RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

SÉCURISATION DU POSTE DE TRAVAIL MULTI-ENVIRONNEMENTS (NON CLASSIFIÉS)

LES FONDAMENTAUX

ANSSI-PA-114
16/01/2026

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Sécurisation du poste de travail multi-environnements (non classifiés) »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	16/01/2026	Version initiale

Table des matières

1
Préambule

Ce document est destiné aux éditeurs de postes de travail multi-environnements afin de les accompagner dans la conception de leur produit et dans l'écriture d'une cible de sécurité en vue d'une évaluation. Il n'est pas à destination d'administrateurs systèmes.

Lorsque des systèmes informatiques (ou environnements) ne possèdent pas le même niveau de sensibilité, sont exposés à des niveaux de menace hétérogènes, ou sont opérés par plusieurs entités différentes, il est recommandé de les cloisonner de manière physique, car ce type de cloisonnement est celui qui apporte les meilleures garanties de sécurité. L'implémentation usuelle du cloisonnement physique aux postes de travail conduit à en dédier un à chaque environnement. Toutefois, pour des raisons de coûts, de mobilité, d'ergonomie ou d'empreinte environnementale, il peut être souhaitable de limiter leur nombre.

Pour résoudre ce paradoxe, ce document présente les fonctions de sécurité attendues sur un poste de travail destiné à faire cohabiter différents environnements. Un tel poste sera appelé « poste de travail multi-environnements ».

Des environnements avec des cas d'usage différents peuvent cohabiter sur un tel poste. On peut donner comme exemples :

- un environnement bureautique pour un utilisateur ;
- un environnement d'administration tel que décrit dans le guide *Recommandations relatives à l'administration sécurisée des SI* [2] ;
- un environnement de développement ;
- un environnement à destination d'auditeurs.

Information

Ce document ne traite que du cloisonnement entre systèmes d'exploitation complets (noyau et applicatifs). L'isolation d'applicatifs au sein d'un système d'exploitation n'est pas traitée mais peut être effectuée au sein de chacun des environnements à l'aide de *sandbox* ou conteneurs.

Les environnements hébergés sur un poste de travail multi-environnements respectant toutes les fonctions de sécurité, recommandations, et hypothèses du présent document peuvent être *Non Protégé* (NP) et *Diffusion Restreinte* (DR) au sens de l'Instruction Interministérielle n°901 [6]. Il est donc possible d'obtenir les combinaisons suivantes : NP/NP, NP/DR et DR/DR, sans se limiter à deux environnements cloisonnés. Un poste peut par exemple héberger un premier environnement

DR pour de la bureautique, un deuxième NP pour l'administration d'un SI X, et un troisième NP pour l'administration d'un autre SI Y.

Attention

Ce document ne traite que des niveaux de sensibilité au maximum *Diffusion Restreinte* (DR) au sens de l'II 901. Il ne traite pas des niveaux de classification *Secret* ou *Très Secret* au sens de l'Instruction Générale Interministérielle n°1300 [9].

Les fonctions de sécurité et recommandations du présent document reposent sur l'hypothèse que le poste multi-environnements est un **poste de travail** et est **mono-utilisateur**. D'autres fonctions de sécurité seraient attendues pour des systèmes avec d'autres usages (serveur, embarqué…) ou pour des postes multi-utilisateurs. Il est également supposé que le poste peut être utilisé en condition de nomadisme au sens du guide *Recommandations sur le nomadisme numérique* [3].

Information

Des travaux avaient été menés au sein de l'ANSSI pour développer CLIP OS 4 et CLIP OS 5[a]. Notamment, CLIP OS 4 avait été agréé pour traiter de manière cloisonnée des informations NP et DR. Ces solutions ne sont maintenant plus maintenues, mais les travaux de conception et de maintenance de ces postes avaient permis d'identifier les fonctions de sécurité qui sont reprises dans ce document.

Les fonctions de sécurité présentées par la suite sont **agnostiques** du système d'exploitation chargé d'assurer le cloisonnement entre les environnements de sensibilités différentes. Toutefois, des exemples d'implémentation sont donnés pour un système Linux afin de les illustrer et d'en montrer la faisabilité.

N'étant pas destiné aux administrateurs, ce document omet les fonctions de sécurité et recommandations liées au contexte de production et n'aborde notamment pas l'infrastructure informatique à laquelle le poste de travail multi-environnements devra être connecté pour satisfaire à la PSSI de l'organisation qui le déploiera. Pour ce faire, un administrateur est invité à se référer au *Guide d'élaboration de politiques de sécurité des systèmes d'information* [1].

a. https://clip-os.org/fr/

2
Principes généraux

2.1 Définitions

Tâche

Une tâche est un ensemble d'instructions chargées en mémoire au fur et à mesure pour être exécutées.

Ressource

Une ressource est une entité (mémoire, réseau, tâche, fichier, données…) utilisée par une tâche.

Politique de sécurité

Une politique de sécurité regroupe un ensemble de règles qui autorisent ou interdisent à une tâche d'effectuer une action sur une ressource.

Machine virtuelle

Le terme machine virtuelle (ou VM pour *Virtual Machine*) renvoie, dans ce document, à celles créées et gérées par un hyperviseur. Pour plus de détails, se référer au guide *Recommandations pour la mise en place de cloisonnement système* [7].

Sandbox

Une *sandbox* est un ensemble de tâches isolé des autres tâches du système grâce à la combinaison de primitives de cloisonnement offertes par le noyau du système d'exploitation (*namespaces*, *cgroups*, changements d'UID/GID…). Le noyau est partagé avec les autres tâches du système.

Domaine

Un domaine est l'environnement d'exécution d'une ou plusieurs tâches sur le socle. Il est défini par l'ensemble des ressources (logicielles et matérielles) sur lesquelles la tâche peut effectuer des actions. Par opposition, une ressource sur laquelle la tâche ne peut pas agir ne fait pas partie de son domaine.

L'objectif d'un domaine est de restreindre un ensemble de tâches aux ressources qui lui sont strictement nécessaires pour assurer sa fonction, et d'ainsi l'isoler des autres

domaines et du socle.

Ce domaine se décline en domaine utilisateur et domaine support.

Domaine utilisateur

Un domaine utilisateur est un domaine destiné à accueillir l'environnement de travail d'un utilisateur, son OS, ses données et logiciels. Dans ce document, on considère qu'il est implémenté sous la forme d'une VM.

Domaine support

Un domaine support est un domaine destiné à accueillir une ou plusieurs tâches qui permettent d'assurer une fonction autre qu'un domaine utilisateur. Il peut être implémenté sous la forme d'une VM ou d'une *sandbox*.

Cloisonnement

Le cloisonnement ou isolation entre domaines a pour objectif de garantir qu'un domaine n'accède pas aux ressources d'un autre domaine, directement ou indirectement, ou bien seulement d'une manière contrôlée par une politique de sécurité. Il protège ainsi le socle et les autres domaines d'actions non-légitimes d'un des domaines.

TCB (Trusted Computing Base)

La TCB est l'ensemble des logiciels et matériels critiques pour la sécurité du système. Un bug ou une vulnérabilité dans un composant de la TCB entraîne généralement la compromission du système complet.

Socle

Le socle est l'ensemble des matériels et logiciels permettant de faire fonctionner les domaines utilisateurs et les domaines supports. Il inclut la TCB, mais peut également contenir d'autres composants (client de synchronisation du temps…) dont la compromission ne devrait pas impacter l'intégralité du système.

Dans notre cas, c'est le socle qui assure l'isolation entre les différents domaines et leur permet de s'exécuter en sécurité (confidentialité, intégrité, authenticité). Seules les tâches strictement nécessaires aux missions du socle sont exécutées dans le socle. Les autres sont isolées dans un domaine.

Moniteur de référence

Le moniteur de référence est le logiciel (ou la partie de logiciel, par exemple du noyau) qui autorise ou interdit l'action d'une tâche sur une ressource, sur la base d'une politique de sécurité.

TPM (Trusted Platform Module)

Composant sécurisé passif, matériel ou virtuel (dénoté dans ce cas vTPM), qui effectue des opérations cryptographiques. Les spécifications des TPM sont régies par une norme internationale (ISO/IEC 11889[a]) élaborée au sein du *Trusted Computing Group* (TCG)[b].

a. https://www.iso.org/standard/66510.html
b. https://trustedcomputinggroup.org/

2.2 Exemple d'architecture

La figure 1 représente un exemple d'architecture de principe d'un poste de travail multi-environnements comportant deux domaines utilisateurs nommés ici `BUREAUTIQUE`. Des VM sont utilisées pour implémenter les domaines utilisateurs, comme détaillé dans la section 2.3. Les principaux échanges d'information sont également représentés.

Pour plus de lisibilité, tous les domaines supports qui pourront ou devront être mis en œuvre ne sont pas représentés sur le schéma.

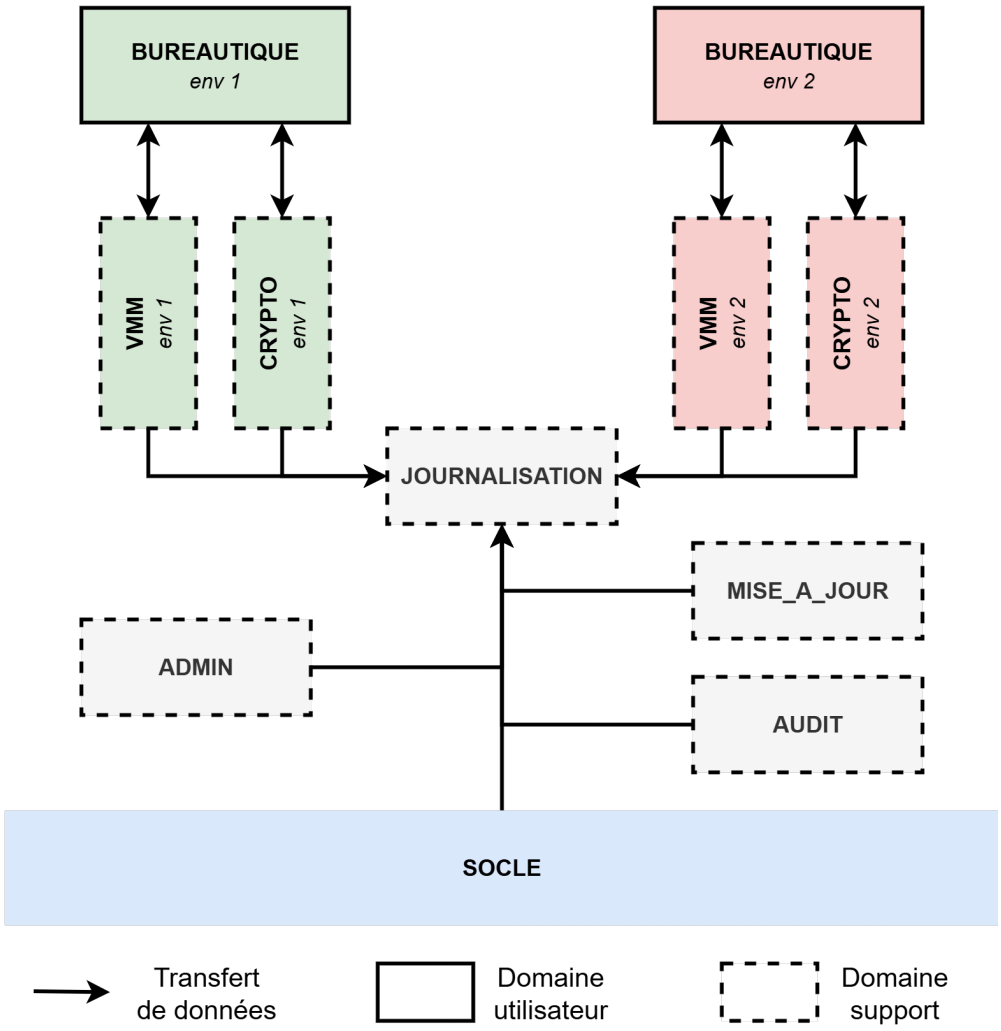

FIGURE 1 – Exemple d'une architecture de principe d'un poste de travail multi-environnements

Un domaine support `VMM` et un domaine support `CRYPTO` sont dédiés à chaque domaine utilisateur. Le domaine support `VMM` isole le *Virtual Machine Manager* (VMM) et les périphériques qu'il émule (cf. 3.6). D'autres domaines supports peuvent être utilisés pour isoler d'autres périphériques émulés. Par exemple, le domaine support `CRYPTO` ici représenté peut contenir un TPM virtuel (vTPM) émulé par le socle.

Le domaine support `JOURNALISATION` est destiné à recevoir les journaux du socle. Les domaines supports `VMM` et `CRYPTO` peuvent également y envoyer leurs journaux. Par contre, comme cela sera

abordé en section 3.11, le domaine support `JOURNALISATION` n'est pas destiné à recevoir les journaux des domaines utilisateurs.

Les domaines supports `ADMIN`, `AUDIT` et `MISE_A_JOUR` sont dédiés aux actions d'exploitation du poste telles que détaillées en section 3.13.

Information

Un poste de travail multi-environnements peut avoir plus de deux domaines utilisateurs en fonction des besoins métier. Toutes les fonctions de sécurité du document sont applicables peu importe le nombre de domaines utilisateurs.

2.3 Choix des technologies de cloisonnement

Les fonctions de sécurité et recommandations de ce document reposent sur l'hypothèse que **des VM sont utilisées pour cloisonner les domaines utilisateurs**. Une VM est donc dédiée pour implémenter chaque domaine utilisateur. Les VM offrent en effet un cloisonnement plus fort et plus complet que les technologies reposant uniquement sur les primitives d'isolation offertes par le noyau du système d'exploitation (*sandbox*…). En complément :

- La surface d'attaque exposée par le socle aux domaines utilisateurs est réduite. Par conséquent, cette surface est plus facilement auditable et il est possible d'accorder une plus grande confiance dans le cloisonnement apporté par une VM.
- Le système d'exploitation des domaines utilisateurs ne partage pas le noyau du socle. De fait, le système d'exploitation du domaine utilisateur n'a pas d'adhérence au socle et aux fonctionnalités que ce dernier supporte. Cela facilite notamment leur prise en charge par des équipes techniques différentes et leur MCO/MCS.

Les domaines supports et les autres fonctions du socle peuvent aussi être cloisonnés en utilisant des VM, mais d'autres technologies de cloisonnement peuvent être employées à la place. Des *sandbox*, telles que définies en section 2.1, peuvent par exemple être utilisées à cet usage.

Attention

Dans le cas où il y aurait plusieurs domaines utilisateurs de même sensibilité, les domaines utilisateurs devront malgré tout être isolés les uns des autres. En effet, une sensibilité identique n'est pas synonyme d'un droit d'accès identique.

Les fonctions de sécurité et recommandations sont destinées à rendre la sécurité du poste de travail multi-environnements indépendante du contenu des VM. Toutefois, dans le cadre du principe de défense en profondeur, il est recommandé de durcir les systèmes installés dans les VM.

3
Fonctions de sécurité

Ce chapitre liste les fonctions de sécurité attendues sur un poste bureautique de travail multi-environnements pour assurer la sécurité du socle et le cloisonnement entre les différents domaines.

Attention

Les exemples donnés ont pour but d'illustrer une fonction de sécurité. Ils ne sont pas toujours suffisants en eux-mêmes pour implémenter pleinement une fonction de sécurité. Notamment, chaque solution devra être adaptée en fonction du contexte.

3.1 Chaîne de démarrage du socle

3.1.1 L'intégrité, l'authenticité et le non-retour en arrière des éléments de la chaîne de démarrage (exécutables et configurations) doivent être assurés de manière à protéger contre les modifications apportées par un attaquant privilégié sur le socle (ex : *root*) ou possédant un accès physique à la machine.

> *Exemple : en mettant en place de manière combinée UEFI Secure Boot et un mécanisme de Measured Boot reposant sur l'utilisation d'un composant de sécurité physique mettant en œuvre une RTM (Root of Trust for Measurements), par exemple un TPM.*

> Note : Le retour en arrière d'éléments de la chaîne de démarrage est autorisé pour implémenter un mécanisme de mise à jour avec *fallback* tel que décrit en section 3.12. Ce retour en arrière doit cependant être limité et contrôlé afin de ne pas nuire à la sécurité du système.

3.1.2 La configuration du *firmware* ne doit pas pouvoir être modifiée par un utilisateur.

> *Exemple : L'accès à l'interface de configuration du firmware est protégée par un mot de passe unique à la machine.*

3.2 Intégrité du socle

3.2.1 L'intégrité et l'authenticité des exécutables doivent être assurées par des mécanismes cryptographiques et ne pas être altérables de manière à les protéger contre les modifications apportées par un attaquant possédant un accès privilégié sur le socle (ex : *root*) ou un accès physique à la machine.

> *Exemple : sous Linux, en utilisant dm-verity.*

3.2.2 L'intégrité de l'image du noyau projetée en mémoire doit être assurée.

> *Exemple : sous Linux, via l'activation du LSM Lockdown.*

3.2.3 Le chargement de code destiné à être exécuté en espace noyau doit être contrôlé en intégrité par un mécanisme cryptographique.

> *Exemple : contrôle de signature des modules noyau.*

3.3 Chiffrement des données

3.3.1 Toutes les données du système (le socle et tous les domaines) doivent être protégées cryptographiquement en confidentialité, intégrité et authenticité par le socle.

> *Exemple : sous Linux, via le mode de chiffrement authentifié offert par cryptsetup, qui combine dm-crypt et dm-integrity.*

3.3.2 Dans le cas où il n'est pas possible, du fait d'une contrainte technique, de protéger certaines données en confidentialité (ex : partition ESP), elles doivent tout de même être protégées cryptographiquement en intégrité et authenticité. De plus, elles ne doivent contenir ni données sensibles ni secrets.

> *Exemple : signature des binaires UEFI pour UEFI Secure Boot. Se référer à la section 3.1 pour plus de détails sur cet exemple précis.*

3.3.3 Un composant de sécurité physique doit être présent et utilisé par le socle afin de protéger les secrets cryptographiques sensibles.

> *Exemple : utiliser un TPM pour sceller le secret de déchiffrement d'une partition et générer une clé privée non-extractible pour le VPN du socle.*

3.3.4 Les données d'un domaine utilisateur doivent être protégées cryptographiquement par le socle en confidentialité à partir d'un secret provenant d'un facteur de connaissance de l'utilisateur légitime du poste. D'autres facteurs peuvent être combinés à ce premier facteur. Seul cet utilisateur doit être en mesure de déchiffrer ce domaine utilisateur (à l'exception de clés mises sous séquestre).

Cette fonction de sécurité peut être assurée par le mécanisme de chiffrement de la fonction de sécurité **3.3.1** si celui-ci répond aux contraintes listées ici.

3.3.5 Les algorithmes cryptographiques et les clés doivent respecter le Référentiel Général de Sécurité [5].

3.4 Protection de la mémoire vive

3.4.1 L'accès aux données en mémoire vive des domaines utilisateurs depuis l'espace utilisateur du socle doit être restreint (pour un utilisateur privilégié ou non).

> *Exemple : sous Linux, en bloquant les accès à la mémoire du noyau et des autres processus (LSM Lockdown, LSM YAMA…).*

3.4.2 Pour éviter les attaques de type *coldboot*, les technologies de chiffrement complet de mémoire DRAM doivent être utilisées.

> *Exemple : en activant Intel TME [1] ou AMD TSME [2].*

3.5 Durcissement du socle

3.5.1 Le socle doit être durci à l'état de l'art en respectant les grands principes de sécurité, notamment :

> le principe de défense en profondeur ;
> le principe de séparation des privilèges ;
> le principe de moindre privilège ;
> le principe de minimisation (réduction de la surface d'attaque).

3.5.2 Les informations sensibles (clés privées, mots de passe…) ne doivent pas subsister en mémoire plus longtemps que strictement nécessaire.

3.5.3 Les recommandations du guide *Recommandations pour la mise en place de cloisonnement système* [7] doivent être respectées. Notamment, l'accès aux ressources doit être contrôlé par un moniteur de référence faisant partie du socle. Sur la base d'une politique de sécurité, ce moniteur de référence autorise ou non les accès.

> *Exemple : sous Linux, cette fonction de sécurité peut être implémentée via des mécanismes de MAC (Mandatory Access Control) tels que SELinux ou AppArmor.*

3.5.4 Les fonctions de sécurité mises à disposition par le matériel, le système d'exploitation et les logiciels utilisés doivent être activées. Toute non-activation doit être dûment justifiée.

3.5.5 Le noyau doit être durci à l'état de l'art.

> *Exemple : sous Linux, en compilant le noyau avec les options de compilation adéquates et en utilisant le patch Linux Hardened [3].*

3.5.6 Le socle doit mettre en place des protections à l'état de l'art contre les attaques micro-architecturales connues (ex : Meltdown et Spectre [4]). Notamment, une attaque de ce type exécutée dans un domaine utilisateur ne doit affecter ni le socle, ni les domaines supports, ni les autres domaines utilisateurs.

> *Exemple : sous Linux, en activant les atténuations des vulnérabilités CPU dans les arguments de ligne de commande du noyau.*

1. https://www.intel.com/content/www/us/en/architecture-and-technology/total-memory-encryption-security-paper.html
2. https://www.amd.com/system/files/TechDocs/memory-encryption-white-paper.pdf
3. https://github.com/anthraxx/linux-hardened
4. https://spectreattack.com/

3.6 Périphériques émulés et VMM

3.6.1 Une instance de VMM doit être dédiée à chaque domaine utilisateur.

3.6.2 Chaque périphérique émulé doit être dédié à un unique domaine utilisateur et ne doit être exposé qu'à celui-ci.

3.6.3 Les périphériques émulés et l'instance de VMM dédiés à chaque domaine utilisateur doivent être isolés dans un domaine support dédié. Les périphériques émulables dans des processus distincts du VMM et des autres périphériques doivent être isolés dans leur propre domaine support.

> *Exemple : sous Linux, si Qemu est utilisé, alors chaque instance de Qemu doit être isolée du reste du système via les mécanismes adéquats (sandbox, politique MAC, réduction des privilèges…).*

> *Exemple : sous Linux, un disque virtio-fs*[5] *est émulé par un processus distinct de celui de Qemu. Il devra donc être isolé dans un domaine support dédié.*

3.6.4 La surface d'attaque exposée par le socle aux domaines utilisateurs doit être minimale.

> Notamment, les seuls périphériques émulés doivent être ceux strictement nécessaires au bon fonctionnement d'un domaine utilisateur.

3.7 Périphériques physiques délégués

3.7.1 Il est préférable d'émuler les périphériques des VM plutôt que de leur déléguer un périphérique physique (*PCI passthrough*). Si un périphérique physique est délégué, cette délégation doit se faire de manière sécurisée et son innocuité doit être démontrée et documentée.

> *Exemple : au minimum via la bonne configuration de l'IOMMU, et sous Linux la mise en œuvre de VFIO.*

3.8 Périphériques physiques externes

Cette section traite des périphériques physiques externes (clavier, carte à puce, clés USB…) qui ne sont pas délégués à un domaine utilisateur au sens de la section 3.7. Ces périphériques sont rattachés au socle et sont contrôlés par les *drivers* du socle. Leurs fonctionnalités peuvent ensuite être accessibles depuis les domaines utilisateurs via des périphériques émulés et des mécanismes logiciels (redirection de flux, *proxy*…).

Pour les périphériques émulés, les fonctions de sécurité décrites dans la section 3.6 doivent être appliquées en complément de celles de la présente section.

5. https://gitlab.com/virtio-fs/virtiofsd

3.8.1 Les périphériques physiques externes ne doivent pas être simultanément accessibles par différents domaines utilisateurs ou par un domaine utilisateur et le socle.

3.8.2 Si un même périphérique physique externe est utilisé par plusieurs domaines utilisateurs ou par le socle de manière alternée, on démontrera et documentera que cette utilisation alternée ne conduit pas à une fuite de données d'un domaine utilisateur ou du socle vers un domaine utilisateur.

3.8.3 Les données inscrites sur un périphérique de stockage amovible (ex : clé USB) depuis un domaine utilisateur ne doivent être lisibles que depuis ce domaine utilisateur. Le fait de pouvoir accéder aux données de ce périphérique depuis d'autres systèmes de l'entité, par exemple les domaines utilisateurs équivalents sur les autres postes de travail multi-environnements, est laissé à la discrétion de la PSSI.

3.8.4 Dans le cas général, le concepteur du poste de travail doit démontrer et documenter que l'utilisation de périphériques de stockage amovibles ne rompt pas l'isolation entre domaines utilisateurs.

3.9 Réseau

Dans cette section, les flux réseaux des domaines supports sont assimilés aux flux du socle. Les fonctions de sécurité s'appliquent donc aux deux.

3.9.1 La configuration réseau du socle ne doit pouvoir être contrôlée ni par un domaine utilisateur ni par l'utilisateur du poste.

> Une exception peut être admise pour que l'utilisateur puisse choisir un réseau Wi-Fi auquel se connecter (voir section 3.17), pour qu'il puisse définir une adresse IP statique pour l'interface réseau du socle, ou pour qu'il puisse choisir un profil prédéfini par un administrateur. Si implémentées, ces exceptions ne doivent pas impacter la sécurité du socle.

3.9.2 La gestion des flux réseaux doit être réalisée en respectant les exigences réglementaires liées à chaque domaine utilisateur. La sensibilité et les contraintes de chaque domaine utilisateur peuvent être différentes et requérir l'usage de tunnels VPN chiffrants dédiés. La sensibilité du socle doit également être prise en compte ici, telle que spécifiée dans la section 4.1.

3.9.3 Les flux originaires du socle doivent transiter dans un VPN chiffrant non-débrayable maîtrisé par l'entité propriétaire du poste, tel que le prévoit le guide *Recommandations sur le nomadisme numérique* [3]. Ce document traite également de la question des portails captifs en nomadisme et de leurs interactions avec les VPN chiffrants non-débrayables.

3.9.4 Si des fonctionnalités d'auto-configuration sur le réseau sont utilisées par le socle, le nombre d'options de configuration acceptées doit être minimal. De plus, ces options ne doivent pas impacter la sécurité du socle.

> *Exemple : si un client DHCP est utilisé, alors les options DHCP qu'il accepte doivent être choisies avec soin et leur impact doit être évalué.*

3.9.5 Les communications réseau entre les domaines utilisateurs et le socle sont interdites, à l'exception de celles strictement requises pour implémenter les fonctions de sécurité décrites dans ce document.

3.9.6 Les communications réseau entre les domaines utilisateurs, à l'intérieur du poste, sont interdites.

> Afin de faciliter le cloisonnement réseau entre les domaines utilisateurs, il est fortement conseillé de ne pas placer les différents domaines utilisateurs dans le même domaine de *broadcast*.

3.9.7 Les domaines utilisateurs ne doivent pouvoir usurper ni un autre domaine utilisateur ni le socle sur les réseaux virtuels du poste.

3.9.8 Les domaines utilisateurs ne doivent accéder au réseau qu'au travers de ressources maîtrisées par le socle afin de s'assurer que les flux réseau des domaines utilisateurs n'échappent pas aux contrôles du socle.

Une exception peut être tolérée pour déléguer une carte réseau physique à un domaine utilisateur (*PCI passthrough*).

> Dans ce cas, les fonctions de sécurité suivantes de cette section ne sont pas applicables pour cette carte réseau.

> Dans ce cas, les fonctions de sécurité de la section 3.7 doivent être prises en compte.

3.9.9 Les domaines utilisateurs ne doivent pas pouvoir usurper une autre machine, le socle, ou un autre domaine utilisateur sur les réseaux extérieurs au poste.

3.9.10 Tous les flux réseau doivent être filtrés par le socle, et seuls les flux strictement nécessaires au bon fonctionnement du poste doivent être acceptés. Notamment, et de manière non-exhaustive, doivent être filtrés :

> tous les flux à destination du socle ;

> tous les flux originaires du socle ;

> tous les flux originaires des domaines utilisateurs ;

> tous les flux transitant dans les tunnels VPN dans le cas où le socle en établit.

3.10 Sources de temps

3.10.1 Le socle doit être en capacité d'utiliser une source de temps intègre pour mettre à jour son temps local.

> *Exemple : en utilisant NTS* [6].

3.10.2 Le socle et les domaines supports doivent avoir une source de temps commune afin de pouvoir corréler leurs évènements de sécurité.

6. https://www.rfc-editor.org/info/rfc8915

3.11 Journalisation

3.11.1 Un domaine support est dédié à la journalisation du socle. Il stocke les journaux et les transmet aux potentiels serveurs distants de journalisation, suivant la PSSI de l'organisation utilisatrice du poste.

3.11.2 Les journaux doivent être protégés en intégrité et en authenticité.

3.11.3 Les journaux du socle contiennent au minimum :

> les dysfonctionnements métier du socle, c'est-à-dire autres que ceux des fonctions de sécurité ;

> les dysfonctionnements des fonctions de sécurité du socle (de manière facilement distinguable des dysfonctionnements métier) ;

> les mises à jour, les modifications de la configuration et les modifications d'éléments cryptographiques ;

> les authentifications (locales ou distantes, et réussies ou échouées) et déconnexions aux différents comptes utilisateur ou système ;

> les occurrences d'usage des diodes ;

> les journaux des éventuels tunnels VPN du socle.

3.11.4 Les journaux ne doivent pas recueillir d'information permettant de s'affranchir d'une fonction de sécurité.

> *Exemple : clés privées, adresses permettant de casser l'ASLR (Address Space Layout Randomization)…*

3.11.5 Les journaux créés à l'intérieur d'un domaine utilisateur ne doivent pas être envoyés au socle. Ils sont recueillis au sein de leur domaine utilisateur et leur export est soumis à la PSSI de ce domaine.

3.12 Mise à jour

3.12.1 Le socle doit rester fonctionnel et sécurisé, même en cas d'échec de la mise à jour. La disponibilité du poste est considérée comme une fonction de sécurité lors de son utilisation en nomadisme.

> *Exemple : utilisation d'un système de mise à jour atomique avec fallback (retour en arrière contrôlé sur une version définie et fonctionnelle).*

3.12.2 L'échec de l'application d'une mise à jour doit être journalisé.

3.12.3 Les mises à jour doivent être signées et ces signatures doivent être contrôlées au moment de leur application.

3.13 Exploitation du socle

Si des actions d'exploitation locales ou distantes doivent être effectuées par un humain, alors celles-ci doivent être contrôlées en respectant les fonctions de sécurité de cette section. Les objectifs sont d'éviter qu'un compte d'exploitation compromis ou détenu par un utilisateur malveillant ne lui permette de compromettre l'intégralité du poste, mais également d'éviter que ces comptes ne puissent apporter trop de modifications spécifiques à un poste et que sa configuration ne dérive ainsi de manière incontrôlée.

3.13.1 Un rôle doit être associé à chaque type d'action d'exploitation. Par exemple, les rôles suivants peuvent être définis :

> **Administrateur** : administration fonctionnelle du socle et des domaines supports (changement de configuration, redémarrage de services locaux…). Ce rôle ne devrait pas avoir besoin d'être un compte administrateur privilégié au sens système (ex : ne devrait pas être *root* sur Linux).

> **Auditeur** : audit du socle et des domaines supports (lecture des journaux, relevé de l'état des services, relevé des versions des différents composants…). Ce rôle ne se substitue pas à la remontée et centralisation des journaux dans le SI.

> **Mise à jour** : gestion des mises à jour du socle et des domaines supports (changement de branche de version, *rollback* de version…). Ce rôle n'a pas pour but de construire les mises à jour (compilation, création de paquets…) ni de les signer. Ces opérations ne devraient pas être réalisées sur le poste.

3.13.2 Chaque rôle doit être clairement défini dans la documentation. Les actions effectuables par ce rôle doivent être listées de manière exhaustive.

3.13.3 Les actions d'exploitation doivent être effectuées dans des domaines supports dédiés à chaque rôle.

3.13.4 Ces domaines doivent disposer de privilèges minimum et ne permettre d'accéder qu'aux ressources nécessaires pour effectuer les actions d'exploitation.

> *Exemple : sous Linux, via un ensemble restreint de capabilities (ou aucune) et une politique de type MAC.*

> *Exemple : sous Linux, via un système de délégation de privilèges tel que polkit.*

3.13.5 Ces domaines ne doivent pas permettre d'accéder aux données des utilisateurs.

3.13.6 Les rôles liés à l'administration doivent respecter le guide *Recommandations relatives à l'administration sécurisée des SI* [2].

3.13.7 L'accès à ces domaines supports doit nécessiter des authentifications fortes au sens du guide *Recommandations relatives à l'authentification multifacteur et aux mots de passe* [8].

Information

Un poste de travail multi-environnements n'a pas forcément besoin que des actions d'exploitation soient effectuées par un humain sur le socle. Celles-ci peuvent être

automatisées. Dans ce cas, il n'est pas nécessaire d'implémenter ces interfaces d'interaction car le système ne doit pas exposer plus d'interfaces que nécessaire.

3.14 Chaîne de démarrage des domaines utilisateurs

3.14.1 Le socle doit fournir aux domaines utilisateurs un mécanisme de démarrage sécurisé au sens de la section 3.1.

3.14.2 Le socle doit fournir à chaque domaine utilisateur un élément de sécurité permettant de mettre en œuvre une RTM (*Root of Trust for Measurements*).

> *Exemple : le socle émule et expose au domaine utilisateur un TPM virtuel (vTPM).*

3.14.3 Chaque élément de sécurité fourni par le socle doit être cloisonné dans un domaine support dédié tel que spécifié en section 3.6. Cet élément doit être assigné à un unique domaine utilisateur et être distinct de celui du socle.

3.15 Authentification de l'utilisateur

3.15.1 L'utilisateur du poste doit obligatoirement s'authentifier sur le socle avant de pouvoir accéder aux domaines utilisateurs ou interagir avec le socle tel que décrit en section 3.17.

3.15.2 Le socle doit authentifier l'utilisateur en respectant la PSSI et les exigences réglementaires de chacun des domaines utilisateurs.

3.16 Affichage de confiance

3.16.1 Le socle doit permettre à l'utilisateur de connaître à tout moment et de manière non ambigüe le domaine avec lequel il interagit.

> *Exemple : en affichant une barre de confiance.*

3.17 Options à la main de l'utilisateur

Il est possible de laisser la possibilité à l'utilisateur de configurer certaines options du socle. Par exemple :

- le changement de son mot de passe ;
- l'activation/désactivation du Wi-Fi et la déclaration du réseau Wi-Fi auquel se connecter ;
- l'association d'un périphérique (carte à puce, microphone…) à un domaine utilisateur ou au socle. Se référer à la section 3.8 pour les fonctions de sécurité à prendre en compte.

3.17.1 Ces options ne doivent impacter ni la sécurité du socle ni le cloisonnement entre domaines.

3.17.2 Un ou plusieurs domaines supports doivent être dédiés à la configuration de ces options.

3.18 Communication entre domaines utilisateurs

Les communications entre domaines utilisateurs sont proscrites. Si l'échange de fichiers entre les différents domaines utilisateurs est nécessaire et autorisé, il est possible de mettre en place le système de diode décrit ci-dessous pour encadrer ces échanges. L'implémentation de ces diodes est donc **optionnelle**.

Information

Alternativement, il est possible de mettre en place une passerelle d'échange de fichiers au sein de son SI. Cette passerelle étant extérieure au poste, elle ne sera pas décrite dans ce document.

Le système de diodes entre domaines utilisateurs possède les propriétés suivantes :

3.18.1 Seuls des dossiers et fichiers peuvent être envoyés.

3.18.2 Les diodes sont unidirectionnelles et dédiées à la communication entre deux domaines utilisateurs identifiés.

3.18.3 Les fichiers d'un domaine utilisateur destinés à être exportés doivent être désignés par une action explicite de l'utilisateur dans ce domaine.

3.18.4 Le transfert d'un fichier doit être accepté par l'utilisateur par l'intermédiaire d'une interface graphique cloisonnée dans un domaine support.

3.18.5 Chaque transfert doit être journalisé dans le domaine support de journalisation du socle. Chaque entrée doit comporter les métadonnées du transfert, comme par exemple :

> le nom du fichier ;
> le *hash* du fichier ;
> l'horodatage ;
> le sens du transfert ;
> la raison du refus de transfert, le cas échéant.

3.18.6 Pour s'assurer de l'innocuité des fichiers transférés, il est possible de mettre en œuvre divers outils de traitement. La décision de transmission du fichier à l'issue de ces traitements est laissé à la discrétion de la PSSI. Parmi les traitements envisagés, on peut par exemple citer :

> une recherche de motifs ;
> une recherche antivirale.

3.18.7 Si des outils d'analyse de fichiers sont déployés, ils doivent être cloisonnés dans un domaine support dédié à cet usage et être exécutés de manière non-privilégiée. Ce domaine doit être instancié pour chaque diode.

Attention

Le système de diodes ne doit pas pouvoir être utilisé pour créer un canal de communication non surveillé d'un domaine utilisateur à un autre.

Les seules communications autorisées entre domaines utilisateurs au sein du poste sont celles utilisant le système de diodes décrit ci-dessus.

4
Recommandations non fonctionnelles

Ce chapitre regroupe, sans définir de nouvelles fonctions de sécurité, les recommandations concernant la conception, le cycle de vie et la documentation d'un poste de travail multi-environnements.

4.1 Niveau de sensibilité

4.1.1 Le socle est considéré d'un niveau de sensibilité au moins égal à celui du plus sensible des domaines utilisateurs. Les contraintes réglementaires relatives à ce niveau de sensibilité doivent donc être respectées par le socle, ce qui peut nécessiter l'ajout de mesures techniques ou organisationnelles supplémentaires à celles de ce document.

4.2 Documentation

4.2.1 Le concepteur du produit doit produire une documentation technique décrivant de manière détaillée l'architecture du poste. Sa conception doit être décrite et justifiée. La surface d'attaque, le modèle d'attaquant et les risques doivent avoir été analysés de manière exhaustive [7].

4.2.2 La liste de tous les composants du poste (logiciels, librairies…) et de leurs versions doit être dressée sous forme d'une SBOM (*Software Bill Of Materials*). Cette liste doit être maintenue à jour et livrée avec chaque mise à jour du poste. Cette SBOM permet notamment de rapidement déterminer si le système est vulnérable lorsque des vulnérabilités sont rendues publiques.

4.3 Procédure d'effacement sécurisé

4.3.1 Une procédure d'effacement sécurisé du poste doit être définie afin d'anticiper son décommissionnement ou son recyclage. Se référer au guide *Recommandations pour le reconditionnement des ordinateurs de bureau ou portables* [4].

7. À titre d'exemple, des documentations de ce type sont accessibles dans le cadre du projet de poste multiniveau CLIP OS (`https://docs.clip-os.org/`) et sur le dépôt de code GitHub dédié (`https://github.com/CLIPOS-Archive/clipos4_doc`).

4.4 Evaluation de sécurité

4.4.1 Les choix de conception du poste doivent permettre à un évaluateur de tester facilement les fonctions de sécurité du poste. En particulier, les fonctions de défense en profondeur doivent pouvoir être testées.

4.5 Défense en profondeur

4.5.1 Le principe de défense en profondeur doit être respecté lors de la conception du poste.

4.6 Maintenance

4.6.1 Les choix de conception du poste doivent prendre en compte le cycle de vie du poste et doivent permettre sa maintien en condition opérationnelle et de sécurité dans le temps (MCO et MCS).

4.6.2 Le délai de mise à disposition d'un correctif doit être spécifié par le développeur du poste au moment de sa conception.

4.6.3 Le processus de mise à jour doit assurer qu'il ne reste pas de vulnérabilité publique sur le socle et les domaines supports.

Bibliographie

[1] *Guide pour l'élaboration d'une politique de sécurité des systèmes d'information*.
Guide Version 1.0, ANSSI, mars 2004.

[2] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[3] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v2.0, ANSSI, novembre 2023.
https://cyber.gouv.fr/guide-nomadisme-numerique.

[4] *Recommandations relatives au reconditionnement des ordinateurs de bureau ou portables*.
Guide ANSSI-PA-097 v1.0, ANSSI, juin 2023.
https://cyber.gouv.fr/guide-reconditionnement-PC.

[5] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[6] *Instruction interministérielle n°901*.
Référentiel Version 1.0, ANSSI, janvier 2015.
https://cyber.gouv.fr/ii901.

[7] *Recommandations pour la mise en place de cloisonnement système*.
Guide ANSSI-PG-040 v1.0, ANSSI, décembre 2017.
https://cyber.gouv.fr/guide-cloisonnement-systeme.

[8] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[9] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, août 2021.
https://cyber.gouv.fr/igi1300.

Version 1.0 - 16/01/2026 - ANSSI-PA-114

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité