[SIPS]	Consignes de sécurité pour la protection du fichier certificat	Atos Worldline

Informations importantes relatives à votre certificat :

Le certificat commerçant est une clef de sécurité unique permettant à chaque commerçant de communiquer de manière chiffrée avec les serveurs sécurisés d'Atos Worldline.
Aussi, le commerçant est responsable de sa conservation.

Le certificat vous est délivré de manière sécurisée, il vous appartient d'en assurer la conservation, et ainsi :

- D'en restreindre l'accès sur votre serveur
- De le sauvegarder de manière chiffrée
- De ne jamais le copier sur un disque non sécurisé
- De ne jamais l'envoyer (e-mail, courrier) de manière non sécurisée

La compromission d'un certificat et son utilisation par un tiers malveillant perturberait le fonctionnement normal de la boutique, et pourrait notamment :

- générer des transactions non justifiées sur le site du commerçant
- provoquer des opérations de caisse injustifiées (des remboursements par exemple)

Aussi, en cas de compromission de certificat, le commerçant est tenu d'en demander au plus vite la révocation puis le renouvellement à notre service clients.

Pour vous aider à conserver votre certificat de manière sécurisée, vous trouverez ci-après quelques règles à respecter impérativement.

REGLE IMPERATIVE : Protection vos accès FTP

Toutes les consignes citées ci-dessous seront sans intérêt si un pirate a facilement accès au serveur FTP ou aux fichiers du site Web marchand. Il est donc important de le protéger par un mot de passe qui respecte toutes les règles de sécurité, donc qu'il soit suffisamment compliqué pour ne pas être deviné ou retrouvé. Il convient par ailleurs de ne point le divulguer et il est fortement conseillé de le modifier régulièrement.

OPTION 1 : Installation du certificat dans un répertoire non internet

Cette première option est la plus sûre pour résoudre les problèmes de paramétrage de sécurité.
Elle consiste à créer un répertoire non accessible par un navigateur web, donc placé à la racine du serveur (au dessus du répertoire /www/) et d'y installer le certificat.

OPTION 2 : Mesures de protection et de gestion d'accès au fichier

Si la première option est impossible (cas d'hébergements mutualisés par exemple), d'autres solutions de sécurisation du certificat sont possibles :

Ce document est propriété d'Atos Worldline. Il ne peut être reproduit ou divulgué sans autorisation écrite préalable.

- **Protection globale bloquant la lecture des répertoires sur site internet (type Apache)**

  Mettre un fichier .htaccess à la racine du site internet contenant une interdiction d'indexation pour toute requête de type POST ou GET.

- **Protection de répertoire par password (type Apache)**

  Vous pouvez demander une authentification par password pour permettre l'accès à certains répertoires. Pour cela il convient de créer 2 types de fichiers : .htaccess et .htpasswd

  Le fichier **.htaccess** est à placer à la racine du répertoire que vous souhaitez protéger. Il contient des directives d'authentification et le chemin d'accès au fichier .htpasswd contenant les couples user/password.

  Le fichier **.htpasswd** doit être installé dans un répertoire non accessible par un navigateur web (au dessus du répertoire /www/).

- **Blocage des robots indexeurs**

  Afin d'éviter l'indexation par les robots des répertoires, il convient de définir un fichier **robots.txt** directement interprétable par les robots indexeurs (Google…).

  Ce fichier permet d'interdire le référencement du contenu d'un répertoire entier en une seule opération. Il suffit donc d'y indiquer le répertoire où est installé le certificat et de lui attribuer une directive « Disallow ».

- **Restriction des droits du fichier**

  Pour les commerçants sous IIS (serveur http de Microsoft), le panneau contrôle web permet de bloquer en lecture/écriture l'accès à tous les répertoires du site internet. Il convient donc de demander à l'hébergeur de configurer les droits d'accès du ou des répertoires à protéger.

  Toutefois, la protection du répertoire peut ne pas être suffisante. Mettre les droits r--r----- sur le fichier certif devrait permettre de ne pas pouvoir afficher son contenu si quelqu'un cherche à y accéder directement.

Ce document est propriété d'Atos Worldline. Il ne peut être reproduit ou divulgué sans autorisation écrite préalable.