Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

7 nov, 2026 · @Gabriel

Objectif : *Comprendre le rôle du BIOS/UEFI et de Secure Boot, faire un choix éclairé pour votre usage (Linux seul, double démarrage avec Windows), et sécuriser le démarrage de votre ordinateur en limitant la dépendance à Microsoft.*

- ***Public visé :*** *Intermédiaire à avancé (utilisateurs de Linux, personnes exigeantes sur la souveraineté numérique)*
- ***Temps estimé :*** *20 à 40 minutes (lecture et réglages)*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *savoir redémarrer l'ordinateur et accéder à l'UEFI (section 10) ; un système Linux pour les commandes avancées (facultatif)*
- ***Fiches associées :*** *N°13 (passer à Linux), N°26 (chiffrement du disque), N°32 (Tails), N°16 (gestionnaire de mots de passe)*

1. Le problème en une minute

Situation	Conséquence
Secure Boot	Bloque les programmes de démarrage non signés (bootkits)… mais les clés installées d'usine sont surtout celles de Microsoft.
Dépendance à Microsoft	Avec Secure Boot actif, la plupart des distributions Linux démarrent grâce à **shim**, un petit programme signé par Microsoft.
Certificats qui expirent	Les certificats Secure Boot de Microsoft de 2011 expirent à partir de **juin 2026** et sont remplacés par ceux de 2023 : sans mise à jour du micrologiciel, certains systèmes risquent de ne plus démarrer après une future mise à jour.
Intel ME / AMD PSP	Des sous-systèmes intégrés aux processeurs, avec un accès très privilégié, au code fermé.
Mot de passe UEFI absent	N'importe qui ayant un accès physique peut démarrer sur une clé USB ou changer les réglages.

Le risque : un attaquant ayant accès physique à la machine, ou un logiciel malveillant persistant au démarrage.

Le bénéfice : un démarrage maîtrisé, et une décision consciente sur Secure Boot.

2. BIOS ou UEFI : rappels

Caractéristique	BIOS (Legacy)	UEFI
Époque	Années 1980, abandonné	Généralisé depuis les années 2010
Interface	Texte, clavier	Souvent graphique, parfois souris

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

Caractéristique	BIOS (Legacy)	UEFI
Disques	Table MBR, 2 To maximum	Table GPT, au-delà de 2 To
Sécurité	Aucune vérification	Secure Boot, mesures avec le TPM

C'est le premier programme qui s'exécute à l'allumage, avant le système d'exploitation.

3. Secure Boot renforce-t-il la dépendance à Microsoft ?

Point clé	Explication
Clés installées d'usine	Sur la plupart des PC, le micrologiciel fait confiance aux clés de Microsoft (et parfois du fabricant).
shim	Pour démarrer avec Secure Boot actif, les distributions Linux utilisent shim, signé par l'autorité « tierce partie » de Microsoft.
Révocations	Microsoft peut révoquer des chargeurs vulnérables. En **août 2024**, une mise à jour Windows (SBAT) a empêché des Linux plus anciens de démarrer sur des PC en double démarrage (« Verifying shim SBAT data failed »).
Windows 11	Exige un UEFI **compatible** Secure Boot et un TPM 2.0.

En clair : sur un PC grand public, la chaîne de confiance de Secure Boot passe par Microsoft. Ce n'est pas une fatalité : vous pouvez désactiver Secure Boot, ou installer vos propres clés.

⚠️ Mais Secure Boot a aussi une vraie utilité : il empêche un logiciel malveillant de s'installer avant le système (bootkit). Le désactiver retire cette protection.

4. Intel Management Engine et AMD PSP

Composant	Fabricant	Rôle	Point de vigilance
Intel Management Engine (ME)	Intel	Démarrage, fonctions de gestion (dont l'administration à distance AMT sur les modèles professionnels)	Microcontrôleur au code fermé, avec accès à la mémoire et au réseau ; des failles graves y ont été corrigées (2017)
AMD Platform Security Processor (PSP)	AMD	Démarrage sécurisé, fonctions de sécurité	Même principe : code fermé, très privilégié

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

Que faire ?

Solution	Efficacité	Difficulté	Matériel
Mettre à jour le micrologiciel	Corrige les failles connues	★☆☆☆☆	Tous
Désactiver AMT (si présent) dans l'UEFI	Supprime l'administration à distance	★★☆☆☆	PC professionnels Intel vPro
me_cleaner (réduction du code ME)	Partielle	★★★★★	Certains modèles, avec un risque de rendre le PC inutilisable
Matériel avec ME neutralisé	Forte	★★☆☆☆ (achat)	Purism, certains modèles System76 ou NovaCustom
Micrologiciel libre (coreboot, Libreboot)	Forte	★★★★★	Matériel compatible limité

Recommandations par profil

Profil	Que faire ?
Usage domestique	Gardez le micrologiciel à jour et désactivez AMT s'il existe. Concentrez-vous sur les mots de passe, la double authentification et les sauvegardes.
Très exigeant	Choisissez du matériel dont le ME est neutralisé, ou un micrologiciel libre.
Journaliste ou militant exposé	Matériel spécialisé, et Tails (fiche N°32) pour les usages sensibles.

5. Vos choix concernant Secure Boot

Choix	Dépendance à Microsoft	Protection au démarrage	Niveau technique
1. Garder Secure Boot avec shim (par défaut)	Oui (indirecte)	✅	★☆☆☆☆
2. Désactiver Secure Boot	Aucune	❌	★☆☆☆☆
3. Ajouter vos clés de machine (MOK)	Partielle (les clés Microsoft restent)	✅	★★★★☆

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

Choix	Dépendance à Microsoft	Protection au démarrage	Niveau technique
4. Remplacer les clés d'usine par les vôtres (par exemple avec sbctl)	Aucune	✅	★★★★★
5. Micrologiciel libre (coreboot, Libreboot)	Aucune	Selon la configuration	★★★★★

Recommandations

Profil	Conseil
Linux seul, grand public	**Gardez Secure Boot** si votre distribution le prend en charge (Ubuntu, Fedora, Debian, Linux Mint…) et faites les mises à jour du micrologiciel. Le désactiver est acceptable si un pilote ou une installation l'exige, en sachant que vous perdez la protection contre les bootkits.
Linux seul, exigeant	Remplacez les clés d'usine par les vôtres (option 4), ou choisissez du matériel prévu pour Linux.
Double démarrage Linux + Windows	Gardez Secure Boot et faites toutes les mises à jour (Windows Update côté Windows, fwupd côté Linux).
Tails	Tails prend en charge Secure Boot ; s'il affiche « Secure Boot Update Needed », mettez à jour le micrologiciel depuis votre système habituel (fiche N°32).

6. Mettre à jour les certificats Secure Boot (2026)

Les certificats Microsoft de 2011 expirent à partir de juin 2026. Les ordinateurs doivent recevoir les nouveaux certificats de 2023 dans la base du micrologiciel.

1. **Sous Windows :** installez toutes les mises à jour (Windows Update).
2. **Sous Linux :** installez les mises à jour du micrologiciel avec fwupd (section 8.2) ; sur un bureau GNOME, Logiciels s'en charge.
3. **Consultez le site du fabricant** si aucune mise à jour n'est proposée.

Vous devez voir :

- les mises à jour de micrologiciel appliquées, et un démarrage normal de vos systèmes.

7. Désactiver Secure Boot (si vous le choisissez)

1. Redémarrez l'ordinateur et entrez dans l'UEFI (section 10).
2. Ouvrez l'onglet **Boot** ou **Security**.

gabriel.ananda@mailo.com
CC BY SA

3. Trouvez **Secure Boot**.
4. Passez-le à **Disabled**.
5. Enregistrez et quittez (souvent F10).

Vous devez voir :

- sous Linux, `mokutil --sb-state` affiche `SecureBoot disabled`.

⚠️ Si votre disque est chiffré avec BitLocker (Windows), récupérez d'abord la **clé de récupération** : changer Secure Boot peut la déclencher.

8. Détails techniques

8.1. La chaîne de confiance avec Secure Boot

```
Micrologiciel UEFI
   │  vérifie la signature de shim (signé par Microsoft)
   ▼
shim
   │  vérifie GRUB (signé par la distribution, ou par une clé MOK)
   ▼
GRUB
   │  vérifie le noyau
   ▼
Noyau Linux (qui vérifie ensuite ses modules)
```

8.2. Distributions et Secure Boot

Distribution	Secure Boot	Remarque
Ubuntu, Fedora, Debian, Linux Mint, openSUSE	✅	shim signé fourni
Arch, Gentoo	⚠️	Configuration manuelle (sbctl, clés personnelles)
Tails	✅	Pris en charge (voir section 6 pour les certificats)

8.3. Vérifier l'état de Secure Boot sous Linux

```
# État de Secure Boot
mokutil --sb-state

# Autre méthode (systemd)
bootctl status | grep -i "secure boot"
```


gabriel.ananda@mailo.com
CC BY SA

8.4. Vos propres clés de machine (MOK)

Utile pour un pilote non signé (NVIDIA, VirtualBox) ou un noyau compilé vous-même.

```
# Proposer l'ajout d'une clé (un mot de passe temporaire vous est demandé)
sudo mokutil --import /chemin/vers/ma_cle.der
sudo reboot
# Au redémarrage, l'écran « MOK Manager » s'affiche : Enroll MOK ›
saisissez le mot de passe

# Lister les clés ajoutées
mokutil --list-enrolled

# Retirer une clé
sudo mokutil --delete /chemin/vers/ma_cle.der
```

Sur Ubuntu et Linux Mint, l'installation d'un pilote propriétaire propose généralement de créer et d'enregistrer cette clé automatiquement.

8.5. Le TPM

Le TPM est une puce (ou un module intégré au processeur) qui protège des clés et mesure le démarrage.

Fonction	Exemple
Stockage protégé de clés	Certificats, clés de chiffrement
Déverrouillage du disque	BitLocker (Windows), LUKS avec `systemd-cryptenroll` (Linux)
Mesure du démarrage	Détecte une modification de la chaîne de démarrage
Authentification	Windows Hello

Le TPM est une norme ouverte (Trusted Computing Group, ISO/IEC 11889), pas une technologie Microsoft. Sous Linux, il est facultatif et s'utilise sans aucun service Microsoft.

```
# Sous Linux : présence du TPM
ls /dev/tpm*
```

Sous Windows : `tpm.msc`.

8.6. Mettre à jour le micrologiciel sous Linux (fwupd)

De nombreux fabricants (Dell, Lenovo, HP, Framework, System76…) publient leurs mises à jour sur le service LVFS.

```
fwupdmgr refresh        # rafraîchir la liste
fwupdmgr get-updates    # voir les mises à jour disponibles
fwupdmgr update         # appliquer les mises à jour
```

Si fwupd ne trouve rien, consultez le site du fabricant.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

9. Autres réglages de sécurité de l'UEFI

Action	Où (selon le fabricant)	Pourquoi
Mettre à jour le micrologiciel	Site du fabricant ou fwupd	Corrige les failles
Mot de passe administrateur (superviseur)	**Security** › **Administrator / Supervisor Password**	Empêche la modification des réglages
Ordre de démarrage : disque interne en premier	**Boot** › **Boot Order**	Avec le mot de passe, empêche un démarrage discret sur une clé USB
Désactiver le démarrage réseau (PXE) si inutile	**Boot** › **Network Boot**	Réduit la surface d'attaque
Protection DMA du noyau / sécurité Thunderbolt	**Security** ou **Thunderbolt**	Limite les attaques par périphérique branché
Désactiver AMT (Intel vPro) si inutile	**Advanced** › **AMT**	Supprime l'administration à distance
Activer le TPM	**Security** › **TPM**	Chiffrement et mesure du démarrage

⚠️ **Notez le mot de passe de l'UEFI** dans votre gestionnaire (fiche N°16) : sur de nombreux portables, un mot de passe perdu impose un passage par le fabricant.

10. Accéder à l'UEFI (touches par marque)

Marque	Touche(s) au démarrage	Remarque
Acer	F2 ou Suppr	–
Asus	F2 ou Suppr	Fixes souvent Suppr, portables F2
Dell	F2	F12 : menu de démarrage
HP	Échap, puis F10	Échap ouvre le menu de démarrage
Lenovo ThinkPad	F1 (Entrée puis F1 sur certains)	F12 : menu de démarrage
Lenovo IdeaPad	F2 ou Fn+F2	Parfois bouton « Novo »
MSI	Suppr	–
PC assemblé	Suppr ou F2	–
Microsoft Surface	Maintenir **Volume +** puis appuyer sur le bouton d'alimentation	–

gabriel.ananda@mailo.com
CC BY SA

Marque	Touche(s) au démarrage	Remarque
Mac à processeur Intel	Pas d'UEFI réglable : **Option** au démarrage pour choisir le disque ; utilitaire de sécurité au démarrage via la récupération (Mac avec puce T2)	–

Depuis Windows 11 : Paramètres › **Système** › **Récupération** › **Démarrage avancé** › **Redémarrer maintenant**, puis **Dépannage** › **Options avancées** › **Paramètres du microprogramme UEFI** › **Redémarrer**.

Depuis Linux : `systemctl reboot --firmware-setup`.

11. Cas fréquents sous Linux

Symptôme	Cause possible	Action
« Secure Boot Violation » à l'installation	Image trop ancienne ou non signée, ou certificats non à jour	Utilisez la dernière version de la distribution ; mettez à jour le micrologiciel ; à défaut, désactivez Secure Boot
« Verifying shim SBAT data failed »	Révocation d'un ancien shim (mise à jour Windows)	Installez la dernière version de votre distribution (désactivez Secure Boot le temps de l'installation si besoin)
NVIDIA ou VirtualBox ne se chargent pas	Modules non signés	Enregistrez une clé MOK (section 8.4)
L'ordinateur redémarre sur la clé USB après installation	Ordre de démarrage	Remettez le disque interne en premier
Mot de passe UEFI perdu	–	Sur un PC fixe, réinitialisation du CMOS (cavalier ou pile) ; sur un portable, souvent le service après-vente du fabricant

12. Tableau récapitulatif des options Secure Boot

Option	Dépendance à Microsoft	Protection au démarrage	Difficulté	Pour qui
Garder Secure Boot + shim	Oui	★★★★☆	★☆☆☆☆	La plupart des utilisateurs
Désactiver Secure Boot	Aucune	★☆☆☆☆	★☆☆☆☆	Cas particuliers
Ajouter des clés MOK	Partielle	★★★★☆	★★★★☆	Pilotes ou noyaux personnalisés

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

Option	Dépendance à Microsoft	Protection au démarrage	Difficulté	Pour qui
Remplacer les clés d'usine	Aucune	★★★★☆	★★★★★	Experts
Micrologiciel libre	Aucune	Variable	★★★★★	Passionnés, matériel compatible

13. Challenge 7 jours

- **Jour 1 :** trouvez la touche d'accès à l'UEFI et explorez les menus sans rien changer.
- **Jour 2 :** notez la version du micrologiciel et appliquez les mises à jour (Windows Update, fwupd ou site du fabricant).
- **Jour 3 :** définissez un mot de passe administrateur de l'UEFI et enregistrez-le dans votre gestionnaire.
- **Jour 4 :** mettez le disque interne en premier dans l'ordre de démarrage ; désactivez le démarrage réseau s'il est inutile.
- **Jour 5 :** vérifiez que le TPM est activé.
- **Jour 6 :** prenez votre décision sur Secure Boot (section 5).
- **Jour 7 :** redémarrez chaque système installé et vérifiez que tout fonctionne.

Vous allez constater :

- vous savez où se trouvent les réglages de démarrage ;
- votre ordinateur est protégé contre les modifications par une personne de passage.

14. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Décision éclairée sur Secure Boot	Protection ou indépendance, en connaissance de cause	Section 5
Mise à jour du micrologiciel et des certificats	Failles corrigées, démarrage assuré après 2026	Sections 6 et 8.6
Mot de passe UEFI + ordre de démarrage	Protection contre les accès physiques	Section 9
Désactivation d'AMT et du PXE si inutiles	Surface d'attaque réduite	Section 9
Matériel ou micrologiciel libres (si besoin)	Moins de dépendance aux composants fermés	Section 4

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°40 : Sécurisez votre BIOS/UEFI – La première porte d'entrée de votre ordinateur V1.1

15. Conclusion générale

Profil	Secure Boot	Intel ME / AMD PSP
Linux seul, grand public	Gardez-le actif avec une distribution compatible	Mises à jour du micrologiciel
Linux seul, exigeant	Vos propres clés	Matériel avec ME neutralisé
Double démarrage avec Windows	Gardez-le actif et faites toutes les mises à jour	Mises à jour du micrologiciel
Journaliste ou militant	Actif, avec Tails pour les usages sensibles	Matériel spécialisé
Partisan du logiciel libre	Micrologiciel libre	Micrologiciel libre

À retenir absolument

- **Secure Boot dépend des clés de Microsoft sur la plupart des PC,** mais il protège contre les bootkits : le garder ou le désactiver est un compromis.
- **Mettez à jour le micrologiciel en 2026 :** les certificats Secure Boot de 2011 expirent.
- **Un mot de passe UEFI et le disque interne en premier** protègent contre les accès physiques.
- **Intel ME et AMD PSP** ne se désactivent vraiment que sur du matériel spécialisé ou avec un micrologiciel libre.

Test final :

1. Je sais entrer dans l'UEFI de mon ordinateur.
2. J'ai vérifié et mis à jour le micrologiciel.
3. J'ai défini un mot de passe administrateur UEFI, enregistré dans mon gestionnaire.
4. Le disque interne est en premier dans l'ordre de démarrage.
5. J'ai pris une décision consciente sur Secure Boot (`mokutil --sb-state` indique l'état choisi).
6. Mon ordinateur démarre normalement sur chaque système.
7. Si tout est coché : vous avez repris le contrôle du démarrage de votre ordinateur ✅

Références

- Tails – Mise à jour des certificats Secure Boot (expiration à partir de juin 2026)
- BleepingComputer – Une mise à jour Windows (SBAT, août 2024) bloque le démarrage de Linux en double démarrage
- Pureinfotech – Configuration requise de Windows 11 (UEFI compatible Secure Boot, TPM 2.0)

gabriel.ananda@mailo.com
CC BY SA