Some things about skimming and superficiality

I2DS2
INTEGRATED INTELLIGENCE, DEFENCE AND SECURITY SOLUTIONS
A TID`s Idea and Innovation Platform

Mircea Constantin Șcheau


32 Countries
Over 458 million people
Austria
Belgium
Bulgaria
Cyprus
Czech Rep.
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
Monaco
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United Kingdom


CT/DD SEPA Migration
Aug, 2014/ Oct '16
EU MIF Regulation
Dec 2015/ June 2016
PSD 2.0
2017/18
ECB Security of Internet Payments
Aug 2015
Single European Payments Area?

Skimming devices improve continuously: smaller, quicker → entirely hidden

Old technology

Better camouflage

Smaller

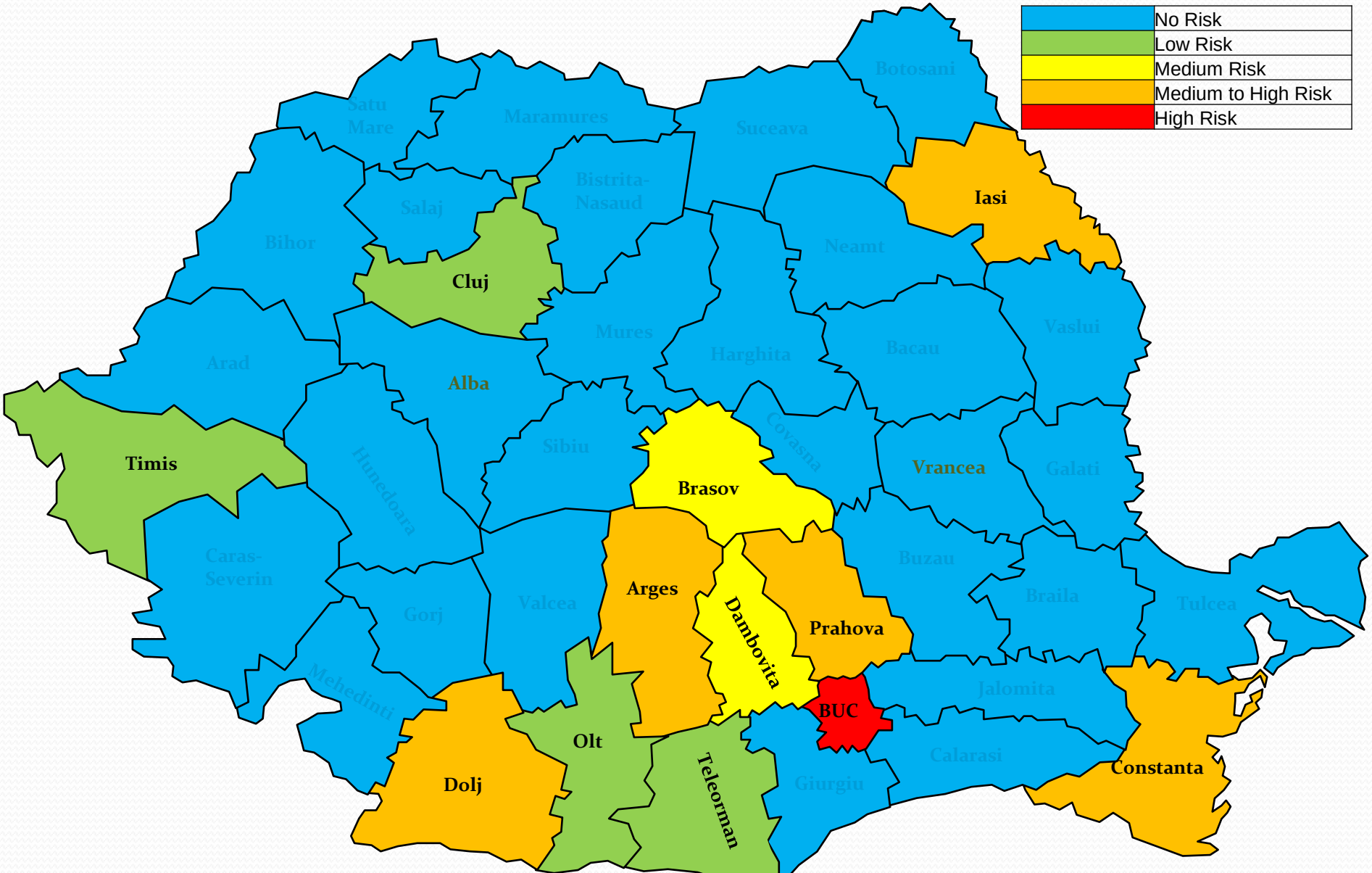
New technology

Video surveillance

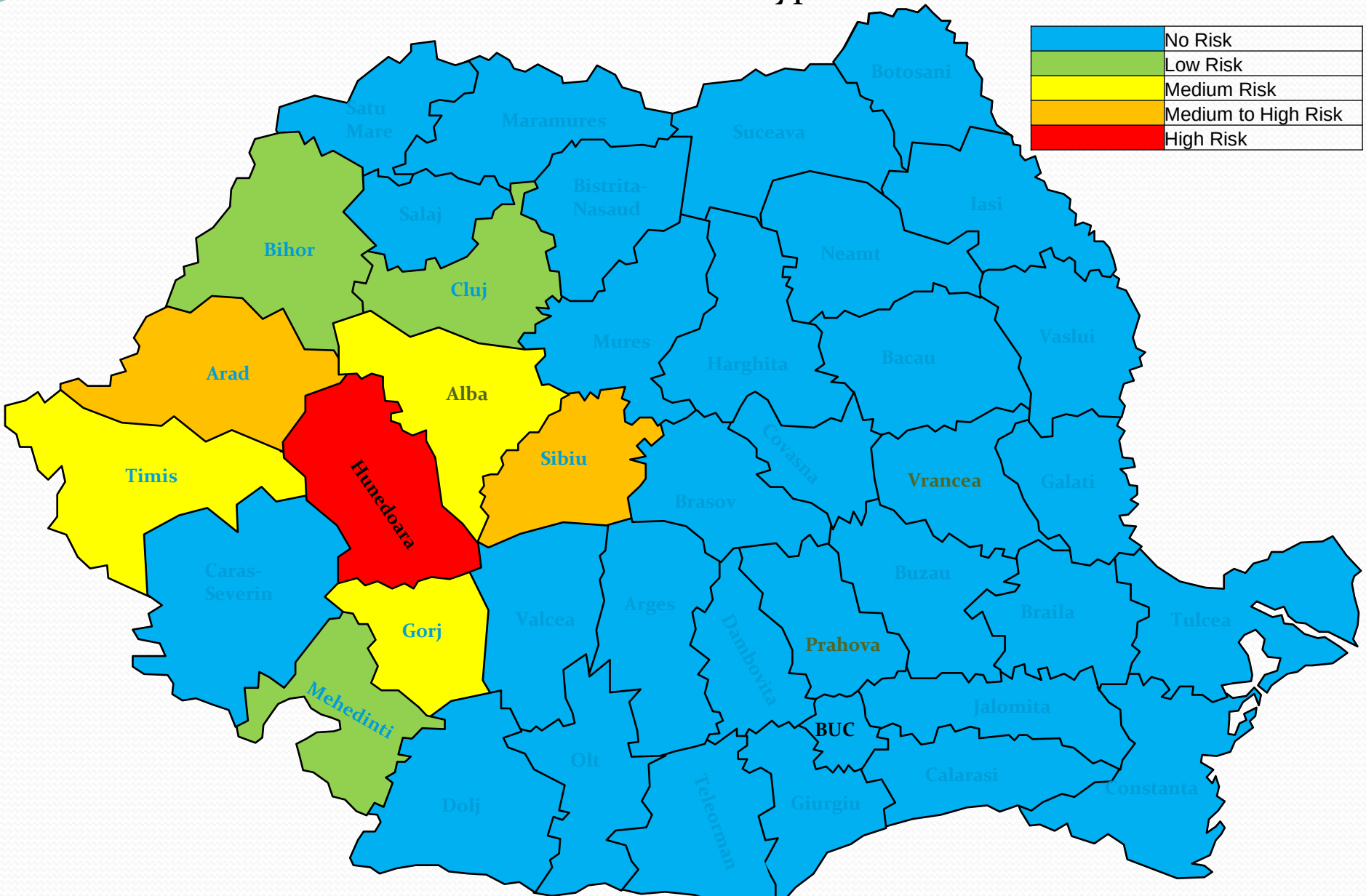

Modele de dispozitive
Vizibile cu memorie
INTRODUCEȚI
CARDUL
Modele montate
În interiorul ATM-ului
Eavesdropping
Modele de dispozitive
Cu transmitere wireless
Tastaturi false
Camere de filmat disim
21/01/2003
21/01/2003

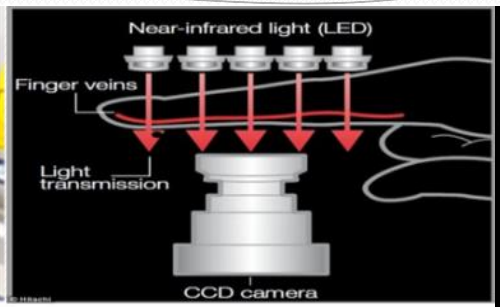
“Fork”

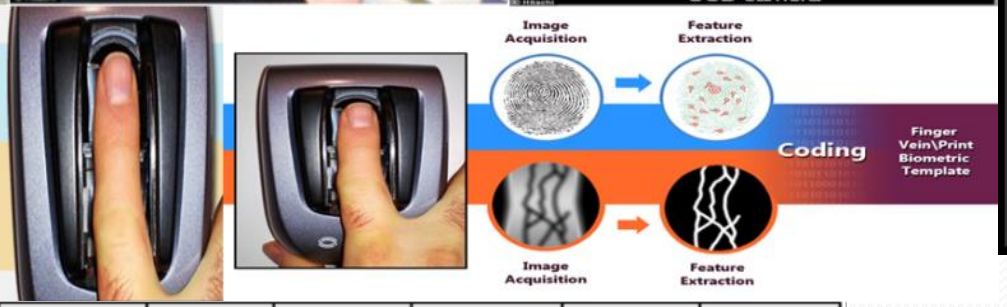
Distribution of skimming cases



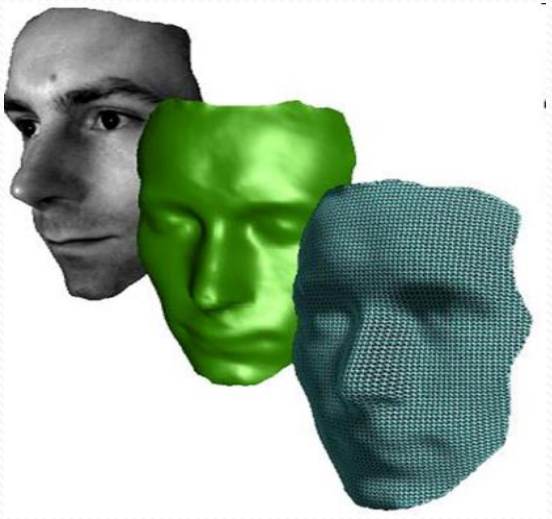
Distribution of "fork" type attacks







Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H



Logo-ul băncii emitente

CHIP

VISA Logo

Hologramă

Număr card

Nume şi prenume deţinător card

Nume card

Data expirării

Hologramă

Număr card

Nume card

Data expirării

Ultraviolet

MasterCard Logo

Banda magnetică

Panel de semnătură

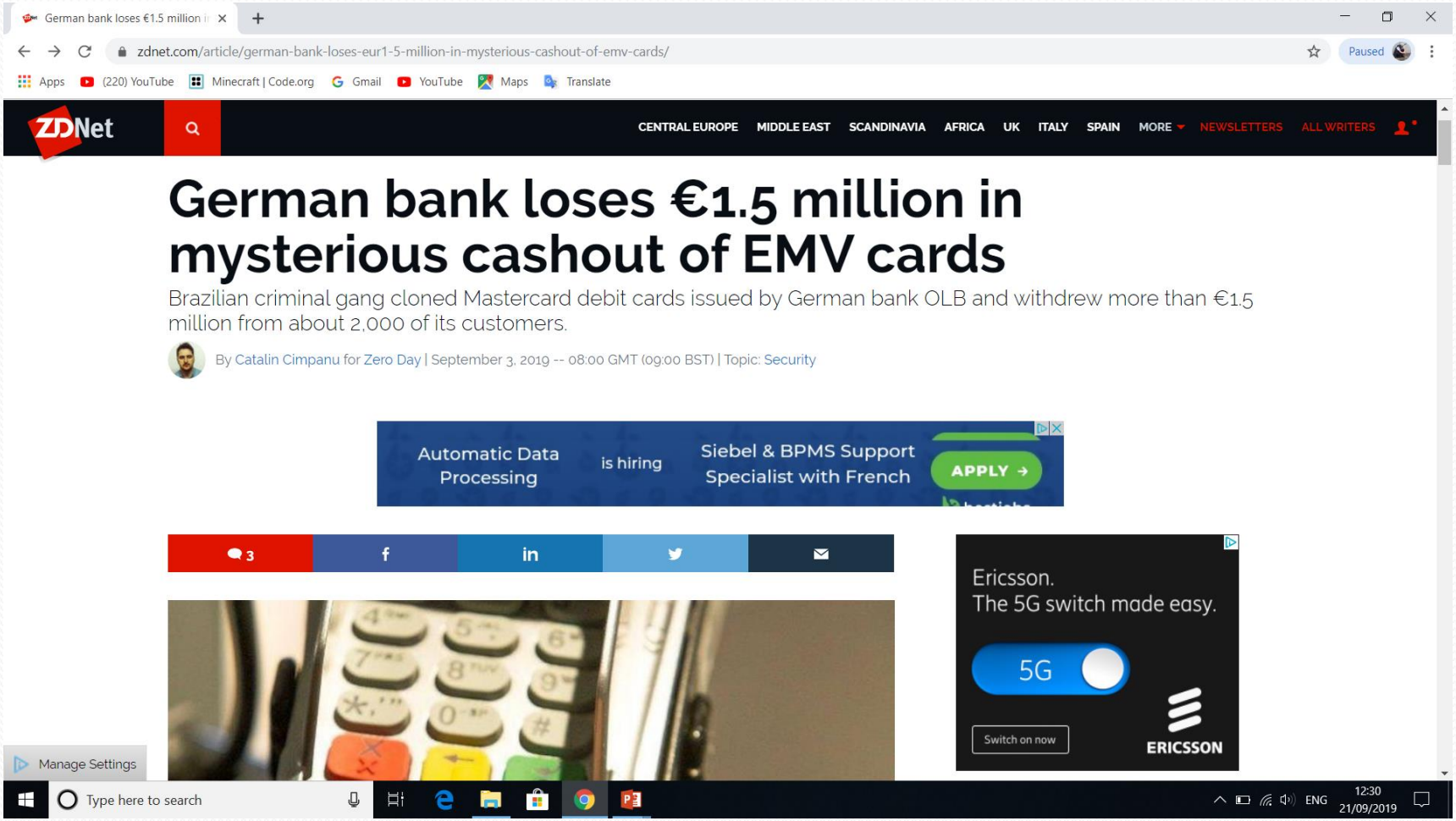
CHIP

Număr CVV2

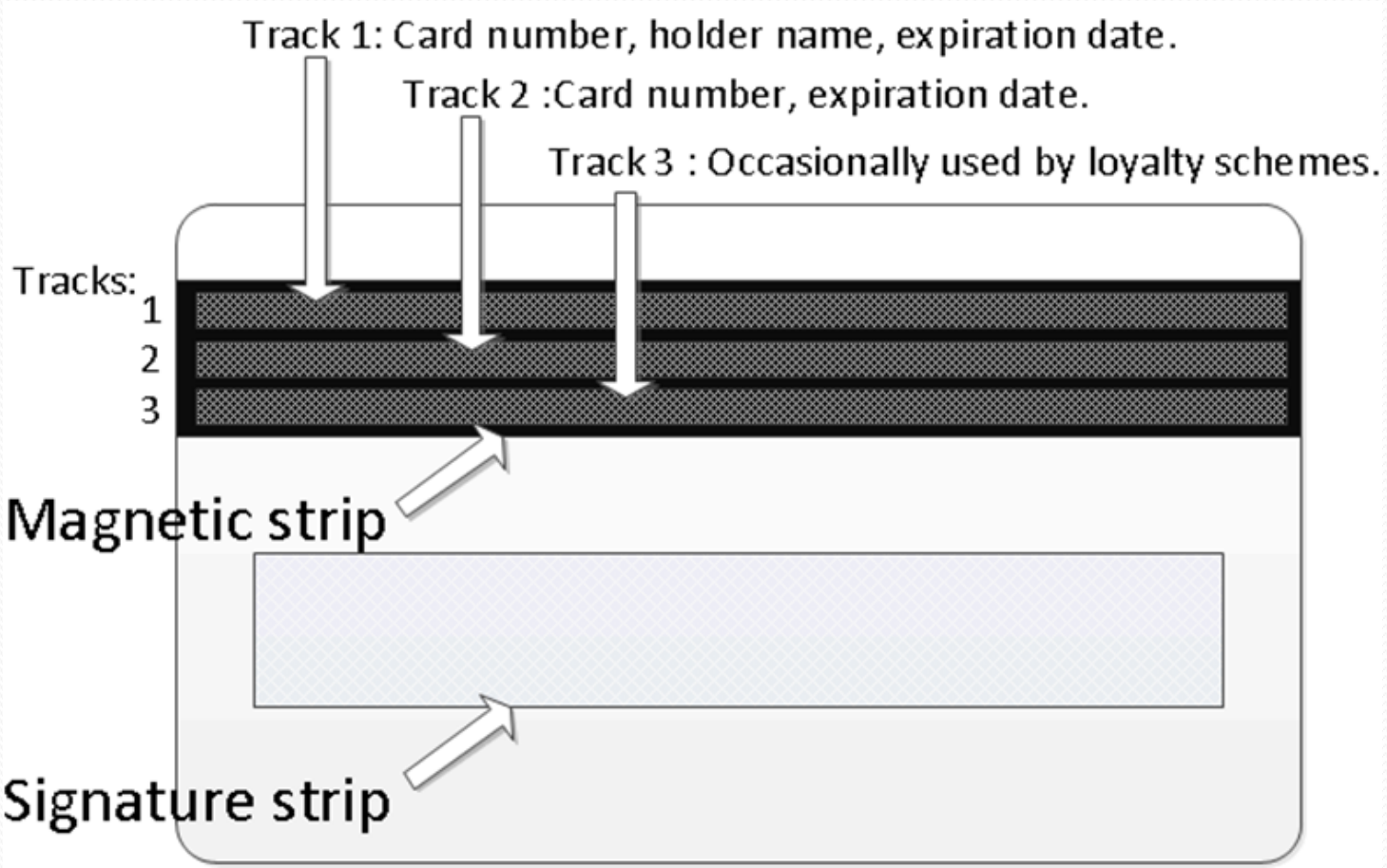
Informaţii de contact pentru carduri pierdute/furate

Ultimele 4 cifre din numărul de card

Card Authorisation



Card Authorisation



Card Authorisation

Track 1: the cardholder name, account number (PAN), expiration date, Service Code, and several other numbers the issuing bank uses to validate the data received. It looks like this:

%B4101990527219 1^LENIK/GRAYSON
^19122011440113577454684434600001 1?

^ “Nope, not real data :)”

Track 2: all of the above except the cardholder name. Most credit card payment systems use Track 2 to process transactions. It’s all a counterfeiter needs to produce a fake card.

Track 2 looks like this:

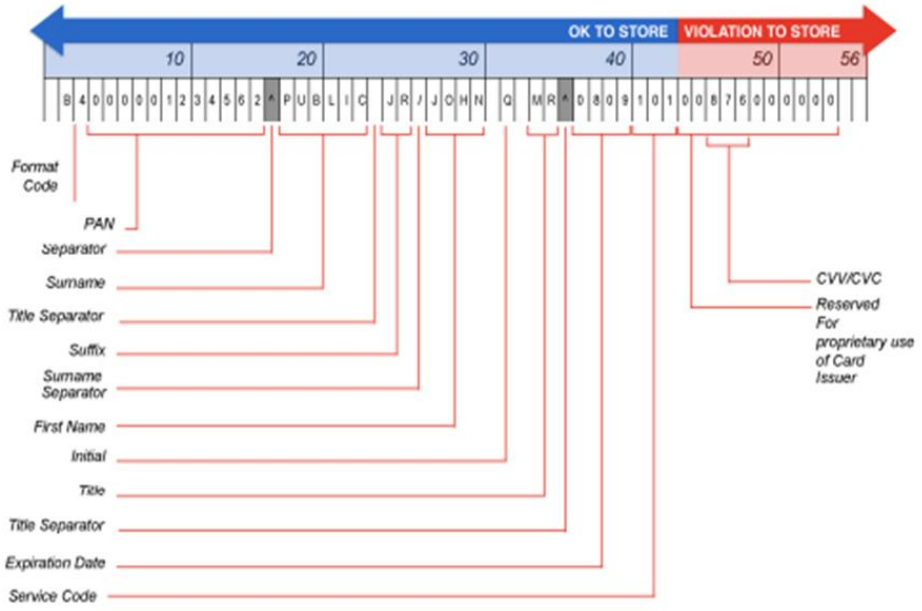
;4101990523272191=19122011440114600011?

^ “Surprise! Also not real”

Card Authorisation

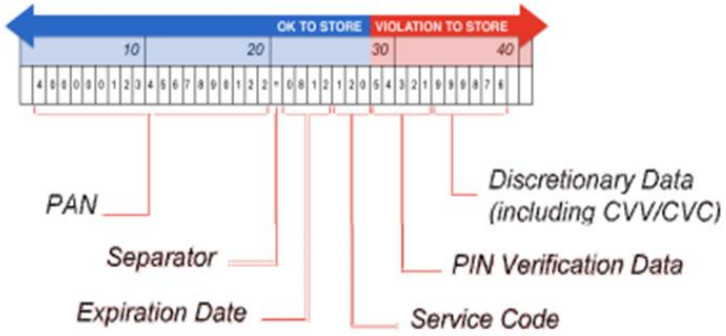
Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters

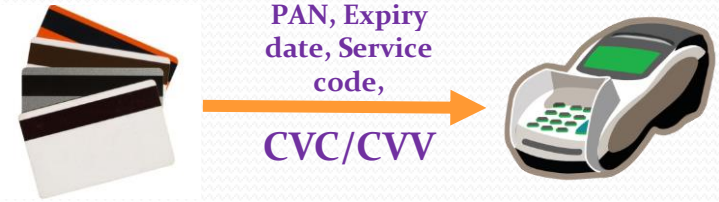


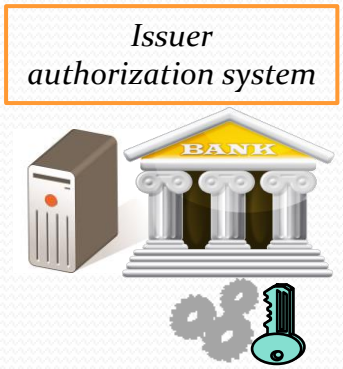
Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters



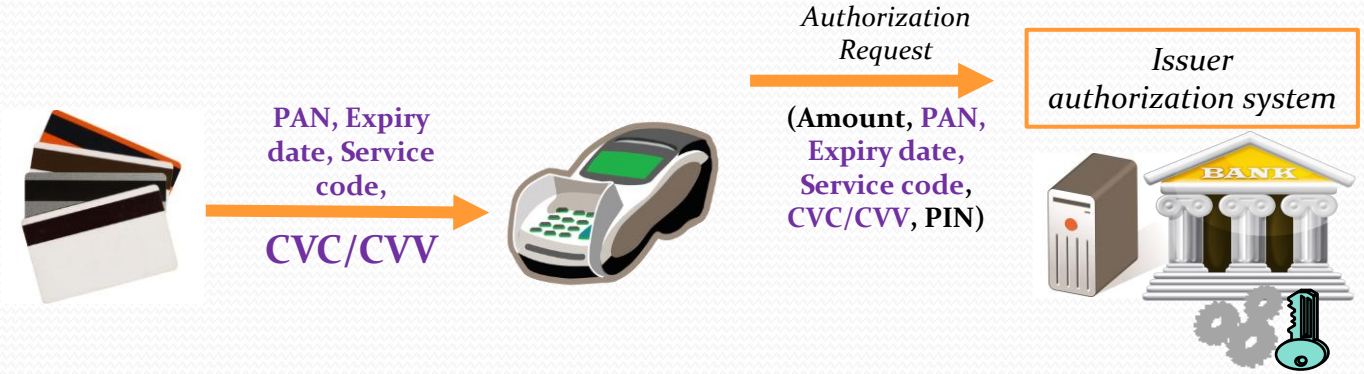
Card Authorisation





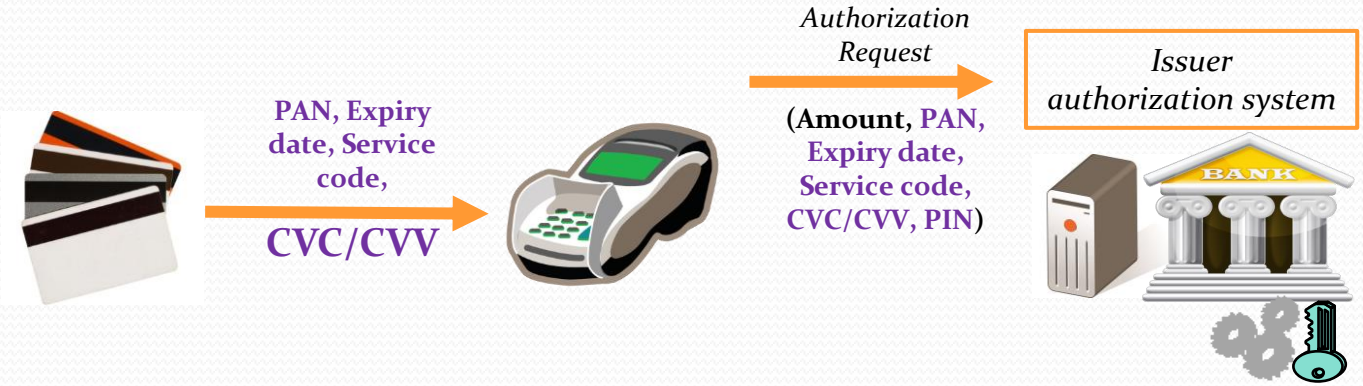
- Magstripe data is read by the POS
- The data is STATIC: identical for each transaction
- CVC/CVV is the encryption of (PAN, Expiry date, Service Code) using a key specific to that card. This key can be retrieved by the issuer authorization system.

Card Authorisation



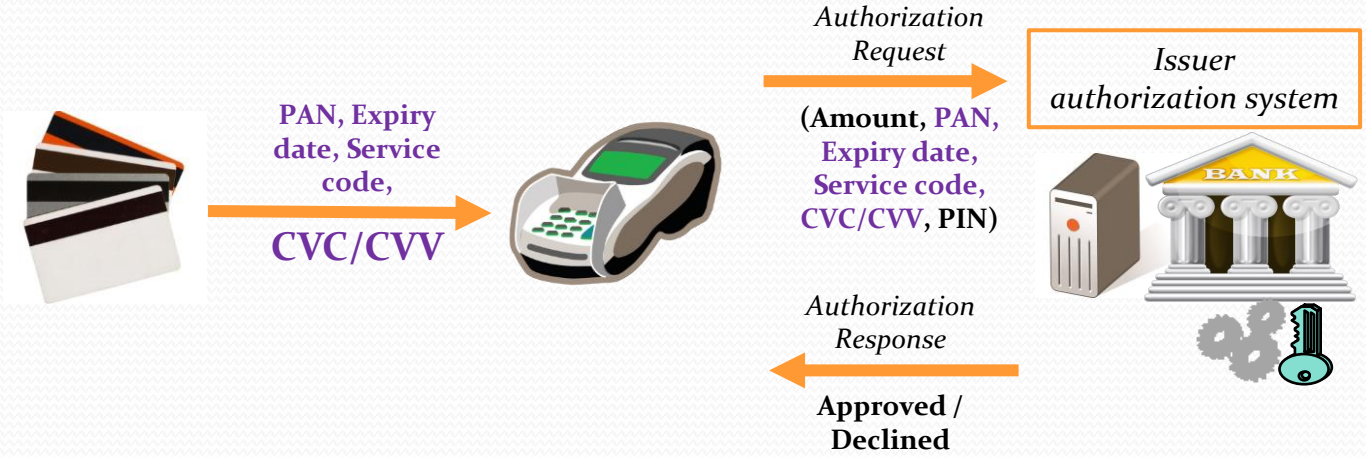
- The POS computes the authorization request and sends it to the issuer authorization system

Card Authorisation



- The authorization system performs risk management
- It also checks the validity of the CVC/CVV by recalculating it using:
  - the (PAN, Expiry date, Service code) transmitted in the authorization request
  - the secret key associated to that card.
- If the CVC/CVV is validated, the card is considered genuine

Card Authorisation



- The authorization response is sent back to the POS.

Card Authorisation

Magstripe cards are easy to clone

Card authentication is based on STATIC data

→ Cloned cards will be considered authentic, since they carry the same data as real cards

TT	RC	CARD	TID	MID	DATA	ORA	ENTI	MCC	TERMINALLOCATION	SUMA	CURR	SERV
21	55	517045******9970	WR870881	074669320	1180822	2116	90	5411	DIST A POPULAR BETIM BRA	1.68	986	1**
21	56	517045******9996	CW028402	030346835	1180822	2116	90	5912	DROGARIA NOVA VALQUEIR RIO DE JANEIR BRA	1.59	986	1**
21	20	517045******9954	WY551036	013358952	1180822	2116	90	5422	CASA DE CARNES 3 MENIN BELO HORIZONT BRA	1.1	986	1**
21	20	517045******9988	IT263466	021061327	1180822	2116	90	5533	REI DO OLEO SAO PAULO BRA	1.83	986	1**
21	20	517045******9947	WW226696	039678660	1180822	2116	90	5691	ROCK SEDA SAO JOSE DOS BRA	1.18	986	1**
21	56	517045******9905	WY776420	021695652	1180822	2116	90	5411	MERCEAR MANTIPAR LTDA CONTAGEM BRA	1.21	986	1**
21	56	517045******9897	WY662668	076625079	1180822	2116	90	4812	AGR TELECOM BELO HORIZONT BRA	1.49	986	1**
21	55	517045******9939	WW336712	029477700	1180822	2116	90	5411	CASA BERTI SAO PAULO BRA	1.96	986	1**
21	20	517045******9921	WW228282	071493484	1180822	2116	90	5300	DECISAO ATACAREJO BELO HORIZONT BRA	1.81	986	1**
21	56	517045******9962	WW010825	055093973	1180822	2116	90	5921	R3 DISTRIBUIDORA BELO HORIZONT BRA	1.13	986	1**
21	20	517045******9889	WY126523	011656573	1180822	2116	90	5422	FRIGOLIM LTDA BELO HORIZONT BRA	1.45	986	1**
21	20	517045******9871	WW216079	066136105	1180822	2116	90	5661	M ESPACO CHIRA COMERCI TAUBATE BRA	1.64	986	1**
21	20	517045******9913	CW030286	008220379	1180822	2116	90	5661	AUTHENTIC FEET C NORTE SAO PAULO BRA	1.45	986	1**
21	41	468918******9897	WY662668	076625079	1180822	42801	90	4812	AGR TELECOM BELO HORIZONTBR	2	986	
21	41	468918******9988	IT263466	021061327	1180822	42801	90	5533	REI DO OLEO SAO PAULO BR	1.86	986	
21	41	468918******9871	WW216079	066136105	1180822	42802	90	5661	M ESPACO CHIRA COMERCIO TAUBATE BR	1.8	986	
21	41	468918******9962	WW010825	055093973	1180822	42802	90	5921	R3 DISTRIBUIDORA BELO HORIZONTBR	1.62	986	
21	41	468918******9947	WW226696	039678660	1180822	42802	90	5691	ROCK SEDA SAO JOSE DOS BR	1.14	986	
21	41	468918******9996	CW028402	030346835	1180822	42802	90	5912	DROGARIA NOVA VALQUEIRE RIO DE JANEIRBR	1.71	986	
21	41	468918******9889	WY126523	011656573	1180822	42803	90	5422	FRIGOLIM LTDA BELO HORIZONTBR	1.55	986	
21	41	468918******9939	WW336712	029477700	1180822	42803	90	5411	CASA BERTI SAO PAULO BR	1.25	986	
21	41	468918******9913	CW030286	008220379	1180822	42803	90	5661	AUTHENTIC FEET C NORTE SAO PAULO BR	1.25	986	
21	41	468918******9905	WY776420	021695652	1180822	42803	90	5411	MERCEAR MANTIPAR LTDA CONTAGEM BR	1.5	986	
21	20	517045******8980	IT263466	021061327	1180823	1411	90	5533	REI DO OLEO SAO PAULO BRA	1.79	986	1**
21	56	517045******8964	WR870881	074669320	1180823	1411	90	5411	DIST A POPULAR BETIM BRA	1.72	986	1**
21	21	517045******8949	WY551036	013358952	1180823	1411	90	5422	CASA DE CARNES 3 MENIN BELO HORIZONT BRA	1.28	986	1**
21	56	517045******8931	WW336712	029477700	1180823	1411	90	5411	CASA BERTI SAO PAULO BRA	1.45	986	1**
21	20	517045******8998	CW028402	030346835	1180823	1411	90	5912	DROGARIA NOVA VALQUEIR RIO DE JANEIR BRA	1.48	986	1**
21	56	517045******8873	WY780858	031487130	1180823	1411	90	5045	MXT CENTER SAO PAULO BRA	1.32	986	1**
21	20	517045******8915	WY662668	076625079	1180823	1411	90	4812	AGR TELECOM BELO HORIZONT BRA	2	986	1**
21	20	517045******8865	WY727326	046025782	1180823	1411	90	5691	OPHICINA COM JUNDIAI BRA	1.6	986	1**
21	20	517045******8907	WY375128	034205748	1180823	1411	90	5411	ALVES NOGUEIRA LTDA IGARAPE BRA	1.28	986	1**
21	20	517045******8923	WY776420	021695652	1180823	1411	90	5411	MERCEAR MANTIPAR LTDA CONTAGEM BRA	1.97	986	1**
21	56	517045******8899	WQ201116	015134903	1180823	1411	90	5921	ACQUA PURA SAO SEBASTIAO BRA	1.4	986	1**
21	20	517045******8881	IS175858	012187160	1180823	1411	90	5231	BAZAR DAS TINTAS SAO PAULO BRA	1.48	986	1**
21	20	517045******8840	WW275200	030868211	1180823	1411	90	5251	NOVAROMALUM SAO PAULO BRA	1.52	986	1**
21	56	517045******8816	WQ403977	015929795	1180823	1411	90	5300	VILLFORT ATACADISTA CONTAGEM BRA	1.84	986	1**
21	20	517045******8832	WQ624921	009958525	1180823	1411	90	5422	CASA DE CARNE BOI GRIL SAO PAULO BRA	1.18	986	1**
21	20	517045******8824	WW233445	034404902	1180823	1411	90	5722	GENARIO F COSTA , SAO PAULO BRA	1.4	986	1**
21	56	517045******8857	WW147978	012348040	1180823	1411	90	5411	LIDER PLUS BETIM BRA	1.33	986	1**
21	56	517045******8956	WW010825	055093973	1180823	1411	90	5921	R3 DISTRIBUIDORA BELO HORIZONT BRA	1.92	986	1**

Card Authorisation

EMV chip transaction – Online

- Transaction initiation: POS and card exchange data
  - Track 2 equivalent data
  - Card settings and capabilities
  - Transaction data (amount, currency, date, etc)
  - ...

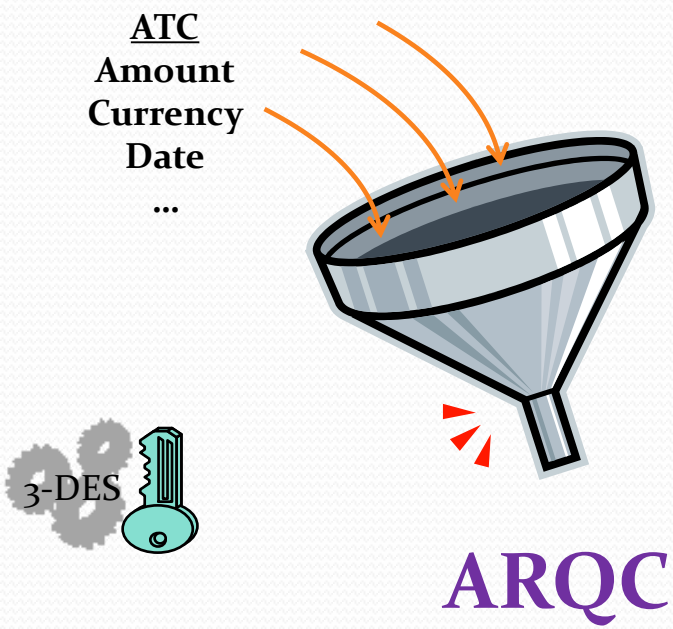
Card Authorisation

EMV chip transaction – Online

- Card generates an Authorization ReQuest Cryptogram (ARQC).
- ARQC is the encryption of card and terminal data using a secret key specific to that card. This key can be retrieved by the issuer authorization system.
- ARQC is a DYNAMIC cryptogram: it is different for each transaction

Card Authorisation

EMV chip transaction

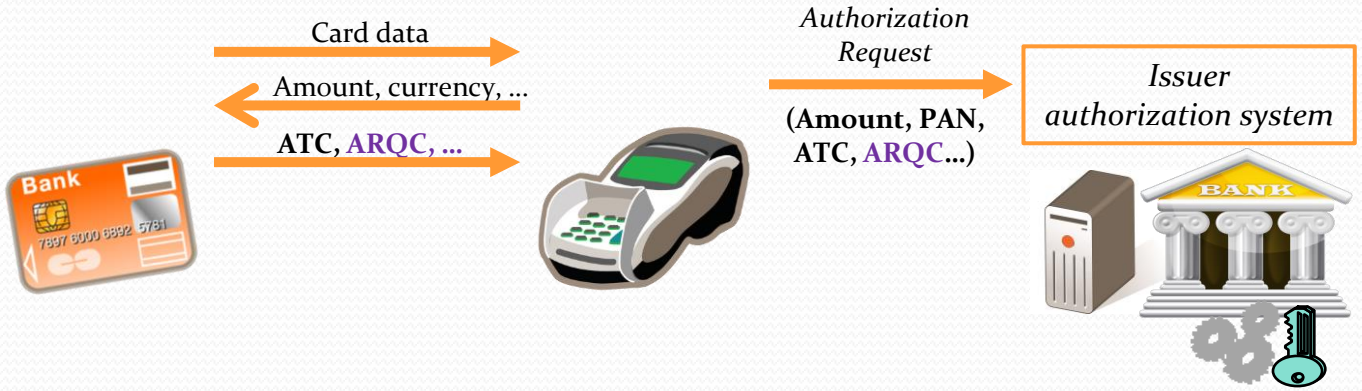


- ATC is a transaction counter
- It is incremented for each transaction

→ The card will never generate the same ARQC value twice

Card Authorisation

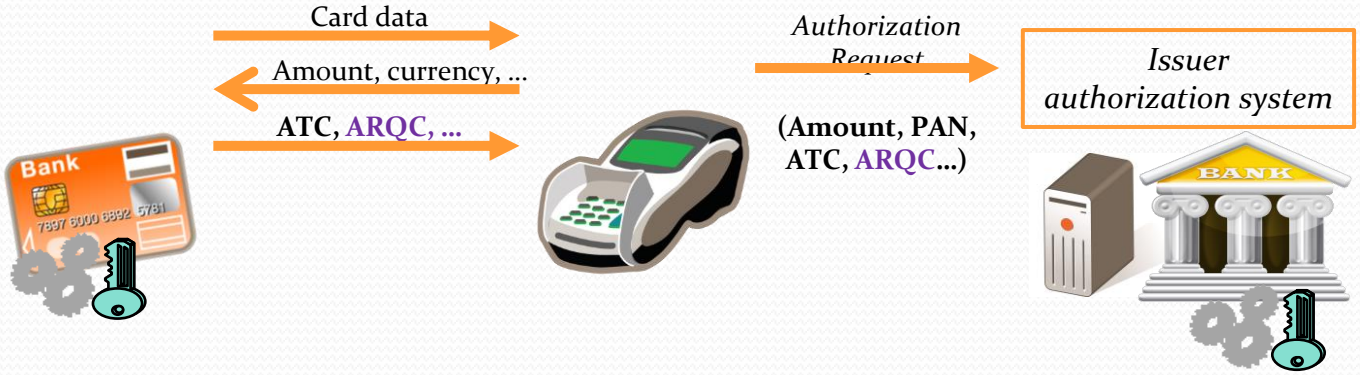
EMV contact transaction – Online



- Authorization request is sent to the issuer authorization system
  - Same data as a mag-stripe transaction
  - Additional EMV data

Card Authorisation

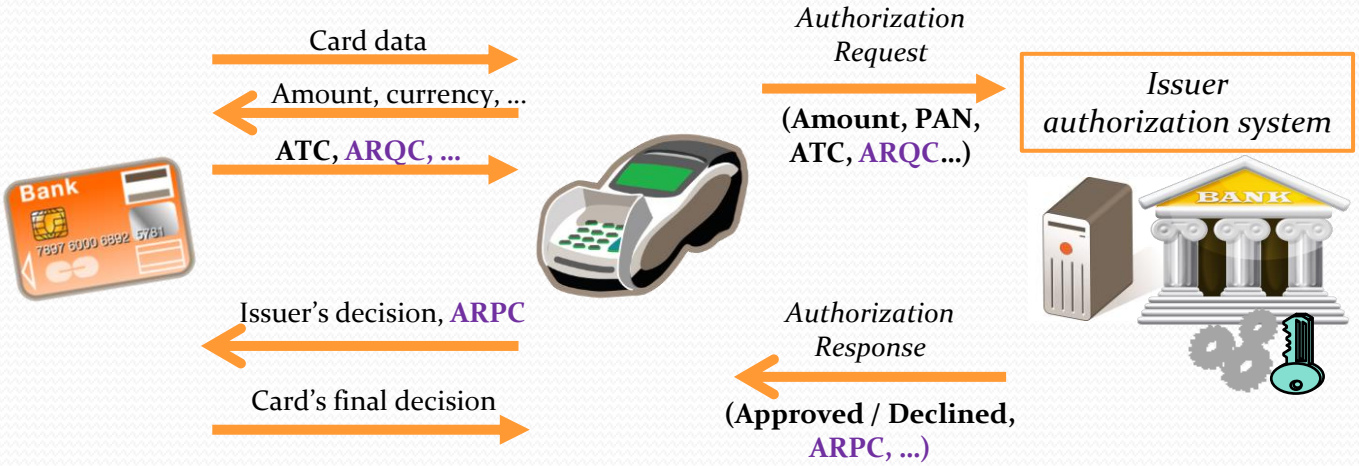
EMV contact transaction – Online



- The authorization system performs risk management
- It also checks the validity of the ARQC by recalculating it using:
  - the data transmitted in the authorization request
  - the secret key associated to that card
- If the ARQC is validated, the card is considered genuine, and there is a guarantee that the transaction data has not been tempered with (amount, ...)

Card Authorisation

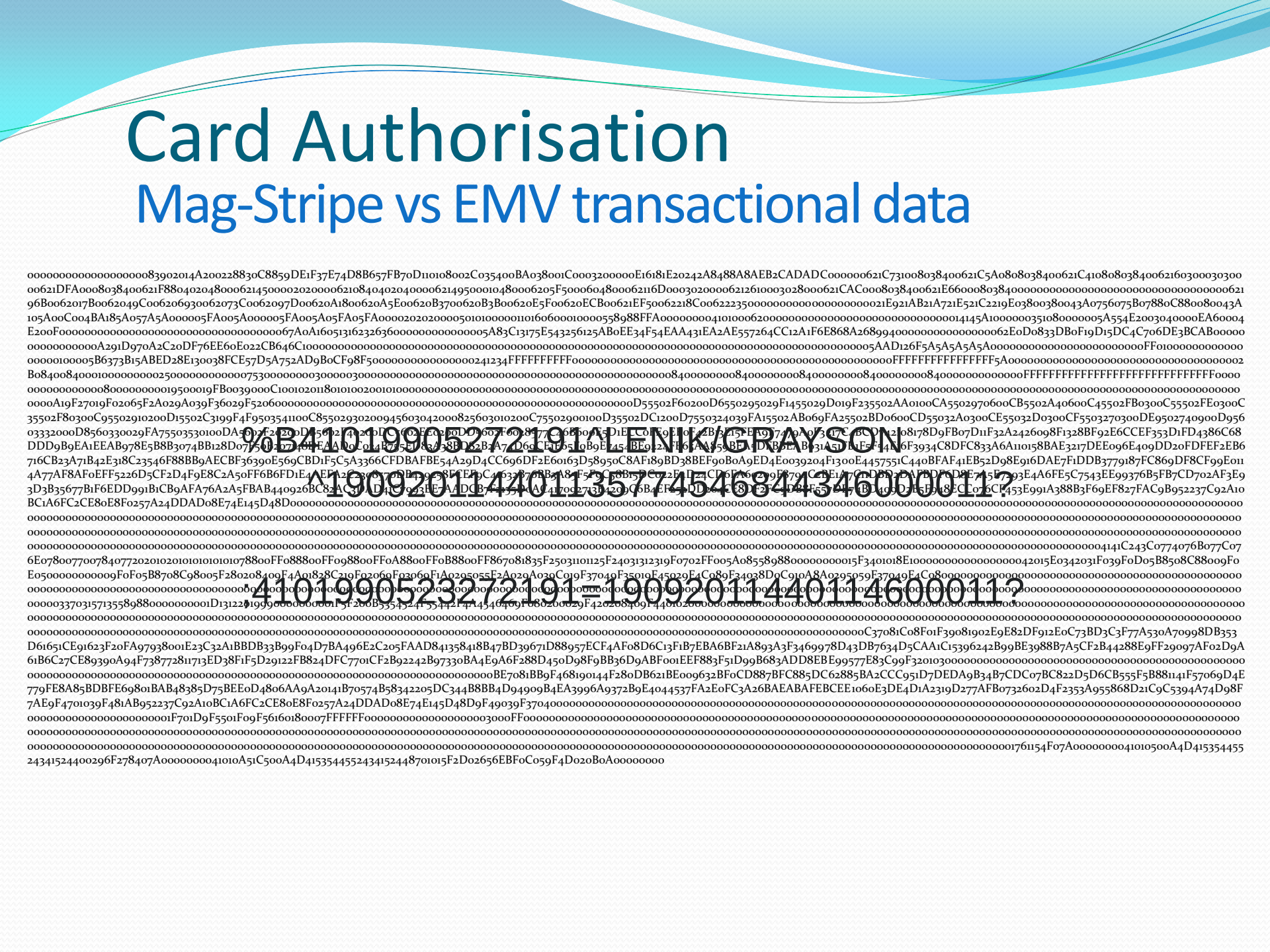
EMV contact transaction – Online



- Issuer host generates an authorization response
- Response may include an Authorization ResPonse Cryptogram that authenticates the issuer and the issuer decision. The card may validate the ARPC before giving its final decision.

Card Authorisation

Mag-Stripe vs EMV transactional data



QUESTIONS?

Mircea Constantin Șcheau

I2DS2

INTEGRATED INTELLIGENCE, DEFENCE AND SECURITY SOLUTIONS

A TID`s Idea and Innovation Platform