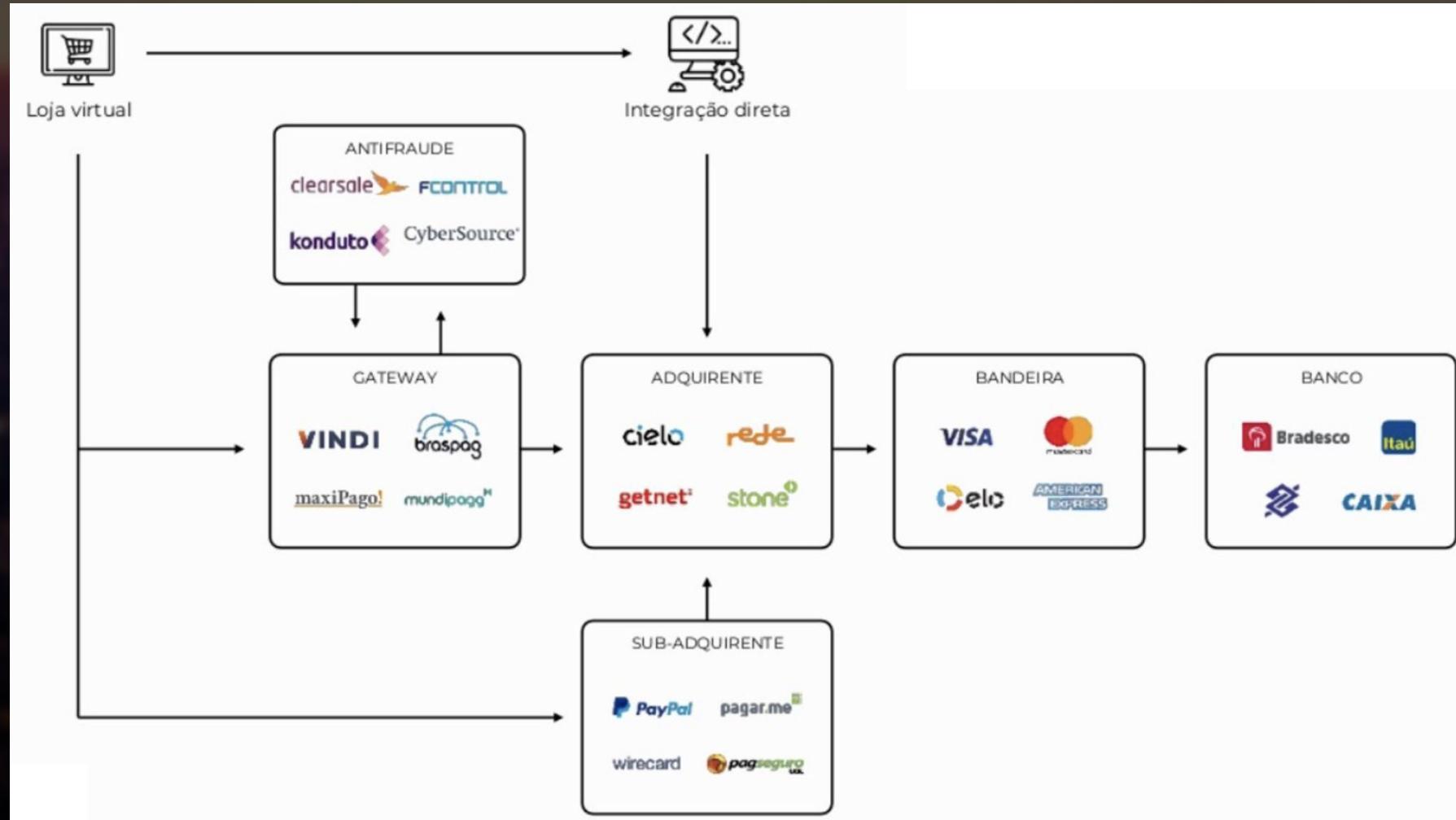
Proxy

# Fraudes em Cartões EMV (pagamento presencial contactless)

Mitigação:

- Implementar limites ao montante que pode ser gasto em uma única transação contactless
- Utilizar métodos de autenticação adicionais, como a exigência de PIN para determinadas transações ou a implementação de autenticação biométrica no caso de dispositivos móveis
- Empregar elementos seguros em cartões e dispositivos de pagamento para armazenar informações sensíveis e impedir o acesso não autorizado
- Utilizar tokenização para substituir os dados do cartão por tokens para cada transação, minimizando o risco de utilização indevida de dados interceptados

# Fraudes em Cartões EMV (Pagamentos Online)



# Fraudes em Cartões EMV (Pagamentos Online)

Validação dos dados do cartão:

Possíveis pontos de falha:

- Validar somente o PAN
- Não limitar quantidade de tentativas para o CVV
- Não efetuar sanitização e validação de inputs
- Ausência de validação semântica e sintática do código

**CARTÃO DE CRÉDITO**

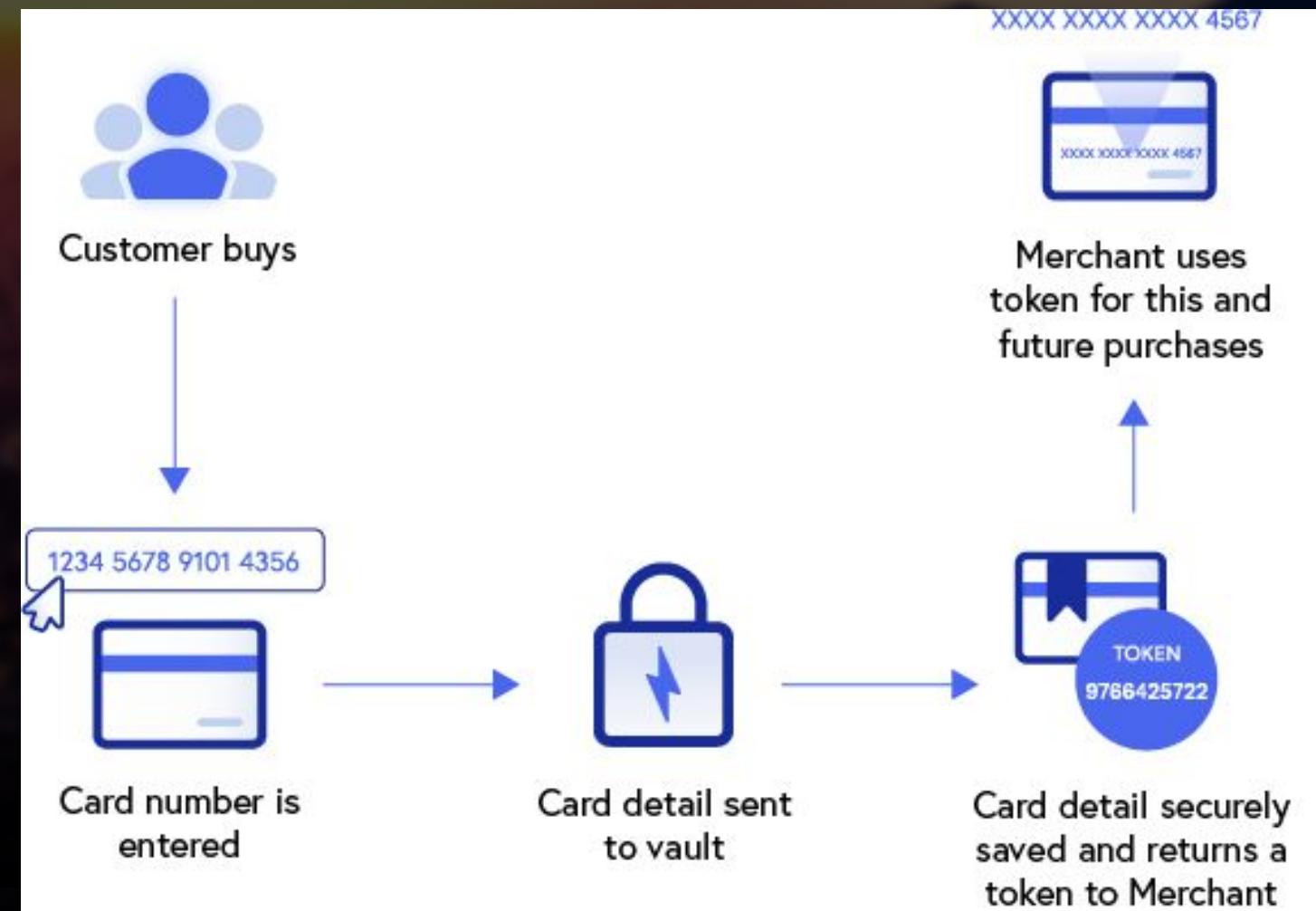
The screenshot shows a payment form for a credit card. On the left, there's a placeholder image of a credit card with a redacted number and a placeholder name. To its right, the card details are shown: 'Número do cartão \*' (Number), 'Nome impresso no cartão \*' (Name on card), 'Valido até .../...' (Valid until), and a checkbox for 'Este é meu cartão padrão' (This is my default card). Below these are fields for 'Validade \*' (Expiration date) and 'Código de verificação \*' (CVV). Further down are fields for 'Apelido para este cartão \*' (Nickname), 'CPF/CNPJ do titular \*' (Holder's CPF/CNPJ), 'Data de nascimento \* - dd/mm/aaaa' (Holder's birthday), and 'Forma de pagamento \*' (Payment method) which lists '1x sem juros - Até 10% de desconto - R\$ 404,22'. Three red arrows point to the 'Validade \*' field, the 'Código de verificação \*' field, and the 'Forma de pagamento \*' dropdown.

# Fraudes em Cartões EMV (Pagamentos Online)

Card tokenization:

Possíveis pontos de falha:

- Possível enumerar cards Ids
- IDOR por falha no controle de acesso
- Possibilidades de utilização de Card Ids cancelados
- Exposição de card Id na URL
- Replay de transação



# Fraudes em Cartões EMV (Pagamentos Online)

Mensageria (ISO8583):

## Fraude do Estorno em Duplicidade:

1. É efetuada uma compra no cartão de crédito VISA
2. Em seguida o usuário solicita estorno da compra
3. É enviado via mensageria um **TC06** ao invés de **TC25** para cancelamento na VISA
4. O estorno é feito e é efetuado crédito imediato na conta (voucher)
5. O gateway de pagamento efetua os ajustes de crédito em D+2
6. O ajuste identifica o pedido de cancelamento e efetua um novo estorno

TRANSACTION TYPE	ID	VISA
Purchase	TC05	TC05
Credit Voucher	TC06	TC06
Funds Return	TC06	TC25

# Fraudes no Pix

## Chave Pix:

00020101021226860014BR.GOV.BCB.PIX2564pix.hubfintech.com.br/qr/v2/9c498a55-8634-40ad-9250-1265d27c41895204000052020865802BR5025Kabum Comercio Eletronico6000See

ID	Nome BR Code	Tam	Valor			
00	Payload Format Indicator	02	01			
26	Merchant Account Information	86	ID	Nome	Tam	Valor
			00	GUI	14	BR.GOV.BCB.PIX
			25	chave	64	pix.hubfintech.com.br/qr/v2/9c498a55-8634-40ad-9250-1265d27c4189
52	Merchant Category Code	04	0000			
53	Transaction Currency	03	986			
58	Country Code	02	BR			
59	Merchant Name	25	KABUM COMERCIO ELETRONICO			
60	Merchant City	09	Sao Paulo			
62	Additional Data Field Template	07	ID	Nome	Tam	Valor
			05	txid	03	***
63	CRC16	04	1833			

# Fraudes no Pix/Boleto

Fraude do pagamento parcial:

1. É lançada uma solicitação para pagamento (via Pix ou boleto) e é gerado um código para faturar (no total de, por exemplo, R\$ 1.000,00)
2. O valor total é alterado para, por exemplo, R\$ 0,01
3. É efetuado o pagamento do valor parcial da fatura de R\$ 0,01
4. A plataforma valida se houve o pagamento ou não
5. O pagamento da fatura é confirmado sem levar em consideração o valor pago, validando apenas o status do pagamento
6. A fatura é fechada como pago no valor total de R\$ 1.000,00

# Referências

- <https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf>
- [https://www.emvco.com/wp-content/uploads/2017/05/A\\_Guide\\_to\\_EMV\\_Chip\\_Technology\\_v2.0\\_20141120122132753.pdf](https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf)
- <https://www.openscdp.org/scripts/tutorial/emv/applicationselection.html>
- <https://www.blackhat.com/presentations/bh-dc-08/Laurie/Presentation/bh-dc-08-laurie.pdf>
- [https://www.emvco.com/wp-content/uploads/2017/05/A\\_Guide\\_to\\_EMV\\_Chip\\_Technology\\_v2.0\\_20141120122132753.pdf](https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf)
- [https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento\\_Pix/II\\_ManualdePadroesparaIniciacaodoPix.pdf](https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/II_ManualdePadroesparaIniciacaodoPix.pdf)
- <https://salmg.net/2017/09/12/intro-to-analyze-nfc-contactless-cards/>
- <https://www.linkedin.com/pulse/cards-payments-101-everything-emv-binoy-baby/>
- <https://salmg.net/2017/09/12/intro-to-analyze-nfc-contactless-cards/>
- [https://www.youtube.com/watch?v=gzR1Rmyjzxw&ab\\_channel=USENIX](https://www.youtube.com/watch?v=gzR1Rmyjzxw&ab_channel=USENIX)





Troféu conquistado  
Apresentação realizada

**MISSÃO  
CONCLUÍDA**

