Bulletin Marketing

Norme FIPS 140-2 et technologie de disque avec autochiffrement

Questions fréquemment posées (FAQ)

Que signifie la mention FIPS 140-2 ?

FIPS (Federal Information Processing Standard) 140-2 est une norme établie par le gouvernement des États-Unis relative au chiffrement et aux conditions de sécurité à respecter dans la conception des produits informatiques destinés à traiter des données *sensibles*, mais non confidentielles.

Quelles sont les exigences de la norme FIPS 140-2 ?

Cette norme vise à garantir que les produits mettent en œuvre des pratiques de sécurité saines, à savoir des méthodes et des algorithmes de chiffrement puissants et approuvés. Elle précise également comment autoriser des personnes et des processus à utiliser le produit et comment concevoir les modules et les composants de manière à sécuriser leurs interactions avec d'autres systèmes.

Pourquoi le chiffrement est-il nécessaire ?

Les disques durs sont souvent retirés des systèmes (retour sous garantie, réparation, fin de contrat de location, réutilisation ou revente), perdus ou volés. Dans de tels cas, les données non protégées qu'ils contiennent ne sont plus sous contrôle et l'entreprise s'expose à des pertes en termes de bénéfices, de parts de marché et de confiance de la part des clients. L'entreprise peut en outre faire l'objet de sanctions civiles pour violation des lois sur la confidentialité des données. Cela peut s'avérer catastrophique pour une organisation, notamment s'il s'agit d'une PME.

- Selon les estimations de Seagate, 50 000 disques, contenant des téraoctets d'informations, sont extraits des centres de traitement des données *quotidiennement.*
- Selon IBM, 90 % des disques renvoyés sous garantie contiennent des données lisibles.

D'après des experts du secteur, tels que le Ponemon Institute, le coût moyen des failles de sécurité augmente chaque année. En 2008, il s'élevait à 6,6 millions de dollars en moyenne, soit 202 dollars par enregistrement compromis.[1]

Selon le Ponemon Institute, 81 % des ordinateurs portables contiennent des données sensibles et 10 % sont perdus ou volés au cours de leur cycle de vie. En outre, on estime à 12 000 le nombre d'ordinateurs portables perdus ou volés chaque semaine uniquement

[1] Étude du Ponemon Institute intitulée « *2008 Annual Study: U.S. Cost of a Data Breach* », février 2009, www.ponemon.org, telle que citée dans l'article « *Data-breach costs rising, study finds* » d'Ellen Messmer publié dans Network World, 02/02/09.

Norme FIPS 140-2 et technologie de disque avec autochiffrement

Questions fréquemment posées

dans les aéroports des États-Unis. Pour une entreprise, la perte d'un ordinateur portable contenant des données sensibles non chiffrées coûte 50 000 dollars en moyenne. Dans les cas extrêmes, ces coûts peuvent avoisiner un million de dollars.[2]

Quels sont les différents niveaux associés à la norme FIPS 140-2 ?

La norme FIPS 140-2 définit quatre niveaux de sécurité. Chaque produit est certifié pour un niveau de sécurité spécifique indiqué sur le certificat FIPS 140-2 qui lui est apposé.

- **Le niveau 1**, habituellement attribué aux produits qui effectuent un chiffrement purement logiciel, pose des conditions très limitées en matière de sécurité. Le produit doit être constitué exclusivement de composants adaptés à un *environnement de production* et offrir une protection contre les failles de sécurité les plus évidentes.
- **Le niveau 2** exige une authentification basée sur les *rôles* (l'authentification des divers utilisateurs n'est pas obligatoire). Il requiert également la capacité de *détecter* les manipulations physiques via des verrouillages physiques ou des plombs permettant de les constater.
- **Le niveau 3** inclut la *résistance* aux manipulations physiques par désassemblage ou modification, afin de rendre le piratage extrêmement difficile. En cas de manipulation, le périphérique doit être en mesure d'effacer les paramètres de sécurité critique. Le niveau 3 requiert également la gestion des clés et une protection cryptographique robuste, l'authentification basée sur l'*identité* et la séparation physique ou logique des interfaces d'entrée et de sortie des *paramètres de sécurité critique*.
- **Le niveau 4** impose une protection avancée contre les manipulations. Il est conçu pour les produits fonctionnant dans des environnements non protégés physiquement.

Quel niveau de certification FIPS 140-2 la société Seagate a-t-elle obtenu ?

Les périphériques de stockage Seagate® avec autochiffrement ont obtenu un certificat FIPS 140-2 de niveau 2.

Pourquoi la société Seagate a-t-elle obtenu une certification FIPS 140-2 de niveau 2 ?

De plus en plus d'organisations souhaitent chiffrer leurs données au repos afin de se protéger en cas de perte ou de vol. La certification FIPS 140-2 de niveau 2 est un gage de sécurité et de qualité pour tous les acheteurs. Elle atteste que les disques Seagate avec autochiffrement FIPS respectent les exigences du gouvernement fédéral des États-Unis en matière de produits de sécurité.

Quels types de produit la norme FIPS 140-2 couvre-t-elle ?

La norme FIPS 140-2 s'applique à tout produit susceptible de stocker ou de transmettre des données sensibles. Cela inclut des matériels tels que périphériques de cryptage des liens, disques durs, disques Flash ou autres supports de stockage amovibles. Les logiciels qui chiffrent les données transmises ou stockées y sont également inclus.

Un tel niveau de sécurité est-il vraiment nécessaire ? Le mot de passe de système d'exploitation n'est-il pas suffisant ?

Les dispositifs de sécurité du système d'exploitation tels que le mot de passe peuvent aisément être contournés. Il suffit de retirer un disque dur et de le monter sur un autre ordinateur. Même les mots de passe BIOS de disque dur ATA montrent leur vulnérabilité lorsqu'ils ne sont pas utilisés avec un disque avec autochiffrement Seagate ou équivalent. En revanche, le chiffrement des données sur le disque dur ou sur un support de stockage est une méthode de protection largement éprouvée.

Quelles organisations ou entreprises exigent la conformité à la norme FIPS 140-2 ?

Aux États-Unis, le NIST (National Institute of Standards and Technology) demande à toutes les administrations fédérales d'utiliser des produits certifiés FIPS 140-2 de niveau 2 pour sécuriser les données dites *sensibles mais non confidentielles* stockées dans les systèmes informatiques et de télécommunication (y compris les systèmes vocaux).[3] Au Canada, le CSE (Communications Security Establishment) demande aux administrations fédérales d'utiliser des modules cryptographiques certifiés FIPS 140-2 de niveau 2 pour sécuriser les données dites *Informations protégées*

[2] Étude Intel intitulée « Stolen Laptops Cost to Business, eWeek », 23 avril 2009 ; Étude du Ponemon Institute, avril 2009.

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html

Norme FIPS 140-2 et technologie de disque avec autochiffrement

Questions fréquemment posées

Conforme FIPS 140-2

(A ou B) stockées dans les systèmes informatiques et de télécommunication (y compris les systèmes vocaux). La certification FIPS 140 est également indispensable pour faire figurer un produit cryptographique dans la liste des produits informatiques avalisés par le gouvernement canadien.[3] Au Royaume-Uni, l'institution Communications-Electronics Security Group recommande l'utilisation de modules cryptographiques estampillés « FIPS 140 Validated ».[4]

Des sociétés civiles du monde entier sont également tenues de se conformer à la norme FIPS 140-2 lorsqu'elles travaillent pour des organismes gouvernementaux aux États-Unis, au Canada ou au Royaume-Uni qui requièrent un chiffrement respectant cette norme. Enfin, de plus en plus de sociétés commerciales à travers le monde, notamment dans les domaines de la finance, de la santé et des marchés verticaux liés à l'infrastructure (sécurité nationale), exigent la conformité à la norme FIPS 140-2. Ces entreprises ont opté pour la norme la plus stricte en matière de protection des données. Elles acceptent la rigueur exigée par la certification FIPS-140, elles estiment que l'application de cette norme est souhaitable et elles ont choisi de s'y conformer pour leurs propres opérations de chiffrement.

Qu'est-ce que la certification FIPS 140-2 ?

La certification FIPS 140-2 est un programme d'évaluation et de validation permettant de vérifier qu'un produit respecte la norme FIPS 140-2. Le NIST a élaboré le programme CMVP (Cryptographic Module Validation Program) afin d'évaluer les caractéristiques des produits par rapport à ces exigences.

Comment obtient-on une certification FIPS 140-2 ?

Pour obtenir le certificat FIPS 140-2 Validated™, un produit doit respecter les caractéristiques de mise en œuvre et de conception établies. Il est ensuite testé et approuvé par l'un des 13 laboratoires indépendants agréés par le NIST.

Quel est le numéro de la norme FIPS 140 en vigueur actuellement ?

Les publications FIPS 140 numérotées constituent une série de normes de sécurité définissant les caractéristiques des modules cryptographiques. L'édition FIPS 140-1 publiée en 1994 a été remplacée par l'édition FIPS 140-2 qui est la norme en vigueur depuis 2001. L'édition FIPS 140-3 est une nouvelle version de la norme en cours d'élaboration depuis 2005. Un avant-projet a été publié en décembre 2009, mais il ne remplacera pas l'édition FIPS 140-2 avant un an, voire plus.

Existe-t-il une liste des produits certifiés FIPS 140-2 Validated ?

Le NIST répertorie les produits commercialisés qui ont obtenu le certificat FIPS 140-2 Validated.
Vous trouverez cette liste sur la page : http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

En quoi la norme FIPS 140-2 est-elle importante pour les partenaires commerciaux de Seagate ?

Les partenaires commerciaux de Seagate peuvent utiliser la certification FIPS 140-2 comme argument marketing attestant de qualités et de fonctionnalités de sécurité critique que d'autres produits ne fournissent pas. Il s'agit d'un élément de différenciation essentiel pour des acheteurs toujours plus attentifs à la sécurité.

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html
[4] www.cesg.gov.uk/

www.seagate.com
Appel gratuit : 00 8004 SEAGATE (732 4283)
(Appel payant : 001 405 324 4714)

AMÉRIQUES Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, États-Unis, +1 831 438 6550
ASIE/PACIFIQUE Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapour 569877, +65 6485 3888
EUROPE, MOYEN-ORIENT ET AFRIQUE Seagate Technology SAS 16-18 rue de Dôme, 92100 Boulogne-Billancourt, France, +33 (0)1 41 86 10 00

© 2010 Seagate Technology LLC. Tous droits réservés. Imprimé aux États-Unis. Seagate, Seagate Technology et le logo Wave sont des marques déposées de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. Le logo FIPS est un certificat délivré par le NIST (National Institute of Standards and Technology) qui ne saurait engager la responsabilité du NIST ou des gouvernements des États-Unis et du Canada concernant les produits certifiés. Les autres noms de produits cités sont des marques ou des marques déposées de leurs propriétaires respectifs. L'exportation ou la réexportation de matériels ou de logiciels avec chiffrement peut être réglementée par les ministères américains du commerce, de l'industrie et de la sécurité (pour plus d'informations, consultez la page www.bis.doc.gov). L'importation et l'utilisation de tels matériels et logiciels en dehors des États-Unis peuvent faire l'objet de contrôles. Seagate se réserve le droit de modifier sans préavis les offres ou les caractéristiques de ses produits. MB605.1-1007FR, juillet 2010