DEVFEST Strasbourg

Voyage au cœur du paiement sans contact

Julien Jimenez
Expert sécurité
Worldline

Aurélie Abraham
Développeuse Fullstack
Ippon Technologies

WORLDLINE

ippon

2024 DEVFEST STRASBOURG

Il était une fois en 2007…
… à Las Vegas

2024 DEVFEST STRASBOURG

Mobile Phone Museum

Announced	Weight
January 2007	112 grams

Features

This NFC-enabled variant of the Nokia 6131 (model number: RM-216) was announced at the CES Show in Las Vegas in January 2007. It was described as a handset that served as a credit card, loyalty card and travel ticket. Nokia showed off a variety of potential NFC applications at its CES booth

READ MORE

‹ Motorola - Timeport L7389e

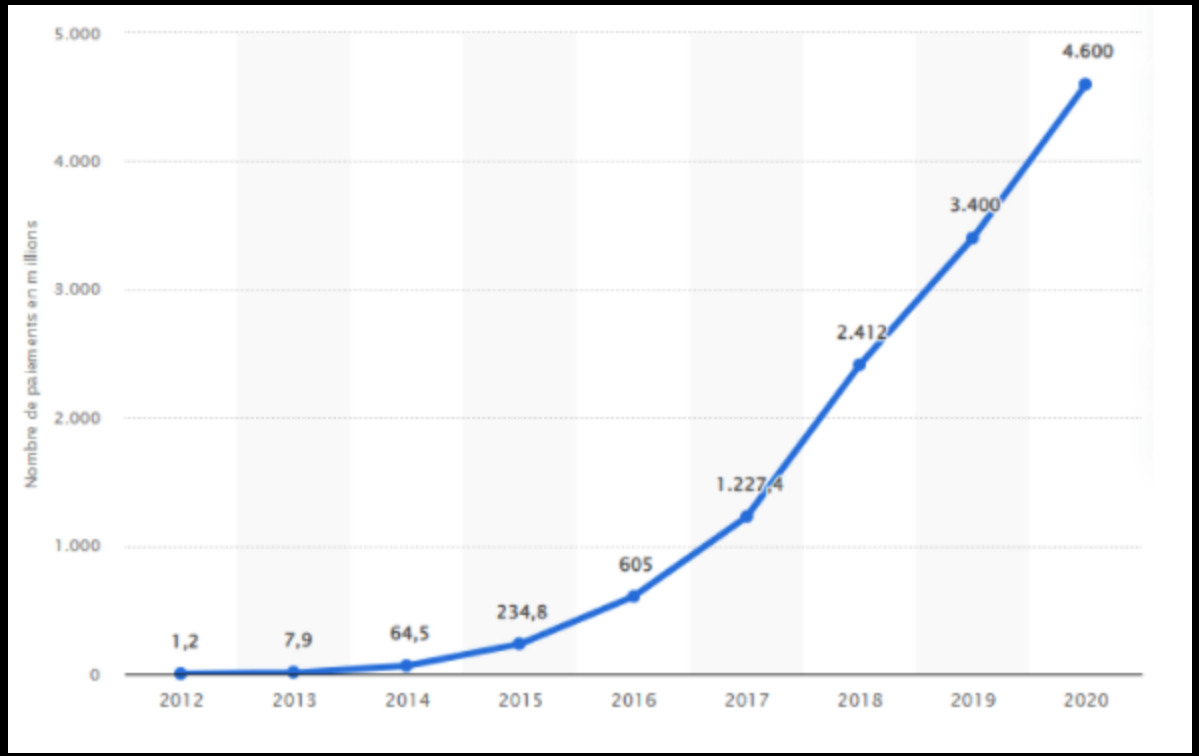
Siemens - E10 ›

https://www.mobilephonemuseum.com/phone-detail/6131-nfc

2024 DEVFEST STRASBOURG

Pendant ce temps à San Francisco…

Evolution du paiement sans contact



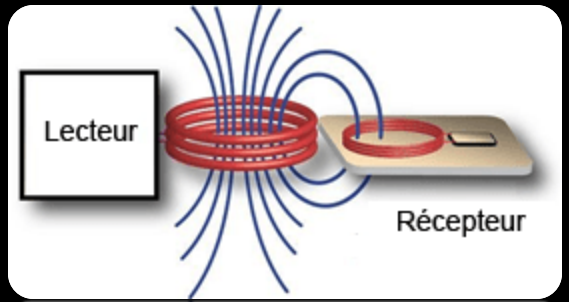
7 Milliards de transactions sans contact en France en 2023

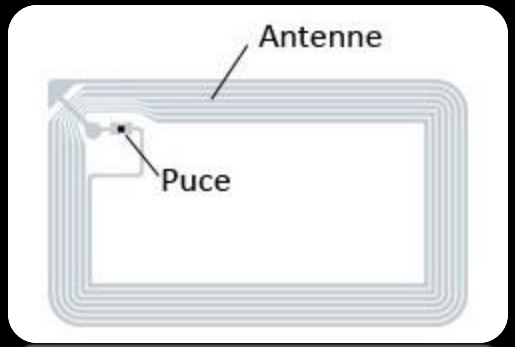
Nombre de paiements réalisés avec des cartes bancaires (CB) sans contact françaises de 2012 à 2020, en millions (source Statista.com)
https://www.cartes-bancaires.com/cb/chiffres/

Le NFC

- Phénomène de l'induction

- Le lecteur envoie l'énergie
- L'antenne dans la carte la récupère pour alimenter sa puce

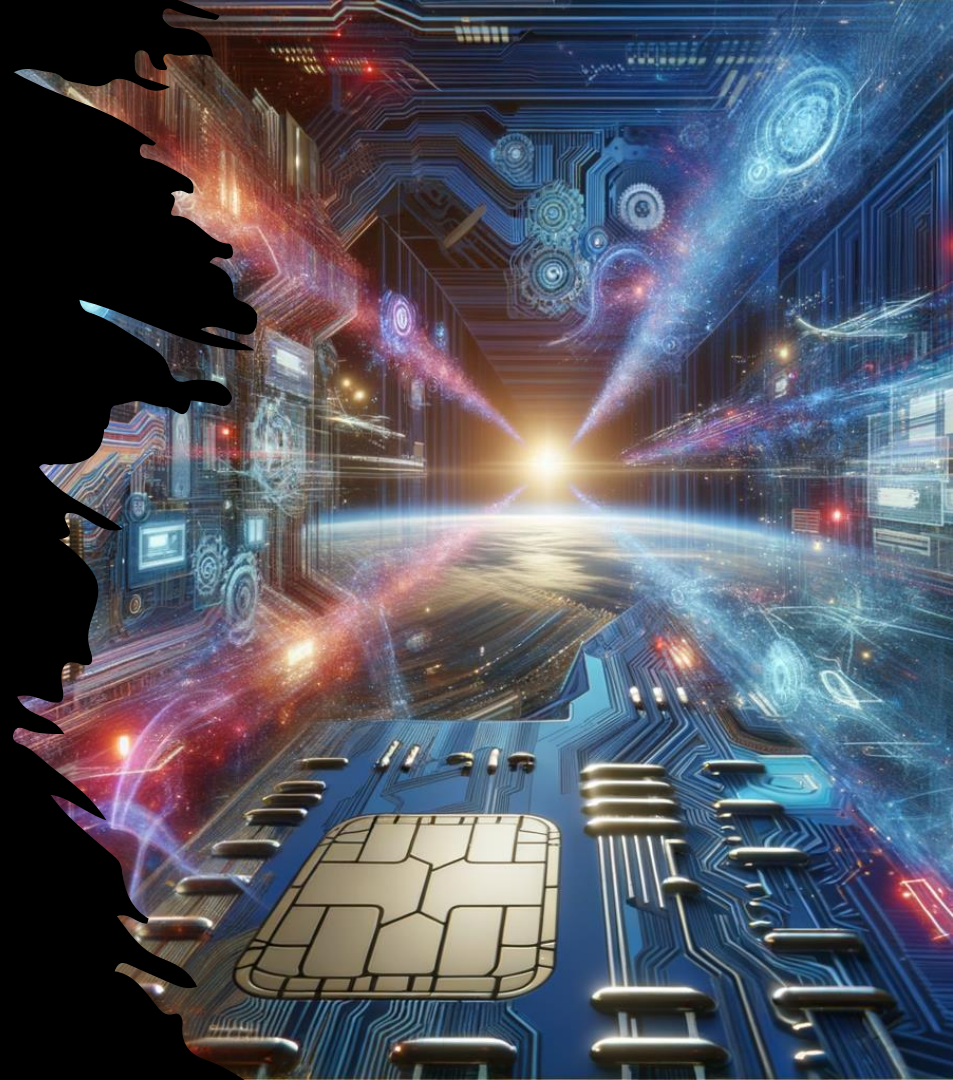


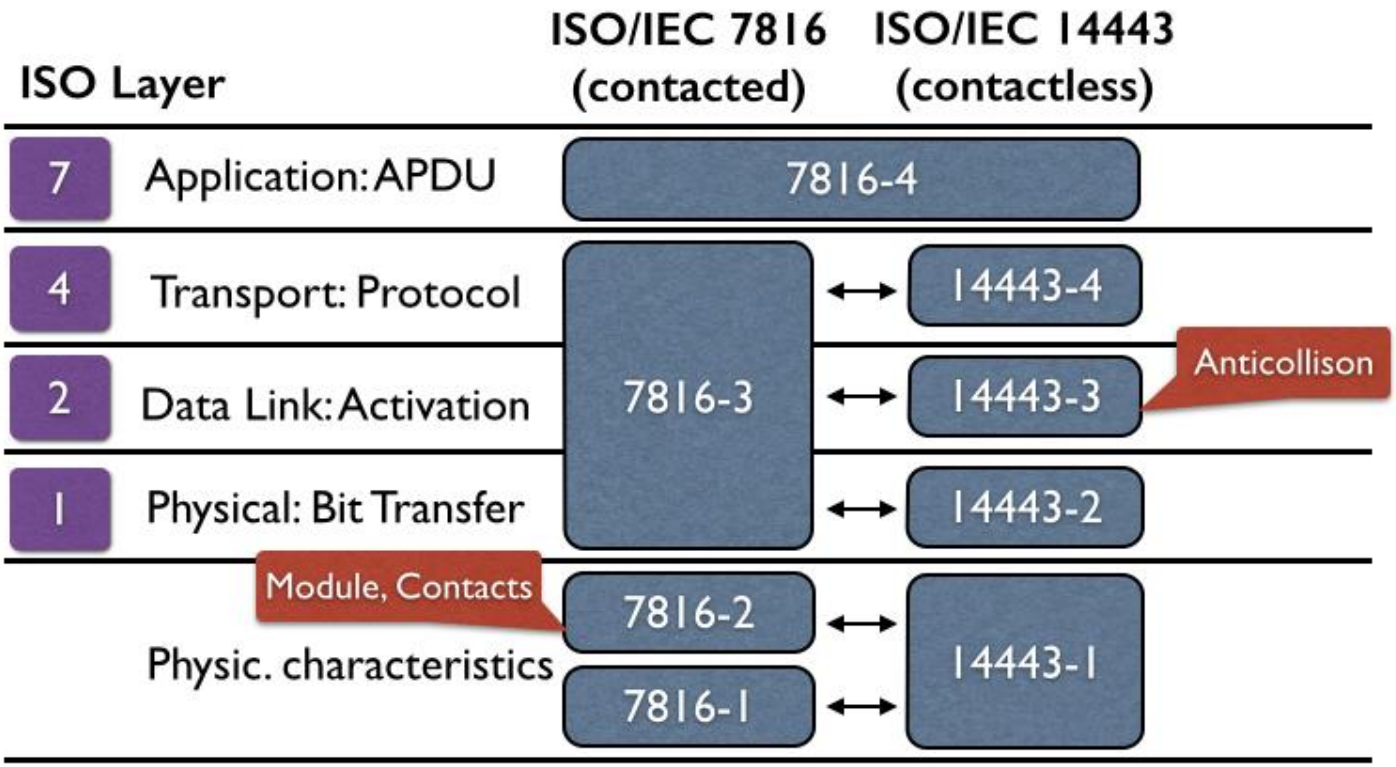


Qu'est-ce qu'un paiement numérique ?

- Identification : Numéro de carte
- Authentification
- Validation de la transaction de transfert d'argent

Plongeons maintenant au cœur de la carte bancaire





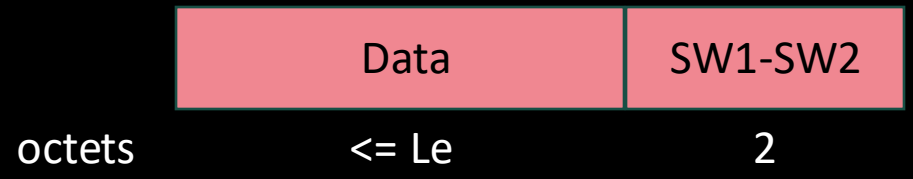
Structure des messages

Application Protocol Data Unit
(APDU)
Commande

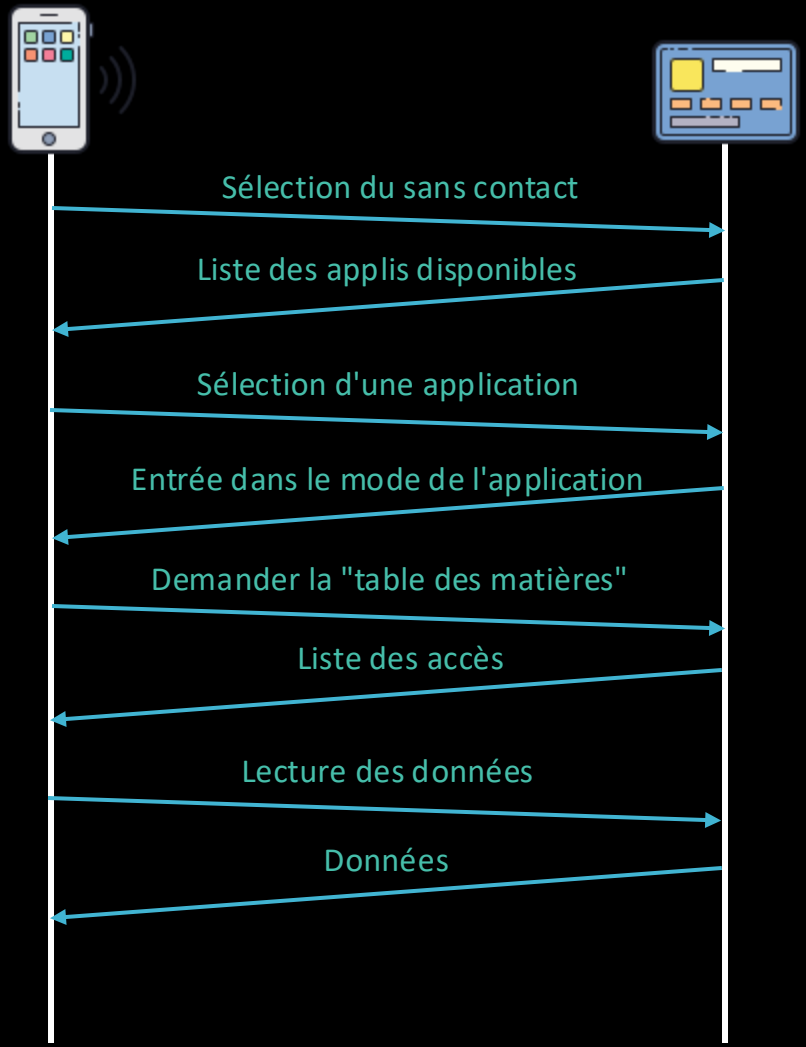
	CLA	INS	P1-P2	Lc	Data	Le
octets	1	1	2	0-3	Lc	0-3

Structure des messages

Application Protocol Data Unit
(APDU)
Réponse



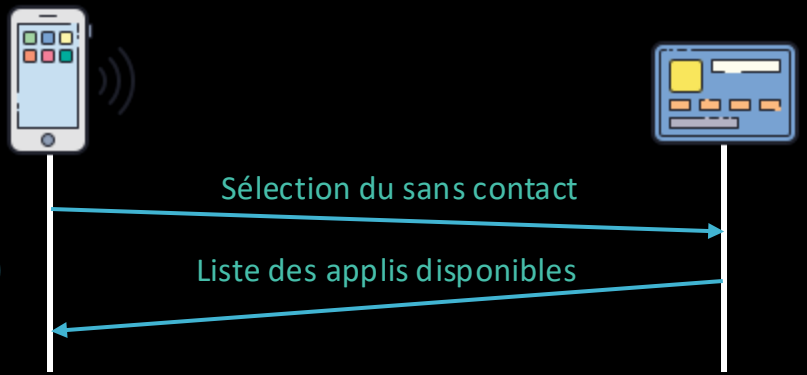
Échanges avec la carte



Exemple : sélection du sans contact

00A4 0400 0E 325041592E5359532E4444463031 00

CLA-INS	P1-P2	Lc	Data	Le
select			"2PAY.SYS.DDF01"	



6F2A(…)C1561134F07**A000000004101**08701019**000**

DEVFEST 2024 STRASBOURG

Applications disponibles

Quelques AIDs

VISA Electron	A0 00 00 00 03 20 10
VISA debit/credit	A0 00 00 00 03 10 10
VISA DPA	A0 00 00 00 03 80 02
MasterCard	A0 00 00 00 04 10 10
Maestro	A0 00 00 00 04 30 60
MasterCard CAP	A0 00 00 00 04 80 02

6F File Control Information (FCI) Template
- 84 Dedicated File (DF) Name
  - 325041592E5359532E4444463031
- A5 File Control Information (FCI) Proprietary Template
  - BF0C File Control Information (FCI) Issuer Discretionary Data
    - 61 Application Template
      - 4F Application Identifier (AID) – card
        - A0000000421010
      - 50 Application Label
        - C B
      - 87 Application Priority Indicator
        - 01
      - 9F2A Unknown tag
        - 03
      - 9F0A Unknown tag
        - 0001050100000000
      - BF63 Unknown tag
        - DF20 Unknown tag
          - 80
    - 61 Application Template
      - 4F Application Identifier (AID) – card
        - A0000000031010
      - 50 Application Label
        - V I S A
      - 87 Application Priority Indicator
        - 02
      - 9F2A Unknown tag
        - 03
      - 9F0A Unknown tag
        - 0001050100000000
      - BF63 Unknown tag
        - DF20 Unknown tag
          - 80

Applications disponibles

DEVFEST 2024 STRASBOURG

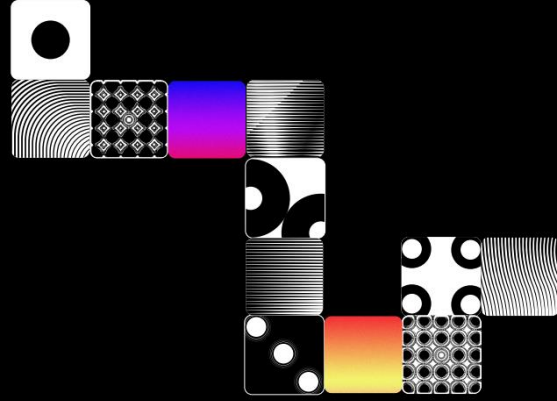
```
Wed Sep 18 16:58:12 2019
 Reader 0: ACS ACR122U PICC Interface 00 00
  Card state: Card inserted,
  ATR: 3B 8C 80 01 50 C1 7D A8 CA 00 00 00 00 00 71 71 83

ATR: 3B 8C 80 01 50 C1 7D A8 CA 00 00 00 00 00 71 71 83
+ TS = 3B --> Direct Convention
+ T0 = 8C, Y(1): 1000, K: 12 (historical bytes)
  TD(1) = 80 --> Y(i+1) = 1000, Protocol T = 0
-----
  TD(2) = 01 --> Y(i+1) = 0000, Protocol T = 1
-----
+ Historical bytes: 50 C1 7D A8 CA 00 00 00 00 00 71 71
  Category indicator byte: 50 (proprietary format)
+ TCK = 83 (correct checksum)

Possibly identified card (using /home/lp1/.cache/smartcard_list.txt):
3B 8C 80 01 50 C1 7D A8 CA 00 00 00 00 00 71 71 83
```

Le lecteur utilisé pour la lecture des informations en NFC est un ACR122U (10€) et le logiciel pcsc_scan de la suite pcsc-tools (disponible sur MacOS et GNU/Linux).

Lire une Visa depuis un Android ?



```
class MainActivity : ComponentActivity() {
    private var nfcAdapter: NfcAdapter? = null
    private var pendingIntent: PendingIntent? = null

    override fun onCreate(savedInstanceState: Bundle?) {
        nfcAdapter = NfcAdapter.getDefaultAdapter(this)
        pendingIntent = PendingIntent.getActivity(...)
        val ndef = IntentFilter(NfcAdapter.ACTION_NDEF_DISCOVERED)
    }

    override fun onResume() {
        nfcAdapter!!.enableForegroundDispatch(this, pendingIntent, null, null)
        nfcAdapter!!.enableReaderMode(
            this, { tag: Tag? -> nfcAdapter!!.disableReaderMode(this@MainActivity)},
            NfcAdapter.FLAG_READER_NFC_A or NfcAdapter.FLAG_READER_NFC_B, options)
    }

    override fun onNewIntent(intent: Intent) {
        val tagFromIntent = intent.getParcelableExtra<Tag>(NfcAdapter.EXTRA_TAG)
        val isoDep = IsoDep.get(tag);
        byte[] apdu = stringToHex("00A404000E325041592E5359532E444446303100");
        byte[] resp = isoDep.transceive(apdu);
    }
}
```

Union Pay

American Express

JCB

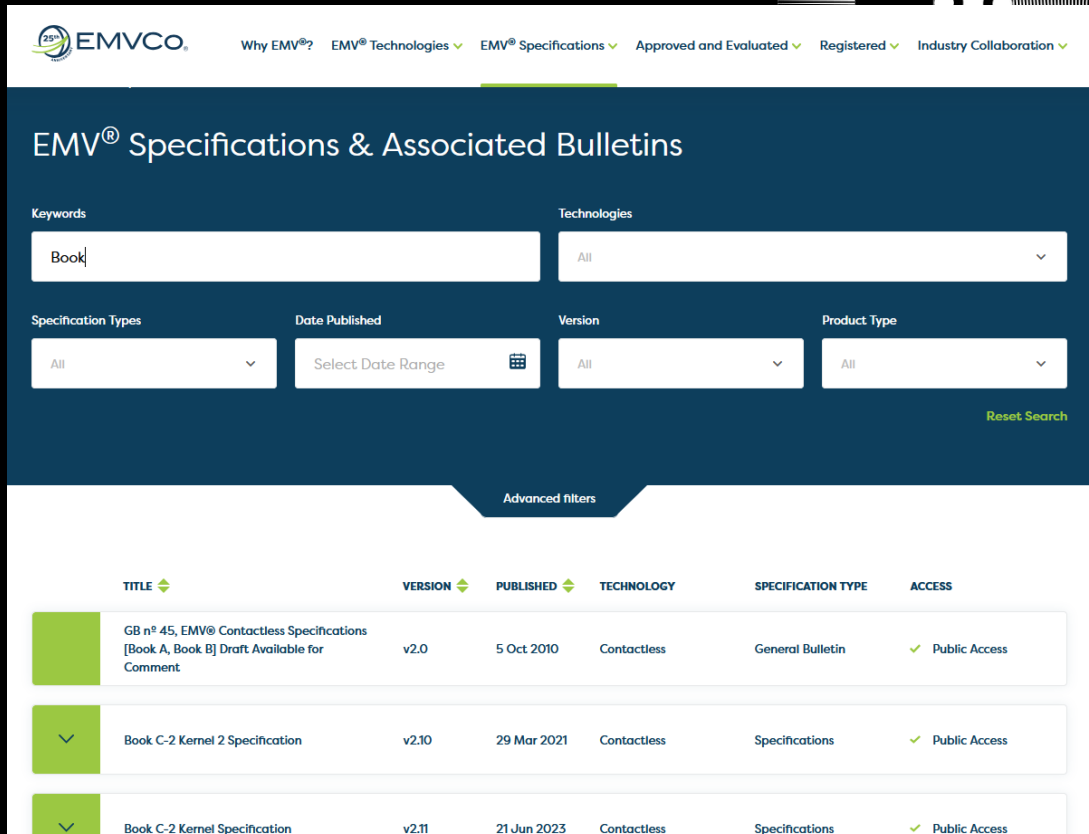
Visa

Europay

MasterCard

Objectifs :

- Garantir l'harmonie des systèmes de paiement
- Maintenir des standards rigoureux
- Protéger les données sensibles lors des transactions
- Innover

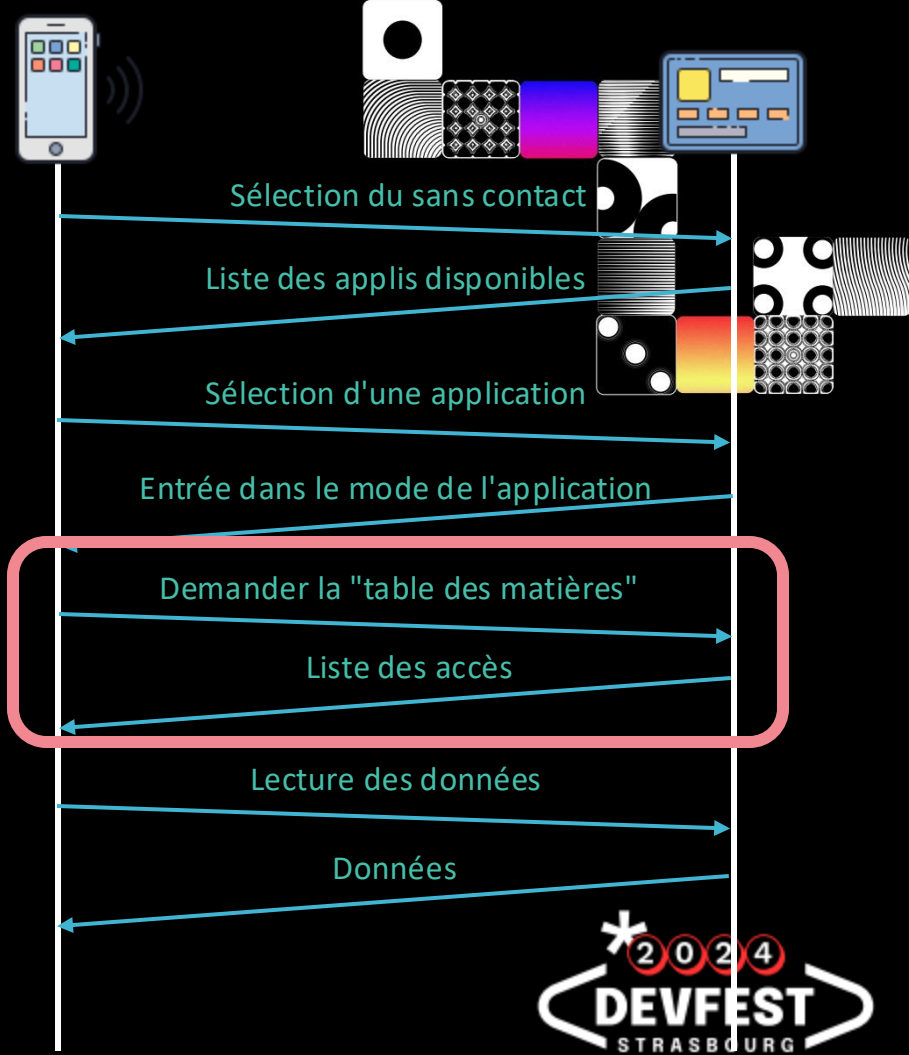


Get Processing Options

- CLA = 80
- INS = A8

- Démarre une transaction de paiement
- Le compteur de transaction est incrémenté (tag 9F36)

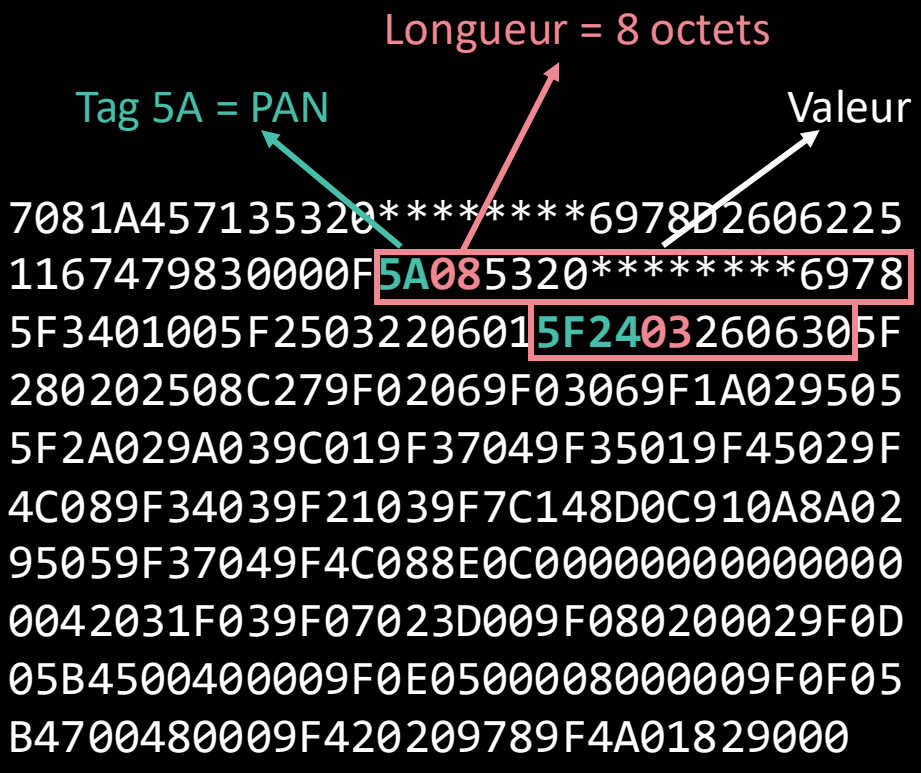
- Réponse : Application File Locator (tag 94)

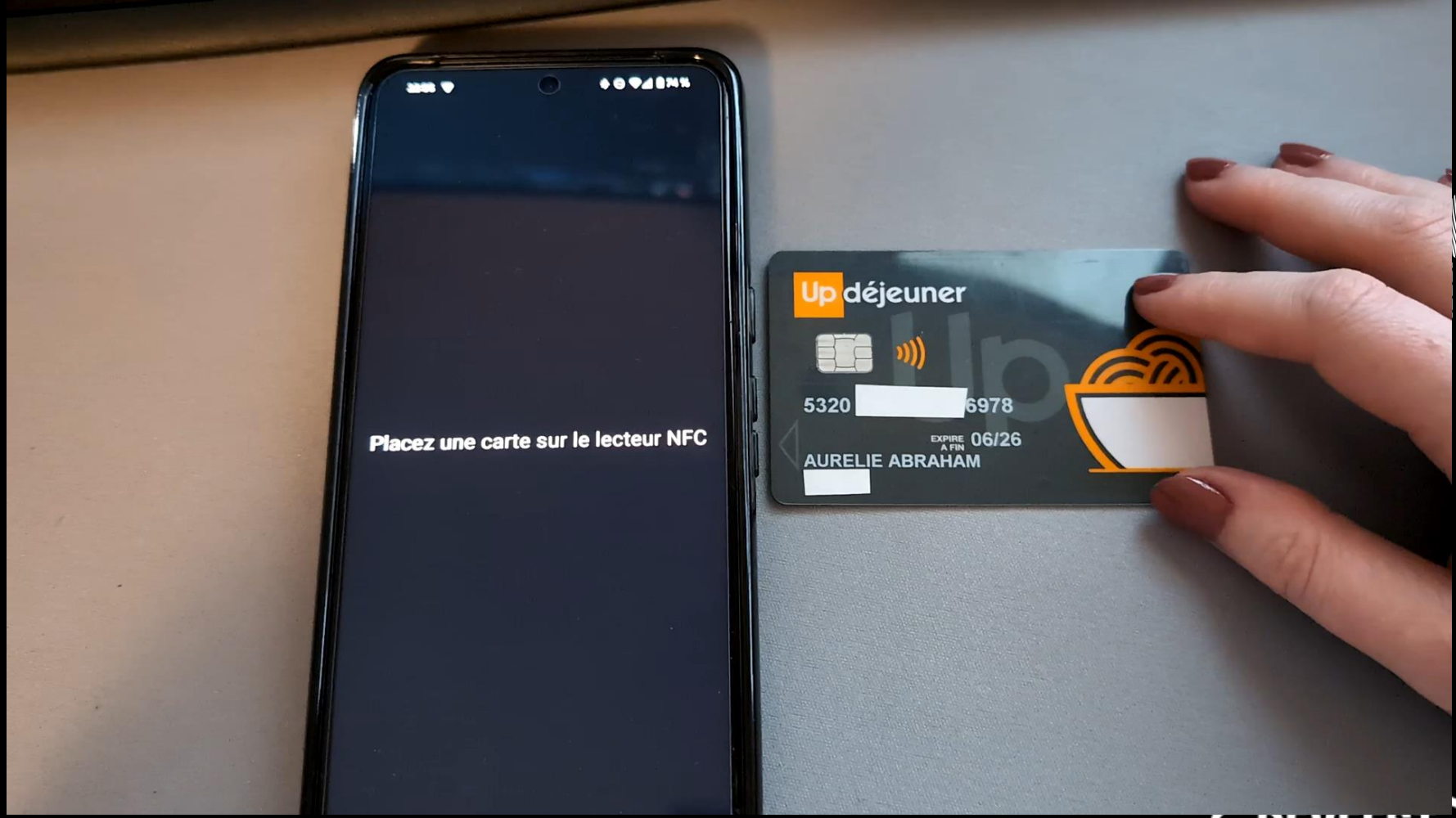


Lecture des données de la carte : Read Records

00B2013400

```
7081A457135320********6978D2606225
116747983000F5A085320********6978
5F3401005F2503220601 5F24032606305F
280202508C279F02069F03069F1A029505
5F2A029A039C019F37049F35019F45029F
4C089F34039F21039F7C148D0C910A8A02
95059F37049F4C088E0C000000000000000042031F039F07023D009F080200029F0D
05B4500400009F0E050008000009F0F05
B4700480009F420209789F4A01829000
```





https://github.com/MisatoKatsuragi/Devfest-Strasbourg-2024/

DEVFEST STRASBOURG

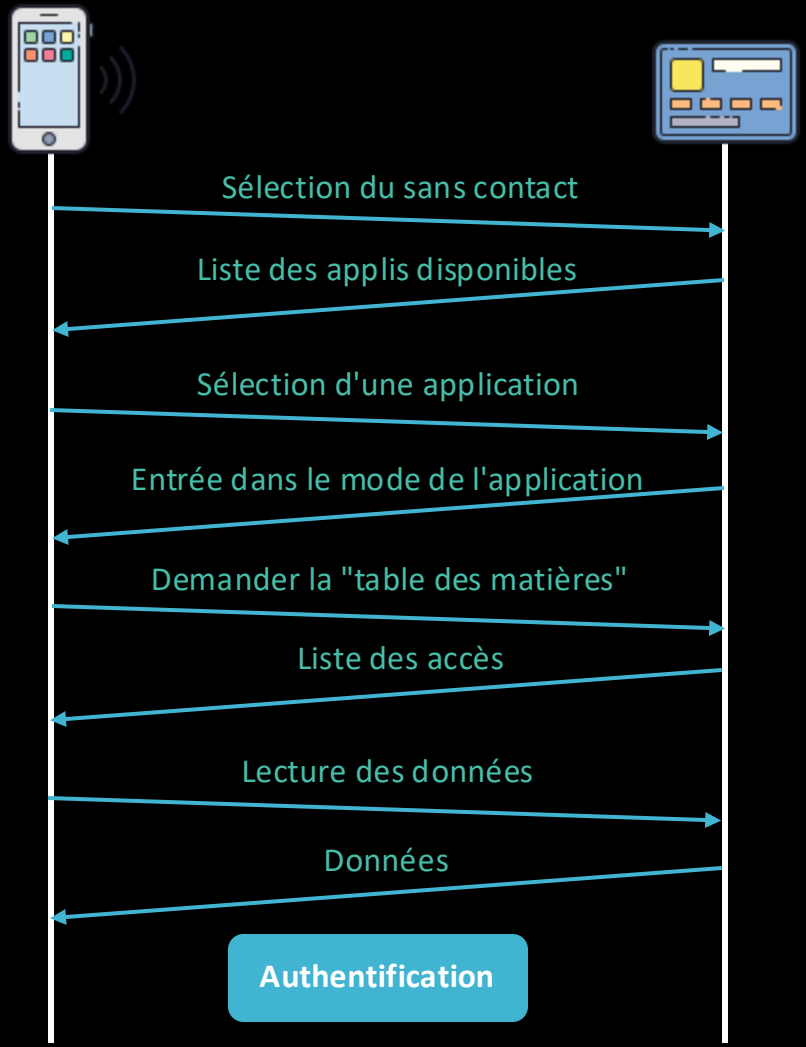
Est-ce qu'on vient de réussir à pirater les cartes bancaires ?

On va donc devoir tous acheter ces fameux portefeuilles en aluminium ?

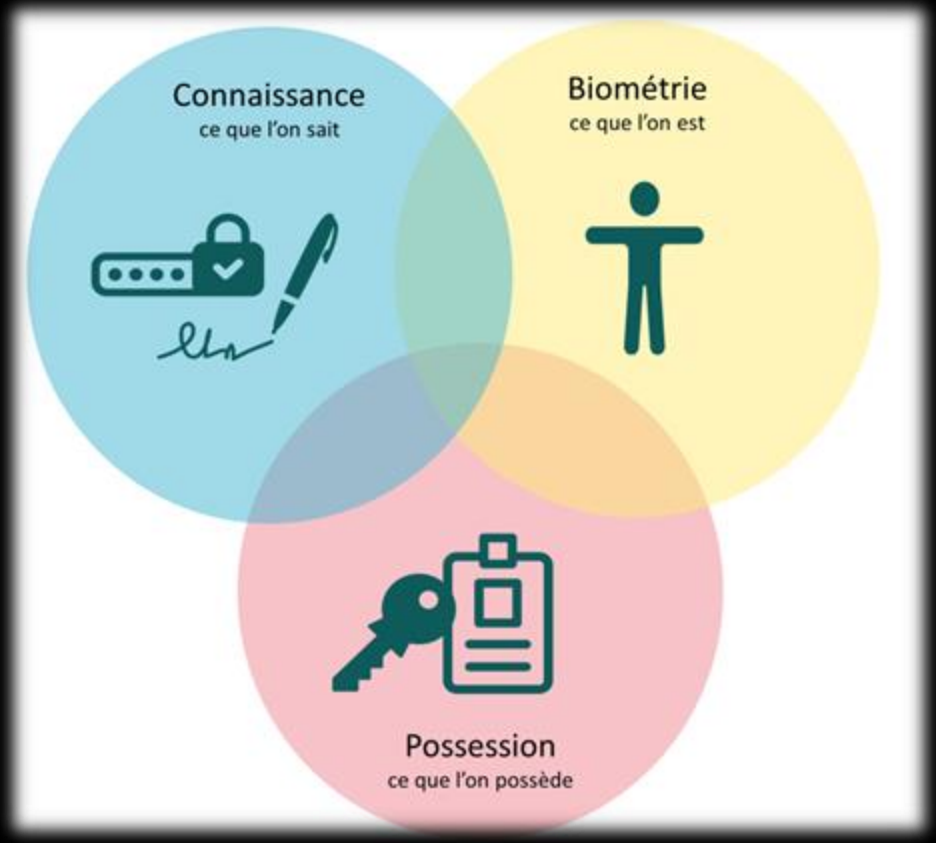
Qu'est-ce qu'un paiement numérique ?

- Identification : Numéro de carte
- **Authentification**
- Validation de la transaction de transfert d'argent

Échanges avec la carte



Qu'est-ce que l'authentification ?



Ce que je connais

- PIN
- Mot de passe
- Question secrète
- Schéma (déblocage par forme)

Mot de passe sécurisé

- Format complexe
- Uniques par application
- Sécurisation du stockage
- Limiter le nombre d'essais
- Forcer le changement régulièrement

- Authentification statique :
  Au moment de l'authentification :
  - le mot de passe est envoyé au serveur
  - Le résultat est comparé à la valeur stockée

99,99% des utilisateurs sont équipés d'un cerveau

Expérience utilisateur

MITM Attaque

Phishing

Keylogger

2024 DEVFEST STRASBOURG

The plaintext offline PIN block shall be formatted as follows:

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

where:

	Name	Value
C	Control field	4 bit binary number with value of 0010 (Hex '2')
N	PIN length	4 bit binary number with permissible values of 0100 to 1100 (Hex '4' to 'C')
P	PIN digit	4 bit binary number with permissible values of 0000 to 1001 (Hex '0' to '9')
P/F	PIN/filler	Determined by PIN length
F	Filler	4 bit binary number with a value of 1111 (Hex 'F')

Table 24: Plaintext Offline PIN Block Format

6.5.12.2 Command Message

The VERIFY command message is coded as shown in Table 22:

Code	Value
CLA	'00'
INS	'20'
P1	'00'
P2	Qualifier of the reference data (see Table 23)
Lc	Var.
Data	Transaction PIN Data
Le	Not present

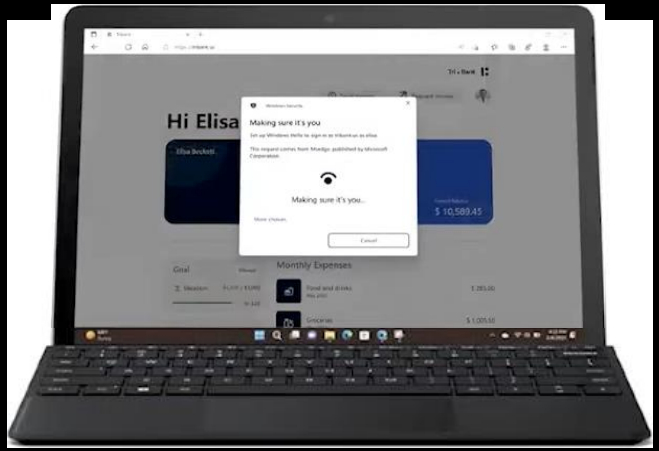
Table 22: VERIFY Command Message

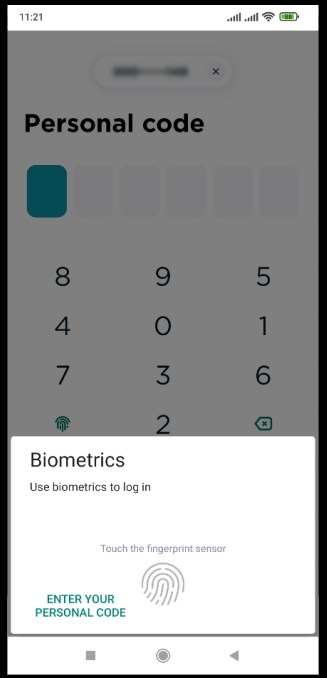
Ce que je suis

80% des smartphone équipés

Les applis smartphone

peuvent facilement utiliser les librairies biométriques iOS/Android





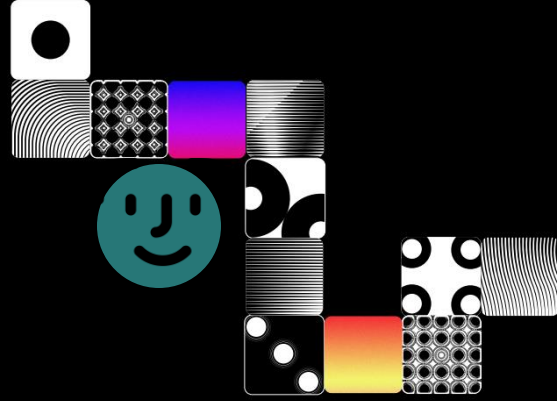
- Empreinte digitale
- Reconnaissance faciale
- Iris
- Forme de la main
- Veines de la main

Utilisation restreinte

Disponible également sur desktop

2024 DEVFEST STRASBOURG

Ce que je suis

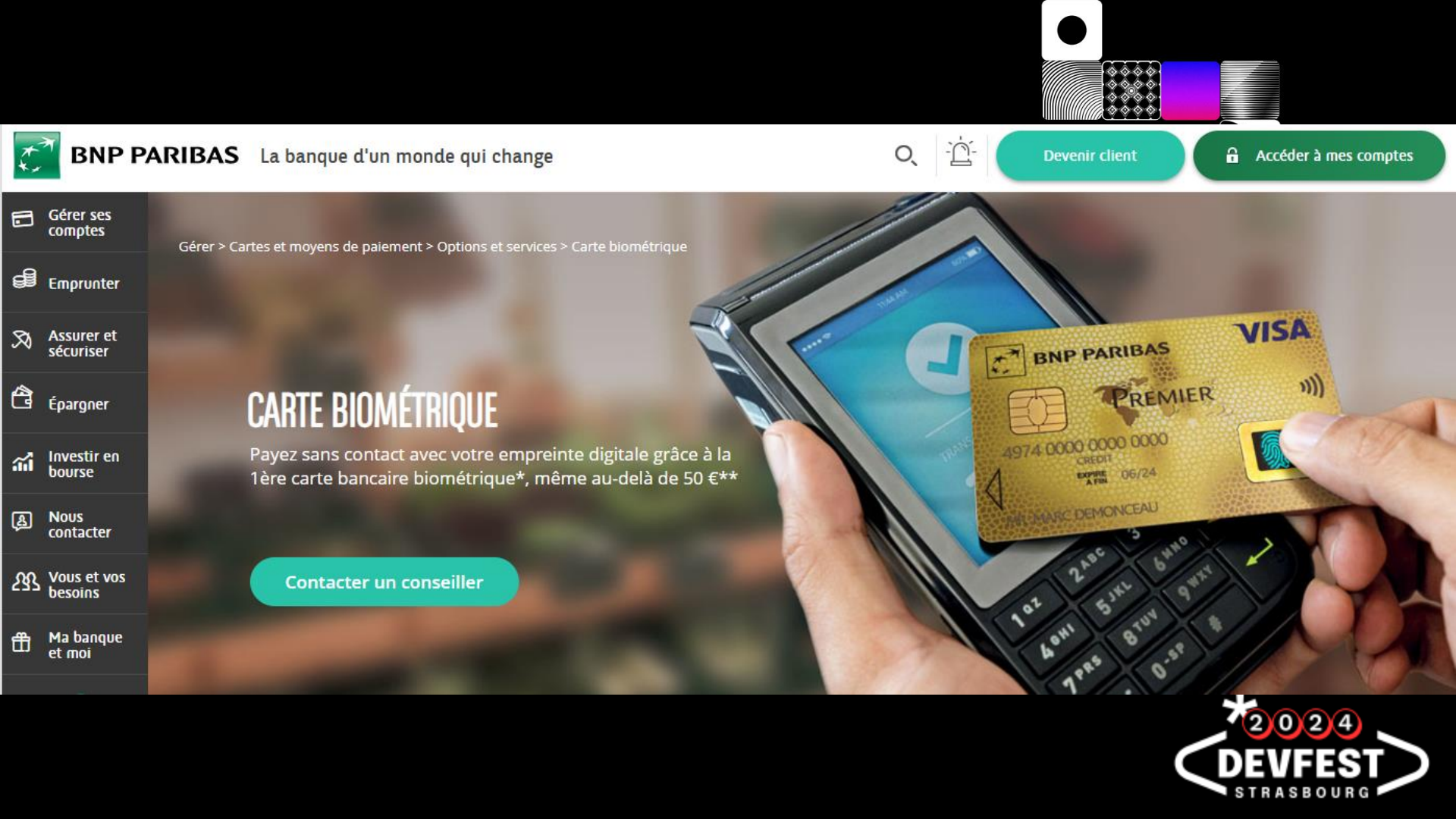


- Voix
- Démarche
- Frappe au clavier
- Gestuelle
- Etc.

Comportementale

- Empreinte digitale
- Reconnaissance faciale
- Iris
- Veines de la main

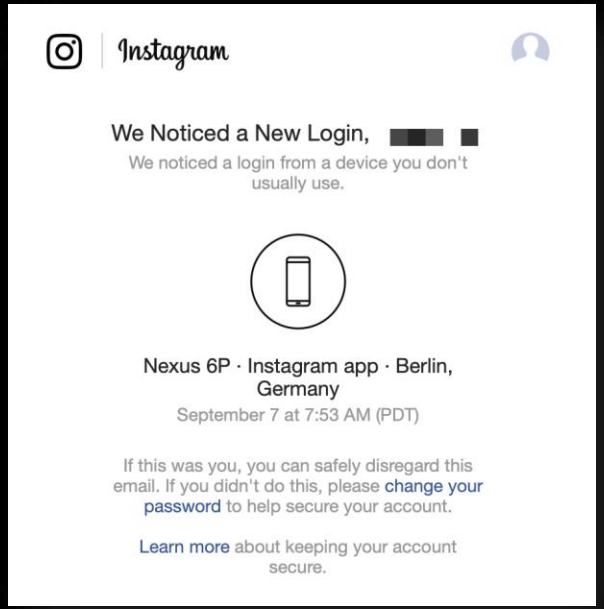
Physiologique



2024 DEVFEST STRASBOURG

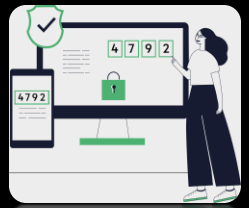
Ce que je possède

Device Fingerprinting



Niveau de sécurité

SMS OTP



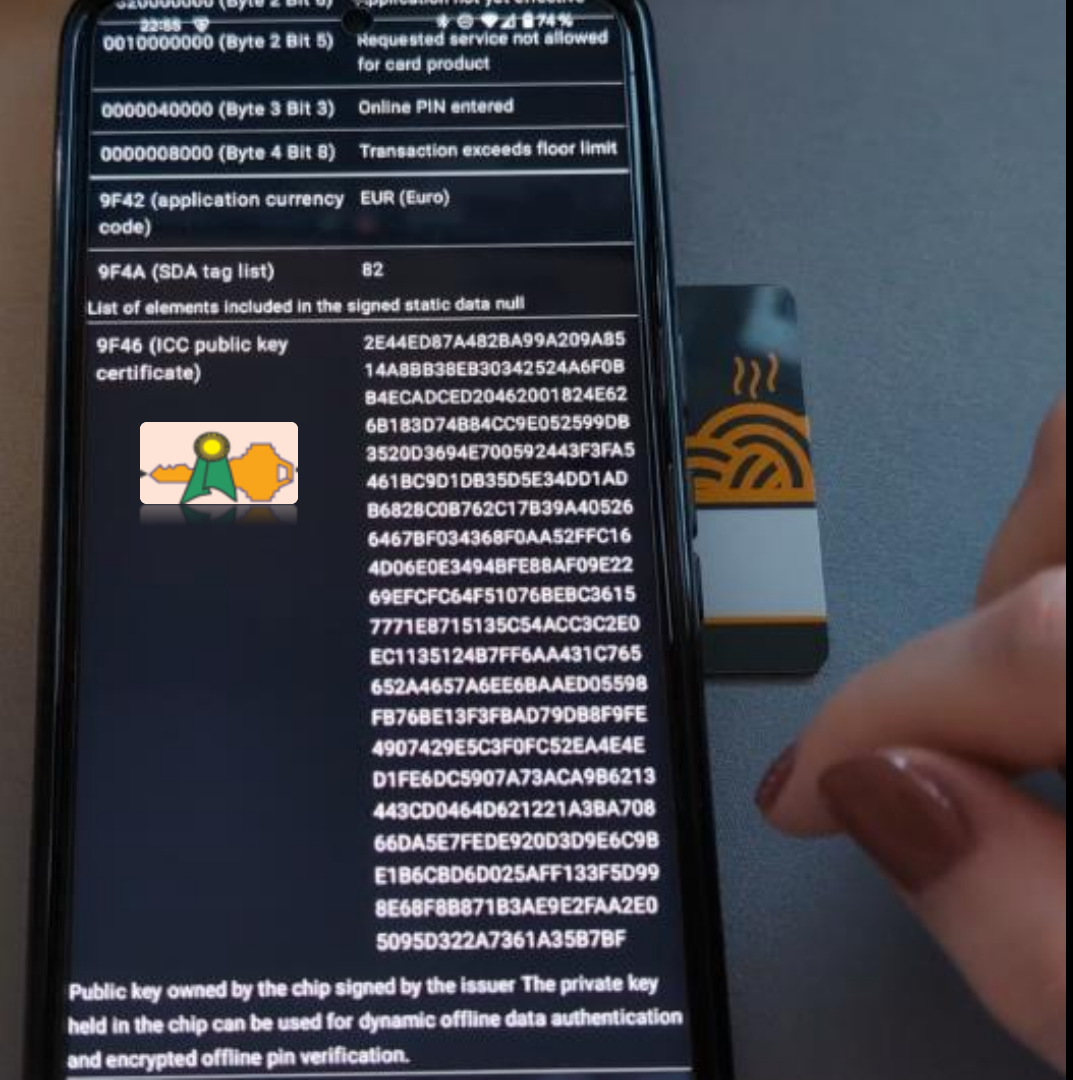
SIM Swaping

Smishing, Vishing

Carte bancaire

2024 DEVFEST STRASBOURG

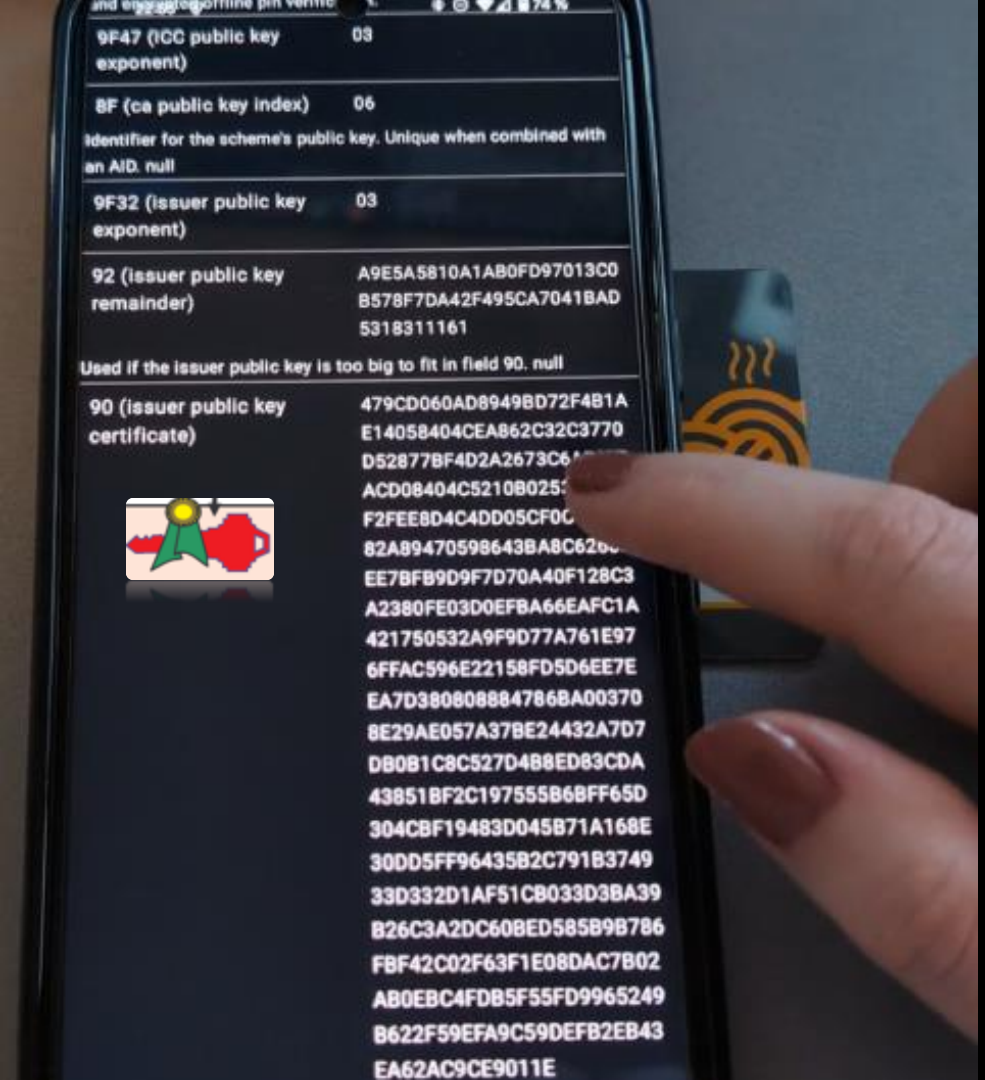
Cryptographie asymétrique



*« ICC **Public Key** Certificate »*

ICC : Integrated Circuit Chip
=> La puce sécurisée de la carte

2024 DEVFEST STRASBOURG

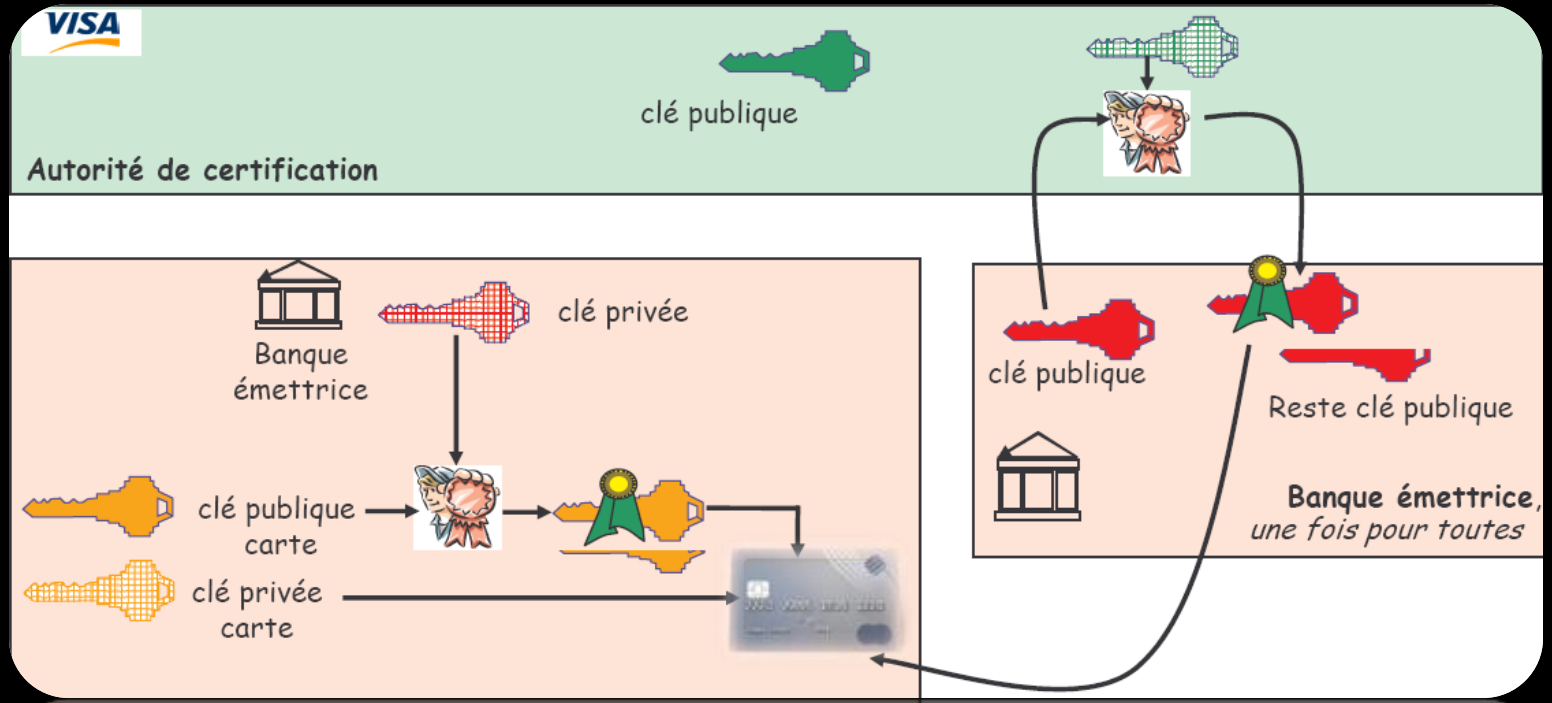


*« Issuer **Public Key** Certificate »*

Issuer : emetteur de la carte bancaire
=> La banque

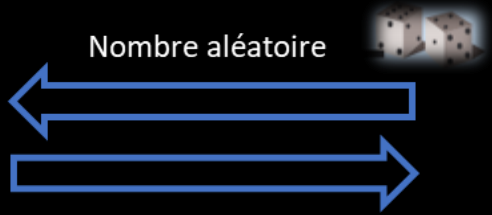
DEVFEST 2024 STRASBOURG

Personnalisation d'un carte bancaire



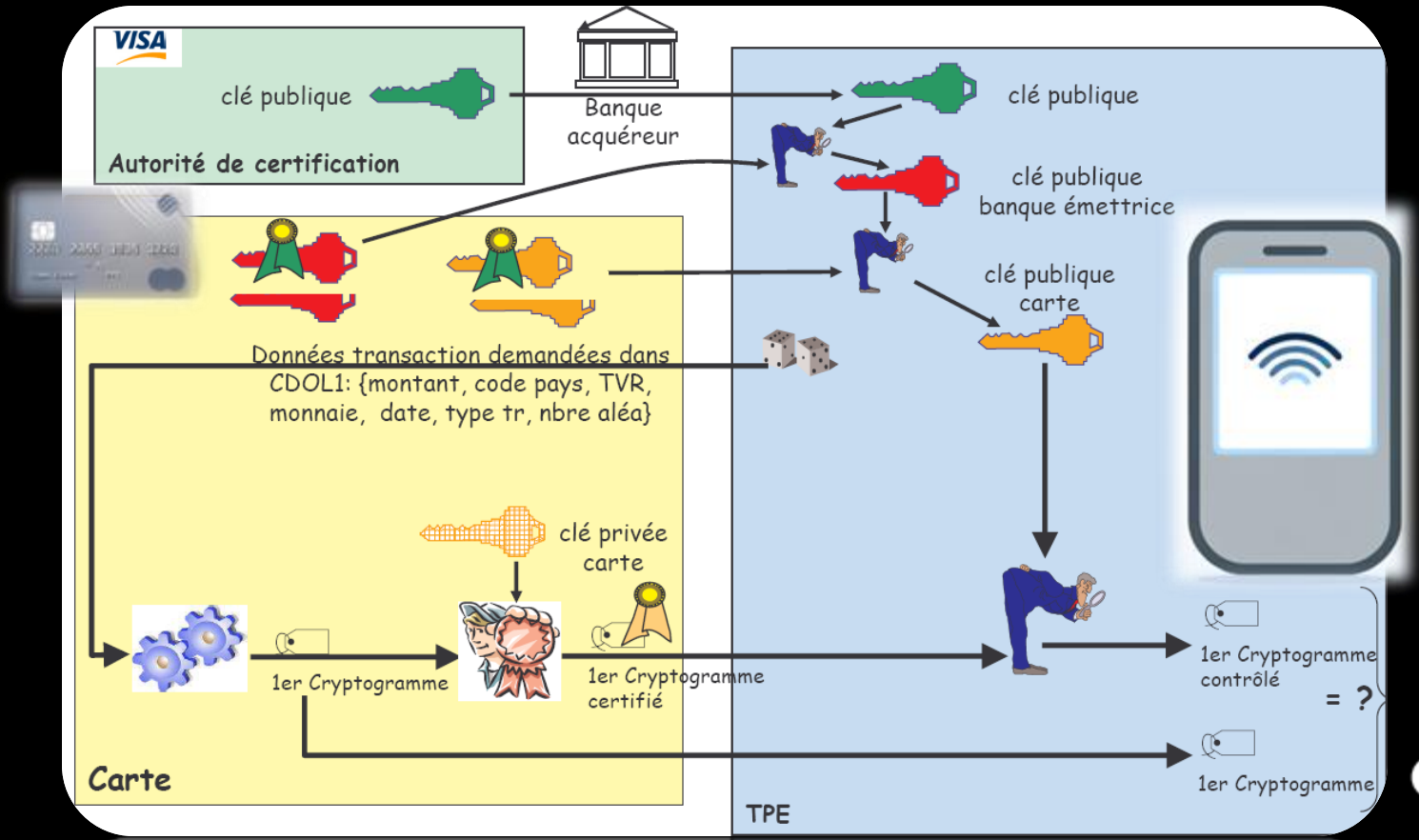
Cryptographie asymétrique

Signature du nombre aléatoire
avec la clef privée



Vérification de la signature

Authentification de la carte EMV



La preuve d'authentification

CARTE BANCAIRE
SANS CONTACT
CREDIT AGRICOLE
CENTRE LOIRE

A0000000421010
CB
LE 17/09/24 A 13:17:45
BRASSERIE L UNIVERS
TOURS
37000
1160693 56480174400017
14806
##########
6E4580B6DA31DED3
001 000010 150 €
MONTANT :
6,10 EUR

DEBIT
TICKET CLIENT
A CONSERVER
MERCI AU REVOIR
13349452

CARTE BANCAIRE
SANS CONTACT

CREDIT AGRICOLE
NORD MIDI-PYRENEES
A0000000041010AA01
Swile TitreResto
Le 28/10/2024 a 13:16:27
RESTO SNC UBRAC
PARIS
75116
5009788
11206
894075 15900026
##########
53F58B7FE3F83981
001 001 000465 € A
No AUTO : 717262

MONTANT :
16,00 EUR
DEBIT

TICKET CLIENT
A CONSERVER
MERCI 136-M-AVEM

CARTE BANCAIRE

SANS CONTACT
Bonjour
A0000000421010
CB
le 28/10/24 a 08:10:49
Montparnasse-Bienvenüe
RATP 75
PARIS
0183464
20041
77566343801906
##########
2E887F8E8066CBA5
406 001 070165
C
No AUTO
:
MONTANT REEL=
19,35 EUR
DEBIT
TICKET CLIENT
A CONSERVER
Merci, au revoir.

2024 DEVFEST STRASBOURG

Avantages de la carte bancaire

Interopérabilité
Facilité de mise en œuvre

Expérience utilisateur

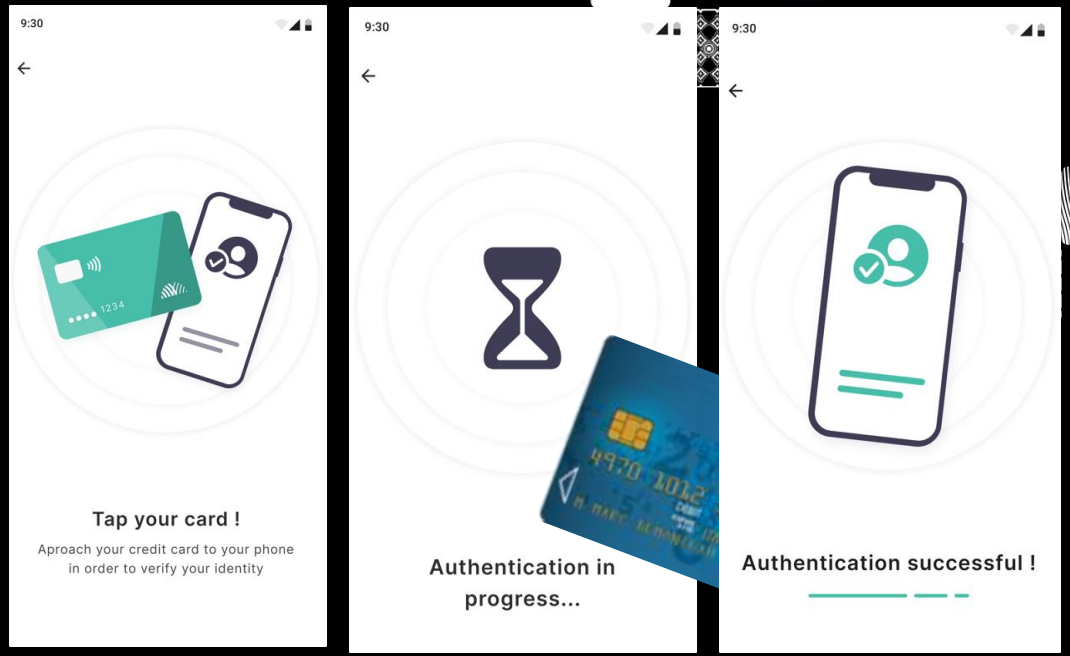
Sécurité & vie privée

- Phishing (smishing, vishing, quishing)
- Evaluation du niveau de sécu
- Stockage des données
- Vie privée

Taux de fraude paiement carte sans contact : 1€10 pour 10 000€

Taux de fraude paiement carte par internet : 16€ pour 10 000€

Conclusion

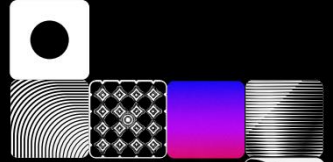


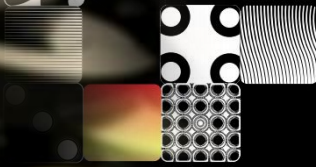
Pourquoi ne pas utiliser la carte bancaire pour sécuriser l’authentification Web?

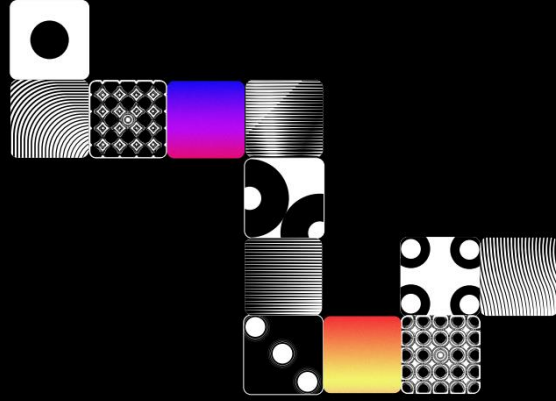
DEVFEST 2024 STRASBOURG

Application Android :

Merci pour vos feedbacks :







Et sur iOS ?

Framework

Core NFC

Detect NFC tags, read messages that contain NDEF data, and save data to writable tags.

iOS 11.0+ | iPadOS 11.0+ | Mac Catalyst 13.0+

Overview

Your app can read tags to give users more information about their physical environment and the real-world objects in it. Using Core NFC, you can read Near Field Communication (NFC) tags of types 1 through 5 that contain data in the NFC Data Exchange Format (NDEF). For example, your app might give users information about products they find in a store or exhibits they visit in a museum.

Your app can also write data to tags, and interact with protocol-specific tags such as ISO 7816, ISO 15693, FeliCa™, and MIFARE® tags.

Core NFC isn't available for use in app extensions, and it requires a device that supports Near Field Communication. To determine if support is available, check the `readingAvailable` class property before starting a reader session.

Topics

The historical bytes extracted from the Type A Answer To Select response.

Required

`var applicationData: Data?`

The application data bytes extracted from the Type B Answer To Request response.

Required

`var proprietaryApplicationDataCoding: Bool`

A Boolean value that indicates whether the application data follows proprietary data coding.

Required

Sending a Command

`func sendCommand(apdu: NFCISO7816APDU, resultHandler: (Result<NFCISO7816ResponseAPDU, any Error>) -> Void)`

Sends an application protocol data unit (APDU) to the tag and receives a response APDU.

`class NFCISO7816APDU`

An object representing an ISO 7816 application protocol data unit (APDU).

`struct NFCISO7816ResponseAPDU`

An object containing the response from the tag.

Instance Methods

`func sendCommand(apdu: NFCISO7816APDU, completionHandler: (Data, UInt8, UInt8, (any Error)?) -> Void)`

Sends an application protocol data unit (APDU) to the tag and receives a response APDU.

Required Default implementation provided.

QUICK READ • August 14, 2024

Developers can soon offer in-app NFC transactions using the Secure Element

Starting with iOS 18.1, developers will be able to offer NFC contactless transactions using the Secure Element from within their own apps on iPhone, separate from Apple Pay and Apple Wallet. Using the new NFC and SE (Secure Element) APIs, developers will be able to offer in-app contactless transactions for in-store payments, car keys, closed-loop transit, corporate badges, student IDs, home keys, hotel keys, merchant loyalty and rewards cards, and event tickets, with government IDs to be supported in the future.

Questions