

[Principe de la montétique] Correction de l'annale 2012-2013

Correction fusionnée avec celle de Quentin <3

Question A

- DAB : Distributeur automatique de billets
- GAB : Guichet automatique de banque
- TPE : Terminal de paiement électronique
- DAC : Distributeur Automatique de Carburant (?)
- HSM : Hardware Security module

Question B

Un paiement à distance est un paiement qui est réalisé sans que le commerçant ne voit le porteur et la carte. (e.g. Les paiements sur internet)

Tous les paiements qui ne se font pas avec un TPE

Question C

- Oui
- Oui
- Oui (*cf slide 34*)
- Oui (*cf slide 34*)
- Oui (*cf slide 32*)
- Non (*C'est la banque émettrice*)
- Oui (*cf slide 32*)
- Oui (*cf slide 33*)
- Non (*Émis par l'émetteur et signé par l'utilisateur*)

Question D (Slides 20-25)

1. Banque émettrice
2. Système de règlement
3. Banque acqureur
4. Système d'émission
5. Système de compensation
6. Système d'acquisition
7. Système d'acception
8. Porteur
9. Carte
10. TPE/DAB

Question E

Afin de concilier anonymat et traçabilité, qui sont *deux caractéristiques antagonistes*, les banques utilisent une *astuce législative* en disant qu'ils ont la traçabilité de la carte (*On sait quelle carte réalise une transaction*) mais *sans jamais prouver qui a utilisé la carte*. Ceci donne ainsi l'anonymat de l'utilisateur

Question F

Le cryptogramme CVx2 se trouve *à l'arrière de la carte* et se compose généralement de *3 chiffres*. Il est utilisé généralement dans les *paiements en ligne ou autrement dit à distance*.

Question G (cf slide 66)

- Oui
- Oui
- Oui
- Oui
- Non
- Non
- Non

Question 1

- 0.077 (Slide 128 en tout petit en bas)
- 130 (Slide 128 en tout petit en bas)
- 1 900 000 000 (puisque 2.637 Milliards fin 2013 #estimation)
- 100% (Slide 89)

Question J

Un HSM offre des *fonctions cryptographiques* et est considéré comme inviolable. Il offre des services comme la *génération*, le *stockage* et la *protection des clés cryptographiques*.

Question K

1. Le *TPE* ou le *DAB*
2. L'autorisation consiste à *vérifier* si le *porteur* a *le droit d'effectuer ou non une transaction*.
3. C'est un *type particulier d'autorisation* qui est utilisé dans quand on ne *connait pas à l'avance le montant de l'achat*. Dans ce cas on *demande une somme maximale* et on *réalise le paiement par la suite* (avec le vrai montant qui doit donc être inférieur à la demande). C'est le cas pour les *DAC*.

Question 1

Ce projet se nomme *SEPA* pour *Single Euro Payments Area*

Question M

Le code PIN de la carte est stocké *à l'intérieur de la carte sous forme chiffrée.*

Question N

- [illegible]

- Non
- Non
- Oui
- Non
- Oui
- Non (*cf slide 58*)