

OBJECTIFS PÉDAGOGIQUES

Acquérir les bases cryptographiques
Les appliquer à la monétique



PUBLIC CONCERNÉ

Services monétiques, banque à domicile, back-office, réseaux d'autorisation, services de gestion des clés.

PRÉ-REQUIS

Connaissance du fonctionnement actuel des systèmes monétiques.

COMPÉTENCES VISÉES

Maîtriser les fondamentaux de la cryptographie monétique.



DÉROULEMENT DE LA FORMATION

Cours théorique en distanciel (classe virtuelle).

MODALITÉS D'ÉVALUATION

Exercices pratiques et mises en situation (validation des acquis au cours et à la fin de la formation).

CALENDRIER 2023

1^{er} et 2 juin 2023 (distanciel)

HORAIRES

9h30 - 13h00

Pauses (durée : 15 minutes) : 11h

TARIFS

1 850 € HT / par participant.

Tarif à partir de la 3^{ème} inscription à la même session : 1 480 € HT



ANIMATEUR

Guillaume DABOSVILLE

Expert en cryptographie et sécurité, Guillaume a commencé sa carrière chez deux encarteurs de renommée mondiale pour lesquels il a conçu et implémenté la sécurité des cartes à puce. Il rejoint CB en septembre 2017 en qualité d'expert Technique Sécurité des Systèmes d'Information. Dans le cadre de ses fonctions actuelles, Guillaume a contribué à l'élaboration d'une nouvelle méthodologie d'évaluation sécuritaire des cartes bancaires. Cette méthodologie d'évaluation a été mise à jour en 2021 pour traiter spécifiquement le cas des cartes bancaires biométriques présentées à l'agrément CB.

Guillaume est également le chef de projet de la migration du système CB vers l'AES, en remplacement des clés TDEA actuelles. Ce projet inclut notamment la mise à jour des clés de raccordement de membres à l'e-RSB (réseau d'interbancaire opéré par la STET). Enfin Guillaume a le jeton de preuve CB pour le Directory Server (3-D Secure).

PROGRAMMES

1^{ère} MATINÉE :

- 1 - Introduction : l'histoire de la cryptographie
- 2 - Terminologie et concepts
 - Cryptographie, cryptologie et cryptanalyse
 - Les secrets
 - La sécurisation
 - Étude de cas : la transaction EMV
- 3 - Cryptographie symétrique
 - Une première intuition
 - Chiffrement à clé secrète (TDES, AES ...)
 - Signature à clé secrète
- 4 - Limites du chiffrement symétrique (1^{ère} partie)
 - Facteur cleptomane : étude de cas d'un échange de secret

2^{ème} MATINÉE :

- 5 - Limites du chiffrement symétrique (2^{ème} partie)
 - Échange d'un secret à distance : le protocole Diffie-Hellman
- 6 - Systèmes à clé publique
 - Chiffrement, signature, authentification
 - Systèmes asymétriques : RSA, courbes elliptiques
- 7 - Paramètres de sécurité
 - Choix des algorithmes, longueurs de clés
- 8 - Conclusion de la formation

