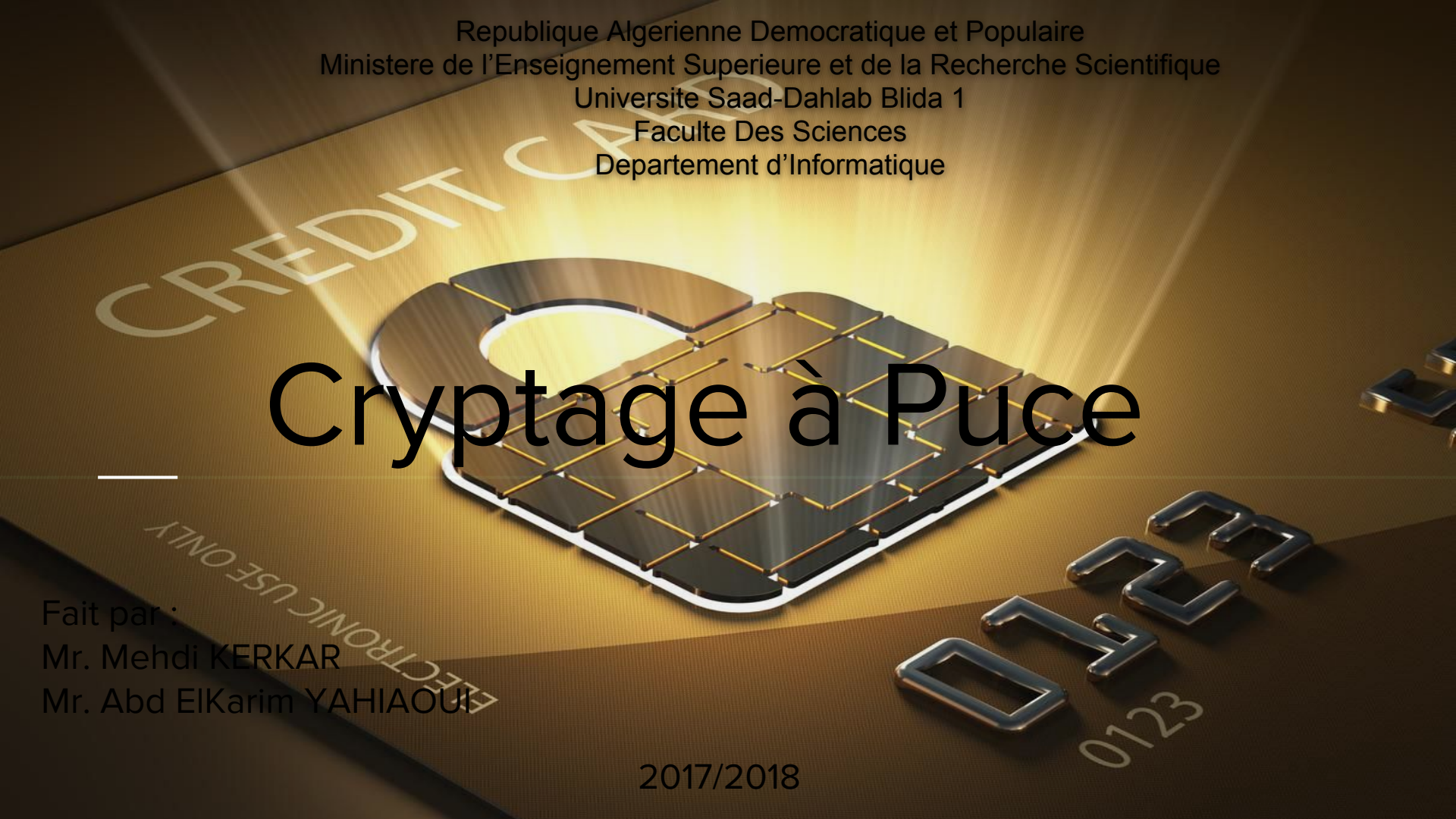
Republique Algerienne Democratique et Populaire
Ministere de l'Enseignement Superieure et de la Recherche Scientifique
Universite Saad-Dahlab Blida 1
Faculte Des Sciences
Departement d'Informatique



Cryptage à Puce

Fait par :
Mr. Mehdi KERKAR
Mr. Abd ElKarim YAHIAOUI

2017/2018

Sommaire

- Introduction
- Carte à puce
- Le standard EMV
- SDA
- Clonage
- DDA
- Attaque Relais
- Conclusion

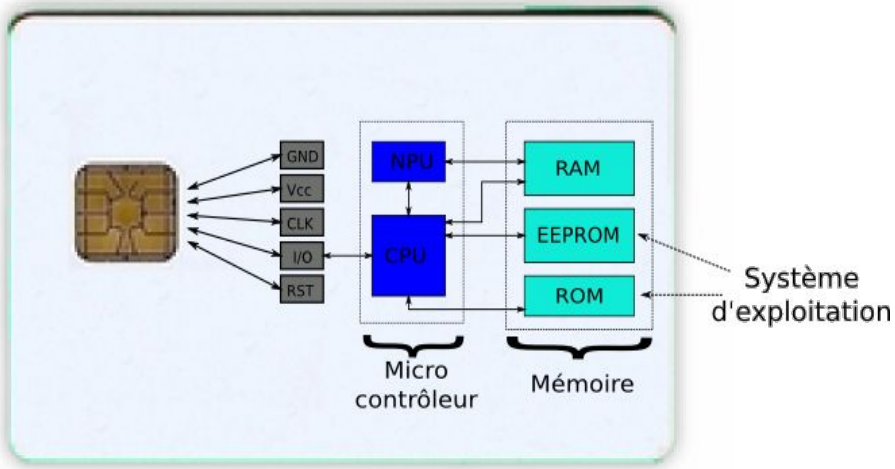
Qu'est-ce que le cryptage à puce ?

Pourquoi la carte à puce

La carte à puce a de multiples applications, à tel point qu'elle est devenue omniprésente dans notre environnement quotidien.

Aujourd'hui cette technologie est principalement utilisée comme moyen d'identification personnelle (dans le cas des badges d'accès, d'une Carte sim ou de la car ent, notamment dans le cas de la Carte bancaire.

- Ce circuit intégré peut se limiter à des circuits de (mémo
- Lecture avec équipements spécialisés et peut s'effectue



Quesque une carte à puce

De quoi se compose tel

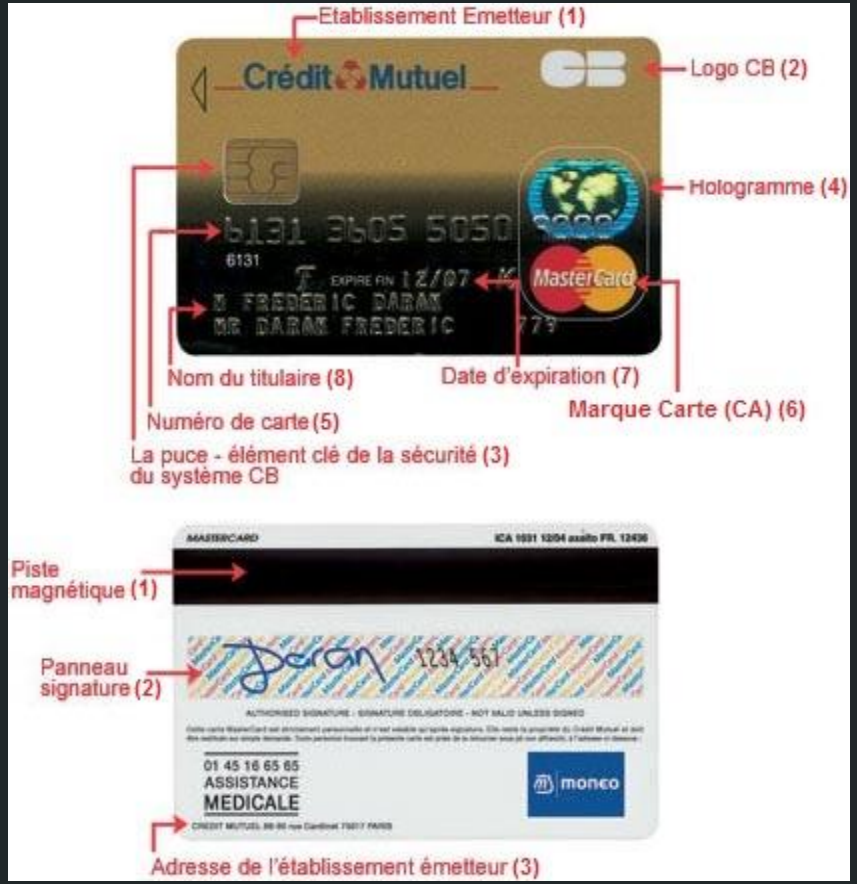
Les Données

Face :

1. Logo Banque Émettrice
2. Logo Carte
3. Puce EMV
4. Hologramme
5. Numéro de carte
6. Marque de la carte (CA)
7. Date Expiration
8. Nom Titulaire

Dos :

1. Piste Magnétique
2. Panneau Signature
3. Adresse Etablissement Émettrice



Normalisation parfaite

la normalisation concerne au moins 3 points:

- Des paramètres physiques : taille de la carte, position de la puce et ses contacts.
- Des paramètres électriques : tension d’alimentation, niveaux électriques utilisés.
- Des paramètres logiciels qui définissent le mode de dialogue avec la carte (commandes).

Standard EMV

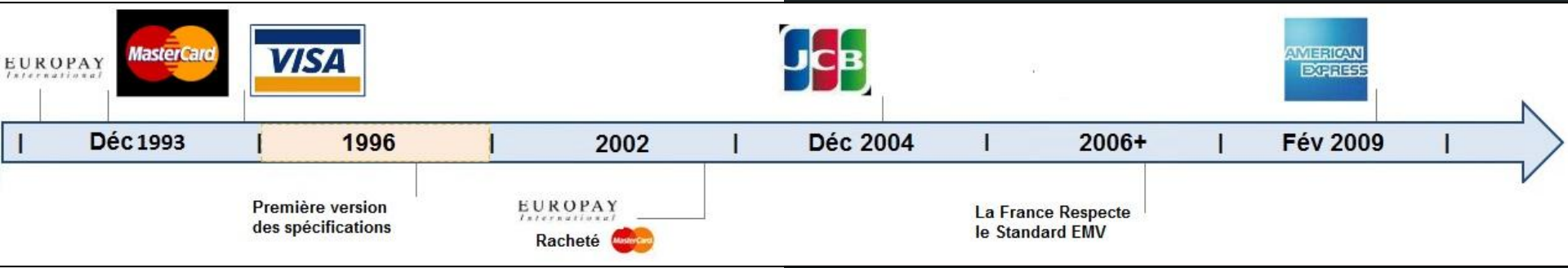
Standard des cartes de paiement depuis 1995

Organismes fondateurs :

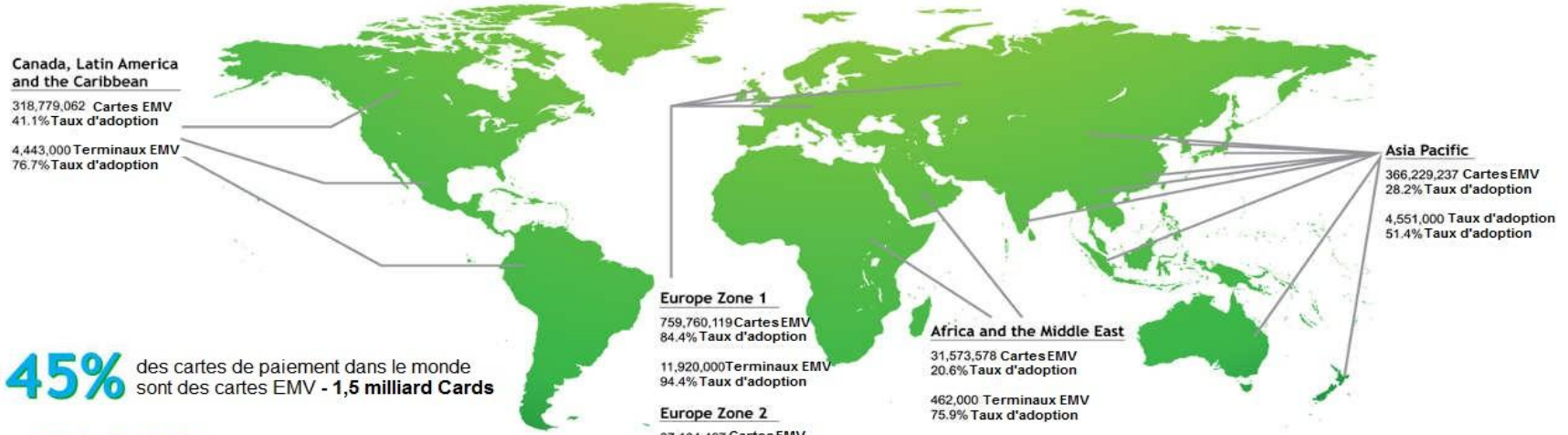
- **Europay** International ;
- **MasterCard** International ;
- **Visa** International ;

Rejoint par :

- le japonais **JCB** International ;
- l'américain **American Express**) ;



EMV par les Nombres



45% des cartes de paiement dans le monde sont des cartes EMV **- 1,5 milliard Cards**

76% des terminaux de paiement du monde sont EMV **- 21,9 millions de terminaux**

EMVCo™

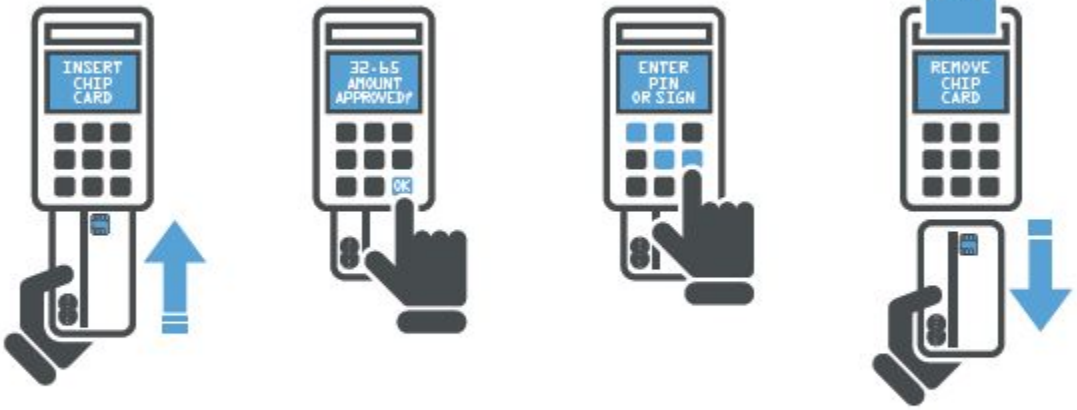
Voici,

Les buts EMV

1. Réduction de la contrefaçon de cartes, le vol et la perte.
2. Utilité à l'international.

Etape payment

COMMENT ÇA MARCHE



1. Insérez votre carte à puce dans un lecteur compatible avec les puces
2. Approuvez le montant
3. Suivez l'invite pour entrer votre code PIN ou pour signer
4. Retirez votre carte à puce lorsque vous y êtes invité

Acteurs du protocole EMV

- **La banque du client** : émetteur de la carte
- **Le client** : Carte bancaire
- **Le TPE ou le DAB** (Terminal de Paiement Electronique / Distributeur Automatique de Billets): marchand
- **Une autorité de certification** : CA

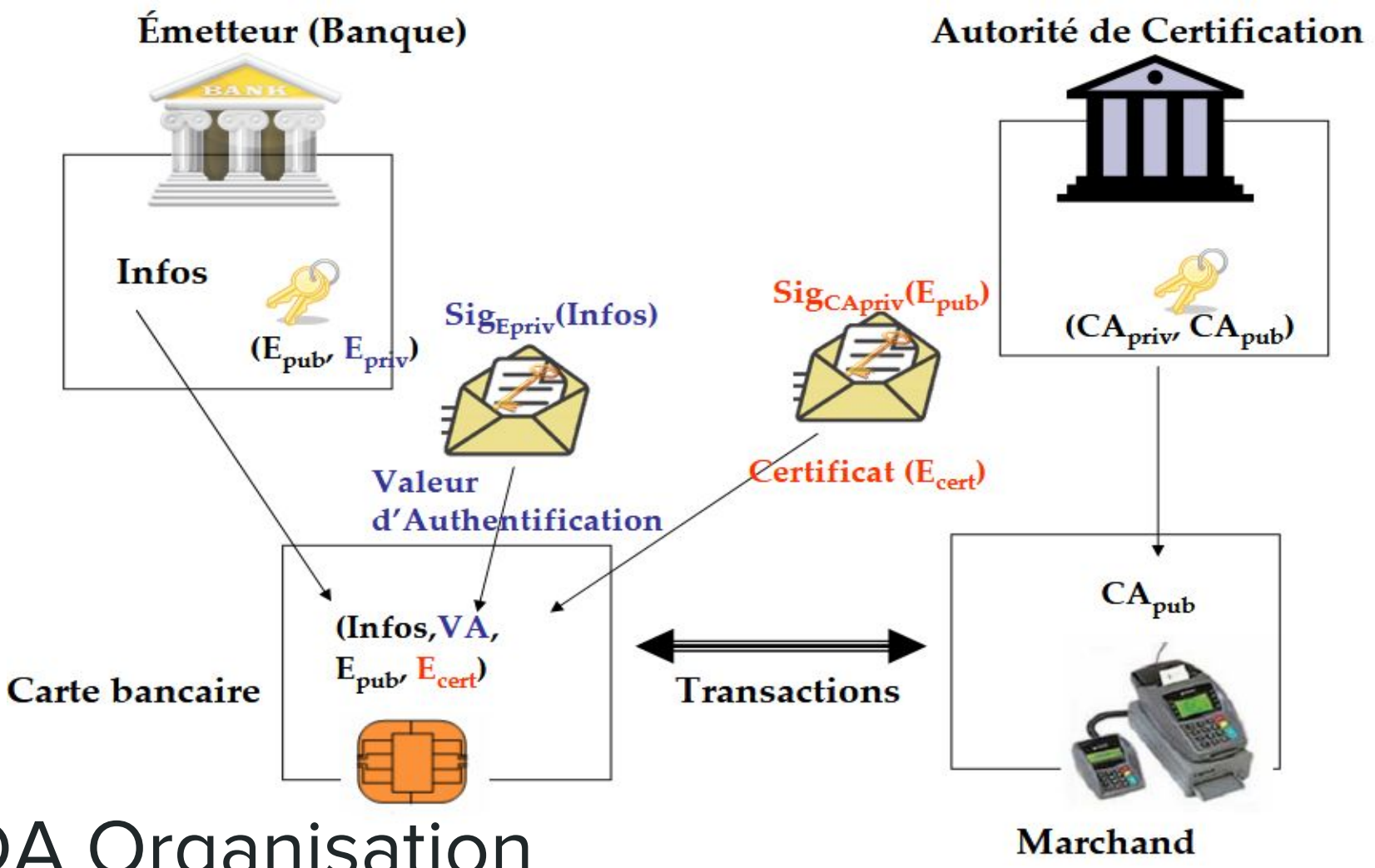
Mécanismes d'authentification

Processus SDA

Static Data Authentication consiste pour le terminal à vérifier une donnée signée mise dans la carte durant sa personnalisation

Processus DDA

Dynamic Data Authentication en plus d’un authentification statique, vérifie si la carte possède un secret délivré par l’émetteur de la carte



SDA Organisation

SDA Utilisation

$VA = Sig_{Epriv}(Infos)$

$E_{cert} = Sig_{CApriv}(E_{pub})$

(Infos, VA, E_{cert})

(Infos, VA, E_{cert})

(Infos, VA, E_{pub}, E_{cert})
Code PIN

RSA(E_{cert}, CA_{pub})=E_{pub}

CA_{pub}

RSA(VA, E_{pub})=Infos' ?= Infos

Demande du code PIN

Code PIN en clair

Carte bancaire

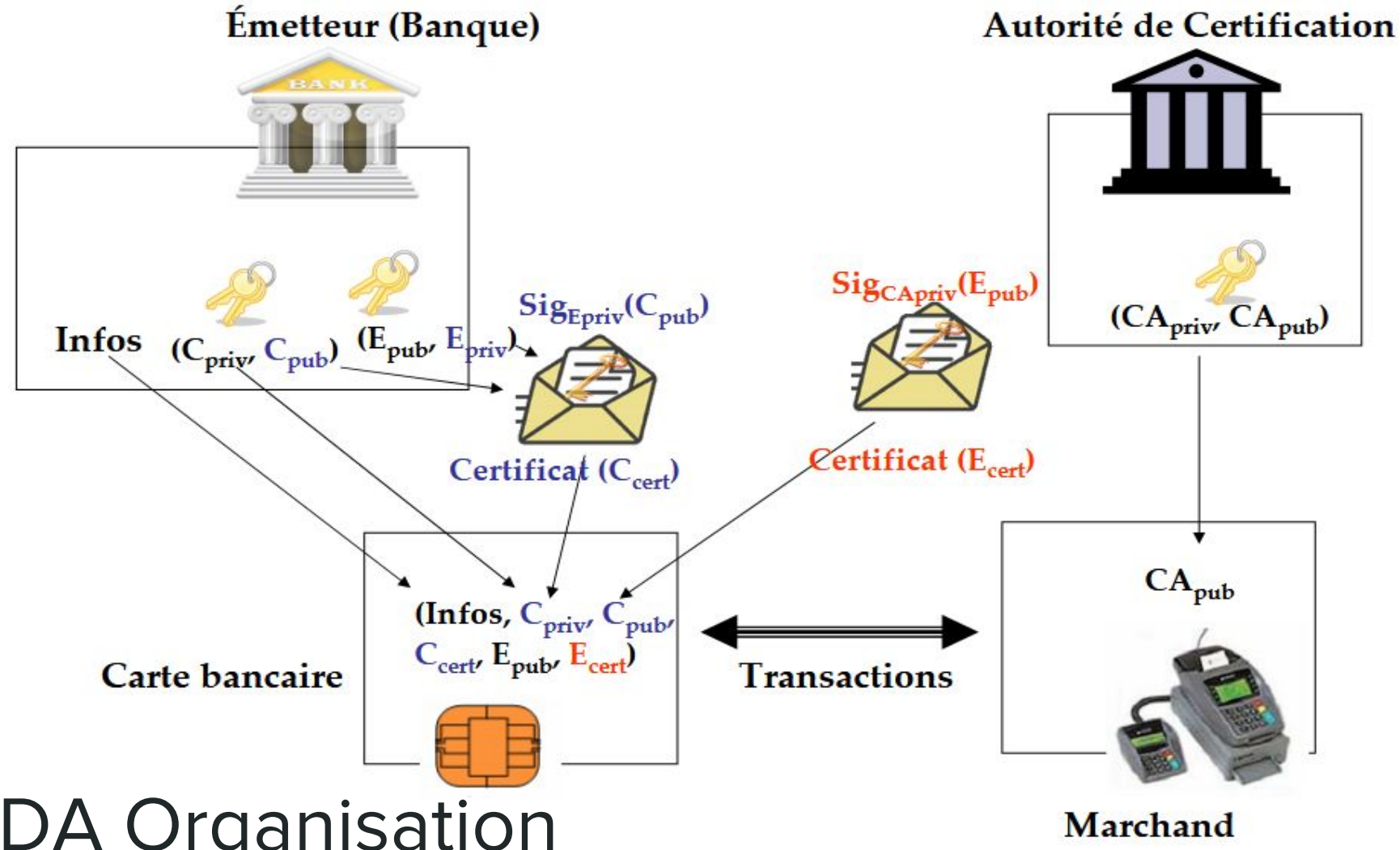
Marchand

Clonage et modification de la carte SDA (HDM)

- Les cartes clonées peuvent être découvertes par transaction en ligne autorisation, car la clé symétrique est difficile à cloner.
- La vérification du code PIN est effectuée par la carte, de sorte que les clones peuvent être programmé pour accepter tout (un Carte Oui).

Résultat: Si une carte SDA est volée, un faux peut être créé. accepté pour les transactions hors ligne, avec n'importe quel code PIN.

Corrections: Passer à DDA.



DDA Organisation

DDA Utilisation

$C_{cert} = Sig_{Epriv}(C_{pub})$

$E_{cert} = Sig_{CApriv}(E_{pub})$

(Infos, C_{cert}, E_{cert})

(Infos, C_{cert}, E_{cert})

T_{alea}

(Infos, C_{pub}, C_{priv}, C_{cert}, E_{pub}, E_{cert})
Code PIN

$Res = Sig_{Cpriv}(C_{alea}, T_{alea}), C_{alea}$

CA_{pub}

$RSA(E_{cert}, CA_{pub}) = E_{pub}$

$RSA(C_{cert}, E_{pub}) = C_{pub}$

$Décrypt(Res, C_{pub}) ?= C_{alea}, T_{alea}$

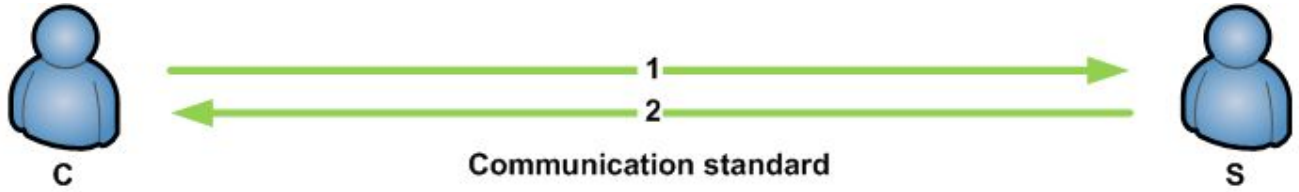
Demande du code PIN

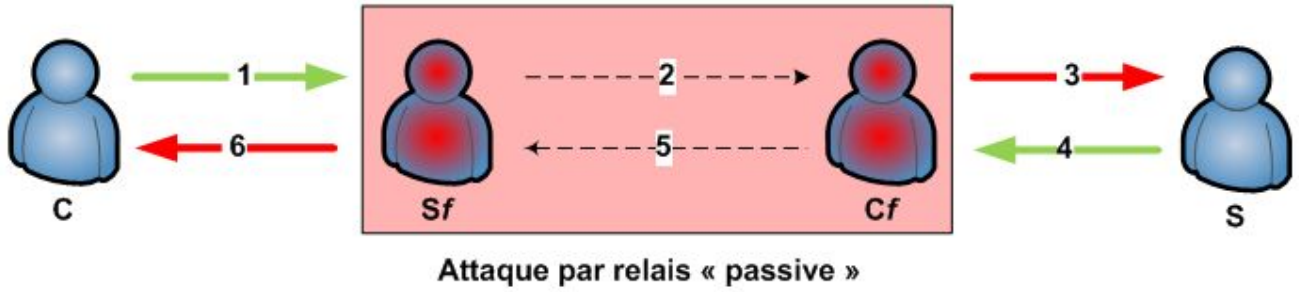
Carte bancaire

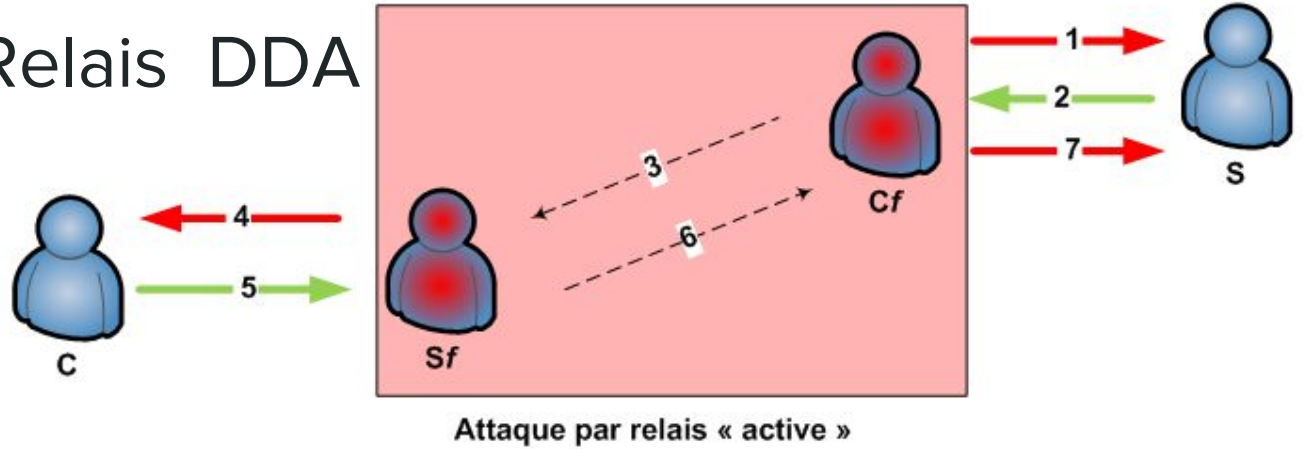
$Crypt_{Cpub}$(Code PIN, alea1, alea2)

Marchand

Attaque Relais DDA







Corrections: Passer à CDA.

Nous vous remercions Q/R

Pour télécharger les Slides

PowerPoint : cryptoPuce(5)MKAY.pdf
Réseau : ssi-master1
Browser IP : @ :8000

```
FileInputStream in = null;
try { in = new FileInputStream(dataFile);
    byte[] buf = new byte[2048];
    int len;
    while ((len = in .read(buf)) != -1) { // in.read(buf) will
    return the size of the read in lettesrs (-1 => when it reach
    the end of file)
        sign.update(buf, 0, len); // update have two prototypes,
        this one , the data in the buffer,  the secodn the offset
        (from where to start) and the last is the number of the
        bytes to use
    }
} finally {
    if ( in != null) in .close();
}

FileOutputStream out = null;
try {
    out = new FileOutputStream(outSignFile);
    byte[] signature = sign.sign();
    out.write(signature);
} finally {
    if (out != null) out.close();
}
```