Directive du Bureau du Chef de l'Information : TI 10.09	Publié : 04/2019
Chapitre : Sécurité des réseaux	Dernière révision : 01/2024
Objet : **COMMERCE ÉLECTRONIQUE**	

1 DIRECTIVE

1.01 Toutes les applications de commerce électronique qui s'appuient sur l'échange de messages au moyen d'un réseau public doivent fournir des contrôles de sécurité qui satisfont aux exigences suivantes en matière de sécurité :

- Protection des renseignements personnels et confidentialité. L'accès à l'information pour les messages contenant une transaction électronique doit être strictement réservé aux parties autorisées;
- Intégrité. Chaque message doit être protégé contre toute modification et contre tout piratage lors de sa transmission de la partie expéditrice à la partie destinataire. Toute modification non autorisée de ce type doit être repérée;
- Authentification. Les deux parties à chaque transaction doivent fournir des informations d'identification vérifiables pour chaque message;
- Non-répudiation. Ni l'une ni l'autre des parties à une transaction électronique achevée ne peuvent nier leur rôle dans la transaction.

2 OBJET

2.01 La présente directive a pour objet d'assurer que toutes les transactions de commerce électronique effectuées au moyen d'un réseau public respectent les renseignements personnels et la confidentialité des clients, garantissent l'exactitude et l'intégrité des transactions financières, authentifient toutes les parties à une transaction et empêchent la répudiation d'une transaction achevée.

3 PORTÉE

3.01 La présente directive s'applique à toutes les applications employées pour réaliser des transactions financières au moyen d'un réseau public, y compris le courrier électronique.

4 RESPONSABILITÉ

4.01 Il incombe à **Planification de la TI** de s'assurer que l'infrastructure appropriée (c.-à-d. matérielle et logicielle) soit établie pour prendre en charge les contrôles requis pour le commerce électronique.

4.02 Il incombe à **Développement des applications de la TI** et à **Soutien technique de la TI** de s'assurer que toutes les applications de commerce électronique utilisent l'infrastructure de commerce électronique approuvée par l'organisation.

5 DÉFINITIONS

5.01 Un **« réseau public »** est tout chemin de communication qui offre le libre accès

à tout membre du public. Cela englobe tous les systèmes de communication au moyen d'Internet et sans fil.

5.02 "**PKI**" (**Public Key Infrastructure**) L'**« ICP » (infrastructure à clé publique)** est un cadre permettant d'échanger des informations en toute sécurité grâce à des méthodes de chiffrement fondées sur la cryptographie à clé publique, à savoir une méthode de chiffrement qui utilise deux clés de chiffrement — une clé publique et une clé privée — pour protéger les messages transmis entre deux parties. Dans ce modèle, l'expéditeur d'un message utilise la clé publique choisie par le destinataire pour chiffrer le message. La clé privée correspondante du destinataire est la seule clé qui peut déchiffrer le message.

5.03 L'**« algorithme de hachage d'un message »** est une formule de calcul d'un seul chiffre (le « chiffre de hachage ») d'un message plus long ou d'une série de textes afin que toute modification du message original modifie selon toute probabilité la valeur du chiffre de hachage correspondant.

5.04 La **« signature numérique »** est une signature qui authentifie l'identité de l'expéditeur d'un message. Une signature numérique ne peut pas être imitée par un imposteur en puissance et peut être horodatée automatiquement. En y intégrant un hachage de message chiffré, la signature peut également garantir que le message original de l'expéditeur n'a pas été modifié pendant sa transmission et empêcher la répudiation ultérieure du message par l'expéditeur.

5.05 Le **« certificat numérique »** est un identificateur électronique utilisé pour établir les informations d'identification du propriétaire du certificat dans Internet. Il est délivré par une autorité de certification (AC) indépendante, associée à des objectifs de sécurité spécifiques (comme des applications commerciales et des interactions d'organismes gouvernementaux). GeoTrust, GlobalSign, Thawte et VeriSign Inc sont des exemples d'AC commerciales bien connues.

6 DIRECTIVES CONNEXES

BCI TI 3.02 – Développement et mise en œuvre d'applications

BCI TI 9.06 – Cryptage des données