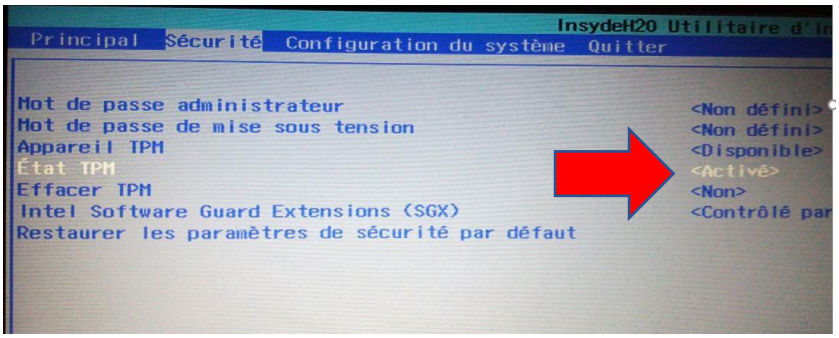
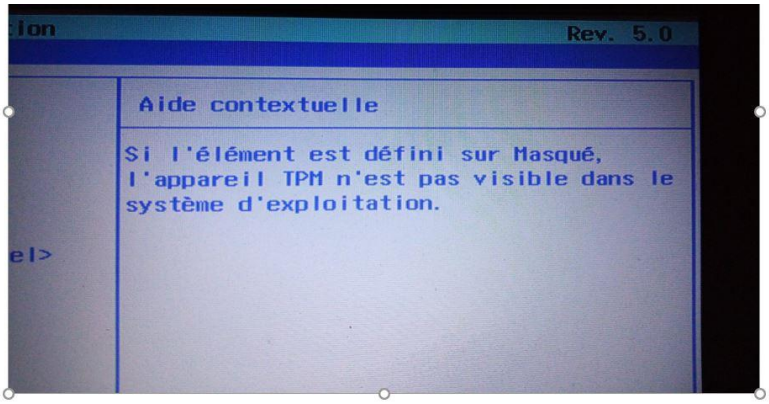
Microsoft définit ce que devra être un PC sécurisé sous Windows 10

Fiche réalisée par Rémi (Nov 2019) à partir des sites ci dessous :

En résumé : A partir des dernières versions de w10, le démarrage d'un ordinateur à partir d'un dvd ou d'une clé Usb n'est pas possible sans désactiver le **module TPM** dans l'UEFI. C'est une manip réservée aux personnes … qui connaissent un peu !!!





[Microsoft définit la sécurité sur Ordinateur]

Grâce au chiffrement et à des fonctions de virtualisation, les machines Windows 10 peuvent être mieux protégées contre les attaques. Module TPM.

Ce document décrit dans le détail quels sont les standards à employer pour concevoir un appareil hautement sécurisé sous Windows 10. Autrement, avec ces recommandations, Microsoft dessine les futurs ordinateurs qui feront tourner son système d'exploitation et que nous utiliserons demain. On y découvre des PC plus sûrs, grâce à différentes couches matérielles.

C'est pourquoi Microsoft commence par définir le matériel en six catégories comprenant le processeur, son architecture, la mémoire (8 Go au minimum), la virtualisation, le module TPM et la vérification du démarrage. **Lire la suite sur le site ci-dessus.**

Recommandations relatives au module de plateforme sécurisée (TPM)

https://docs.microsoft.com/fr-fr/windows/security/

S'applique à : Windows10

Cette rubrique fournit des recommandations concernant la technologie du module de plateforme sécurisée (TPM) pour Windows 10.

Pour consulter une description générale des fonctionnalités du TPM, voir la rubrique Vue d'ensemble de la technologie de module de plateforme sécurisée.

Conception et mise en œuvre du TPM

Traditionnellement, les TPM sont des puces discrètes gravées sur la carte mère d'un ordinateur. Ces implémentations permettent au fabricantOEM de l'ordinateur d'évaluer et de certifier leTPM séparément du reste du système. Même si les implémentations de TPM discrets restent courantes, elles peuvent être problématiques pour des appareils intégrés de petite taille ou consommant peu d'énergie. Certaines implémentations plus récentes de TPM intègrent la fonctionnalitéTPM dans le même chipset que d'autres composants de la plateforme tout en fournissant une séparation logique semblable à celle des puces de TPM discrètes.

Les TPM sont passifs: ils reçoivent des commandes et renvoient des réponses. Pour tirer pleinement parti des avantages d'un TPM, l'OEM doit intégrer avec soin le matériel système et le microprogramme avec le TPM pour lui envoyer des commandes et réagir à ses réponses. Les TPM ont été initialement conçus pour garantir sécurité et confidentialité au propriétaire et aux utilisateurs d'une plateforme, mais les versions plus récentes offrent les mêmes avantages de sécurité et de confidentialité au matériel système proprement dit. Toutefois, avant de pouvoir être utilisé pour les scénarios avancés, un TPM doit être approvisionné. Windows10 approvisionne automatiquement un module TPM. Cependant, si l'utilisateur prévoit de réinstaller le système d'exploitation, il lui faudra peut-être effacer ce module au préalable afin que Windows puisse en tirer pleinement parti.

Le module de plateforme sécurisée 2,0 n'est pas pris en charge dans les modes hérité et CSM du BIOS. Le mode BIOS doit être configuré pour les appareils dotés du module de plateforme 2,0 sécurisée en natif uniquement. Les options d'héritage et de compatibilité des modules de prise en charge (CSM) doivent être désactivées. Pour une sécurité supplémentaire, activez la fonctionnalité de démarrage sécurisé.

Les systèmes d'exploitation installés sur le matériel en mode hérité empêchent le système d'exploitation de démarrer lorsque le mode BIOS devient UEFI. Utilisez l'outil MBR2GPT avant de modifier le mode BIOS qui prépare le système d'exploitation et le disque pour prendre en charge UEFI.

TPM discret, intégré ou microprogramme?

Il existe trois options d'implémentation pour les TPM:

- Une puce TPM discrète sous forme de composant indépendant dans son propre package de semi-conducteurs
- Solution TPM intégrée, utilisant un matériel dédié intégré dans un ou plusieurs packages de semi-conducteurs avec, mais généralement séparée, d'autres composants
- Solution TPM sous forme de microprogramme, exécutant le module TPM dans le microprogramme dans le mode d'exécution approuvé d'une unité de calcul d'usage général

Windows utilise n'importe quel TPM compatible de la même manière. Microsoft ne fournit pas de recommandation concernant la méthode d'implémentation du TPM. Il existe une vaste gamme de solutions TPM disponibles pour répondre à tous les besoins.

Dans quelle mesure le TPM est-il important pour les utilisateurs?

Pour les utilisateurs finaux, le TPM est en arrière-plan, mais il est malgré tout très important. Le TPM est actuellement utilisé pour WindowsHello et WindowsHelloEntreprise. À l'avenir, il sera intégré à de nombreuses autres fonctionnalités de sécurité clés dans Windows. Le TPM permet de sécuriser le code confidentiel et de chiffrer les mots de passe. Par ailleurs, il s'appuie sur notre expérience globale de Windows10, qui fait de la sécurité un véritable pilier central. L'utilisation de Windows sur un système équipé d'un TPM assure une couverture de la sécurité plus étendue et plus complète.

Conformité du TPM2.0 pour Windows10

Windows 10 pour les éditions de bureau (famille, professionnel, entreprise et éducation)

- Depuis le 28 juillet2016, les nouveaux modèles, nouvelles gammes ou nouvelles séries d'appareils doivent implémenter et activer par défaut le TPM2.0. Il en va de même pour les modèles, gammes ou séries existants si vous appliquez une mise à jour majeure à leur configuration matérielle, pour le processeur ou la carte graphique, par exemple. (Les détails sont fournis dans la section3.7 de la page consacrée à la configuration matérielle requise.) L'obligation d'activer le module de plateforme sécurisée 2.0 s'applique uniquement à la fabrication des nouveaux appareils. Pour obtenir des recommandations TPM pour des fonctionnalités Windows spécifiques, voir TPM et fonctionnalités Windows.