RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

RECOMMANDATIONS POUR LES ARCHITECTURES DES INTERCONNEXIONS MULTINIVEAUX

GUIDE ANSSI

ANSSI-PA-101
01/10/2024

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Recommandations pour les architectures des interconnexions multiniveaux »**. Il est téléchargeable sur le site `cyber.gouv.fr`.
Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab.
Conformément à la Licence Ouverte v2.0, le document peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	01/10/2024	Version initiale

Table des matières

1 Introduction **4**
- 1.1 Objectif du guide . . . 4
- 1.2 Organisation du guide . . . 5
- 1.3 Convention de lecture . . . 6

2 Terminologie **8**
- 2.1 Définitions . . . 8
  - 2.1.1 Interconnexions . . . 8
  - 2.1.2 SI haut et SI bas . . . 9
  - 2.1.3 Interconnexions indirectes et interconnexions directes . . . 10
- 2.2 Types des données à transférer et contraintes de transfert . . . 12

3 Précautions d'emplois **16**

4 Principes directeurs **18**
- 4.1 Justification du besoin . . . 18
- 4.2 Homologation des interconnexions des systèmes d'information classifiés . . . 20
- 4.3 Besoins et services de sécurité . . . 22
  - 4.3.1 Besoins de sécurité . . . 22
  - 4.3.2 Services de sécurité d'une interconnexion montante . . . 22
  - 4.3.3 Services de sécurité d'une interconnexion descendante . . . 23
- 4.4 Dispositifs de sécurité essentiels . . . 24
  - 4.4.1 Dispositifs de sécurité essentiels pour une interconnexion montante . . . 26
  - 4.4.2 Dispositifs de sécurité essentiels pour une interconnexion descendante . . . 27
- 4.5 Protection contre les signaux compromettants . . . 29

5 Architectures des interconnexions multiniveaux directes **31**
- 5.1 Interconnexions montantes . . . 31
  - 5.1.1 Interconnexion montante pour le transfert de fichiers . . . 31
  - 5.1.2 Interconnexion montante pour le transfert de flux . . . 35
- 5.2 Interconnexions descendantes . . . 36
  - 5.2.1 Interconnexion descendante avec visualisation exhaustive . . . 36
  - 5.2.2 Interconnexion descendante avec analyse exhaustive et automatisée de contenu 42
  - 5.2.3 Interconnexion descendante avec aiguillage de confiance . . . 45
- 5.3 Cas particulier des interconnexions bidirectionnelles . . . 48

6 Architectures des interconnexions multiniveaux indirectes **49**
- 6.1 Interconnexion montante indirecte . . . 51
- 6.2 Interconnexion descendante indirecte . . . 53

7 Mesures de protection des interconnexions **57**
- 7.1 Bonnes pratiques pour la conception et le développement des dispositifs de sécurité essentiels . . . 57
- 7.2 Bonnes pratiques d'architecture d'une interconnexion multiniveau . . . 61

8 Administration des interconnexions **63**

Annexe A Homologation de sécurité **67**

Liste des recommandations **69**

Bibliographie **73**

1 Introduction

1.1 Objectif du guide

La législation française impose [1] que les informations et supports dont la divulgation ou l'accès est de nature à porter atteinte à la défense et à la sécurité nationale soient soumis à la protection du secret de la défense nationale. Il existe deux niveaux de classification du secret de la défense nationale [2] : Secret et Très Secret.

Lorsque les informations classifiées sont dématérialisées, elles sont traitées par des systèmes d'information classifiés qui doivent faire l'objet de mesures de protection particulières décrites dans l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD (IGI 1300) du 9 août 2021 [8] et dans ses éventuelles déclinaisons sous forme d'instructions ministérielles.

La doctrine générale de sécurisation des systèmes d'information classifiés est celle de l'isolation physique. Le principe d'isolation physique interdit toute forme d'échange de données entre le système d'information classifié et d'autres systèmes d'information. Le respect strict de ce principe rend théoriquement impossible toute compromission du système d'information isolé autrement que par un accès physique au système d'information. Ainsi, l'IGI 1300 interdit par principe toute interconnexion entre un système d'information classifié et un système d'information non classifié ou de niveau de classification différent. Pour ce faire, il convient de se reporter à la section 6.2.2 de l'IGI 1300 [8].

Dans la pratique, pour des besoins d'exploitation tels que le maintien en condition de sécurité et le maintien en condition opérationnelle, il peut être nécessaire de permettre des échanges entre un système d'information classifié et un système d'information non classifié. Il peut également exister, pour certains systèmes d'information classifiés, des besoins opérationnels spécifiques nécessitant une interconnexion avec un système d'information non classifié ou de classification différente.

L'IGI 1300 prévoit la possibilité de déroger à l'interdiction de principe en cas de besoin opérationnel strictement nécessaire. Cependant, la création d'interconnexion rompt le principe d'isolation physique stricte du système d'information classifié, et l'expose par exemple à l'injection de codes malveillants et l'exfiltration d'informations classifiées. Par conséquent, la création d'une interconnexion doit demeurer exceptionnelle et être strictement contrôlée.

À la date de publication de ce guide, la majeure partie des interconnexions multiniveaux (cf. section 2.1.1) sont réalisées à l'aide de supports amovibles. Ce type d'interconnexion est dite « indirecte » car il assure une rupture des signaux électriques ou lumineux intentionnels [3] entre les

1. Article R2311-3 du Code de la défense.
2. Article R2311-2 du Code de la défense.
3. La problématique des signaux parasites compromettants doit également être traitée pour ce type d'interconnexion.

systèmes d'information. En revanche, l'utilisation de supports amovibles restreint le transfert de données aux fichiers, excluant les échanges d'information en temps réel tels que les flux vidéos ou les flux de téléphonie pour lesquels une interconnexion « directe » est nécessaire.

Ce guide explicite les principes et recommandations de sécurité pour la création d'interconnexions multiniveaux directes et indirectes. Il s'adresse aussi bien aux autorités d'emploi de systèmes d'information classifiés qu'aux entreprises souhaitant développer des solutions d'interconnexions multiniveaux. Il se concentre principalement sur la protection de la confidentialité des informations classifiées dans le cadre d'interconnexions multiniveaux.

Au travers de cas d'usage simples, ce guide vise à apporter des principes d'architecture et des mécanismes de sécurité importants, qu'il convient de considérer dans l'élaboration des interconnexions multiniveaux. Ces éléments doivent être adaptés à chaque contexte et emploi. Ces cas d'usage n'ont pas vocation à apporter des architectures directement prêtes à l'emploi et opérationnelles. Il appartient à chaque projet d'identifier les mécanismes de sécurité adaptés à chaque contexte, en fonction d'une analyse des risques prenant en compte les contextes multiniveaux. Pour les interconnexions descendantes, une étude complémentaire devra nécessairement être menée afin de déterminer les canaux cachés à traiter et à la probabilité de fuite d'informations classifiées. L'objectif consistera alors à mettre en œuvre les principes et les mécanismes de sécurité proposés par le guide afin de limiter les risques de fuite et les rendre acceptables par l'autorité d'homologation.

Attention

L'organisation du guide et ses recommandations sont abordées sous le prisme de la confidentialité du SI classifié, telle que définie dans l'IGI 1300. Pour autant, les recommandations permettent également de répondre aux besoins d'intégrité et disponibilités pour les interconnexions multiniveaux.

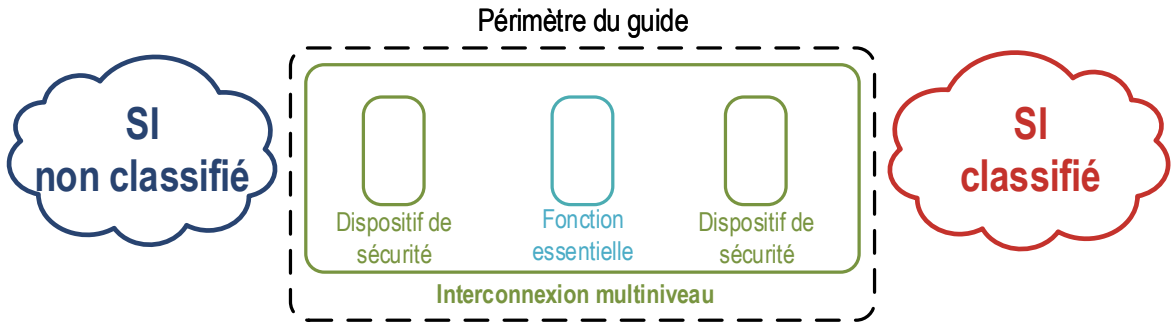

FIGURE 1 – Périmètre du guide

1.2 Organisation du guide

Le chapitre 2 définit le vocabulaire des interconnexions multiniveaux.

La chapitre 3 souligne les risques auxquels s'exposent les SI classifiés de plus haut niveau et devant intégrer une interconnexion multiniveau. Il propose des points d'attention que les autorités d'emploi doivent instuire.

Le chapitre 4 explicite le cadre réglementaire dans lequel doit nécessairement s'inscrire un projet d'interconnexion multiniveau et donne les principes directeurs régissant l'architecture des interconnexions multiniveaux.

Les chapitres 5 et 6 présentent respectivement des exemples d'architectures d'interconnexions directes et d'architectures d'interconnexions indirectes, que celles-ci soient montantes ou descendantes (le chapitre 2 explicite ces différents termes). Ces chapitres indiquent, pour chaque exemple d'architecture, les « fonctions de sécurité essentielles » qui doivent nécessairement être assurées par l'interconnexion multiniveau.

Le chapitre 7 a pour objet de préciser les mesures de sécurité génériques recommandées pour assurer l'intégrité des sous-systèmes constituant une interconnexion multiniveau (serveurs, chiffreurs, diodes, etc.).

Enfin, le chapitre 8 traite de l'administration des interconnexions.

1.3 Convention de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* et l'utilisation de l'icône ⚖ signifient que la recommandation est directement liée à une mesure de sécurité issue de l'IGI 1300. La formulation *il est recommandé* est utilisée pour tout ce qui relève des bonnes pratiques et complète la réglementation.

Pour certaines recommandations de ce guide, il est proposé plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée

Cette recommandation permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

En outre, dans l'objectif d'une démarche itérative de sécurisation, les recommandations alternatives permettent d'établir des cibles intermédiaires et d'identifier des étapes nécessaires pour atteindre la recommandation à l'état de l'art.

La liste récapitulative des recommandations est disponible en page 69.

2
Terminologie

Objectif

Ce chapitre a pour but de définir le vocabulaire propre aux systèmes de transferts de données multiniveaux.

2.1 Définitions

2.1.1 Interconnexions

Pour échanger des données entre deux systèmes d'information (SI), il est nécessaire de réaliser une interconnexion entre ces deux SI.

Interconnexion

Dispositif ou ensemble de dispositifs rendant possible le transfert d'information entre deux SI.

Interconnexion multiniveau

Interconnexion entre un système d'information classifié et un système d'information non classifié ou d'un niveau de classification différent.

Exemple

Exemples d'interconnexions multiniveaux de SI :

- SI homologué Diffusion Restreinte (DR) ⟷ SI homologué Secret
- SI homologué Secret ⟷ SI homologué Très Secret
- SI public [4] ⟷ SI homologué Secret

Information

Les *interconnexions multidomaines*, qui désignent les interconnexions entre deux SI de même niveau de classification ou de niveaux de classification équivalents par accords de sécurité [5] (p. ex. Secret ⟷ Secret OTAN, Secret Spécial-France ⟷ Secret UE) ne sont pas détaillées dans ce guide. Selon les SI interconnectés, l'interconnexion multidomaine peut être soumise à d'autres réglementations (p. ex. réglementation

4. Un SI public est entendu ici comme un réseau de classe 0 tel que défini dans l'II 901.

OTAN). Contrairement aux interconnexions multiniveaux, les interconnexions multidomaines ne sont pas soumises à une interdiction de principe dans l'IGI 1300. Bien que les recommandations de sécurité puissent différer pour les interconnexions multidomaines, il est recommandé de mettre en œuvre les principes des interconnexions multiniveaux aux interconnexions multidomaines. En effet, le risque associé à une interconnexion multidomaine peut être aussi élevé que pour une interconnexion multiniveau. En particulier, le transfert d'une information Secret Spécial France sur un système d'information étranger, au travers d'une interconnexion multidomaine, correspond à une divulgation du secret de la défense nationale qui est couverte par l'article 413-10 du code de la défense.

2.1.2 SI haut et SI bas

Lorsqu'une interconnexion multiniveau est réalisée entre deux SI, il est possible de distinguer un « SI haut » dont les données sont à protéger et un « SI bas ». L'approche de ce guide consiste à détailler des recommandations pour la protection du SI haut. Aucune recommandation n'est prévue pour la protection du SI bas. Si ce dernier doit également être protégé vis-à-vis du SI haut, une démarche similaire doit être appliquée en lui attribuant le rôle de SI haut. Par exemple, une entité disposant d'un SI DR de classe 2 (au sens de l'II 901) et souhaitant recevoir des informations depuis un système d'information Secret qu'elle ne maîtrise pas, peut mettre en œuvre une interconnexion montante bien que le niveau de sensibilité du SI qu'elle maîtrise soit inférieur à celui du SI avec lequel il s'interconnecte. Cependant, dans la suite de ce document, le SI haut est considéré comme étant celui dont le niveau de classification des informations traitées est le plus élevé.

SI haut

SI dont le niveau de confidentialité des données ou des traitements est supérieur, relativement au SI auquel il est interconnecté. Le SI haut est parfois aussi appelé *niveau haut*.

SI bas

SI dont le niveau de confidentialité des données ou des traitements est inférieur, relativement au SI auquel il est interconnecté. Le SI bas est parfois aussi appelé *niveau bas*.

Information

Il est possible de s'inspirer des principes de ce guide dans le cadre d'interconnexions entre systèmes de niveaux équivalents, mais dont les autorités d'emploi diffèrent. Ainsi, une autorité d'emploi d'un SI pourra décider de mettre en place une interconnexion avec un autre SI n'étant pas sous sa maîtrise. Elle pourra alors considérer le SI dont elle a la maîtrise comme le SI haut, et le SI qu'elle ne maîtrise pas comme le SI bas. Rappelons que ceci n'a de sens que si l'autorité d'emploi considère que la confidentialité des données du SI qu'elle maîtrise et leur non divulgation au SI externe est le critère de sécurité essentiel.

5. Les exigences relatives aux problématiques *TEMPEST* et aux agréments des produits ne sont pas strictement équivalentes et peuvent nécessiter de d'appuyer sur la réglementation OTAN ou UE plutôt que la réglementation française.

Attention

Lorsqu'un SI est homologué pour un niveau de classification, cela signifie qu'il est apte à traiter des informations dont le niveau de classification est au plus égal à ce niveau. Cela n'exclut pas que des données d'un niveau de classification inférieur ou non classifiées puissent également y être traitées.

Lorsque le besoin fonctionnel est de pouvoir importer des données depuis le SI bas vers le SI haut, alors l'interconnexion permettant ce transfert est appelée interconnexion *montante*.

Interconnexion multiniveau montante

Interconnexion permettant le transfert unidirectionnel de données du SI bas vers le SI haut. Par simplification, les appellations *interconnexion multiniveau montante* et *interconnexion montante* sont équivalentes dans la suite du document.

Lorsque le besoin fonctionnel est de pouvoir exporter des données depuis le SI haut vers le SI bas, alors l'interconnexion permettant ce transfert est appelée interconnexion *descendante*. Les informations échangées au travers d'une interconnexion descendante doivent être d'un niveau de confidentialité inférieur ou égal au niveau pour lequel le SI bas est homologué.

Interconnexion multiniveau descendante

Interconnexion permettant le transfert unidirectionnel de données du SI haut vers le SI bas. Par simplification, les appellations *interconnexion multiniveau descendante* et *interconnexion descendante* sont équivalentes dans la suite du document.

Attention

Une interconnexion multiniveau descendante, telle que celles décrites dans ce guide, ne fait pas de déclassification ni de déclassement [6] de l'information. En effet, la déclassification ou le déclassement d'une information est une procédure administrative codifiée dans l'article R. 2311-4 du code de la défense, qui n'est pas l'objet de ce guide.

Lorsque le besoin fonctionnel est de pouvoir à la fois importer et exporter des données entre SI haut et le SI bas, alors l'interconnexion permettant ces transferts est appelée *interconnexion bidirectionnelle*.

Interconnexion multiniveau bidirectionnelle

Interconnexion permettant le transfert de données du SI bas vers le SI haut et inversement.

2.1.3 Interconnexions indirectes et interconnexions directes

Il est également pertinent de distinguer les interconnexions selon leur nature : *directe* ou *indirecte*. Comme énoncé dans l'introduction, la majorité des interconnexions multiniveaux sont, à la date

6. Un déclassement est une modification du niveau de classification d'une information, qui reste classifiée à l'issue du déclassement (p. ex. déclasser une information du niveau Très Secret au niveau Secret).

de rédaction de ce guide, des interconnexions montantes mettant en œuvre des supports amovibles afin d'assurer le maintien en condition opérationnelle (MCO) et le maintien en condition de sécurité (MCS) des systèmes d'information classifiés. Par l'utilisation de supports amovibles, ces interconnexions indirectes montantes imposent une action physique, généralement réalisée par un être humain par la connexion d'un support amovible, pour réaliser le transfert des données.

Par la nécessité d'une action humaine, les transferts de données par interconnexion indirecte peuvent sembler moins risqués que les interconnexions directes. En effet, en cas de compromission du SI haut, il ne peut théoriquement pas y avoir de transfert automatique et incontrôlé de données au travers de l'interconnexion, puisqu'une action humaine et nécessaire. Néanmoins, les risques d'exfiltration sont bien présents dans le cadre des interconnexions indirectes, y compris lorsque l'entité utilise exclusivement des supports amovibles qu'elle maîtrise et interdit toute connexion de supports amovibles externes. De nombreux outils sophistiqués ont été spécifiquement conçus et exploités pour exfiltrer des données depuis des systèmes d'information isolés, aussi appelés « *air gap* », à l'instar de USBferry, USBStealer, Agent.BTZ, Remsec ou encore PlugX[7]. Il est donc important de bien comprendre qu'il est tout à fait possible d'exfiltrer de façon automatisée et ciblée, sans compromettre un personnel de l'entité ciblée, des informations d'un système d'information pourtant totalement « déconnecté ».

Attention

Par la nécessité d'une action humaine, les transferts de données par interconnexion indirecte peuvent sembler moins risqués que l'utilisation d'interconnexions directes. Il faut être très attentif au faux sentiment de sécurité que peut procurer la nécessité d'une action humaine pour le transfert de données et notamment aux nombreuses attaques connues sur les interconnexions indirectes utilisant des périphériques USB.

Information

Les interconnexions indirectes ne sont pas définies dans l'IGI 1300, dont la terminologie « interconnexion » correspond aux interconnexions directes de ce guide. Cependant, l'IGI 1300 traite de l'utilisation de supports amovibles comme moyen de transfert d'information entre un SI classifié et un autre SI[8], ce qui correspond aux interconnexions indirectes de ce guide lorsque l'autre SI est non classifié ou de classification différente.

Interconnexion indirecte

Interconnexion réalisée avec une rupture dans la transmission intentionnelle des signaux électriques ou lumineux entre les deux SI (p. ex. support amovible, impression puis numérisation de document).

Sas

Dispositif ou ensemble de dispositifs permettant de réaliser une interconnexion *indirecte* entre deux SI. Un sas utilise un ou plusieurs supports amovibles pour acheminer les données entre les deux SI.

7. https://web-assets.esetstatic.com/wls/en/papers/white-papers/eset_jumping_the_air_gap_wp.pdf.
8. Se référer au chapitre 6.8.2 de l'IGI 1300 [8].

Point d'extraction de données (PED)

Poste informatique depuis lequel les données sont extraites ou exportées du SI.

Point d'insertion de données (PID)

Poste informatique dans lequel les données sont insérées ou importées dans le SI.

Un inconvénient majeur des interconnexions indirectes est l'impossibilité de réaliser des communications en temps contraint. En effet, la rupture de continuité des signaux électriques et l'utilisation d'un support de stockage d'information devant être physiquement déplacé depuis un point d'extraction vers un point d'insertion imposent le recours à des blocs de données. Lorsque le besoin d'échange d'information correspond à une communication en temps contraint (p. ex. un flux vidéo de surveillance d'un lieu), il est nécessaire de pouvoir transmettre l'information sans rupture des signaux, c'est-à-dire d'avoir recours à une interconnexion directe.

Interconnexion directe

Interconnexion réalisée par une continuité de signaux électromagnétiques entre les deux systèmes d'information (p. ex. câble réseau, diode optique).

2.2 Types des données à transférer et contraintes de transfert

En phase d'étude d'un projet d'interconnexion multiniveau, il est indispensable d'identifier formellement les différents besoins d'échange d'information entre les deux SI à interconnecter. En effet, la conception de l'interconnexion multiniveau (identification du type d'interconnexion, directe ou indirecte, montante ou descendante) dépend du strict besoin d'échange d'information, du type de données à transférer et des contraintes temporelles pesant sur ces transferts.

Dans le cadre de ce guide, les types de données suivants ont été retenus :

Fichiers (ou documents)

Un fichier (ou document) est un ensemble de données numériques manipulable comme une unité cohérente.
On distingue :

Fichier/document fortement structuré :
Fichier dont la structure (ensemble des champs et ordonnancement de ces champs) est entièrement décrite dans un modèle de données et dont toutes les valeurs possibles des champs sont définies dans le modèle de données.

Fichier/document moyennement structuré :
Fichier dont la structure est entièrement décrite dans un modèle de données, mais pouvant comporter des champs libres d'une taille bornée mais non né-

gligeable au regard de la taille d'une information classifiée (p. ex. fichier XML respectant une DTD (*Document type definition*) peu restrictive).

Fichier/document non structuré :
Fichier dont la structure n'est pas descriptible par un modèle de données.

Flux

Un flux de données est une suite de données numériques générées et transmises en continu pendant une certaine durée.
Le volume total des données à transférer n'est pas nécessairement prédéterminé au début du transfert et, même si la plupart du temps une unité de base existe, le flux est découpé en sous-ensembles de données de taille arbitraire.
On distingue :

Flux structuré :
Flux respectant une grammaire stricte (p. ex. flux vidéo en provenance d'une caméra, flux syslog). Cette grammaire permet de limiter le risque de canaux cachés, sans toutefois le supprimer (exemple du *watermarking* dans un flux vidéo).

Flux non structuré :
Flux ne respectant pas une grammaire vérifiable (p. ex. flux de supervision non structuré, flux chiffré).

Des contraintes temporelles peuvent peser sur la durée maximale tolérable pour effectuer le transfert d'une quantité bornée de données. Un vocabulaire spécifique permet de distinguer les différents cas de figure.

Contraintes temporelles pour le transferts des données

Temps réfléchi :
Les contraintes temporelles pesant sur le transfert des données ne répondent pas à des exigences de délivrance dans des délais imposés et autorisent par conséquent que les vérifications de sécurité soient faites par un humain.

Temps réflexe :
Les contraintes temporelles pesant sur le transfert des données répondent à des exigences de délivrance dans des délais imposés et empêchent (ou rendent très difficile) que les vérifications de sécurité soient faites par un humain.

Temps réel :
Les contraintes temporelles pesant sur le transfert des données doivent impérativement être maîtrisées sous peine de porter atteinte à la sécurité des personnes ou des biens (notion de *temps réel dur* ou temps réel strict). Dans le cas d'une interconnexion *temps réel*, cette exigence de délivrance en une durée imposée va se cumuler avec les exigences de sécurité pesant par ailleurs sur l'interconnexion. La réponse aux objectifs de performance temporelle est généralement recherchée via l'obtention d'une certification adaptée (p. ex. niveaux DAL – *Development Assurance Level* – des normes avioniques).

À titre d'exemples, voici des cas d'usage illustrant ces différentes contraintes temporelles :

- *temps réfléchi* : le transfert des mises à jour de l'environnement logiciel d'un SI classifié depuis Internet ;
- *temps réflexe* : le transfert régulier de la position d'un véhicule vers un SI de classification inférieure ;
- *temps réel* : le transfert des valeurs mesurées de vitesse par un capteur d'un aéronef à un ordinateur de bord sur une liaison AFDX [9].

Dans la plupart des systèmes de communication, il est possible d'identifier des canaux cachés. Lorsqu'un vecteur d'information est détourné par un utilisateur ou un programme malveillant pour transmettre des informations d'une façon imprévue par le système de communication, on parle alors de canal caché. L'exploitation d'un canal caché se caractérise par deux entités malveillantes complices exploitant le système de façon détournée afin d'échanger des informations. Prenons l'exemple du mécanisme de verrou de fichier sur le système d'exploitation GNU/Linux. La connaissance de l'état verrouillé ou libre d'un fichier est un vecteur d'information. Deux processus complices, ne disposant *a priori* pas de canal de communication légitime pour échanger de l'information, mais disposants tous les deux de la capacité de verrouiller le fichier, peuvent échanger de l'information en verrouillant et déverrouillant successivement dans le temps le fichier, chaque état représentant par exemple la valeur 1 ou 0 d'un bit. Remarquons qu'aucun des deux processus n'excèdent les permissions qui leur ont été initialement octroyées puisqu'ils ont légitimement le droit de demander à verrouiller le fichier. Ils enfreignent en revanche la politique de sécurité du système d'information s'il n'était pas prévu qu'ils puissent s'échanger des informations.

Il est utile de distinguer le canal caché du canal auxiliaire. Le canal auxiliaire consiste en la fuite involontaire d'information d'une entité légitime. Cette fuite d'information est exploitée à l'insu de l'entité légitime par une seconde entité malveillante afin de retrouver des informations. Par exemple, l'évolution de la consommation électrique d'un FPGA lors de calculs d'exponentiations modulaires avec une implémentation faible de RSA peut être exploitée pour déduire, bit à bit, la valeur de la clé privée. Les signaux parasites compromettants sont également une forme de canal auxiliaire.

Ces canaux cachés et auxiliaires représentent une menace importante de compromission d'informations classifiées lorsqu'il n'est pas possible de démontrer que le SI haut est totalement exempt de code malveillant, c'est-à-dire dans la plupart des cas. Le cas des canaux auxiliaires doit être traité par le respect de la réglementation en vigueur concernant les signaux parasites compromettants.

Canal caché

Canal de communication non intentionnel ou non autorisé qui permet à deux entités complices de transférer des informations d'une manière qui transgresse la politique de sécurité du système, mais qui n'excède pas les autorisations d'accès des entités.

Exemples de canaux cachés :

- Utilisation de la stéganographie pour communiquer des informations classifiées dans des images d'apparence non sensible.

9. *Avionics Full-Duplex Switched Ethernet* (ARINC 664) est une spécification pour une liaison de données temps réel pour l'avionique critique.

- Contrôle de la fréquence d'envoi des messages au travers d'une interconnexion pour communiquer en morse.
- Utilisation des valeurs non significatives d'une position GPS régulièrement transmise pour encoder des messages.

La protection en confidentialité, intégrité, et anti-rejeu des informations transmises sous forme de paquets IP entre deux systèmes d'information est souvent réalisée par l'utilisation du protocole IPsec configuré en mode tunnel avec le protocole ESP. Cette configuration permet de protéger des informations confidentielles sur un réseau qui ne l'est pas. Une autre utilisation, moins courante, consiste à cloisonner des paquets non confidentiels d'un réseau qui l'est. On parle alors de *tunnel inversé*.

Tunnel inversé

Chiffrement de flux non sensibles pour leur transport sur un réseau sensible.

3
Précautions d'emplois

Le présent guide traite exclusivement de l'interconnexion entre deux systèmes d'information (SI) respectivement nommés SI haut et SI bas dans le guide.

Attention

Les systèmes d'information classifiés ne sont par nature pas destinés à s'interconnecter avec des systèmes non classifiés. Toute interconnexion engendre des risques importants. Seule une intégration des considérations multiniveaux lors de la phase de conception permet de réduire les risques de manière suffisante. Ceci implique de réévaluer les risques pour les SI historiques, notamment au regard de la confidentialité des données et du risque de compromission de ces données et du SI classifié.

R1

Concevoir le SI haut pour intégrer la problématique multiniveau si un besoin opérationnel est identifié

La prise en compte, au plus tôt, des besoins métier relatifs au multiniveau et des considérations de sécurité inhérentes durant la conception du SI haut permet de maîtriser les risques de manière optimale.

Si une interconnexion doit être mise en œuvre sur un système d'information historique, ce guide recommande une méthodologie de travail et des concepts d'architecture pour réduire les risques au minimum. Un certain nombre de fonctions et dispositifs de sécurité y sont également décrits. Ces derniers doivent être utilisés en fonction de la nature de l'interconnexion souhaitée et de l'analyse de risques.

Attention

Quoi qu'il en soit, l'autorité d'emploi du SI haut reste responsable de la sécurité du système d'information, des données traitées et des éventuelles compromissions qui pourraient intervenir. Elle doit évaluer et gérer les risques tout au long du cycle de vie de son SI haut, et en particulier lors de l'introduction d'une interconnexion multiniveau sur un SI haut existant [10]. Il conviendra en conséquence d'adapter les dispositifs de sécurité et les fonctions essentielles pour répondre à ces besoins.

Ce guide traite spécifiquement le cas de l'interconnexion dite « multiniveau », c'est-à-dire d'un système permettant de réaliser des transferts de données entre un système d'information classifié et un système d'information non classifié ou de niveau de classification différent.

10. Se référer au guide de l'ANSSI sur l'homologation de sécurité en neuf étapes simples [1].

R2

Revoir la conception du SI haut en vue de mettre en œuvre une interconnexion multiniveau

La sécurité du SI haut doit être traitée par ailleurs, dans la mesure où elle contribue de manière substantielle au niveau de sécurité global du dispositif multiniveau. En particulier, il convient de s'assurer :

- de la mise en œuvre d'un dispositif de labélisation des données permettant de gérer le cycle de vie de la donnée ;
- de la complétude et la clarté des consignes transmises aux opérateurs manipulant le processus de labélisation et les opérations de contrôle ;
- du déploiement de l'ensemble des mécanismes de contrôle sur l'interconnexion, qu'ils soient automatiques ou humains, et au-delà des seules problématiques de labélisation.

La notion d'interconnexion doit s'entendre comme un ensemble de fonctions de sécurité qui doivent composer celle-ci. De plus, la notion d'interconnexion ne porte aucune connotation géographique. En d'autres termes et compte tenu de la multiplicité des cas d'usages et des combinaisons possibles de systèmes d'information haut et bas, le guide n'a pas été élaboré pour spécifier quelle partie de système d'information porte quelle fonction de sécurité mais se borne uniquement à dire lesquelles doivent être présentes.

En particulier pour les interconnexions descendantes, la sécurité des SI haut doit être particulièrement étudiée afin que son architecture intègre les mécanismes de sécurité nécessaires pour réduire significativement le risque de fuite d'informations. D'une manière générale, « l'ajout d'une interconnexion constitue un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés » (cf. IGI 1300 - section 6.2.2 autres interconnexions). Ainsi, qu'il y ait une ou plusieurs autorités d'homologation et, quel que soit le choix de combinaison de périmètre de couverture, le SI haut, le SI bas et l'interconnexion doivent impérativement faire l'objet d'une homologation.

L'interconnexion de systèmes d'information non classifiés (dont les SI « Diffusion Restreinte » [9]) ou de même niveau de classification n'est pas abordée. Dans le cas d'une interconnexion multidomaine [11], celle-ci n'est pas soumise à une interdiction de principe dans l'IGI 1300.

Attention

Il est toutefois nécessaire d'assurer la sécurité des interconnexions multidomaines. La section 6.2.1 de l'IGI 1300 [8] peut apporter des éléments de précisions en ce sens. Certaines recommandations du guide pourront être appliquées pour concevoir les interconnexions multidomaines et pour la gestion du besoin d'en connaître.

11. Interconnexion entre deux systèmes d'information de même classification.

4
Principes directeurs

Objectif

Ce chapitre énonce les principes directeurs devant régir tout projet d'interconnexion multiniveau.

4.1 Justification du besoin

Par principe, les interconnexions multiniveaux sont interdites. L'IGI 1300 [8] indique en section 6.2.2. :

Interdiction de principe et stricte nécessité opérationnelle

Les interconnexions entre systèmes d'information de niveaux de classification différents ou entre un système d'information classifié et un système d'information non classifié sont par principe interdites. Toute interconnexion de ce type dérogeant à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation.

Il est donc toutefois possible de réaliser des interconnexions multiniveaux à la condition qu'un besoin opérationnel strictement nécessaire le justifie. Pour qu'un besoin d'échange multiniveau puisse être considéré comme strictement nécessaire, il faut notamment démontrer que les informations ne peuvent pas être générées directement dans le SI cible. Par exemple, lorsqu'un SI classifié doit disposer d'une base de temps, la possibilité d'acquérir une horloge atomique doit être privilégiée plutôt que la synchronisation avec une base de temps d'un SI non classifié ou de classification différente.

R3

Éviter de créer des besoins d'interconnexion multiniveau

Lorsque des données doivent être transférées depuis un SI d'un niveau de classification donné, vers un SI de niveau de classification différent, la possibilité de générer les données directement dans le SI cible plutôt que de réaliser une interconnexion multiniveau doit être étudiée.

Lorsqu'un besoin d'échange multiniveau est strictement nécessaire, alors il est envisageable de réaliser une interconnexion multiniveau en dérogation à l'interdiction de principe. Cependant, l'interconnexion multiniveau ne peut être utilisée que pour réaliser les transferts de données répondant au besoin d'échange identifié comme strictement nécessaire. En conséquence, le besoin d'échange doit être décrit le plus précisément possible, idéalement sous la forme d'une liste des besoins de transferts de données.

R4

Identifier exhaustivement les besoins de transferts de données

L'autorité d'emploi doit établir la liste exhaustive des besoins de transferts de données. Il doit être associé, pour chaque besoin, une justification métier, le sens du transfert (import ou export de données), et une description du format des données. Toute évolution du besoin d'échange doit se traduire par une mise à jour de la liste des besoins de transferts de données (ajout, modification ou suppression). La nouvelle liste doit être approuvée par l'autorité d'homologation avant toute modification de l'interconnexion.

Lorsqu'il est identifié qu'une information doit être échangée depuis un SI haut vers un SI bas, c'est que cette information est d'un niveau de confidentialité inférieur ou égal au niveau pour lequel le SI bas est homologué [12]. Il est peut-être possible de générer cette information directement dans le SI bas, puis de l'exporter vers le SI haut au travers d'une interconnexion unidirectionnelle montante. Comme indiqué en introduction, ce guide prend pour hypothèse que la protection de la confidentialité des informations relevant du secret de la défense nationale est le critère de sécurité le plus important. Ainsi, lorsqu'une information doit être échangée entre deux SI de classification différentes, il est moins risqué du point de vue de la protection de la confidentialité des informations les plus sensibles, d'échanger une information depuis le SI bas vers le SI haut, plutôt que l'inverse. En effet, un échange depuis le SI haut vers le SI bas expose d'éventuels canaux cachés qu'un agent malveillant pourrait exploiter pour compromettre des informations du SI haut. Privilégier les interconnexions montantes est similaire à la prise en compte du principe *no read up, no write down* du modèle de sécurité de Bell–LaPadula [13] dans un système.

R5

Privilégier les interconnexions montantes

Il est recommandé de privilégier des interconnexions montantes, vis-à-vis d'interconnexions descendantes. En effet, si une même information doit être synchronisée dans deux SI de niveaux de classification différents, il est recommandé de privilégier la génération de cette information dans le SI bas et de prévoir son transfert dans le SI haut plutôt que l'inverse.

L'approche consistant à prioriser le critère de la confidentialité des données diffère, par les principes d'architecture mis en œuvre, d'une approche qui prioriserait le critère de l'intégrité. Revenons sur l'exemple de la base de temps cité en introduction de la recommandation R3 : il peut être pertinent d'étudier une interconnexion depuis un SI haut vers un SI bas pour synchroniser le SI bas avec une base de temps qui se situerait dans le SI haut, ce qui semble pourtant en contradiction avec la recommandation R5. Cette étude a du sens, mais elle ne s'appuie pas sur la qualité haute ou basse du niveau de confidentialité des SI à synchroniser, mais sur la qualité haute ou basse de leur niveau d'intégrité. Ainsi, lorsque le critère de l'intégrité est le critère de sécurité prioritaire, les interconnexions descendantes sont préférables, depuis le SI de niveau d'intégrité haut vers le SI niveau d'intégrité bas. Ceci correspond au modèle de sécurité de Biba, dont le principe est *no read down, no write up*. Le modèle de sécurité Biba est adapté aux contextes de SI industriels pour lesquels l'intégrité du SI et de ses données est généralement un critère de sécurité prioritaire. Ainsi, il n'est pas possible, lorsqu'un même SI est à la fois haut du point de vue de la confidentialité et

12. Il est rappelé qu'une interconnexion descendante ne fait pas de déclassification de l'information.
13. Modèle de sécurité initialement développé dans le cadre de l'utilisation de systèmes Multics en contexte multiniveau par le département de la défense états-unien. "*Secure Computer System : Unified Exposition and Multics Interpretation*". David Elliott Bell, Leonard J. LaPadula.

de l'intégrité, vis-à-vis d'un autre SI, de respecter simultanément les deux modèles de sécurité, ce qui impose de choisir un critère de sécurité prioritaire pour déterminer le sens de l'interconnexion à privilégier. Dans ce guide, c'est le critère de la confidentialité qui est retenu, ce qui amène à privilégier les interconnexions montantes.

4.2 Homologation des interconnexions des systèmes d'information classifiés

L'interconnexion d'un système d'information classifié à un autre système d'information constitue un changement significatif qui nécessite un renouvellement de l'homologation du SI classifié ainsi qu'une homologation spécifique de l'interconnexion. L'IGI 1300 [8] indique à la section 6.2. :

Homologation d'une interconnexion multiniveau

Toute interconnexion d'un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent est homologuée au niveau du système d'information le plus élevé. Cette interconnexion fait l'objet d'une homologation spécifique. L'ajout d'une interconnexion constitue un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.

La réglementation impose un renouvellement de l'homologation des SI interconnectés. Ce renouvellement implique de réviser l'analyse des risques des SI interconnectés, notamment au regard de l'ajout de l'interconnexion. Cette révision de l'analyse des risques doit permettre de s'assurer que la mise en place de cette interconnexion ne crée pas des risques inacceptables pour les SI interconnectés et permet d'identifier formellement les objectifs de sécurité attendus de l'interconnexion. Dans le cadre d'une analyse des risques suivant la méthodologie EBIOS Risk Manager [5], il est nécessaire d'identifier l'interconnexion dans les scénarios opérationnels liés à l'exfiltration d'informations classifiées et les scénarios opérationnels de compromission du SI haut. L'annexe A consacrée à l'homologation de sécurité des interconnexions multiniveaux précise les modalités de prise en compte de cette analyse des risques.

R6

Réviser l'analyse des risques du SI haut

L'autorité d'homologation du SI haut doit faire réviser l'analyse des risques du SI haut afin de prendre en compte les nouveaux risques engendrés par l'interconnexion.

La révision de l'analyse des risques ne doit pas se limiter à l'étude des risques portant sur la confidentialité des données classifiées du SI haut ; elle doit réviser l'ensemble des risques éventuellement modifiés sur les valeurs métier du SI haut.

R7

Réviser l'analyse des risques du SI bas

Lorsque le SI bas est classifié ou homologué au niveau Diffusion Restreinte, l'autorité d'homologation du SI bas doit faire réviser l'analyse des risques du SI bas afin de prendre en compte les nouveaux risques engendrés par l'interconnexion.

La réglementation impose également de réaliser une homologation spécifique à l'interconnexion. Selon le contexte de conception, développement et déploiement de l'interconnexion, qu'il soit un environnement tactique (matériel embarqué sur un théâtre d'opérations), ou un bâtiment protégé sur le territoire national, l'interconnexion est plus ou moins exposée à des sources de risques qui lui sont propres. Pour ce faire, il est nécessaire de réaliser une analyse des risques spécifiques à l'interconnexion.

Bien que les sources de risques puissent être similaires à celles identifiées dans l'analyse des risques du SI haut, cette analyse des risques diffère de cette dernière par son périmètre. Ainsi, dans l'exemple d'une analyse des risques suivant la méthodologie EBIOS Risk Manager [5], il est nécessaire d'identifier notamment des scénarios stratégiques et opérationnels spécifiques à l'interconnexion, comme le piégeage de composants de l'interconnexion pendant leur transport, la perte d'intégrité des binaires des composants de l'interconnexion, la compromission du SI de développement des composants de l'interconnexion, le rayonnement électromagnétique propre à l'interconnexion, l'attaque de l'interconnexion depuis le SI haut, le SI bas ou le cas échéant son SI d'administration.

Les valeurs métier de l'interconnexion doivent correspondre aux services rendus par l'interconnexion, comme le transfert de données dans un temps garanti, l'inspection contre les codes malveillants à des fins de protection du SI haut, etc.

R8

⚖ Réaliser une analyse des risques spécifique à l'interconnexion

L'autorité d'homologation du SI haut doit réaliser une analyse des risques spécifique à l'interconnexion prenant en compte les spécificités de son déploiement, afin de déterminer ses propres besoins de protection.

Deux, voire trois, analyses des risques sont donc nécessaires, l'une pour déterminer les besoins de sécurité du SI haut que l'interconnexion doit couvrir, et l'autre pour déterminer les besoins de sécurité de l'interconnexion multiniveau pour sa propre protection. En dehors de contextes extrêmement spécifiques (p. ex. SI haut réduit à un composant matériel totalement maîtrisé), il est nécessaire, dans une approche multiniveau, de considérer qu'un attaquant possédant des moyens et une motivation très élevés est capable de faire exécuter un code malveillant sur le SI haut. Il faut donc éviter toute approche consistant à attribuer un niveau de confiance au SI haut dans le but de réduire l'estimation de la probabilité de compromission du SI haut et ainsi de réduire les exigences de sécurité attendues des dispositifs de sécurité [14] de l'interconnexion.

Un équilibre est à trouver entre la définition d'une posture trop souple, augmentant de manière inacceptable le risque de compromission du SI haut ou de divulgation d'informations classifiées, et une posture trop rigide conduisant *in fine* les utilisateurs à contourner la politique de sécurité (p. ex. échanges non contrôlés de données au moyen de supports amovibles), annulant de fait les bénéfices d'une interconnexion maîtrisée. Or, cette recherche d'équilibre doit se faire dans un cadre réglementaire contraint et implique, dans certains cas, des autorités multiples.

14. Se référer à la section 6.5.2 de l'IGI 1300 [8].

4.3 Besoins et services de sécurité

4.3.1 Besoins de sécurité

Un produit, quel qu'il soit, a pour objectif de rendre un ou plusieurs services. Pour apporter un niveau d'assurance satisfaisant sur sa capacité à fournir ses services de façon sécurisée (c'est-à-dire en donnant des assurances quant aux niveaux de disponibilité, d'intégrité et de confidentialité des services rendus), des fonctions de sécurité sont généralement embarquées dans ce produit pour sa propre protection. Dans le cas particulier d'un produit de sécurité (tels que ceux utilisés dans une interconnexion multiniveau), les services rendus par le système sont eux-mêmes des *services de sécurité*.

Information

Dans la suite de ce document, de manière à ne pas créer d'ambiguïté, le terme « services de sécurité » est utilisé pour désigner les fonctions de sécurité rendues par l'interconnexion (directe ou indirecte), dont le but est de protéger le système d'information interconnecté et décrites dans le chapitre 5, tandis que les fonctions de sécurité utilisées comme *mesures de protection* des produits de l'interconnexion sont décrites dans le chapitre 7.

Ainsi, les services de sécurité de l'interconnexion doivent être cohérents avec les besoins de sécurité du SI haut. Ces besoins de sécurité sont définis par l'analyse des risques du SI haut. Ils sont à distinguer des besoins de sécurité propres à l'interconnexion, dont le but est de protéger l'interconnexion elle-même, en adéquation avec l'analyse des risques spécifiques à l'interconnexion, et qui sont couverts par les *mesures de protection* de l'interconnexion.

Par définition, le SI haut héberge des informations relevant du secret de la défense nationale d'un niveau de classification supérieur au niveau d'homologation du SI bas. Du point de vue de la protection du secret de la défense nationale, le besoin de sécurité *essentiel* de l'interconnexion multiniveau est la protection de la confidentialité des données classifiées du SI haut. Selon que l'interconnexion est montante ou descendante, la protection de la confidentialité des données classifiées est apportée par l'unidirectionnalité des échanges pour les interconnexions montantes ou par le contrôle d'autorisation des données à transférer pour les interconnexions descendantes.

Selon les particularités du SI haut, d'autres besoins de sécurité tels que l'innocuité ou l'intégrité des échanges peuvent s'avérer d'une aussi grande importance que la protection du secret de la défense nationale.

4.3.2 Services de sécurité d'une interconnexion montante

La finalité opérationnelle d'une interconnexion montante est le transfert de données depuis le SI bas vers le SI haut. En conséquence, le transfert de données depuis le SI haut vers le SI bas n'est pas nécessaire. La meilleure façon d'assurer qu'aucune divulgation d'informations classifiée ne puisse avoir lieu au travers de l'interconnexion est de bloquer tout transfert de données depuis le niveau haut vers le niveau bas. L'ajout d'une interconnexion montante introduit des risques pour l'intégrité et la disponibilité du SI haut par le biais des données qui sont introduites dans ce

SI. La confidentialité des données du SI haut n'est, *a priori*, pas affectée, à condition qu'il soit impossible d'exploiter l'interconnexion montante pour envoyer de l'information vers le SI bas. Cette impossibilité doit se caractériser par une preuve de l'unidirectionnalité du transfert des données.

Le service de sécurité essentiel d'une interconnexion montante est l'unidirectionnalité, le service de sécurité assurant que seuls les transferts de données depuis le SI bas vers le SI haut sont possibles. En d'autres termes, il s'agit de garantir l'impossibilité de transmettre des données depuis le SI haut vers le SI bas.

Ce service de sécurité est dit *essentiel* car il couvre le besoin de sécurité *essentiel* de protection des informations classifiées du SI haut.

Une interconnexion montante doit également proposer les services de sécurité suivants :

- le contrôle d'innocuité, le service de sécurité assurant l'innocuité des informations transmises afin de protéger l'intégrité du SI haut ;
- le contrôle d'autorisation, le service de sécurité assurant que les informations transférées depuis le SI bas vers le SI haut sont autorisées à être transmises vers le SI haut ;
- la journalisation des transferts, le service de sécurité permettant d'enregistrer les informations relatives à chaque transfert (par exemple les données transférées - fichiers, flux, etc. -, l'horodatage du transfert, les noms des fichiers) et la responsabilité du transfert. La journalisation est utilisée par le processus de détection et les processus de remédiation et de crise pour inventorier les données entrantes dans le SI haut.

Dans certains contextes opérationnels, il est nécessaire de pouvoir acquitter la réception des données transmises depuis le SI bas vers le SI haut. Afin de ne pas remettre en cause l'unidirectionnalité de la chaîne montante, il existe deux possibilités.

- La première possibilité est de faire réaliser l'acquittement du transfert par l'interconnexion, sans compromettre la fonction d'unidirectionnalité, c'est-à-dire que l'acquittement est réalisé par un composant de l'interconnexion situé du côté du SI bas vis-à-vis de la fonction d'unidirectionnalité. Il est alors possible de vérifier que l'information a bien été acheminée au moins jusqu'au composant de l'interconnexion portant cette fonction. Un signal de vie du composant portant cette fonction peut être périodiquement envoyé vers le SI haut afin de détecter des problématiques d'acheminement entre le composant portant la fonction d'acquittement et le SI haut.
- La seconde possibilité est de faire émettre l'acquittement par le SI haut, ce qui implique un transfert de données depuis le SI haut vers le SI bas. Cette seconde possibilité doit être traitée comme une interconnexion descendante avec une chaîne de transmission descendante distincte de la chaîne montante (R52), ce qui la rend significativement plus compliquée à réaliser que la première.

4.3.3 Services de sécurité d'une interconnexion descendante

La finalité opérationnelle d'une interconnexion descendante est le transfert de données depuis le SI haut vers le SI bas. En conséquence, le transfert de données depuis le SI bas vers le SI haut n'est pas nécessaire. L'ajout d'une interconnexion descendante introduit un risque pour la confidentialité

des données du SI haut. Il faut garantir que seules les données autorisées à être exportées vers le SI bas peuvent être transférées par l'interconnexion descendante. La disponibilité et l'intégrité du SI haut ne sont, *a priori*, pas affectées dès lors qu'il n'est pas possible d'injecter des données vers le SI haut par le biais de l'interconnexion descendante. À cet effet, une bonne façon de protéger le SI haut contre l'injection de codes malveillants est de bloquer tout transfert de données depuis le SI bas vers le SI haut à l'aide d'un mécanisme d'unidirectionnalité.

Information

L'unidirectionnalité d'une interconnexion descendante ne permet pas de garantir qu'aucune information classifiée ne peut être divulguée au travers de l'interconnexion. Ce service de sécurité n'est donc pas la fonction de sécurité essentielle, car il ne protège pas d'une exfiltration d'informations classifiées.

Le service de sécurité essentiel d'une interconnexion descendante est le contrôle d'autorisation de transfert, le service de sécurité assurant que seules les données de niveau de sensibilité inférieur ou égal au niveau de sensibilité du SI bas, et dont le transfert est autorisé, peuvent être transférées depuis le SI haut au SI bas.

Ce service de sécurité est dit *essentiel* car il couvre le besoin de sécurité *essentiel* de protection des informations classifiées du SI haut. Le contrôle d'autorisation peut s'appuyer sur des mécanismes d'authentification, de vérification d'empreinte cryptographique, de filtrage des données sur la base d'une liste d'autorisations ou encore d'analyse humaine.

Une interconnexion descendante doit également proposer les services de sécurité suivants :

- l'unidirectionnalité, le service de sécurité assurant que seuls les transferts de données depuis le SI haut vers le SI bas sont possibles. En d'autres termes, il s'agit de garantir l'impossibilité de transmettre des données depuis le SI bas vers le SI haut ;
- la journalisation des transferts, le service de sécurité permettant d'enregistrer les informations relatives à chaque transfert (par exemple les données transférées - fichiers, flux, etc. -, l'horodatage du transfert, les noms des fichiers) et la responsabilité du transfert. La journalisation est utilisée par le processus de détection et les processus de remédiation et de crise pour inventorier les données sortantes du SI haut.

4.4 Dispositifs de sécurité essentiels

Les dispositifs de sécurité sont des moyens matériels ou logiciels destinés à protéger les informations traitées par le système ou à protéger le système lui-même. Une interconnexion propose un ensemble de services de sécurité, chacun s'appuyant sur un ou plusieurs dispositifs de sécurité. Seuls les dispositifs de sécurité réalisant le ou les services de sécurité *essentiels* doivent être agréés.

L'IGI 1300 [8] indique en section 6.2.2 :

Moyens essentiels de protection contre les accès non autorisés

L'interconnexion [multiniveau] est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non autorisés aux informations classifiées ou au système.

Information

Les agréments relatifs à la mention de protection Diffusion Restreinte et les agréments relatifs au secret de la défense nationale se distinguent par la procédure permettant leur obtention. Un agrément Diffusion Restreinte est délivré par l'ANSSI à l'issue, dans la plupart des cas, d'une qualification, généralement de niveau standard. Il arrive cependant qu'un tel agrément soit délivré sans être assorti d'une qualification – soit parce qu'il a été instruit dans un processus spécifique, soit parce que la procédure de qualification a révélé des défauts rédhibitoires pour un usage généraliste, mais acceptables dans un contexte d'emploi spécifique objet de l'agrément. Les agréments relatifs à la protection du secret de la défense nationale font, quant à eux, toujours l'objet d'une instruction dans un processus spécifique, sans recourir à une qualification. Les évaluations techniques sont conduites par l'ANSSI ou la DGA-MI.

Les agréments pour la protection d'informations classifiées de la défense nationale sont exigés par la section 6.5.2 de l'IGI 1300 [8] dont les termes sont rappelés ci-après :

Agrément de sécurité des moyens essentiels de protection

Un dispositif de sécurité mis en place dans un système d'information qui traite d'informations classifiées est agréé par l'agence nationale de la sécurité des systèmes d'information lorsqu'il est utilisé, en complément de mesures organisationnelles de sécurité, comme un moyen essentiel de protection contre les accès non autorisés aux informations classifiées ou au système.

Information

Les agréments pour la protection d'informations classifiées OTAN ou UE sont conditionnés à une seconde évaluation par une agence tierce : SECAN [15] (US) pour l'OTAN, une agence d'un autre État membre reconnue comme *Appropriately QUalified Authority* (AQUA) pour l'UE – l'agrément étant dans ce dernier cas délivré *in fine* par le Conseil de l'UE.

Les moyens essentiels de protection d'une interconnexion multiniveau doivent être agréés [16]. Les autres dispositifs de sécurité mis en œuvre dans une interconnexion multiniveau ne sont pas obligatoirement agréés, mais peuvent toutefois bénéficier d'une évaluation par un centre d'évaluation agréé par l'ANSSI (p. ex. un Centre d'évaluation de la sécurité des technologies de l'information – CESTI).

15. *Military Committee Communications and Information System Security and Evaluation Agency* (SECAN) est l'agence de l'OTAN responsable des évaluations techniques et de la délivrance des agréments des produits protégeant les informations classifiées de l'OTAN. L'évaluation par le SECAN n'est pas obligatoire si le produit ne met pas en œuvre de mécanisme cryptographique (p. ex. une diode optique).

16. Se référer à la section 6.5.2 de l'IGI 1300 [8].

R9

⚖ Utiliser des dispositifs de sécurité agréés pour les services de sécurité essentiels

L'autorité d'emploi doit s'assurer que les dispositifs portant les services de sécurité essentiels de l'interconnexion sont agréés par l'ANSSI pour cet usage.

Lorsqu'il est fait usage de dispositifs de sécurité agréés, ces derniers doivent être employés conformément aux conditions d'emploi délivrées avec l'agrément du produit. Ces conditions indiquent les règles à suivre pour que l'agrément puisse être considéré comme valide. À titre d'exemple, un dispositif agréé peut disposer d'un boîtier spécialement conçu pour détecter une ouverture ou un perçage malveillant, pouvant conduire à un piégeage du composant. Il est alors précisé dans les conditions d'emploi que le boîtier du dispositif doit toujours être visible et régulièrement inspecté pour que son agrément soit valide.

R10

⚖ Respecter les conditions d'emploi des dispositifs agréés

L'autorité d'emploi doit s'assurer que les dispositifs agréés sont utilisés conformément aux conditions d'emploi lorsqu'ils sont utilisés en tant que moyens de protection essentiels au sens de l'IGI 1300.

Ces rappels réglementaires étant faits, il convient d'identifier quels sont les *moyens essentiels de protection* dans les interconnexions montantes, d'une part, et dans les interconnexions descendantes, d'autre part, ce qui est l'objet de la section suivante.

4.4.1 Dispositifs de sécurité essentiels pour une interconnexion montante

Dans le cas d'une interconnexion montante, le *moyen essentiel de protection* contre les accès non autorisés aux informations classifiées du SI haut est le dispositif de sécurité garantissant l'unidirectionnalité des transferts de données. Ce dispositif de sécurité, que l'on peut qualifier de « diode », est constitué de la fonction d'unidirectionnalité et de son ou ses socles d'exécution. En conséquence, conformément à l'IGI 1300, le dispositif de sécurité diode doit être agréé par l'ANSSI. Le niveau de classification associé à l'agrément est celui du SI haut. Par exemple, une interconnexion directe montante entre un SI homologué au niveau Secret (niveau bas) et un SI homologué au niveau Très Secret (niveau haut) nécessite que l'interconnexion comporte un dispositif de type diode disposant d'un agrément Très Secret. Si cette interconnexion montante est indirecte, et emploie donc un support amovible, il est nécessaire de disposer d'un mécanisme garantissant que seule la lecture est possible sur le support amovible lors de sa connexion au point d'insertion de données du SI haut. Ce mécanisme, s'il est utilisé en tant que service de sécurité essentiel (absence de diode agréée entre le point d'insertion haut et le reste du SI haut), doit disposer d'un agrément Très Secret.

R11

⚖ Interconnexion montante : Garantir l'unidirectionnalité des transferts de données (fonction de sécurité essentielle)

Une interconnexion montante doit mettre en œuvre un service de sécurité permettant de garantir l'unidirectionnalité des transferts de données. Il s'agit de la *fonction de sécurité essentielle* d'une interconnexion montante qui doit être assurée par un dispositif de sécurité agréé.

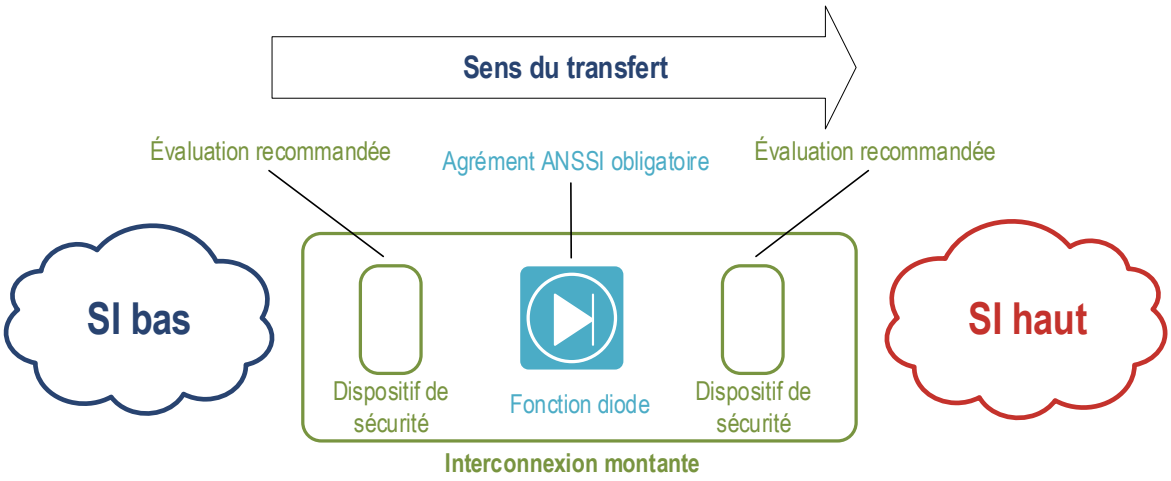

FIGURE 2 – Évaluations de sécurité d'une interconnexion montante

4.4.2 Dispositifs de sécurité essentiels pour une interconnexion descendante

Dans le cas d'une interconnexion descendante, le *moyen essentiel de protection* est le service de sécurité garantissant le contrôle d'autorisation de transfert des informations. Ce moyen garantit que les informations classifiées du SI haut ne sont pas transmises au SI bas. Le dispositif de sécurité essentiel devant faire l'objet d'un agrément est constitué du service de sécurité « contrôle d'autorisation » et de son ou ses socles d'exécution. En conséquence, conformément à l'IGI 1300, le dispositif de sécurité « contrôle d'autorisation » doit être agréé par l'ANSSI. Le niveau de classification associé à l'agrément est celui du SI haut. Par exemple, une interconnexion directe descendante entre un SI homologué au niveau Secret (niveau bas) et un SI homologué au niveau Très Secret (niveau haut) nécessite que l'interconnexion soit constituée d'un dispositif de contrôle d'autorisation disposant d'un agrément Très Secret.

R12

⚖ Interconnexion descendante : Garantir le contrôle de l'autorisation de transmission des données (fonction de sécurité essentielle)

Une interconnexion descendante doit mettre en œuvre un service de sécurité permettant de garantir que seules les données explicitement autorisées à être transmises vers le niveau bas peuvent transiter. Il s'agit de la *fonction de sécurité essentielle* d'une interconnexion descendante qui doit être assurée par un dispositif de sécurité agréé.

Quelle que soit l'architecture retenue, il existe toujours une possibilité d'exfiltration d'informations par l'utilisation de canaux cachés. La présence de canaux cachés et leur débit dépendent de l'architecture physique et logicielle retenue. Il est impératif de savoir identifier le plus exhaustivement possible l'ensemble des canaux cachés ainsi que leur débit maximal de fuite.

R13

Interconnexion descendante : Caractériser les canaux cachés

Le concepteur d'une interconnexion descendante doit caractériser et documenter les canaux cachés de l'interconnexion descendante pouvant être utilisés pour transférer des données depuis le niveau haut vers le niveau bas. La documentation intègre les conditions d'exploitation de chaque canal caché, le débit maximal atteignable ainsi que les mesures de sécurité associées.

Il est possible d'évaluer plusieurs formes de canaux cachés :

- les canaux cachés inhérents au système considéré ;
- les canaux cachés dépendant de la configuration du système ;
- les canaux cachés exploitables après l'ajout de mesures complémentaires.

Les canaux cachés inhérents au système ne dépendent pas de sa configuration. Il s'agit d'une propriété de fonctionnement du système qui n'est pas configurable. Par exemple, un processus d'une machine virtuelle peut exploiter le temps d'accès à une donnée en cache d'un CPU utilisé par un autre processus dans une autre machine virtuelle [17]. Ces canaux cachés doivent être documentés, dans la mesure du possible, par le concepteur de la solution.

Les canaux cachés dépendant de la configuration du système ne peuvent pas être évalués sans la connaissance de la configuration du système. Dans le cadre de la fonction d'analyse exhaustive automatisée (voir 5.2.2), un canal caché peut être établi par un attaquant ayant connaissance des messages autorisés par le filtre, et envoyant des séquences de messages autorisés selon un encodage qu'il aura lui même défini pour, *in fine*, exfiltrer des informations du SI haut.

Les canaux cachés exploitables après l'ajout de mesures complémentaires correspondent à l'évaluation des canaux cachés résiduels issus des deux catégories précédentes lorsque des mesures additionnelles, parfois externes au système concerné, ont été ajoutées de sorte à réduire leur exploitabilité ou leur furtivité. En reprenant l'exemple précédent de l'attaquant envoyant des séquences de messages selon son propre encodage, une mesure de détection pourrait consister à déclencher une alerte lorsque l'envoi d'une succession de messages qui, bien qu'autorisés, sont incohérents par rapport à une utilisation normale du système. Une évaluation du temps de détection et du temps avant la coupure du service doit alors être évalué.

Dans une logique de défense en profondeur, et en inspiration du paradigme de sécurité *data-centric security* [18], il est avantageux de marquer les données, lorsque c'est possible, dans le SI haut, le plus tôt possible dans leur cycle de vie et idéalement dès leur création. Ce marquage, lorsqu'il n'est pas effectué par un dispositif agréé par l'ANSSI pour cet usage, ne peut pas constituer un élément décisionnel de confiance pour l'autorisation de transfert d'une information du SI haut vers le SI bas, mais est utile pour détecter et éviter d'éventuelles erreurs d'acheminement de données vers l'interconnexion descendante.

17. https://gruss.cc/files/hello.pdf.
18. *Data-centric security* (DCS) est un concept de sécurité ayant pour objectif premier de protéger prioritairement la donnée.

R14

Interconnexion descendante indirecte : Marquer la sensibilité des données dans le SI haut

Il est recommandé de mettre en œuvre un marquage de la sensibilité des données au niveau du SI haut, à l'aide d'une nomenclature de noms de fichiers permettant de facilement identifier les informations classifiées.

Information

La recommandation R14 participe à élever le niveau de confiance placé dans l'interconnexion descendante, mais l'intérêt qu'elle procure ne doit pas être surestimé. En effet, la plus-value en matière de sécurité est très dépendante de la qualité du processus de marquage au niveau haut.

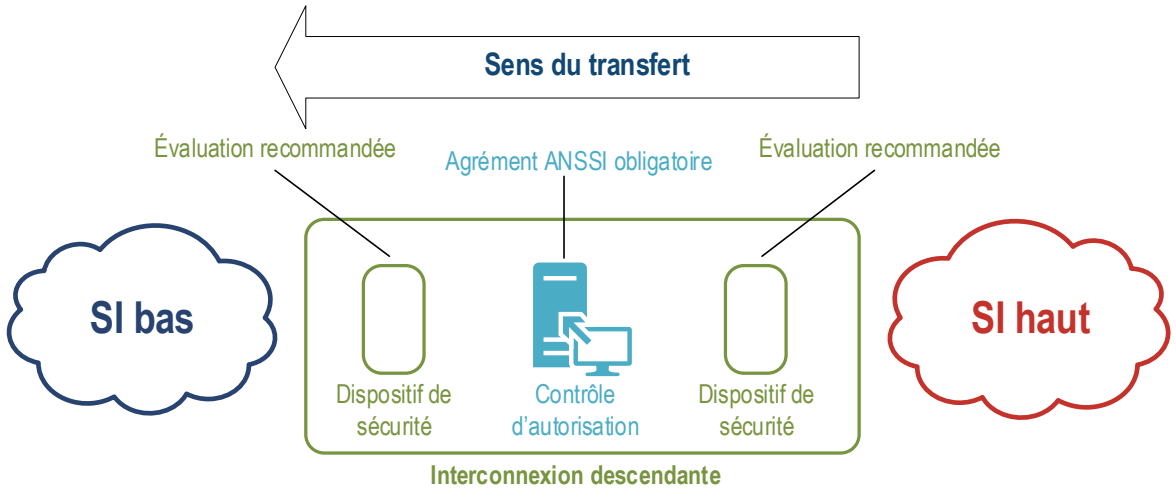

FIGURE 3 – Évaluations de sécurité d'une interconnexion descendante

Information

L'utilisation d'un dispositif d'unidirectionnalité (p. ex. diode optique) n'est pas obligatoire dans le cadre d'une interconnexion descendante, mais est très fortement recommandée par la protection qu'il apporte à l'interconnexion et au SI haut en bloquant toute donnée qui serait issue du SI bas vers le SI haut.

Maintenant que la façon d'identifier les *services de sécurité essentiels* d'une interconnexion, au sens de la réglementation, a été explicitée, il convient d'identifier des modèles d'architecture d'interconnexion directe ou indirecte permettant de traiter différents types de données, selon différentes contraintes temporelles. Cela est l'objet des deux chapitres suivants.

4.5 Protection contre les signaux compromettants

Une interconnexion multiniveau est susceptible de traiter des informations classifiées et certains de ses composants sont intégrés au sein d'un ou plusieurs SI classifiés. Le risque de fuite d'informations

par des signaux parasites compromettants, également appelé menace *TEMPEST*, doit donc être pris en compte pour chacun des éléments de l'interconnexion lorsqu'ils sont présents au sein d'un SI classifié ou à sa frontière. De même, l'usage des technologies sans-fil dans un SI classifié est strictement encadré.

R15

⚖ Prendre en compte les fuites par signaux compromettants dans les SI classifiés

L'instruction interministérielle n° 300 (II 300) impose de protéger les systèmes d'information classifiés contre les signaux compromettants, qu'ils soient intentionnels ou parasites.

Afin de prendre en compte ces menaces le plus efficacement possible, l'II 300 propose une démarche de sécurisation adaptée au niveau de classification visé, à l'affaiblissement des locaux hébergeant les systèmes d'information classifiés ainsi qu'au matériel envisagé pour réaliser l'interconnexion. Des mesures de protection sont alors préconisées afin de limiter les risques de fuites par les signaux compromettants. Cette démarche peut être réalisée avec le concours de l'autorité nationale TEMPEST (ANSSI).

R16

⚖ Mettre en œuvre une démarche de sécurisation contre les signaux compromettants

La mise en œuvre de cette démarche permet de limiter les risques de fuites par les signaux compromettants.

5
Architectures des interconnexions multiniveaux directes

Objectif

Ce chapitre présente des exemples d'architectures pour des interconnexions multiniveaux directes. Les schémas qui suivent présentent les fonctions de sécurité attendues dans des interconnexions multiniveaux directes montantes et descendantes et permettent d'en préciser l'ordonnancement recommandé.
Les entités désirant mettre en œuvre une interconnexion multiniveau directe sont libres de proposer une architecture différente dès lors que celle-ci répond aux mêmes objectifs de sécurité.

5.1 Interconnexions montantes

Il est rappelé que la fonction de sécurité essentielle d'une interconnexion montante est la fonction d'unidirectionnalité.

Dans cette section, deux cas d'interconnexions montantes sont considérés : d'une part, l'interconnexion montante unidirectionnelle pour le transfert de fichiers, d'autre part, l'interconnexion montante unidirectionnelle pour le transfert de flux. Les types de données à transférer (fichiers et flux) ont été définis en section 2.2.

5.1.1 Interconnexion montante pour le transfert de fichiers

Nom de l'interconnexion	Interconnexion montante pour le transfert de fichiers
Dispositif de sécurité essentiel	Dispositif d'unidirectionnalité
Exemples de données échangeables	Tout type de fichier
Temps opérationnel	Temps réfléchi

Une interconnexion montante de transfert de fichiers peut être utilisée pour transférer tout type de fichier, comme des fichiers de mises à jour, des fichiers textuels ou des images, au travers d'un dispositif empêchant tout retour d'information, depuis un SI bas vers un SI haut.

Exemple de cas d'usage

Dans le cadre du maintien en condition de sécurité d'un réseau classifié, il est nécessaire de pouvoir récupérer des fichiers pour les mises à jour logicielles depuis des sources externes. Une interconnexion montante unidirectionnelle peut être utilisée pour permettre la transmission des fichiers de mise à jour depuis un système d'information connecté à Internet.

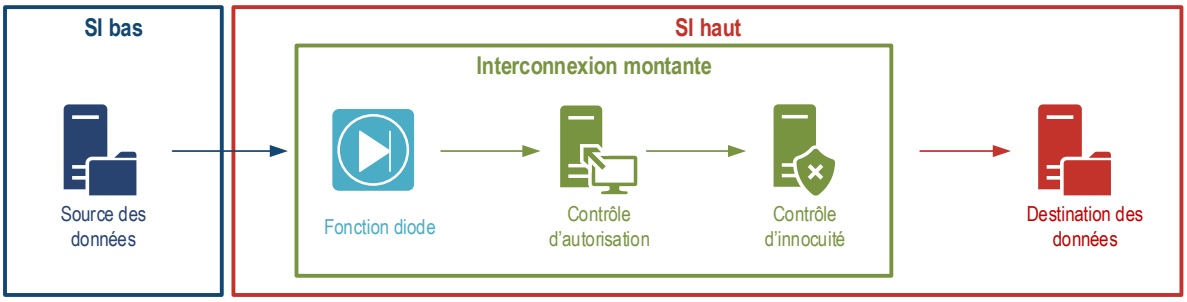

FIGURE 4 – Architecture d'une interconnexion montante pour le transfert de fichiers

Dans l'architecture présentée à la figure 4, le service de sécurité utilisé comme moyen essentiel, au sens de l'IGI 1300, de protection contre les accès non autorisés aux informations classifiées du SI haut est la fonction d'unidirectionnalité ou « fonction diode ». La fonction diode garantit l'unidirectionnalité des transferts de données et empêche ainsi toute fuite d'information depuis le SI haut vers le SI bas au travers de l'interconnexion. L'architecture propose également deux autres services de sécurité : un contrôle d'autorisation et enfin un contrôle d'innocuité, qui contribuent tous les deux à la protection de l'intégrité du SI haut. Idéalement, la fonction d'unidirectionnalité est positionnée avant les autres services de sécurité afin de limiter leur exposition au SI bas et renforcer la confiance que l'on peut accorder à leurs traitements. En effet, en cas d'exécution de code malveillant sur les dispositifs portant ces services, un canal de contrôle ne pourra pas être établi au travers de la diode, rendant l'exploitation plus complexe.

R17

Interconnexion montante pour le transfert de fichiers : Positionner la fonction diode en amont de l'interconnexion

Il est recommandé de positionner le dispositif garantissant l'unidirectionnalité des transferts en amont de l'interconnexion. Par ce choix, les autres services de sécurité disposent d'une isolation relative vis-à-vis du SI bas, ce qui réduit leur surface d'attaque.

Information

Il est rappelé que le dispositif portant la fonction d'unidirectionnalité dans une interconnexion montante est considéré comme le moyen essentiel, au sens de l'IGI 1300, de protection contre les accès non autorisés aux informations classifiées du SI haut et doit faire l'objet d'un agrément de sécurité délivré par l'ANSSI.

Lorsque les données à transférer vers le SI haut ont été signées par l'entité les ayant produites (p. ex. mise à jour logicielle signée par l'éditeur du logiciel), il est recommandé d'effectuer un contrôle de l'authenticité de ces données. Ce contrôle se traduit par la vérification de la validité de la signature, mais aussi le contrôle de l'origine de la signature (p. ex. vérification du *distinguished name* d'un certificat).

R18

Interconnexion montante pour le transfert de fichiers : Contrôler l'autorisation du transfert des fichiers par une vérification de signature

Il est recommandé d'intégrer un mécanisme d'autorisation de transfert de fichiers au sein d'une interconnexion montante. Le mécanisme s'appuie idéalement sur la vérification de l'authenticité du fichier au regard d'une liste d'expéditeurs autorisés [19] à transmettre des fichiers, par la vérification d'une signature cryptographique.

Lorsque les données ne sont pas signées par l'émetteur des données (qui peut être un autre SI que le SI bas), il est possible de les faire signer par un dispositif du SI bas.

R18 -

Interconnexion montante pour le transfert de fichiers : Faire signer par un dispositif du SI bas les fichiers à transmettre vers le SI haut

Lorsque les fichiers à transmettre vers le SI haut ne peuvent pas être signés par l'émetteur, il est recommandé de les faire signer par le SI bas après s'être assuré de leur besoin de transmission vers le SI haut.

Lorsque ceci est également impossible, un niveau dégradé de sécurité pourrait s'appuyer sur des conventions de nommage des fichiers. Dans tous les cas, il est important de s'assurer que les fichiers sont autorisés à être transférés vers le SI haut pour limiter la propagation de codes malveillants.

R18 - -

Interconnexion montante pour le transfert de fichiers : S'appuyer sur une convention de nommage des fichiers

Lorsque les fichiers à transmettre vers le SI haut ne peuvent ni être signés par l'émetteur, ni par un dispositif du SI bas, il est possible de s'appuyer sur une convention de nommage des fichiers pour déterminer lesquels sont autorisés à être transférés vers le SI haut.

Une fois que les fichiers sont autorisés à être transférés vers le SI haut, il peut être utile de faire un dernier contrôle pour vérifier que ces derniers ne contiennent pas de code malveillant. Cette fonction est positionnée après le contrôle d'autorisation, car la surface d'attaque d'un mécanisme de vérification de signature est généralement très inférieure à la surface d'attaque d'un antivirus.

19. Dans le cas de fichiers préalablement téléchargés, cette liste peut être composée de noms de domaines autorisés.

R19

⚖ Interconnexion montante pour le transfert de fichiers : Réaliser un contrôle d'innocuité des fichiers

Il est recommandé qu'une interconnexion montante réalise un contrôle d'innocuité des fichiers à transférer. Ce contrôle d'innocuité est idéalement positionné en aval de la diode, du côté du SI haut, afin de bénéficier des mêmes politiques antivirales que le SI haut.

Lorsqu'un code malveillant est détecté, il doit être mis en quarantaine pour investigation. S'il s'agit d'un faux positif, un administrateur a la possibilité de sortir ce document de la quarantaine. S'il s'agit d'un vrai positif, l'investigation doit être poussée pour déterminer les raisons ayant permis au fichier de passer avec succès le contrôle d'autorisation (la clé privée du destinataire a-t-elle été compromise ?). Ces informations de traçabilité doivent être conservées conformément à la réglementation en vigueur, c'est-à-dire pour une durée d'au moins 3 ans pour les SI de niveau Secret, et d'au moins 5 ans pour les SI de niveau Très Secret [20].

Information

Il est possible de faire réaliser par le SI bas, en supplément du contrôle d'innocuité présenté à la figure 4, un contrôle d'innocuité préalable au transfert de fichiers vers l'interconnexion montante. Ce contrôle, idéalement réalisé par une solution distincte de celle utilisée dans l'interconnexion, et possiblement identique aux solutions déjà existantes dans le SI bas, a pour objectif de réduire l'exposition des composants de l'interconnexion aux codes malveillants. Ce contrôle d'innocuité supplémentaire n'est pas une obligation réglementaire.

Lorsqu'un fichier analysé par le contrôle d'innocuité ne répond pas à la politique de sécurité du SI haut, il est recommandé de le conserver dans une zone de quarantaine afin de permettre une récupération du fichier sur un système distinct pour investigation.

R20

Interconnexion montante pour le transfert de fichiers : Mettre en quarantaine les fichiers bloqués

Il est recommandé de mettre en œuvre une fonction de quarantaine pour les données n'ayant pas été transmises à terme en raison d'un problème de sécurité à l'instar d'un blocage par le contrôle d'innocuité, d'un échec de vérification de la signature du fichier ou de non respect du format autorisé.

Il est souhaitable, afin de faciliter la recherche de la cause d'une éventuelle compromission d'un poste du SI haut, de conserver l'historique des fichiers transférés. La durée n'est pas prescrite par la réglementation et peut être adaptée en fonction de la volumétrie des échanges.

20. Se référer à la section 6.6.4.2 de l'IGI 1300 [8].

R21

Interconnexion montante pour le transfert de fichiers : Enregistrer les fichiers transférés

Il est recommandé d'enregistrer une copie horodatée de tous les fichiers transférés pour une durée conforme aux durées prescrites dans l'IGI 1300 ou toute autre réglementation applicable au SI haut.

Pour le cas des fichiers n'ayant pas fait l'objet d'une mise en quarantaine et selon la volumétrie des fichiers transférés, il peut être acceptable de ne conserver qu'un condensat des fichiers transférés, associé aux métadonnées adéquates, plutôt que le fichier complet.

R21 -

Interconnexion montante pour le transfert de fichiers : Enregistrer les métadonnées et condensats des fichiers transférés

Il est recommandé d'enregistrer les métadonnées et condensats des fichiers transférés lorsque la volumétrie des fichiers ne permet pas, de façon raisonnable, une conservation conformément à la réglementation en vigueur.

5.1.2 Interconnexion montante pour le transfert de flux

Nom de l'interconnexion	Interconnexion montante pour le transfert de flux
Dispositif de sécurité essentiel	Dispositif d'unidirectionnalité
Exemples de données échangeables	Tout type de flux sans connexion (voix, vidéo etc.)
Temps opérationnel	Temps réflexe

Exemple de cas d'usage

Une interconnexion montante pour le transfert de flux peut servir à la récupération de la position des fantassins alliés, issue d'un SI Restreint OTAN, sur un SI d'un avion de combat, de niveau Secret OTAN, effectuant une mission d'appui aérien afin d'éviter les tirs fratricides.

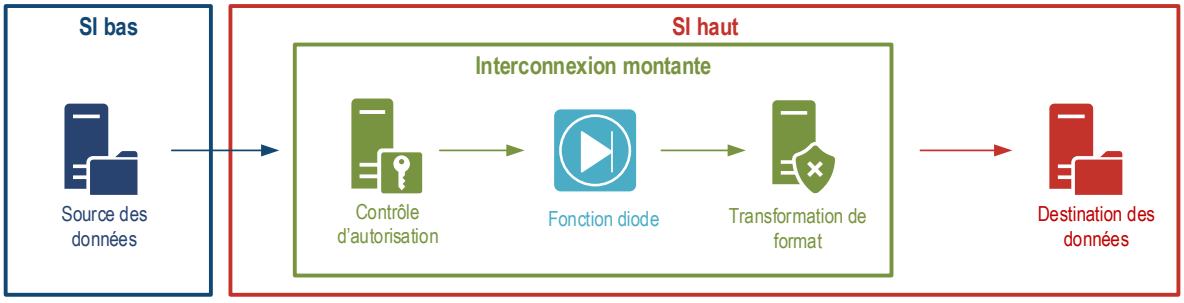

FIGURE 5 – Architecture d'une interconnexion montante pour le transfert de flux

En l'absence d'authentification des données, il est recommandé d'authentifier la source des flux en exploitant les fonctions inhérentes aux protocoles utilisés (p. ex. connexion TLS, tunnel IPsec).

L'authentification de la source des flux sert ainsi de contrôle d'autorisation (autorisation d'une liste définie de sources de flux) avant le passage par la fonction d'unidirectionnalité, cette dernière ne permettant pas l'utilisation de ces protocoles bidirectionnels.

R22

Interconnexion montante pour le transfert de flux : Contrôler la source des flux en amont

Il est recommandé de contrôler la source des flux en amont de l'interconnexion. Ce contrôle s'appuie sur une liste des sources autorisées à transmettre des flux vers le SI haut.

R23

Interconnexion montante pour le transfert de flux : Enregistrer les métadonnées associées aux flux

Il est recommandé de conserver dans les journaux les métadonnées associées aux flux reçus par le contrôle d'autorisation pour une durée conforme à la réglementation en vigueur.

Les deux services suivants sont la fonction d'unidirectionnalité, et la fonction de transformation de format. La fonction d'unidirectionnalité est préférablement positionnée le plus en amont possible, pour les propriétés d'isolation qu'elle confère aux autres dispositifs, d'où son positionnement dans l'architecture présentée à la figure 5. La fonction de transformation de format vise à réduire la surface d'attaque, en opérant, par exemple, un transcodage.

R24

Interconnexion montante pour le transfert de flux : Effectuer une transformation de format

Il est recommandé, lorsque plusieurs codecs peuvent être utilisés pour transporter l'information d'un flux, d'effectuer un transcodage avant la transmission du flux vers le serveur ou le client du SI haut.

5.2 Interconnexions descendantes

5.2.1 Interconnexion descendante avec visualisation exhaustive

Nom de l'interconnexion	Interconnexion descendante avec visualisation exhaustive
Dispositif de sécurité essentiel	Dispositif de visualisation exhaustive
Exemples de données échangeables	Données textuelles analysables par un être humain
Temps opérationnel	Temps réfléchi

Cette architecture emploie un dispositif permettant à un être humain, ci-après nommé « opérateur » de faire la revue des informations candidates à une transmission vers le SI bas, afin de déterminer si le niveau de sensibilité de ces informations est compatible avec le transfert et le cas échéant d'autoriser le transfert. Les informations sont présentées dans un format qui leur permet

d'être visualisées de façon exhaustive par l'opérateur. L'opérateur doit disposer du temps nécessaire pour analyser les informations présentées et ne doit donc pas être contraint en temps pour prendre sa décision.

R25

⚖ Interconnexion descendante avec visualisation exhaustive : Définir les règles de contrôle et de validation des informations ayant vocation à être transférées vers le niveau bas

L'entité doit élaborer un ensemble de règles de gestion et de contrôle claires à destination des utilisateurs du SI, ainsi que des opérateurs ou des mécanismes de contrôle. Les opérateurs doivent être sensibilisés à la compréhension et aux respects de ces règles. Ce type de contrôle ne peut être employé que si l'opérateur dispose d'une capacité à déterminer la sensibilité des informations qui lui sont présentées, ce qui peut nécessiter la mise à disposition d'un ensemble de règles à suivre par l'opérateur pour déterminer le niveau de sensibilité. Selon la politique de sécurité de l'entité, l'opérateur effectuant la revue peut être la personne à l'origine du transfert de l'information. Ce dernier s'assure alors que l'information visualisée correspond effectivement et uniquement à l'information qu'il souhaite envoyer.

Attention

L'interconnexion descendante avec visualisation exhaustive doit idéalement avoir deux opérateurs distincts : un opérateur du SI haut (cela peut aussi être un processus) qui transmet les données transférables à l'interconnexion, et un second opérateur qui contrôle visuellement les données transférables vers le SI bas.

Interconnexion descendante avec visualisation exhaustive au point d'interconnexion

Exemple de cas d'usage

Une interconnexion descendante avec visualisation exhaustive peut servir au transfert du contenu textuel d'un courrier électronique, depuis un système d'information de commandement classifié au niveau Secret OTAN vers un système d'information tactique classifié au niveau Restreint OTAN.

L'architecture d'interconnexion descendante avec visualisation exhaustive repose sur l'hypothèse qu'un opérateur peut déterminer, par une revue humaine, la sensibilité des informations présentées au point d'interconnexion afin d'autoriser ou refuser leur transfert. Cet opérateur peut être l'émetteur des données ou une autre personne ayant les connaissances suffisantes du métier pour faire cette détermination. Afin de garantir l'absence de transmission de données classifiées, la totalité des données à transmettre doivent être présentées et visualisées par l'opérateur. Si une donnée (p. ex. une métadonnée), ne peut pas être validée par un opérateur, alors elle doit l'être par un autre mécanisme tel qu'un contrôle par analyse exhaustive des données, décrit à la section 5.2.2.

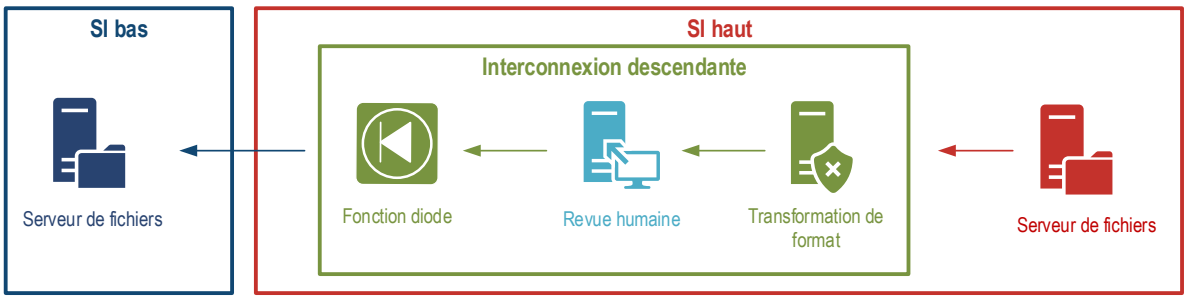

FIGURE 6 – Architecture d'une interconnexion descendante avec visualisation exhaustive colocalisée

R26

⚖ Interconnexion descendante avec visualisation exhaustive : Mettre en œuvre un mécanisme de visualisation exhaustive des données à transmettre

L'interconnexion descendante avec visualisation exhaustive doit mettre en œuvre un système permettant à l'opérateur une visualisation de la totalité des données à transmettre afin que ce dernier puisse autoriser ou refuser le transfert vers le SI bas.

Lorsqu'une donnée ne peut pas être visualisée, ou que sa représentation graphique ne permet pas à un opérateur de déterminer sa sensibilité (p. ex. donnée chiffrée, signature du fichier), la donnée doit être supprimée.

R27

Interconnexion descendante avec visualisation exhaustive : Supprimer les données non visualisables

Le système de visualisation doit supprimer toute donnée non visualisable.

En pratique, la garantie que seules les données visualisées sont transférées se fait préférablement par une extraction des données du fichier d'origine, une visualisation de ces données dans la fonction de visualisation, et une réécriture des données visualisées et validées sur un nouveau fichier créé par le système de visualisation. Cette méthode limite grandement la possibilité de transmettre des données qui n'auraient pas été visualisées (p. ex. métadonnées du fichier d'origine).

R28

Interconnexion descendante avec visualisation exhaustive : Créer un nouveau fichier à partir des données visualisées

Il est fortement recommandé que le système de visualisation crée un nouveau fichier à partir des données visualisées lorsque l'opérateur confirme l'autorisation de transfert.

Une fois que l'opérateur a donné son autorisation de transfert des données visualisées, ces données ne doivent en aucun cas être modifiables par un processus susceptible d'accéder, légitimement ou non, à des données du SI haut. Cette garantie peut être apportée par l'architecture physique retenue (câblage), par des mécanismes de cloisonnement évalués et agréés (p. ex. mécanismes de cloisonnement internes à un système d'exploitation, mécanismes de virtualisation) ou par des mécanismes de signature cryptographique (voir la section 5.2.1).

R29

⚖ Interconnexion descendante avec visualisation exhaustive : Garantir l'intégrité des données après la visualisation exhaustive

Le socle portant le mécanisme de visualisation exhaustive doit garantir qu'aucune modification des données après leur visualisation et validation, n'est possible par un processus susceptible d'accéder, de façon légitime ou illégitime, à de l'information non autorisée à être transférée.

Afin de complexifier les attaques visant à usurper un compte permettant d'autoriser le transfert de données, une authentification forte et multifacteur doit être mise en œuvre.

R30

⚖ Interconnexion descendante avec visualisation exhaustive : Garantir une authentification forte et multifacteur de l'opérateur

Le service de sécurité de visualisation exhaustive doit être accessible uniquement aux utilisateurs authentifiés au moyen d'une authentification forte et multifacteur [21].

Les interfaces des équipements, logiciels et codes doivent être conçues pour réduire au maximum tout risque de validation ou de transfert par erreur d'un fichier. Leur implémentation doit prendre en compte les différents profils utilisateurs de la plateforme. Ainsi, il est par exemple utile de mettre en place des mécanismes de double validation des données visualisées afin d'éviter une validation par erreur.

R31

Interconnexion descendante avec visualisation exhaustive : Confirmer deux fois le transfert d'un fichier

Il est recommandé que le système de visualisation exhaustive impose une double confirmation à l'opérateur avant de transférer le fichier vers le SI bas.

L'enregistrement des transferts autorisés est obligatoire, afin de faciliter l'investigation d'une éventuelle compromission d'informations classifiées. Lorsque, pour des raisons de volumétrie de transfert, la conservation du fichier entier n'est pas possible, il peut être acceptable d'enregistrer le condensat du fichier, son nom, son origine, le nom de l'opérateur ayant validé le transfert, la date et l'heure du transfert, la signature du fichier par l'opérateur.

R32

⚖ Interconnexion descendante avec visualisation exhaustive : Enregistrer les transferts autorisés par l'opérateur

L'interconnexion descendante doit enregistrer une copie de tous les fichiers autorisés à être transférés, la date du transfert, et la signature du fichier par l'opérateur ayant autorisé le transfert de façon à garantir l'imputabilité de l'opérateur. La durée de conservation se fait conformément à la réglementation en vigueur [22].

Afin de tracer d'éventuelles erreurs ou tentatives de transfert d'informations non autorisées, l'enregistrement des données dont le transfert a été refusé par l'opérateur est souhaitable pour investigation. Une fois que l'identification des causes de l'envoi de données non autorisées vers la station

21. Les bonnes pratiques sont explicitées dans le guide sur l'authentification multifacteur et les mots de passe [7].

de visualisation exhaustive a été réalisée, les données peuvent être supprimées et la conservation des métadonnées liées à l'événement est suffisante (p. ex. nom du fichier, date, raison du refus).

R33

Interconnexion descendante avec visualisation exhaustive : Enregistrer les données dont le transfert a été refusé par l'opérateur

Il est recommandé d'enregistrer les données dont le transfert a été refusé par l'opérateur de la visualisation exhaustive. L'événement est horodaté et journalisé. La cause du rejet par l'opérateur doit être précisée (abandon du transfert, informations dont le niveau de classification est incompatible avec le transfert). Les données dont le transfert a été refusé doivent être protégées au moins au même niveau que le niveau de classification du SI haut.

Enfin, l'architecture proposée positionne une fonction d'unidirectionnalité au plus proche du SI bas, afin d'isoler le plus possible les composants de l'interconnexion. Cette fonction d'unidirectionnalité n'apporte aucune garantie sur l'impossibilité d'utiliser l'interconnexion comme vecteur de divulgation d'informations classifiées, le dispositif la portant n'est donc pas nécessairement agréé. Cette fonction de sécurité n'est pas essentielle, mais contribue à protéger l'intégrité du SI haut.

R34

Interconnexion descendante avec visualisation exhaustive : Mettre en œuvre l'unidirectionalité des transferts

Il est recommandé d'intégrer une fonction d'unidirectionnalité des transferts de données.

Interconnexion descendante avec déport de la visualisation exhaustive

Exemple de cas d'usage

Une interconnexion descendante avec déport de la visualisation exhaustive peut servir à la transmission de documents Diffusion Restreinte élaborés dans un SI classifié étendu sur plusieurs sites géographiques distincts vers un SI Diffusion Restreinte et en limitant le nombre d'interconnexions physiques multiniveau. Chaque site géographique peut disposer de sa propre station de visualisation, tandis qu'un seul site nécessite l'intégration de l'interconnexion physique.

Lorsque la fonction de visualisation exhaustive n'est pas réalisée sur un dispositif de sécurité situé au point d'interconnexion physique avec le SI bas, les informations validées peuvent alors transiter sur des équipements réseau traitant des informations classifiées. Il pourrait alors être possible pour un attaquant situé sur le SI haut, entre le point d'interconnexion physique et le dispositif de sécurité portant la fonction de visualisation exhaustive, d'injecter des informations classifiées dans les données validées à destination du SI bas. Afin de se prémunir de ce scénario, il est efficace d'assurer l'authenticité des données validées par la visualisation exhaustive jusqu'au point

22. Se référer à la section 6.6.4.4 de l'IGI 1300 [8] : *Les données de traçabilité des transferts sont archivées sur une durée d'au moins trois ans pour le niveau* Secret *et cinq ans pour le niveau* Très Secret.

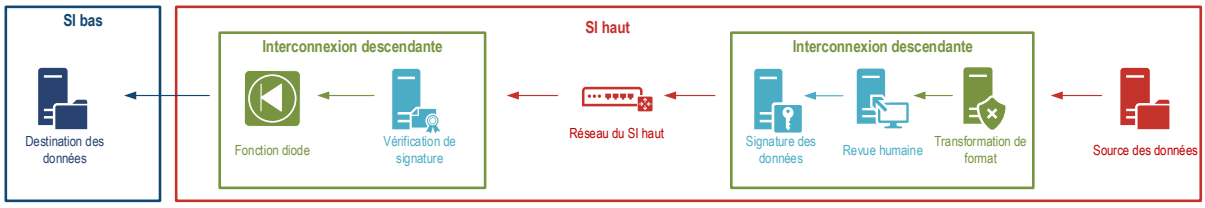

FIGURE 7 – Architecture d'une interconnexion descendante temps réfléchi avec visualisation décentralisée

d'interconnexion physique vers le SI bas. Une méthode adaptée consiste à apposer une signature cryptographique au fichier validé par l'opérateur. Il est également possible d'enrichir les données validées par des informations supplémentaires, comme le niveau de sensibilité des informations ou les destinataires de ces informations. Ces informations supplémentaires sont alors apposées aux données validées, et signées. Ce principe est une forme de labellisation des données et peut servir à catégoriser les données d'un SI.

La signature cryptographique est préférablement réalisée par une clé privée spécifique à l'opérateur afin de garantir l'imputabilité de l'autorisation des transferts. Le contrôle de la validité de la signature, ou éventuellement, de l'adéquation entre le niveau de sensibilité renseigné dans le label et le niveau de sensibilité du SI bas, se fait au point d'interconnexion physique par une fonction de vérification de signature. La confiance dans ce type de contrôle repose autant sur le mécanisme de visualisation exhaustive que sur le mécanisme de signature et de vérification de la signature. Ces trois fonctions sont donc essentielles pour la protection de la confidentialité des informations classifiées du SI haut. Ainsi, dans ce type d'architecture, les dispositifs portant ces fonctions doivent faire l'objet d'un agrément correspondant au niveau de classification du SI haut.

Dans cette architecture, tout fichier signé est susceptible d'être transmis vers le SI bas. L'accès à la fonction de signature doit donc être conditionné à l'autorisation préalable des données à être transmises, par le système de visualisation exhaustive.

R35

⚖ Interconnexion descendante : Garantir la visualisation exhaustive avant la signature

Le système de labellisation doit garantir que l'opérateur a procédé à la visualisation et l'autorisation du fichier avant d'apposer le label et sa signature.

Afin d'éviter qu'un attaquant puisse injecter des informations non autorisées entre le moment où les informations ont été validées par l'opérateur, et le moment de l'appel à la fonction de la signature, il est nécessaire de garantir qu'aucune modification des données validées n'est possible avant la signature. La seule exception serait l'enrichissement des données par l'utilisation du mécanisme de labellisation décrit dans le paragraphe précédent.

R36

⚖ Interconnexion descendante : Garantir que seules les données autorisées peuvent être signées

Le socle portant le mécanisme de visualisation exhaustive doit garantir qu'aucune modification du contenu du fichier n'est possible entre le moment de sa visualisation

et le moment de son éventuelle labellisation ou signature cryptographique.

Afin de permettre à l'opérateur de détecter une signature intempestive ou involontaire, l'opérateur doit être tenu informé de la signature avec succès de données validées.

R37

Interconnexion descendante : Informer l'opérateur de la signature des données

En cas de réussite de la labellisation, la visualisation exhaustive doit afficher un bandeau qui indique que le label du document est signé avec la clé de l'opérateur.

5.2.2 Interconnexion descendante avec analyse exhaustive et automatisée de contenu

Nom de l'interconnexion	Interconnexion descendante avec analyse exhaustive et automatisée de contenu
Dispositif de sécurité essentiel	Dispositif d'analyse exhaustive de contenu
Exemples de données échangeables	Fichiers ou datagrammes structurés prédéfinis
Temps opérationnel	Temps réflexe [23]

Le contrôle d'autorisation se fait de façon automatisée par la vérification du format, de la syntaxe et de la sémantique des données selon une grammaire autorisée prédéfinie. Ce type de contrôle permet un traitement en temps contraint d'informations structurées (p. ex. pistes radar, messagerie tactique hors texte libre).

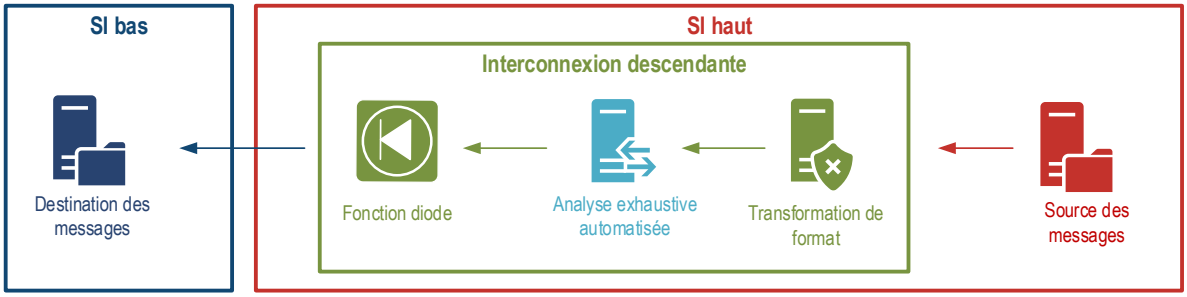

FIGURE 8 – Architecture d'une interconnexion descendante avec contrôle par analyse exhaustive automatisée de contenu

R38

Interconnexion descendante avec analyse exhaustive de contenu : Définir les règles de contrôle et de validation à mettre en oeuvre par le mécanisme de contrôle automatisé afin de vérifier les informations transférées vers le niveau bas

L'entité doit élaborer un ensemble de règles de gestion et de contrôle claires qui doivent être implémentées sur les mécanismes de contrôle automatisés.

23. La possibilité d'atteindre une capacité de temps réel est envisageable selon les socles techniques utilisés.

Un transfert avec une analyse de contenu pouvant prendre la forme d'une analyse exhaustive syntaxique et sémantique du contenu d'un fichier peut être envisagé si le format de la donnée est déterministe, c'est-à-dire s'il est possible de déterminer une grammaire exhaustive n'autorisant que des champs aux valeurs connues à l'avance.

Dans cette architecture, le dispositif permettant l'analyse exhaustive automatisée de contenu est le dispositif de sécurité garantissant que seules les données autorisées peuvent être transmises vers le niveau bas. Il s'agit du dispositif de sécurité essentiel de l'interconnexion descendante.

R39

Interconnexion descendante avec analyse exhaustive de contenu : Mettre en œuvre une analyse exhaustive de contenu

L'interconnexion doit mettre en œuvre une analyse exhaustive automatisée de contenu. Ce contrôle permet de vérifier que chaque champ du bloc de données à transférer correspond à une valeur de champ définie et autorisée dans un dictionnaire de valeurs autorisées.

L'absence d'information classifiée dans le message à transmettre ne peut être obtenue que si l'ensemble des champs bloc de données sont effectivement contrôlés. Il est donc nécessaire que le dispositif d'analyse garantisse que l'ensemble des champs sont contrôlés. Tout champ non contrôlé doit être détecté et entraîner une exclusion de ce champ voire un refus de transfert du message entier.

R40

Interconnexion descendante avec analyse exhaustive automatisée de contenu : Garantir l'exhaustivité des données contrôlées

Il est fortement recommandé que l'interconnexion garantisse que les données à transférer soient contrôlées de manière exhaustive par le dispositif d'analyse exhaustive automatisée de contenu.

Bien que chaque valeur de champ soit contrôlée, la distribution de ces champs dans un bloc de données peut permettre une combinatoire éventuellement exploitable pour créer un canal caché.

R41

Interconnexion descendante avec analyse exhaustive de contenu : Limiter les agencements de champs de données autorisés

Il est fortement recommandé de restreindre au strict besoin les agencements possibles des champs de données dans les blocs de données à transmettre.

La grammaire définissant la syntaxe et les valeurs autorisées doit avoir une taille réduite. En effet, plus elle est grande, plus un attaquant peut exploiter la variété des messages autorisés pour construire son langage propre et l'exploiter en tant que canal caché. À titre d'exemple, une grammaire n'autorisant qu'un seul champ pouvant contenir 37 valeurs distinctes peut théoriquement permettre à un attaquant de coder les 26 lettres de l'alphabet latin, le caractère espace, ainsi que les 10 chiffres et ainsi exfiltrer tout type de texte. La limitation de la grammaire permet de réduire les possibilités d'exploitation de messages autorisés comme un canal caché d'exfiltration d'informations.

R42

Interconnexion descendante avec analyse exhaustive de contenu : Limiter la grammaire des données

Il est fortement recommandé de limiter au strict besoin la grammaire des données à transférer.

Comme énoncé dans l'exemple précédent, malgré la limitation de la grammaire, un attaquant présent, par l'intermédiaire d'un code malveillant qui s'exécuterait sur le SI haut, pourrait être en mesure de forger des messages valides (c'est-à-dire des messages conformes au filtre utilisé par le dispositif d'analyse exhaustive). Afin de limiter l'exploitation de l'envoi de messages autorisés comme canal caché par un attaquant présent sur le SI haut, un ensemble de mesures techniques peuvent permettre de réduire le risque associé, comme la supervision des messages envoyés au regard d'une activité préalablement établie comme normale ou l'authentification de la source des messages. Ces mécanismes doivent être sélectionnés et configurés selon le contexte du métier auquel l'interconnexion est associée.

R43

Interconnexion descendante avec analyse exhaustive de contenu : Détecter des envois intempestifs de messages conformes

Il est recommandé de mettre en œuvre un mécanisme de détection d'envois intempestifs de messages conformes au filtre.

L'authentification de la source des messages à transférer ne permet pas de se prémunir d'un attaquant ayant piégé l'équipement émetteur des messages, mais permet de se prémunir d'un attaquant contrôlant uniquement un équipement réseau du SI haut utilisé pour la transmission entre l'émetteur et l'interconnexion.

R44

Interconnexion descendante avec analyse exhaustive de contenu : Authentifier la source des messages à transférer

Il est recommandé de mettre en œuvre un mécanisme d'authentification de la source des messages à transférer.

Afin de faciliter une investigation à la recherche d'une éventuelle exploitation d'un canal caché utilisant des messages valides, il est utile de conserver les messages transférés, ainsi que la date et l'heure de leur transfert, et si possible l'origine du message. Selon la volumétrie, il n'est pas forcément obligatoire de conserver le message entier, il peut être suffisant de conserver uniquement la référence des champs autorisés présents dans le message (index des champs autorisés de la configuration du filtre), ou de façon dégradée, uniquement un condensat du message.

R45

Interconnexion descendante avec analyse exhaustive de contenu : Enregistrer les métadonnées des transferts

L'interconnexion descendante doit enregistrer les informations relatives aux messages transférés, tels que la date, le contenu et l'origine du message transféré.

5.2.3 Interconnexion descendante avec aiguillage de confiance

Nom de l'interconnexion	Interconnexion descendante avec aiguillage de confiance
Dispositif de sécurité essentiel	Dispositif d'aiguillage des flux
Exemples de données échangeables	Flux voix ou vidéo
Temps opérationnel	Temps réflexe ou temps réel

Le contrôle se fait par isolation du système sur lequel l'information est produite. Cette technique s'appuie sur l'hypothèse que le système producteur d'information produit exclusivement, sur une période de temps identifiable précisément, des informations dont le niveau de confidentialité est inférieur ou égal au niveau de confidentialité du SI bas. Ce type de contrôle permet un traitement en temps contraint d'informations non structurées (p. ex. voix, vidéo, données de capteurs). Le dispositif d'aiguillage permet d'assurer que le système producteur d'information est soit uniquement connecté au SI haut, soit uniquement connecté au SI bas, séquentiellement dans le temps. Il peut prendre, par exemple, la forme d'un interrupteur physique connectant deux circuits, d'un interrupteur électronique par portes logiques.

Interconnexion descendante avec aiguillage colocalisé

Exemple de cas d'usage

Une interconnexion descendante avec aiguillage de confiance colocalisé peut servir, par exemple, à un pilote d'avion de reconnaissance pour transmettre une vidéo de surveillance d'un théâtre d'opération tantôt sur un moyen de transmission de type Secret OTAN, tantôt sur un moyen de transmission de type Restreint OTAN. Le pilote sélectionne, dans le premier cas, la position de l'aiguillage pour router le flux du capteur vidéo vers le moyen de transmission équipé d'un chiffrement Secret OTAN, pour transmettre la vidéo vers, par exemple, un centre de commandement aérien. Le pilote sélectionne, dans un second temps, la position de l'aiguillage pour router le flux vers un moyen de transmission équipé d'un chiffrement de niveau Restreint OTAN, pour envoyer la vidéo vers, par exemple, un réseau tactique utilisé par des fantassins. La source du flux d'information (le capteur vidéo) et l'interconnexion physique multiniveau (l'aiguillage vers l'une ou l'autre radio) sont colocalisées dans l'avion.

La fonction permettant de garantir que seules les informations autorisées sont transmises vers le SI bas est la fonction d'aiguillage. Le dispositif portant cette fonction doit donc être agréé. En pratique, le type de dispositif permettant un aiguillage peut être physique (p. ex. un interrupteur permettant la connexion d'un circuit ou d'un autre circuit électrique) ou logiciel (p. ex. utilisation de circuits reprogrammables).

R46

Interconnexion descendante : Mettre en œuvre un aiguillage

L'interconnexion descendante doit mettre en œuvre un aiguillage de confiance permettant d'isoler la source des données à transférer vers le SI bas.

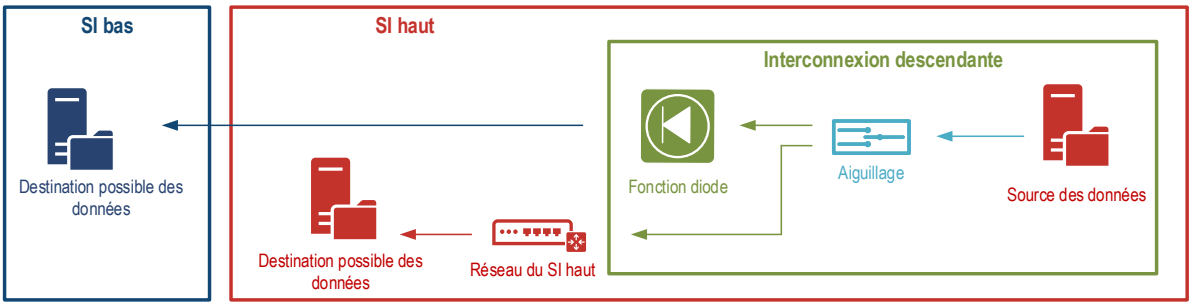

FIGURE 9 – Architecture d'une interconnexion descendante avec aiguillage

Une autre hypothèse forte de ce modèle est que la source du flux ne peut pas contenir d'informations classifiées lorsque l'aiguillage permet une transmission vers le SI bas. Ainsi, un capteur ne doit pas contenir de dispositif de stockage de ses informations, et sa mémoire vive doit être limitée, ou l'alimentation de cette dernière doit être coupée entre deux changements de position de l'aiguillage.

R47

Interconnexion descendante : Garantir l'absence de capacité de rétention d'informations classifiées dans la source

Il est recommandé de sélectionner la source de flux de sorte qu'elle ne puisse pas enregistrer d'informations classifiées.

Afin de tracer les transmissions d'informations, il est nécessaire de journaliser la position de l'aiguillage.

R48

Interconnexion descendante : Enregistrer la position de l'aiguillage

L'interconnexion descendante doit enregistrer en tout temps la position de l'aiguillage de confiance.

Afin d'éviter les erreurs d'utilisation pouvant entraîner une compromission d'informations classifiées, la position de l'aiguillage doit être clairement visible par l'opérateur, et l'information de la position doit être fiable. La fiabilité du mécanisme permettant d'informer l'opérateur sur la position de l'aiguillage peut faire partie des évaluations relatives à l'agrément du dispositif.

R49

Interconnexion descendante : Rendre vérifiable la position de l'aiguillage

L'interconnexion descendante doit rendre vérifiable la position de l'aiguillage à l'opérateur en tout temps.

Le dispositif d'aiguillage, lorsqu'il prend la forme d'un interrupteur physique contrôlé directement par un opérateur présent physiquement devant le dispositif, peut être contrôlé sans mécanisme d'authentification supplémentaire lorsque cela est autorisé par la politique de sécurité du système. Lorsque l'aiguillage est de type électronique ou numérique, l'authentification de l'utilisateur sur le système de contrôle est alors nécessaire pour prévenir une usurpation de son identité sur le

système. Il est alors recommandé de mettre en place une authentification forte et multifacteur.

R50

Interconnexion descendante avec aiguillage : Garantir une authentification forte et multifacteur de l'opérateur

Lorsque la commande de l'aiguillage se fait électroniquement ou numériquement, le changement de position de l'aiguillage doit être réservé à des utilisateurs authentifiés au moyen d'une authentification forte et multifacteur. [24].

Interconnexion descendante avec déport d'aiguillage

Exemple de cas d'usage

Une interconnexion descendante avec déport d'aiguillage de confiance peut permettre à un centre de commandement aérien, équipé d'un SI Secret OTAN et de plusieurs opérateurs de communication, de communiquer avec des avions de combat à un niveau Secret OTAN et avec des avions civils à un niveau Public en conservant un nombre limité d'interconnexions physiques entre les deux réseaux.

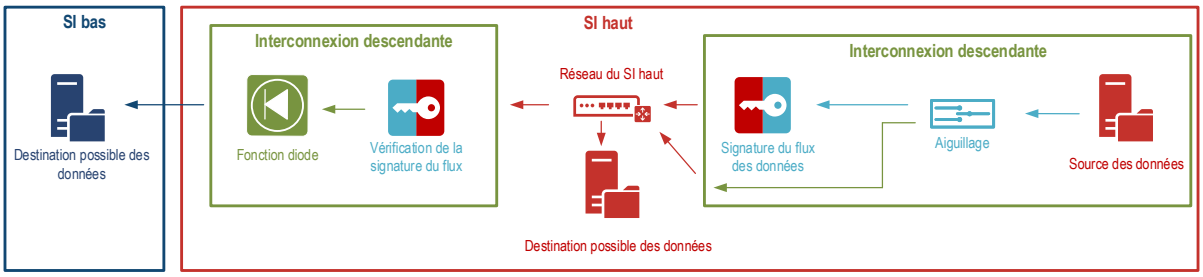

FIGURE 10 – Architecture d'une interconnexion descendante avec déport d'aiguillage

Dans cette architecture, il peut y avoir plusieurs aiguillages et une seule interconnexion physique avec un SI bas. L'utilisation d'une solution de signature de flux permet de garantir que les informations issues de l'aiguillage ne sont pas altérées en traversant le réseau du SI haut. Il s'agit ici de garantir qu'il est impossible d'insérer des informations classifiées dans le flux à destination du SI bas. On utilise alors un mécanisme de *tunnel inversé*. Par exemple, avec l'utilisation d'IPsec, c'est le service d'authenticité et non de confidentialité qui est garant, dans cet exemple, de l'autorisation des informations à être transférées vers le SI bas, et *in fine* de la protection des informations classifiées. Ainsi, le dispositif portant la solution de signature de flux doit être agréé.

24. Les bonnes pratiques sont explicitées dans le guide sur l'authentification multifacteur et les mots de passe [7].

R51

Interconnexion descendante : Mettre en œuvre une solution agréée de signature des flux

L'interconnexion descendante doit mettre en œuvre une solution agréée de signature des flux.

5.3 Cas particulier des interconnexions bidirectionnelles

Quand il existe un besoin de transfert d'informations simultanément dans le sens montant et dans le sens descendant, c'est-à-dire une capacité d'échanges bidirectionnels, il est fortement recommandé d'utiliser deux socles physiquement distincts pour les fonctions essentielles de chaque sens (montant et descendant) et d'appliquer les recommandations correspondant à la fois au sens montant et au sens descendant.

Le cloisonnement des fonctions montantes et descendantes réduit notamment le risque d'exploitation d'une vulnérabilité sur le socle des fonctions de l'interconnexion montante pour mettre en défaut les fonctions de l'interconnexion descendante.

R52

Séparer physiquement les traitements montant et descendant

Il est fortement recommandé de séparer physiquement les traitements des transferts dans le sens montant de celui des transferts dans le sens descendant.

6
Architectures des interconnexions multiniveaux indirectes

Objectif

Ce chapitre présente des exemples d'architectures pour des interconnexions multiniveaux indirectes. Les schémas qui suivent présentent les fonctions de sécurité attendues dans des interconnexions multiniveaux indirectes montantes et descendantes et permettent d'en préciser l'ordonnancement recommandé.
Les entités désirant mettre en œuvre une interconnexion multiniveau indirecte sont libres de proposer une architecture différente dès lors que celle-ci répond aux mêmes objectifs de sécurité.

Comme défini dans le chapitre 2, une interconnexion est considérée comme indirecte lorsqu'il n'existe pas une chaîne continue de signaux électromagnétiques (câbles SFTP, fibre optique) entre le SI haut et le SI bas. Cette propriété est notamment vérifiée lorsque les données sont dans un premier temps inscrite sur un support amovible (clé USB, carte SD, disque dur externe) depuis le premier SI, puis lue sur le second SI.

À date de la rédaction de ce guide, dans la très grande majorité des cas, des clés USB sont utilisées pour réaliser ce type de transfert. En effet, le protocole USB est supporté par la quasi-totalité des ordinateurs, et les clés USB sont simples et pratiques d'utilisation. Cependant, le protocole USB est utilisé pour de nombreux autres usages que le simple transfert de données, à l'instar des périphériques d'interface humaine (p. ex. clavier, souris), de lecteurs de disques externes, caméras, etc. Il revient au périphérique de déclarer ses capacités, ce qui ouvre la voie à certaines attaques comme BadUSB [25].

Il existe également des attaques sophistiquées [26] utilisant des périphériques USB pourtant maîtrisés par des organisations pour extraire des données depuis des SI réputés « isolés ». En effet, de nombreuses attaques par périphériques USB ont exploité des vulnérabilités du traitement des fichiers .LNK [27] (raccourcis Microsoft Windows) par le processus *explorer.exe*. C'est par exemple le cas de Stuxnet [28] mais aussi d'attaques moins médiatisées, exploitant cette même classe de vulnérabilité pour faire exécuter un code malveillant sur un système d'information « isolé » sans nécessiter d'action utilisateur autre que l'ouverture de l'explorateur de fichiers sur la clé USB. Ce type d'attaque, combiné à un formatage astucieux de système de fichiers de la clé USB (p. ex. depuis le SI non

25. https://en.wikipedia.org/wiki/BadUSB.
26. https://attack.mitre.org/techniques/T1052/001/.
27. Les CVE-2010-2568, CVE-2017-8464 et CVE-2020-0729 sont de bons exemples.
28. https://fr.wikipedia.org/wiki/Stuxnet.

isolé) pour créer une seconde partition cachée, permet d'échanger des commandes et des fichiers au gré des connexions des supports amovibles entre le système d'information connecté à Internet et le système d'information déconnecté.

Pour toutes ces raisons, l'utilisation de supports amovibles entre un système d'information classifié et un système d'information non classifié ou de classification différente est réglementée, notamment au travers de la section 6.8.2 de l'IGI 1300 [8] :

L'utilisation de supports amovibles entre un système d'information classifié et un système d'information non classifié ou de classification différente est par principe interdite. Toute dérogation à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation et les mesures de protection minimales suivantes s'appliquent :

- *une analyse de risque est conduite pour identifier les mesures techniques et organisationnelles visant à prévenir tout risque de sortie incontrôlée d'information classifiée lié aux cas d'usage de ces supports amovibles ;*
- *les échanges d'information entre un système d'information classifié et un système d'information non classifié ou de classification différente s'effectuent au moyen de points de connexion des supports amovibles mettant en œuvre des dispositifs de sécurité utilisés comme moyens essentiels de protection contre les accès non-autorisés aux informations classifiées. Ces dispositifs de sécurité sont agréés (cf. 6.5.2).*

Les architectures qui suivent utilisent les termes « point d'insertion de données » (PID) et « point d'extraction de données » (PED) définies à la section 2.1.3. Afin de réduire le risque d'injection d'un code malveillant, d'exfiltration accidentelle ou d'utilisation d'un périphérique piégé susceptible d'endommager le SI auquel il est connecté [29], il est nécessaire de maîtriser les supports amovibles utilisés pour l'interconnexion des systèmes.

R53

Interconnexions indirectes : Dédier des supports amovibles pour une interconnexion de SI

Lorsque des supports amovibles réinscriptibles sont utilisés pour réaliser de multiples transferts depuis un PED vers un PID, ils doivent être identifiés et dédiés à cette tâche. Des mesures techniques empêchent l'utilisation de ces supports ailleurs que sur les PED et les PID explicitement autorisés. Ces mesures techniques peuvent être de nature physique (p. ex. un connecteur spécifique permet de brancher le support amovible sur un PED ou un PID, mais pas sur d'autres systèmes du SI haut ou du SI bas) ou de nature logicielle (p. ex. une solution mettant en œuvre des moyens cryptographiques).

29. https://fr.wikipedia.org/wiki/USB_Killer.

6.1 Interconnexion montante indirecte

Nom de l'interconnexion	Interconnexion montante indirecte
Dispositif de sécurité essentiel	Point d'insertion en lecture seule
Exemples de données échangeables	Tout type de fichier
Temps opérationnel	Temps réfléchi

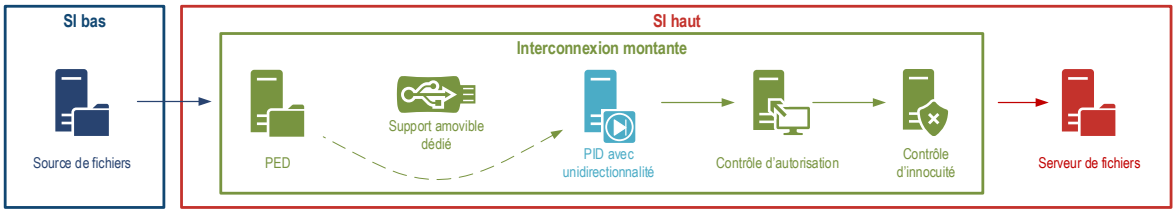

FIGURE 11 – Architecture d'une interconnexion montante indirecte

Comme pour les interconnexions directes, la fonction de sécurité protégeant contre les accès non autorisés aux informations classifiées dans une interconnexion montante indirecte est la fonction d'unidirectionnalité. Il existe plusieurs façons de garantir la lecture seule sur le PID [30].

Une première possibilité est d'utiliser un support non réinscriptible, tel qu'un CD-R, entre le PED et le PID.

R54

Interconnexion montante indirecte : Utiliser un support amovible non réinscriptible

Il est recommandé d'utiliser un support amovible non réinscriptible pour le transfert d'information entre le PED et le PID.

Cette méthode, qui apporte une assurance élevée pour un coût d'évaluation de sécurité relativement faible, n'est cependant pas adaptée aux besoins de transferts fréquents de faibles volumes de données, qui impliquerait d'acheter un nombre important de supports à usage unique. Une autre solution est d'utiliser des supports amovibles disposant d'un mode inscriptible et d'un mode en lecture seule, tels que certaines cartes SD ou clés USB. Lorsque le support amovible porte la fonction de sécurité essentielle, celle-ci doit être évaluée dans le cadre d'un agrément de sécurité du support amovible.

R55

Interconnexion montante indirecte : Utiliser un support amovible permettant la lecture seule

Il est recommandé d'utiliser un support amovible disposant d'une capacité de bascule dans un mode n'autorisant que la lecture de son système de fichiers.

Une autre possibilité est d'assurer que le système de fichiers du support amovible est monté en lecture seule sur le PID. Les mécanismes du système d'exploitation garantissant l'absence de droit

30. Dans le cas d'un système GNU/Linux, il est également recommandé d'utiliser les options `noexec` et `nosuid`.

d'écriture sur le système de fichiers du support amovible sont donc alors utilisés en tant que fonction de sécurité essentielle et doivent être évalués dans le cadre d'un agrément de sécurité du PID.

R56

Interconnexion montante indirecte : Monter le système de fichiers du support amovible en lecture seule sur le PID

Il est recommandé de monter le système de fichiers du support amovible en lecture seule sur le PID.

Il est important d'observer que cette fonction d'unidirectionnalité des échanges repose sur le système d'exploitation du PID dont l'évaluation de sécurité peut s'avérer irréaliste, particulièrement s'il s'agit d'un noyau comportant plus d'une dizaine de millions de lignes de codes tel que le noyau GNU/Linux ou Windows. En revanche, cette dernière recommandation reste applicable même lorsque le mécanisme permettant de monter en lecture seule le système de fichiers du support amovible sur le PID n'est pas utilisé en tant que fonction de sécurité essentielle garantissant l'unidirectionnalité du transfert. Elle doit alors être utilisée en tant que mesure de défense en profondeur sans être soumise à une obligation réglementaire d'évaluation de sécurité.

Sur le schéma de la figure 11, le PED est représenté comme faisant partie du SI haut, bien qu'il ne doive jamais contenir d'informations du SI haut. Cela est motivé par le fait que les composants d'une interconnexion multiniveau sont de la responsabilité de l'autorité d'emploi du SI haut. En revanche, il ne peut pas être administré par des outils du SI haut sans créer un contournement de la fonction d'unidirectionnalité. Son administration est possible par des outils d'administration dédiés ou, pour des raisons pratiques et dans un mode dégradé, des outils d'administration du SI bas. Il convient de prendre en compte que la réduction de la surface d'attaque du PED contribue à la réduction du risque de piégeage des supports amovibles s'y connectant, notamment dans le cas de périphériques USB.

Une fois l'information récupérée sur le PID, il est recommandé de procéder au contrôle d'autorisation et à la vérification d'innocuité des fichiers à transférer. Les recommandations de la section 5.1.1 s'appliquent ici.

R57

Interconnexion montante indirecte : Analyser les fichiers avant leur transfert vers l'interconnexion

Il est recommandé, avant tout transfert d'un fichier depuis le SI bas vers le PED, d'analyser le contenu du fichier. Cette analyse a pour objectif de protéger le PED et plus généralement les composants de l'interconnexion montante par la détection et le blocage de codes malveillants avant leur envoi vers l'interconnexion.

La recommandation R57 peut être réalisée par le moteur d'analyse antivirale du SI bas.

Il est également souhaitable de restreindre l'accès au PED au strict nécessaire, toujours dans un but de réduction de surface d'attaque.

R58

Interconnexion montante indirecte : Restreindre l'accès au PED

Il est recommandé de restreindre l'accès réseau et utilisateurs au PED. Seuls les équipements et utilisateurs qui en ont le strict besoin peuvent interagir avec le PED.

6.2 Interconnexion descendante indirecte

Un exemple d'architecture d'interconnexion descendante indirecte consiste à mettre en œuvre deux supports amovibles dédiés, nommés « H » et « B » ainsi qu'une station permettant la visualisation exhaustive des fichiers à transférer. Tout comme son équivalent en interconnexion directe, la fonction de sécurité essentielle ici est la visualisation exhaustive, qui n'est pertinente que si l'ensemble des données peuvent être visualisées par un être humain.

Nom de l'interconnexion	Interconnexion descendante indirecte par visualisation exhaustive
Dispositif de sécurité essentiel	Contrôle d'autorisation
Exemples de données échangeables	Tout type de fichier
Temps opérationnel	Temps réfléchi

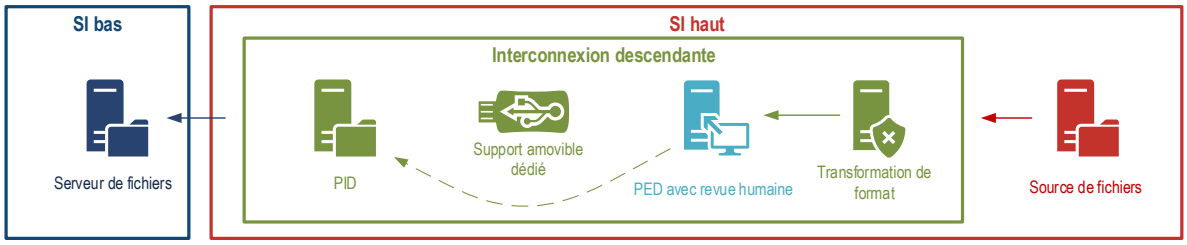

FIGURE 12 – Architecture d'une interconnexion descendante indirecte

La première étape consiste à écrire les données du SI haut candidates à l'export vers le SI bas sur le support amovible « H ». Afin de limiter le risque de contournement de la station de visualisation exhaustive, il est nécessaire de trouver une méthode imposant son utilisation. Une solution technique permettant d'imposer le passage par la station de visualisation exhaustive est de faire chiffrer les données au niveau du PED de sorte que seule la station de visualisation exhaustive soit en mesure de les déchiffrer.

R59

Interconnexion descendante indirecte : Chiffrer les données à exporter au niveau du PED

Il est recommandé de faire chiffrer par le PED les données à exporter sur le support amovible « H ».

La station de visualisation exhaustive, par sa nature de frontière entre le SI haut et le SI bas, peut se retrouver exposée à des données classifiées du SI haut. Afin d'assurer, si ce cas devait se présenter, l'impossibilité pour ces données d'être enregistrées de façon persistante sur le système puis exportées vers le PID, il est nécessaire d'empêcher toute fonction d'écriture en mémoire persistante sur

la station de visualisation exhaustive. Ainsi, toute donnée sur la station de visualisation doit rester volatile et être effacée après visualisation. Une façon d'obtenir cette propriété est d'installer le système de la station de visualisation exhaustive sur une mémoire morte [31].

R60

Interconnexion descendante indirecte : Utiliser une mémoire morte pour la station de visualisation exhaustive

Il est recommandé que la station de visualisation exhaustive ne dispose que d'une mémoire morte en tant que stockage persistant.

Lorsque les données visualisées sont autorisées à être transférées vers le SI bas, la station de visualisation exhaustive permet d'écrire ces données sur le support amovible « B ».

Afin d'éviter d'exposer la solution logicielle de visualisation exhaustive à des données non maîtrisées, susceptibles d'être vecteur d'attaques, il est recommandé de disposer de deux ports physiques distincts au niveau de la station de visualisation exhaustive. Un port monté en lecture seule pour le support amovible « H », pour lequel la solution de visualisation exhaustive affiche le contenu, et un port physique permettant un montage du volume avec les droits en lecture et écriture, pour que le système d'exploitation puisse copier les données validées par la visualisation exhaustive vers le support amovible « B ».

R61

Interconnexion descendante indirecte : Dédier un port physique pour chaque support amovible

Il est recommandé que la station de visualisation exhaustive dispose d'un port physique dédié au support amovible « H », qui n'est monté qu'en lecture seule, et un port physique pour le support amovible « B », qui peut être monté en lecture et écriture.

La station de visualisation exhaustive est le dispositif de sécurité essentiel de l'interconnexion descendante indirecte. Tout utilisateur de la station de visualisation exhaustive est responsable des données qui sont transférées vers le SI bas. Il est donc essentiel de pouvoir authentifier avec un niveau de confiance élevé les utilisateurs de la station de visualisation exhaustive.

R62

Interconnexion descendante indirecte : Définir une politique d'authentification renforcée pour les utilisateurs de la station de visualisation exhaustive

Tout utilisateur amené à s'authentifier sur un composant d'une interconnexion multiniveau doit disposer d'un compte nominatif. Un nombre de tentatives successives d'authentifications infructueuses a pour effet de verrouiller le compte utilisateur (le déverrouillage automatique du compte passé un certain délai n'est pas recommandé). Enfin, il est recommandé que les utilisateurs d'une interconnexion multiniveau indirecte soient authentifiés au moyen d'un système d'authentification forte. À défaut, les contraintes régissant les secrets d'authentification doivent être adaptées au niveau des données manipulées.

Afin de faciliter les investigations en cas de compromission d'information du SI haut, il est nécessaire de conserver une trace des transferts du SI haut vers le SI bas. Cependant, la recommandation

31. https://fr.wikipedia.org/wiki/Mémoire_morte.

R60 portant sur l'utilisation d'une mémoire morte pour la station de visualisation exhaustive rend difficile son utilisation pour conserver les traces des transferts. Il est envisageable de conserver toutes les données envoyées vers le point d'extraction (côté haut), ainsi qu'une empreinte des données reçues sur le point d'insertion (côté bas), comme dans l'exemple qui suit.

Exemple

Dans le cas d'un transfert de données au moyen d'une interconnexion descendante indirecte, un exemple d'architecture pouvant répondre à la recommandation R33 consiste à rendre obligatoire la copie des données à transférer vers un espace tampon. Cet espace a les propriétés suivantes :

- les utilisateurs y disposent de dossiers nominatifs et personnels sur lesquels ils n'ont toutefois aucun droit de suppression ni de modification des autorisations (listes de contrôle d'accès) ;
- il est le seul espace accessible depuis le PED ;
- toute donnée y étant déposée est archivée pendant une durée déterminée.

Du fait de ces propriétés, toute donnée déposée dans l'espace tampon est archivée tout en apportant une preuve de chaque transfert réalisé, sans pour autant nécessiter de mécanisme de signature complémentaire (les ACL positionnées au niveau de la zone tampon, couplées à l'authentification forte des utilisateurs sur le PED apportent une preuve suffisante pour la traçabilité).
Du côté du point d'insertion de données, pour chaque donnée reçue, un calcul d'empreinte est effectué et est archivé sur le poste. Cette empreinte n'est pas effaçable par un simple utilisateur.
En cas de compromission, la recherche de données classifiées dans le point d'extraction (côté haut) permet d'identifier d'éventuels fichiers contenant des informations classifiées susceptibles d'avoir été transmis à la station de visualisation exhaustive. La présence d'une empreinte correspondante dans le point d'insertion (côté bas) prouve que le fichier a bien été transmis vers le SI bas.

R63

⚖ Interconnexion descendante indirecte : Imputer les échanges du SI haut vers le SI bas

L'interconnexion descendante indirecte doit disposer d'un moyen d'imputation des données transférées du SI haut vers le SI bas.

Afin de protéger le point d'extraction de données d'une compromission venant du SI haut, une bonne mesure de défense en profondeur consiste à analyser les fichiers qui lui sont envoyés afin de détecter d'éventuels codes malveillants. Cette analyse peut être conduite par la solution antivirale du SI haut.

R64

Interconnexion descendante indirecte : Analyser les fichiers avant leur transfert

Avant toute copie d'un fichier depuis le PED (SI haut) vers un support amovible, il est recommandé d'analyser le contenu de chaque fichier. Cette analyse peut mettre en œuvre une ou plusieurs des stratégies de protection suivantes :

- vérifier la présence de marqueurs de sensibilité (cf. recommandation R14), de manière à prévenir le transfert de données non autorisées du niveau haut vers le niveau bas ;
- détecter la présence de code malveillant : il est recommandé d'utiliser sur le PED un moteur d'analyse antivirale différent des moteurs mis en œuvre au niveau des SI haut et bas ;
- imposer des quotas concernant le volume maximal de données transférable en fonction du type de donnée considéré, du moment du transfert, etc.

7
Mesures de protection des interconnexions

Objectif

Ce chapitre a pour objectif de donner des recommandations pour la protection des dispositifs constituant les interconnexions multiniveaux. Les recommandations données dans ce chapitre sont génériques ; les mesures de protection doivent en pratique être déterminées par l'analyse des risques spécifique à l'interconnexion. Il n'est pas possible de définir un ensemble strict, toujours applicable, de mesures de protection, car ces dernières dépendent des choix d'architectures physique et logicielle retenus pour l'interconnexion, ainsi que des choix technologiques, des mesures environnementales et organisationnelles.

7.1 Bonnes pratiques pour la conception et le développement des dispositifs de sécurité essentiels

Le dispositif de sécurité essentiel est constitué du matériel et logiciel assurant les fonctions de sécurité essentielles décrites à la section 4.4.

Afin d'accroître significativement les chances de succès d'obtention d'un agrément pour un dispositif de sécurité portant un service de sécurité considéré comme essentiel au sens de l'IGI 1300, il est recommandé de restreindre le plus possible sa surface d'attaque. Cela peut être obtenu par une limitation des fonctions portées par le dispositif de sécurité sujet à l'agrément. Dans l'idéal, le dispositif est exclusivement dédié aux fonctions de sécurité essentielles, aux fonctions de sécurité concourant à la protection de ces fonctions (p. ex. contrôle d'authenticité du code au démarrage) et aux fonctions nécessaires à leur utilisation (p. ex. authentification des utilisateurs). L'utilisation de socles matériels disposant de propriétés garantissant l'intégrité des fonctions rendues est à privilégier, comme par exemple l'utilisation d'ASIC, de PROM, et de *fuse* pour le stockage de certificats utilisés dans la chaîne de démarrage sécurisée. La réduction du volume de code permettant l'exécution des fonctions essentielles est à rechercher (p. ex. codage de l'ensemble des fonctions nécessaires dans un FPGA, utilisation de *microkernels* formellement évalués).

R65

Dédier les dispositifs de sécurité essentiels

Il est recommandé de dédier les dispositifs de sécurité portant les fonctions de sécurité essentielles à ces seules fonctions de sécurité et celles nécessaires à leur protection et leur utilisation. Ces dispositifs utilisent idéalement du matériel dédié avec un volume de code réduit au strict minimum.

Un dispositif de sécurité essentiel constitue la principale frontière de sécurité contre les accès non autorisés aux informations classifiées. Pour cette raison, il est nécessaire de garantir l'intégrité des traitements réalisés par ce dernier.

En tant que frontière de sécurité, un dispositif de sécurité doit disposer d'une architecture garantissant l'étanchéité des données avant et après traitement. Un canal de communication interne au dispositif ne doit pas être utilisé pour transmettre à la fois des données non traitées et des données traitées.

R66

Dédier les canaux de communication internes aux types de données traitées

Il est recommandé qu'un dispositif de sécurité dispose de canaux de communication internes dédiés aux types de données traitées.

Cette recommandation est par exemple atteinte pour un dispositif de contrôle syntaxique et sémantique lorsqu'un canal est physiquement dédié à la réception de données du SI haut (avant traitement), et un canal est physiquement dédié pour la transmission vers le SI bas (données traitées, et dans le cas de leur transmission, autorisées à être transmises vers le SI bas).

Information

Dans le cadre d'un agrément, l'ensemble des fonctions de sécurité utilisées comme mesures de protection du service de sécurité, comme les fonctions de démarrage sécurisé, de vérification de l'authenticité des configurations, d'authentification des utilisateurs, peuvent être évaluées. Il est donc nécessaire de ne pas s'appuyer sur des souches logicielles non évaluables (p. ex. système d'exploitation propriétaire dont l'éditeur ne souhaite pas fournir le code pour évaluation, souche logicielle libre trop volumineuse pour être évaluée).

En premier lieu, l'intégrité de la plateforme physique doit être garantie. Il est nécessaire que cette dernière soit protégée contre le piégeage. Une première mesure consiste à restreindre l'accès physique au dispositif de sécurité essentiel. Cette restriction se caractérise par l'utilisation d'un local physique dont l'accès est réservé aux personnes ayant besoin d'accéder au dispositif de sécurité et par l'utilisation d'un boîtier sécurisé disposant de mécanismes permettant la détection de l'ouverture ou du perçage.

R67

Restreindre l'accès physique au dispositif de sécurité essentiel

Il est recommandé de restreindre l'accès physique au dispositif de sécurité essentiel.

Lorsque le dispositif de sécurité essentiel s'appuie sur des fonctions logicielles pour protéger les informations classifiées contre les accès non autorisés, il est nécessaire de garantir l'authenticité

de ces fonctions logicielles. Cette garantie peut être atteinte par l'utilisation d'un module de sécurité utilisé comme racine de confiance (p. ex. un TPM – *Trusted Platform Module*) afin de vérifier l'authenticité de chaque fonction logicielle avant son exécution. Ces vérifications sont à faire dès le début de la séquence de démarrage, jusqu'à l'exécution des fonctions assurant le service de sécurité essentiel.

R68

Vérifier l'authenticité des fonctions logicielles

Il est recommandé d'intégrer au dispositif de sécurité essentiel un mécanisme de vérification de l'authenticité des fonctions logicielles avant leur exécution.

Le service de sécurité apporté par le dispositif de sécurité essentiel peut parfois dépendre de sa configuration, spécifique à l'environnement dans lequel ce dernier est utilisé. Dans ce cas, l'authenticité de la configuration est aussi importante que l'authenticité des fonctions logicielles, et doit donc également être vérifiée.

R69

Vérifier l'authenticité des configurations

Il est recommandé que le dispositif de sécurité essentiel dispose de mécanismes lui permettant de vérifier l'authenticité de toute nouvelle configuration avant son utilisation.

L'authenticité des éléments de configuration peut être apportée par une signature des éléments de configuration. Cette signature s'appuie idéalement sur une clé privée externe au dispositif de sécurité. Cette clé privée est d'un niveau de classification au moins aussi élevé que le niveau des informations du SI haut. L'utilisation de tout type de configuration dont l'authenticité ne peut être garantie est à proscrire dans la mesure du possible.

Il est possible que le dispositif de sécurité, au cours de son utilisation, nécessite de nouvelles versions des logiciels utilisés ou des configurations utilisées. Ces nouvelles versions viennent parfois corriger des vulnérabilités. Ainsi, il est nécessaire de s'assurer que les anciennes versions, qui disposent d'une signature valide, ne puissent être réinstallées sur l'équipement. Ce mécanisme peut s'appuyer sur une liste de condensats de versions révoquées ou une liste de certificats révoqués.

R70

Révoquer les versions obsolètes des logiciels et des configurations

Il est recommandé que le dispositif de sécurité essentiel dispose d'un mécanisme permettant de révoquer les versions obsolètes de logiciels et de configurations.

Afin de garantir une traçabilité des modifications des versions des fonctions logicielles et des configurations et faciliter d'éventuelles investigations en cas d'incident, il est nécessaire de journaliser toutes les modification du dispositif de sécurité. La conservation des traces peut être faite localement sur le dispositif (sauf lorsque le dispositif ne dispose que d'une mémoire morte), sur un collecteur de traces dédié à l'interconnexion, ou de façon dégradée dans un collecteur du SI haut mutualisé avec d'autres ressources.

R71

Journaliser les modifications de configuration du dispositif de sécurité

Il est recommandé de journaliser toutes les modifications, ajouts ou suppressions de fonctions logicielles, de configurations ou de secrets.

Le risque d'une erreur aléatoire de traitement ou d'une malfaçon entraînant des comportements inattendus n'est jamais nul. Cependant, il convient d'assurer que leur survenue est prise en compte dans le développement du dispositif de sécurité essentiel, et particulièrement que ce dernier dispose d'un état d'erreur sécurisé. Dans cet état, le cloisonnement entre le SI haut et le SI bas est garanti.

Pour atteindre l'objectif de cette recommandation, il est généralement utile de redonder certains traitements de sécurité, afin de garantir que la défaillance d'un composant responsable d'une vérification ou d'un traitement ne puisse pas, à elle seule, compromettre le service de sécurité rendu par le dispositif de sécurité essentiel.

R72

Garantir le cloisonnement même en cas de défaillance du dispositif

Il est recommandé que le dispositif de sécurité essentiel garantisse le cloisonnement des SI et la protection des données du SI haut en toute condition, y compris dans ses modes dégradés ou ses états d'erreur. Les besoins en disponibilité de l'interconnexion ne doivent jamais remettre en cause la fiabilité des cloisonnements et contrôles mis en œuvre.

Les composants de l'interconnexion doivent être développés en respectant l'état de l'art en matière de développement sécurisé, par exemple en se référant au guide [10] publié par le ministère des Armées et aux guides [2] et [3] publiés par l'ANSSI.

R73

Suivre l'état de l'art en matière de développement sécurisé

Les composants de l'interconnexion doivent être développés en suivant l'état de l'art en matière de développement sécurisé.

Le piégeage du code ou du matériel d'un dispositif de sécurité essentiel lors de sa conception pourrait mettre en défaut ses fonctions de sécurité. Ainsi, une attention particulière doit être accordée à l'environnement de conception, développement et fabrication de ces dispositifs. Par exemple, une infrastructure à clé publique garantissant l'authencitité du code d'une fonction logicielle de filtrage syntaxique et sémantique doit être classifiée au même niveau que le niveau d'agrément visé par le dispositif de sécurité.

R74

Assurer un niveau de sécurité de l'environnement de développement du dispositif de sécurité cohérent du niveau d'agrément ciblé

Les composants de l'interconnexion doivent être développés dans un environnement respectant des exigences de sécurité cohérentes du niveau d'agrément ciblé par ce dispositif.

Afin de réduire la probabilité de vulnérabilité dans les solutions utilisées, et dans le même temps une réactivité accrue pour mettre à disposition un correctif de sécurité en cas de vulnérabilité découverte, il est souhaitable d'utiliser des protocoles standards et éprouvés.

R75

Utiliser des protocoles standards et éprouvés

Il est recommandé d'utiliser des protocoles standards et éprouvés pour les communications avec et entre les composants de l'interconnexion.

7.2 Bonnes pratiques d'architecture d'une interconnexion multiniveau

Le cloisonnement des services de sécurité d'une interconnexion évite qu'une élévation de privilège opérée au sein d'une fonction n'affecte d'autres fonctions.

R76

Cloisonner les services de sécurité

Il est recommandé de cloisonner les services de sécurité au sein d'une interconnexion multiniveau.

En cas d'utilisation de cloisonnement logique dans un système, on pourra s'appuyer sur le guide de l'ANSSI portant sur les bonnes pratiques de cloisonnement [6].

L'architecture d'une interconnexion, notamment les moyens permettant de transporter l'information depuis un service de sécurité vers un autre service de sécurité doit empêcher qu'un échange non autorisé de données permette de contourner une fonction de sécurité, comme par exemple la fonction d'unidirectionnalité. Ces garanties peuvent être obtenues par des choix de câblage physique ou l'authentification systématique des communications entre les dispositifs de sécurité.

R77

Assurer l'impossibilité de contourner les services de sécurité

L'architecture doit définir le chaînage des différents éléments mis en œuvre dans l'interconnexion et garantir l'incontournabilité des services de sécurité, et plus particulièrement du service de sécurité essentiel. Cette assurance peut être atteinte, par exemple, par la répartition des services sur des équipements physiquement distincts ou au moyen d'une authentification mutuelle des composants portant les services de sécurité.

Afin de réduire la surface d'attaque de chaque composant, il est souhaitable d'assurer un filtrage des flux entre chaque composant de l'interconnexion.

R78

Filtrer les flux entre les services de sécurité

Il est recommandé de filtrer les flux entre chaque composant de l'interconnexion afin d'assurer que seuls les flux autorisés et documentés existent entre les services de sécurité.

Les dispositifs de sécurité essentiels doivent réglementairement disposer d'un agrément de sécurité. De manière non exclusive, il est recommandé d'utiliser des produits disposant d'un visa de sécurité pour les services de sécurité de l'interconnexion.

R79

Utiliser des produits disposant d'un visa de sécurité

Il est recommandé d'utiliser, lorsqu'ils existent, des produits disposant d'un visa de sécurité pour assurer les services de sécurité de l'interconnexion.

S'il est fait usage de supports amovibles autres que dans les cas précisés dans les architectures des interconnexions indirectes, il convient de limiter leur usage au strict nécessaire et de garantir qu'ils ne peuvent pas être utilisés pour contourner les dispositifs de sécurité de l'interconnexion. L'utilisation de supports amovibles sur des systèmes d'information classifiés est réglementée [32].

R80

⚖ Maîtriser l'usage des supports amovibles

L'autorité d'emploi du SI haut doit assurer la maîtrise des supports amovibles utilisés dans l'interconnexion.

32. Se référer au paragraphe 6.8 de l'IGI 1300 [8].

8
Administration des interconnexions

Objectif

Ce chapitre vise à donner des recommandations pour l'administration des interconnexions multiniveaux.

Comme tout composant d'un SI, les composants d'une interconnexion, qu'elle soit montante ou descendante, doivent être administrés de manière sécurisée. Pour cela, il est nécessaire de se référer aux recommandations de l'ANSSI relatives à l'administration sécurisée.

R81

Appliquer les recommandations de l'ANSSI relatives à l'administration sécurisée de SI

Une interconnexion multiniveau doit être administrée de manière sécurisée selon les recommandations de l'ANSSI rassemblées dans le guide afférent [4].

Cependant, une interconnexion multiniveau a la particularité d'avoir des composants de part et d'autre d'une frontière entre deux niveaux de classification assurée par le ou les dispositifs de sécurité essentiels. Cette particularité induit des précautions à prendre dans le cadre de l'administration des composants de l'interconnexion multiniveau, pour ne pas créer des chemins de contournement des dispositifs de sécurité essentiels. Ainsi, tout composant situé du côté du SI bas, vis-à-vis des dispositifs de sécurité assurant les fonctions essentielles de sécurité (unidirectionnalité dans le sens montant, et contrôle d'autorisation dans le sens descendant) ne doit pas être accessible depuis un composant situé du côté du SI haut.

Les composants les plus critiques sont évidemment les dispositifs de sécurité essentiels. Ainsi, les actions privilégiées sur ces derniers sont critiques, particulièrement si une modification de la configuration des composants peut permettre une fuite d'informations classifiées (p. ex. configuration d'un filtre syntaxique et sémantique). Dans ce cas, il peut être judicieux de restreindre les actions d'administration à un accès physique au dispositif de sécurité lui-même, ou d'utiliser une chaîne d'administration dédiée.

R82

Dédier les outils d'administration des dispositifs de sécurité essentiels

Il est recommandé de dédier les outils d'administration des dispositifs de sécurité essentiels, en utilisant directement des capacités d'administration locales au dispositif, ou en utilisant des outils et moyens d'accès distants dédiés aux actions d'administration des dispositifs de sécurité essentiels.

Lorsqu'il n'est pas possible d'utiliser des outils d'administration dédiés pour les dispositifs de sécurité essentiels ou lorsqu'il s'agit d'administrer les autres composants de l'interconnexion situé du côté du SI haut vis-à-vis du dispositif de sécurité essentiel garantissant la frontière entre le SI haut et le SI bas, il est nécessaire de réaliser l'administration depuis le système d'information d'administration du SI haut.

R82 -

Utiliser les outils du système d'information d'administration du SI haut pour administrer les dispositifs de sécurité essentiels

À défaut d'une chaîne d'administration dédiée aux dispositifs de sécurité essentiels, il est recommandé d'utiliser le système d'information d'administration du SI haut pour administrer les composants de l'interconnexion situés du côté du SI haut relativement au dispositif de sécurité essentiel.

Les dispositifs de sécurité non essentiels, et situées du côté du SI haut relativement aux dispositifs de sécurité essentiels peuvent bénéficier d'une administration dédiée lorsqu'elle existe ou, à défaut, d'une administration depuis le système d'administration du SI haut.

R83

Utiliser les outils du système d'information d'administration du SI haut pour administrer les dispositifs situés du côté du SI haut

À défaut d'une chaîne d'administration dédiée aux composants situés du côté du SI haut relativement au dispositif de sécurité essentiel, il est recommandé d'utiliser le système d'information d'administration du SI haut pour administrer les composants de l'interconnexion situés du côté du SI haut relativement au dispositif de sécurité essentiel.

Les composants de l'interconnexion situés du côté du SI bas relativement au dispositif de sécurité essentiel garantissant la frontière entre le SI haut et le SI bas (par exemple, un guichet bas d'une diode d'une interconnexion montante, un point d'insertion de données d'une interconnexion descendante indirecte) ne peuvent pas être administrés depuis le système d'information d'administration du SI haut sans créer un contournement du dispositif de sécurité essentiel de l'interconnexion. Ainsi, leur administration doit être dédiée ou réalisée depuis le SI bas.

R84

Dédier l'administration des dispositifs situés du côté du SI bas

Il est recommandé de dédier les outils d'administration des composants situés du côté du SI bas relativement au dispositif de sécurité essentiel. Il est possible d'utiliser directement des capacités d'administration locales au dispositif, ou en utilisant des outils et moyens d'accès distants dédiés à ces actions d'administration, et sans accès au SI haut.

Lorsque l'utilisation d'outils d'administration des dispositifs situés du côté du SI bas n'est pas possible, il demeure envisageable d'administrer les dispositifs situés du côté du SI bas par le système d'information d'administration du SI bas.

R84 -

Utiliser les outils du système d'information d'administration du SI bas pour administrer les dispositifs situés du côté du SI bas

À défaut d'outils dédiés aux dispositifs situés du côté du SI bas relativement au dispositif de sécurité essentiel, il est recommandé d'utiliser le système d'information d'administration du SI bas pour administrer ces dispositifs.

Il est nécessaire d'assurer avec un haut niveau de confiance que les actions d'administration ne sont réalisées que par une population d'administrateurs bien identifiée. À cet effet, la mise en place d'une authentification forte (réglementairement obligatoire) et multifacteur est fortement recommandée.

R85

Mettre en œuvre une authentification forte et multifacteur des administrateurs

Il est fortement recommandé de mettre en œuvre une authentification forte et multifacteur des administrateurs pour les actions d'administration sur les dispositifs de l'interconnexion, notamment lorsque les outils d'administration sont mutualisés.

Les actions d'administration doivent être tracées et archivées afin d'identifier les causes d'une éventuelle compromission. Une politique de tracabilité et d'archivage des actions d'administration doit être définie et appliquée.

R86

Définir et appliquer une politique de traçabilité des actions d'administration

Il est fortement recommandé de définir et d'appliquer une politique de traçabilité des actions d'administration, incluant l'archivage, sur les dispositifs de l'interconnexion. Les durées d'archivage sont définies dans l'IGI 1300 et sont d'un minimum de 3 ans pour le niveau Secret et 5 ans pour le niveau Très Secret.

Les actions d'administration sur l'interconnexion étant critiques, la confiance accordée aux personnes responsables de ces actions l'est aussi. Par leurs actions, elles sont en mesures d'accéder ou faciliter l'accès à des informations du SI haut. Ces personnes doivent donc être habilitées au moins au même niveau que celui des informations manipulées par le SI haut.

R87

⚖ Habiliter les administrateurs d'une interconnexion au minimum au niveau du SI haut

Les administrateurs d'une interconnexion doivent être habilités (en incluant les mentions de manipulation) à un niveau au moins aussi élevé que le niveau des informations manipulées par le SI haut.

Des vulnérabilités sont susceptibles d'être identifiées dans les dispositifs de l'interconnexion après leur déploiement. Afin de maintenir un niveau de sécurité acceptable, il est nécessaire de réaliser les mises à jour des dispositifs de l'interconnexion, en particulier l'application des correctifs de sécurité, dès que possible. À cet effet, une politique de maintien en condition de sécurité (MCS) doit être définie et appliquée aux dispositifs de l'interconnexion.

R88

Définir et appliquer une politique de MCS

Il est fortement recommandé de définir et d'appliquer une politique de MCS aux dispositifs de l'interconnexion. Cette politique précise notamment les fréquences de déploiement et les procédures de test des mises à jour de sécurité.

Dans le cycle de vie de l'interconnexion, certains services ou logiciels peuvent être amenés à ne plus être utilisés, d'autres peuvent être présents mais non utilisés. Toujours dans une optique de maintien de l'interconnexion dans un état de sécurité optimal, il est nécessaire de vérifier régulièrement que la surface d'attaque des dispositifs de l'interconnexion est minimale.

R89

Réduire la surface d'attaque des dispositifs de l'interconnexion

Il est recommandé de s'assurer régulièrement que seuls les logiciels strictement nécessaires au bon fonctionnement de l'interconnexion sont présents. Tout code non utilisé doit être supprimé.

Annexe A
Homologation de sécurité

Toute interconnexion multiniveau doit faire l'objet d'une homologation spécifique, l'instruction générale interministérielle n°1300 [8], précise :

Autorité d'homologation d'une interconnexion multiniveau

Toute interconnexion d'un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent est homologuée au niveau du système d'information le plus élevé. Cette interconnexion fait l'objet d'une homologation spécifique. L'ajout d'une interconnexion constitue un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.
L'autorité d'homologation est par défaut l'autorité d'homologation du système d'information du niveau le plus élevé, mais elle peut être aussi désignée après concertation entre les autorités d'homologation de chaque système d'information interconnecté. L'autorité d'homologation est le secrétariat général de la sécurité et de la défense nationale, ou toute autorité à qui il en délègue la responsabilité, dans les cas suivants :
- pour les transferts d'informations entre un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent, dont l'un n'est pas sous maîtrise nationale ;
- pour les transferts d'informations entre un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent, dont l'un est amené à traiter des informations classifiées de l'Union européenne ou de l'OTAN ;
- lorsque l'utilisation de dispositifs de sécurité agréés est obligatoire mais n'est pas possible, notamment lorsqu'il n'existe pas de dispositif de sécurité agréé ou lorsqu'il n'est pas agréé au bon niveau.
L'interconnexion est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non autorisés aux informations classifiées.

Un SI est considéré « sous maîtrise nationale » lorsque l'entité française :

- est propriétaire des équipements, ce qui exclut le cas d'un SI prêté ou loué par une entité étrangère à l'entité française ;
- administre elle-même le SI ;
- opère elle-même le SI, c'est-à-dire que les utilisateurs du SI sont sous la responsabilité directe de l'entité française, ce qui exclut le cas d'un SI prêté ou loué à une entité étrangère par l'entité française.

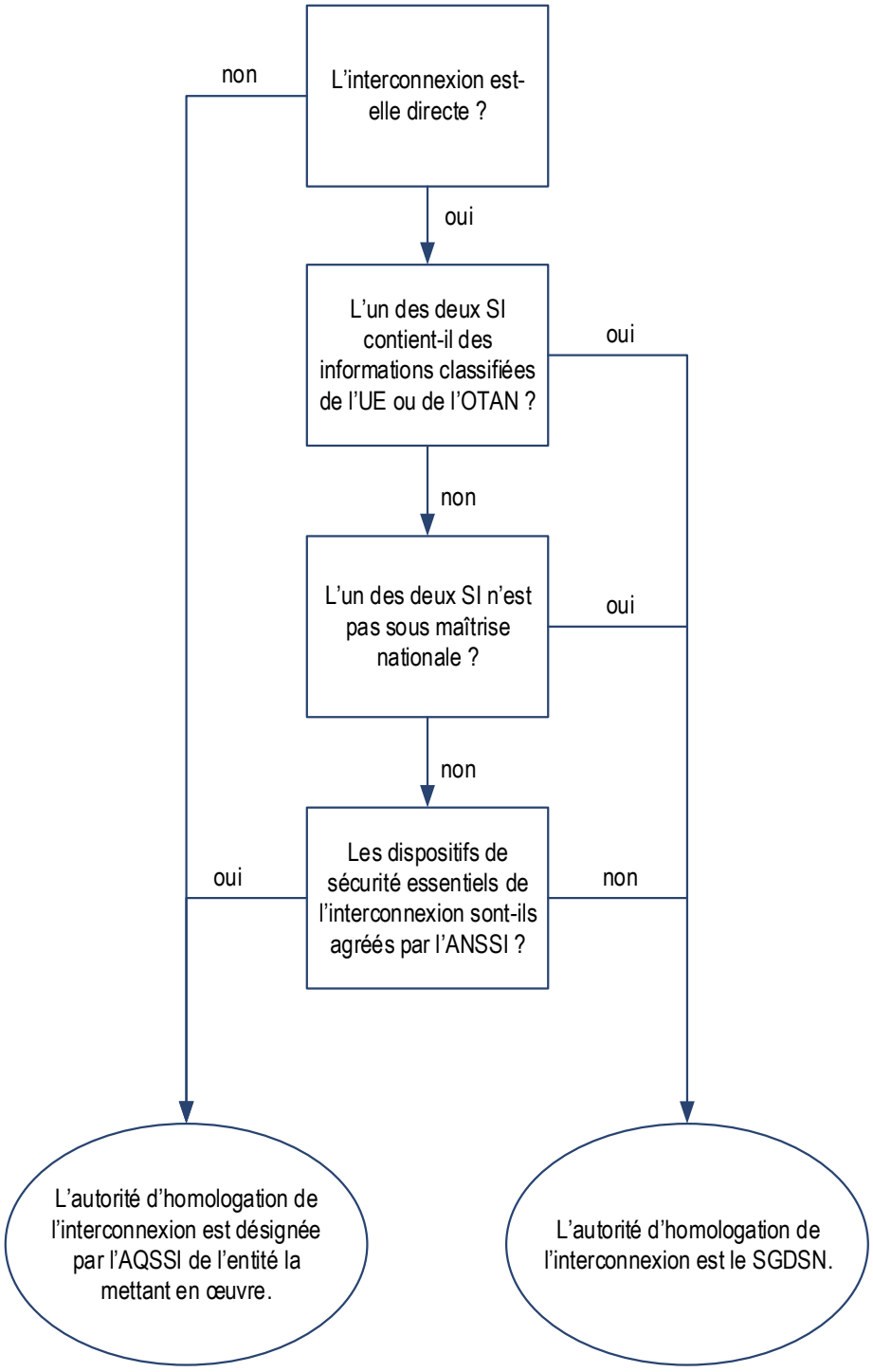

FIGURE 13 – Autorité d'homologation d'une interconnexion multiniveau

Liste des recommandations

R1	Concevoir le SI haut pour intégrer la problématique multiniveau si un besoin opérationnel est identifié	16
R2	Revoir la conception du SI haut en vue de mettre en œuvre une interconnexion multiniveau	17
R3	Éviter de créer des besoins d'interconnexion multiniveau	18
R4	Identifier exhaustivement les besoins de transferts de données	19
R5	Privilégier les interconnexions montantes	19
R6	⚖ Réviser l'analyse des risques du SI haut	20
R7	⚖ Réviser l'analyse des risques du SI bas	21
R8	⚖ Réaliser une analyse des risques spécifique à l'interconnexion	21
R9	⚖ Utiliser des dispositifs de sécurité agréés pour les services de sécurité essentiels	26
R10	⚖ Respecter les conditions d'emploi des dispositifs agréés	26
R11	⚖ Interconnexion montante : Garantir l'unidirectionnalité des transferts de données (fonction de sécurité essentielle)	26
R12	⚖ Interconnexion descendante : Garantir le contrôle de l'autorisation de transmission des données (fonction de sécurité essentielle)	27
R13	Interconnexion descendante : Caractériser les canaux cachés	28
R14	Interconnexion descendante indirecte : Marquer la sensibilité des données dans le SI haut	29
R15	⚖ Prendre en compte les fuites par signaux compromettants dans les SI classifiés	30
R16	⚖ Mettre en œuvre une démarche de sécurisation contre les signaux compromettants	30
R17	Interconnexion montante pour le transfert de fichiers : Positionner la fonction diode en amont de l'interconnexion	32
R18	Interconnexion montante pour le transfert de fichiers : Contrôler l'autorisation du transfert des fichiers par une vérification de signature	33
R18-	Interconnexion montante pour le transfert de fichiers : Faire signer par un dispositif du SI bas les fichiers à transmettre vers le SI haut	33
R18- -	Interconnexion montante pour le transfert de fichiers : S'appuyer sur une convention de nommage des fichiers	33
R19	⚖ Interconnexion montante pour le transfert de fichiers : Réaliser un contrôle d'innocuité des fichiers	34
R20	Interconnexion montante pour le transfert de fichiers : Mettre en quarantaine les fichiers bloqués	34
R21	Interconnexion montante pour le transfert de fichiers : Enregistrer les fichiers transférés	35
R21-	Interconnexion montante pour le transfert de fichiers : Enregistrer les métadonnées et condensats des fichiers transférés	35
R22	Interconnexion montante pour le transfert de flux : Contrôler la source des flux en amont	36
R23	Interconnexion montante pour le transfert de flux : Enregistrer les métadonnées associées aux flux	36
R24	Interconnexion montante pour le transfert de flux : Effectuer une transformation de format	36
R25	⚖ Interconnexion descendante avec visualisation exhaustive : Définir les règles de contrôle et de validation des informations ayant vocation à être transférées vers le niveau bas	37

R26	⚖ Interconnexion descendante avec visualisation exhaustive : Mettre en œuvre un mécanisme de visualisation exhaustive des données à transmettre	38
R27	Interconnexion descendante avec visualisation exhaustive : Supprimer les données non visualisables	38
R28	Interconnexion descendante avec visualisation exhaustive : Créer un nouveau fichier à partir des données visualisées	38
R29	⚖ Interconnexion descendante avec visualisation exhaustive : Garantir l'intégrité des données après la visualisation exhaustive	39
R30	⚖ Interconnexion descendante avec visualisation exhaustive : Garantir une authentification forte et multifacteur de l'opérateur	39
R31	Interconnexion descendante avec visualisation exhaustive : Confirmer deux fois le transfert d'un fichier	39
R32	⚖ Interconnexion descendante avec visualisation exhaustive : Enregistrer les transferts autorisés par l'opérateur	39
R33	Interconnexion descendante avec visualisation exhaustive : Enregistrer les données dont le transfert a été refusé par l'opérateur	40
R34	Interconnexion descendante avec visualisation exhaustive : Mettre en œuvre l'unidirectionalité des transferts	40
R35	⚖ Interconnexion descendante : Garantir la visualisation exhaustive avant la signature	41
R36	⚖ Interconnexion descendante : Garantir que seules les données autorisées peuvent être signées	42
R37	Interconnexion descendante : Informer l'opérateur de la signature des données	42
R38	Interconnexion descendante avec analyse exhaustive de contenu : Définir les règles de contrôle et de validation à mettre en oeuvre par le mécanisme de contrôle automatisé afin de vérifier les informations transférées vers le niveau bas	43
R39	Interconnexion descendante avec analyse exhaustive de contenu : Mettre en œuvre une analyse exhaustive de contenu	43
R40	Interconnexion descendante avec analyse exhaustive automatisée de contenu : Garantir l'exhaustivité des données contrôlées	43
R41	Interconnexion descendante avec analyse exhaustive de contenu : Limiter les agencements de champs de données autorisés	43
R42	Interconnexion descendante avec analyse exhaustive de contenu : Limiter la grammaire des données	44
R43	Interconnexion descendante avec analyse exhaustive de contenu : Détecter des envois intempestifs de messages conformes	44
R44	Interconnexion descendante avec analyse exhaustive de contenu : Authentifier la source des messages à transférer	44
R45	Interconnexion descendante avec analyse exhaustive de contenu : Enregistrer les métadonnées des transferts	44
R46	Interconnexion descendante : Mettre en œuvre un aiguillage	46
R47	Interconnexion descendante : Garantir l'absence de capacité de rétention d'informations classifiées dans la source	46
R48	Interconnexion descendante : Enregistrer la position de l'aiguillage	46
R49	Interconnexion descendante : Rendre vérifiable la position de l'aiguillage	46

R50	Interconnexion descendante avec aiguillage : Garantir une authentification forte et multi-facteur de l'opérateur	47
R51	Interconnexion descendante : Mettre en œuvre une solution agréée de signature des flux	48
R52	Séparer physiquement les traitements montant et descendant	48
R53	Interconnexions indirectes : Dédier des supports amovibles pour une interconnexion de SI	50
R54	Interconnexion montante indirecte : Utiliser un support amovible non réinscriptible	51
R55	Interconnexion montante indirecte : Utiliser un support amovible permettant la lecture seule	51
R56	Interconnexion montante indirecte : Monter le système de fichiers du support amovible en lecture seule sur le PID	52
R57	Interconnexion montante indirecte : Analyser les fichiers avant leur transfert vers l'interconnexion	52
R58	Interconnexion montante indirecte : Restreindre l'accès au PED	53
R59	Interconnexion descendante indirecte : Chiffrer les données à exporter au niveau du PED	53
R60	Interconnexion descendante indirecte : Utiliser une mémoire morte pour la station de visualisation exhaustive	54
R61	Interconnexion descendante indirecte : Dédier un port physique pour chaque support amovible	54
R62	Interconnexion descendante indirecte : Définir une politique d'authentification renforcée pour les utilisateurs de la station de visualisation exhaustive	54
R63	⚖ Interconnexion descendante indirecte : Imputer les échanges du SI haut vers le SI bas	55
R64	Interconnexion descendante indirecte : Analyser les fichiers avant leur transfert	56
R65	Dédier les dispositifs de sécurité essentiels	58
R66	Dédier les canaux de communication internes aux types de données traitées	58
R67	Restreindre l'accès physique au dispositif de sécurité essentiel	58
R68	Vérifier l'authenticité des fonctions logicielles	59
R69	Vérifier l'authenticité des configurations	59
R70	Révoquer les versions obsolètes des logiciels et des configurations	59
R71	Journaliser les modifications de configuration du dispositif de sécurité	60
R72	Garantir le cloisonnement même en cas de défaillance du dispositif	60
R73	Suivre l'état de l'art en matière de développement sécurisé	60
R74	Assurer un niveau de sécurité de l'environnement de développement du dispositif de sécurité cohérent du niveau d'agrément ciblé	60
R75	Utiliser des protocoles standards et éprouvés	61
R76	Cloisonner les services de sécurité	61
R77	Assurer l'impossibilité de contourner les services de sécurité	61
R78	Filtrer les flux entre les services de sécurité	62
R79	Utiliser des produits disposant d'un visa de sécurité	62
R80	⚖ Maîtriser l'usage des supports amovibles	62
R81	Appliquer les recommandations de l'ANSSI relatives à l'administration sécurisée de SI	63
R82	Dédier les outils d'administration des dispositifs de sécurité essentiels	63

R82-	Utiliser les outils du système d'information d'administration du SI haut pour administrer les dispositifs de sécurité essentiels	64
R83	Utiliser les outils du système d'information d'administration du SI haut pour administrer les dispositifs situés du côté du SI haut	64
R84	Dédier l'administration des dispositifs situés du côté du SI bas	64
R84-	Utiliser les outils du système d'information d'administration du SI bas pour administrer les dispositifs situés du côté du SI bas	65
R85	Mettre en œuvre une authentification forte et multifacteur des administrateurs	65
R86	Définir et appliquer une politique de traçabilité des actions d'administration	65
R87	⚖ Habiliter les administrateurs d'une interconnexion au minimum au niveau du SI haut	65
R88	Définir et appliquer une politique de MCS	66
R89	Réduire la surface d'attaque des dispositifs de l'interconnexion	66

Bibliographie

[1] *L'homologation de sécurité en neuf étapes simples*.
Guide ANSSI-PA-096 v1.0, ANSSI, août 2014.
https://cyber.gouv.fr/guide-homologation-securite.

[2] *Règles de programmation pour le développement d'applications sécurisées en Rust*.
Guide ANSSI-PA-074 v1.0, ANSSI, juin 2020.
https://cyber.gouv.fr/publications/regles-de-programmation-pour-le-developpement-dapplications-securisees-en-rust.

[3] *Règles de programmation pour le développement sécurisé de logiciels en langage C*.
Guide ANSSI-PA-073 v1.2, ANSSI, juillet 2020.
https://cyber.gouv.fr/publications/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c.

[4] *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.

[5] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, mars 2024.
https://cyber.gouv.fr/ebios-rm.

[6] *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.

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

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

[9] *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte*.
Guide ANSSI-PG-075 v1.2, ANSSI, septembre 2021.
https://cyber.gouv.fr/guide-archi-sensible-dr.

[10] *Développement des applications informatiques et des logiciels robustes du ministère de la Défense*.
Directive n°40/DEF/DGSIC, Ministère des Armées, mai 2017.

Version 1.0 - 01/10/2024 - ANSSI-PA-101

ISBN : 978-2-11-167154-6 (papier)
ISBN : 978-2-11-167155-3 (numérique)
Dépôt légal : octobre 2024

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