

# RECOMMANDATIONS POUR LES ARCHITECTURES DES SYSTÈMES D'INFORMATION SENSIBLES OU DIFFUSION RESTREINTE

---

## GUIDE ANSSI

ANSSI-PG-075  
24/09/2021

### PUBLIC VISÉ :

Développeur

Administrateur

RSSI

DSI

Utilisateur





# Informations



## Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte** ». Il est téléchargeable sur le site [www.ssi.gouv.fr](http://www.ssi.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 [33].

Conformément à la Licence Ouverte v2.0, le guide 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, ces 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	28/08/2020	Version initiale
1.1	28/12/2020	Modifications mineures
1.2	24/09/2021	Modifications mineures (Bibliographie : ajustement de la référence bibliographique IGI 1300; section 1.1 : ajout d'un renvoi vers la version anglaise du guide; section 4.2 : suppression d'une phrase inutile)

# Table des matières

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Objectif du guide . . . . .	4
1.2	Organisation du guide . . . . .	5
1.3	Convention de lecture . . . . .	5
<b>2</b>	<b>Systèmes d'information (SI) non classifiés</b>	<b>7</b>
2.1	Besoins de protection en confidentialité des informations . . . . .	7
2.2	Définition des SI sensibles et des SI usuels . . . . .	10
2.3	Détermination du régime de protection des informations sensibles . . . . .	15
2.4	Homologation d'un SI sensible . . . . .	16
<b>3</b>	<b>Typologies de SI sensibles</b>	<b>18</b>
3.1	Représentation des typologies d'architecture . . . . .	18
3.1.1	Conventions graphiques pour les schémas d'architecture . . . . .	18
3.1.2	Les classes de SI . . . . .	19
3.2	Différentes architectures de SI sensibles . . . . .	20
3.2.1	SI sensible physiquement isolé . . . . .	20
3.2.2	SI sensible physiquement cloisonné . . . . .	22
3.2.3	SI sensible sans SI usuel . . . . .	24
3.3	Critères influençant les choix d'architecture des SI sensibles . . . . .	27
<b>4</b>	<b>Interconnexions directes de SI sensibles</b>	<b>30</b>
4.1	Généralités . . . . .	30
4.2	Interconnexion d'un SI sensible avec un second SI sensible . . . . .	31
4.3	Interconnexion d'un SI sensible de classe 1 avec un SI de classe 0 . . . . .	33
4.3.1	Nature des dispositifs de sécurité de la passerelle de classe 1 . . . . .	34
4.3.2	Positionnement des dispositifs de sécurité de la passerelle de classe 1 . . . . .	36
4.3.3	Navigation Web . . . . .	37
4.3.4	Transfert via Internet de documents sensibles chiffrés . . . . .	40
4.3.5	Accès via Internet à des informations issues d'une application sensible . . . . .	41
4.4	Échanges sécurisés pour les utilisateurs . . . . .	43
4.4.1	Cas des SI de classe 2 . . . . .	44
4.4.2	Cas des SI de classe 1 . . . . .	44
<b>5</b>	<b>Sécurisation au sein des SI sensibles</b>	<b>47</b>
5.1	Produits et prestataires de service de confiance . . . . .	47
5.2	Chiffrement . . . . .	49
5.3	Cloisonnement interne du SI sensible et durcissement des systèmes . . . . .	49
5.4	Marquage . . . . .	51
5.5	Gestion des authentifiants et des droits d'accès . . . . .	53
5.6	Protection contre les codes malveillants . . . . .	56
5.7	Gestion des périphériques et des supports amovibles . . . . .	57
<b>6</b>	<b>Sécurisation des postes de travail sensibles</b>	<b>62</b>
6.1	Maîtrise des postes de travail des SI sensibles . . . . .	62

6.2	Connexion des postes de travail au réseau . . . . .	63
6.3	Architecture des postes de travail . . . . .	65
6.4	Nomadisme . . . . .	70
6.5	Réseaux sans fil . . . . .	73
<b>7</b>	<b>Administration des SI sensibles</b>	<b>77</b>
7.1	Généralités . . . . .	77
7.2	SI d'administration . . . . .	78
7.2.1	Cas des SI sensibles physiquement isolés . . . . .	79
7.2.2	Cas des SI sensibles physiquement cloisonnés . . . . .	80
7.2.3	Cas des SI sensibles sans SI usuel . . . . .	82
7.3	Administration à distance . . . . .	83
7.4	Maintien en condition de sécurité (MCS) . . . . .	83
7.5	Journalisation et supervision de sécurité . . . . .	85
<b>Annexe A</b>	<b>Informations sensibles, DR et usuelles - Explications détaillées</b>	<b>87</b>
A.1	Définitions . . . . .	87
A.2	Différences d'ordre juridique entre les informations DR et les informations non DR .	91
<b>Annexe B</b>	<b>Niveaux de sensibilité des informations</b>	<b>94</b>
<b>Annexe C</b>	<b>Visas de sécurité</b>	<b>95</b>
<b>Annexe D</b>	<b>Nomadisme - Mesures de sécurité II 901 et guide ANSSI</b>	<b>98</b>
<b>Annexe E</b>	<b>Administration des SI - Mesures de sécurité II 901 et guide ANSSI</b>	<b>99</b>
<b>Annexe F</b>	<b>Mesures de sécurité II 901</b>	<b>100</b>
	<b>Liste des recommandations</b>	<b>104</b>
	<b>Bibliographie</b>	<b>106</b>

# 1

## Introduction

### 1.1 Objectif du guide

L'instruction interministérielle n° 901/SGDSN/ANSSI (II 901) du 28 janvier 2015 [28] définit les objectifs et les mesures de sécurité minimales relatifs à la protection des informations sensibles, notamment celles relevant du niveau Diffusion Restreinte (DR).

Le présent guide donne des recommandations pour la conception de l'architecture des systèmes d'information (SI) qui hébergent des informations sensibles. De manière générale, il apporte des conseils techniques pour la mise en pratique de l'II 901.

La préoccupation première de ce guide est l'architecture technique des SI sensibles (dont les SI DR). L'attention du lecteur est attirée sur le fait que certains champs de l'II 901 ne sont pas traités dans ce document (sécurité physique et environnementale, sécurité liée aux développements informatiques...) ou sont partiellement traités (gouvernance de la sécurité des systèmes d'information). En outre, certains aspects techniques ne sont pas traités dans cette version du guide (téléphonie sur IP, système d'information de contrôle d'accès...). Pour mettre en œuvre un SI conforme à l'II 901, il est donc nécessaire d'appliquer des mesures supplémentaires allant au-delà des recommandations détaillées dans ce document.

La lecture préalable de l'II 901 facilitera la compréhension de ce guide.

Les mesures de sécurité décrites dans l'II 901 sont organisées en fonction d'objectifs de sécurité et repérées au moyen d'articles numérotés ou d'identifiants uniques (p. ex. *INT-QUOT-SSI*). Ce guide ayant été pensé comme un outil, il est fait référence à ces articles et à ces identifiants dans des notes de bas de page chaque fois que cela est jugé pertinent. Inversement, l'annexe F de ce guide liste les mesures de sécurité de l'II 901 et donne, pour chacune, des renvois vers les sections de ce guide où la mesure en question est abordée (ou des renvois vers d'autres publications de l'ANSSI).

Ce guide présente des recommandations pertinentes au regard de l'état de l'art technique, des menaces et de la réglementation. Son application, bien que non suffisante pour atteindre le niveau de sécurité requis, pourra néanmoins contribuer à la spécification d'un socle de sécurité pour un SI sensible. La création de ce socle de confiance est la première étape de la méthode d'analyse de risque *EBIOS Risk Manager* [20], dont l'utilisation est recommandée pour apprécier et traiter les risques pesant sur un SI.

Une mention de restriction de diffusion équivalente à Diffusion Restreinte attribuée à une information par un État étranger ou une organisation internationale soumet, en France, cette information aux règles de protection énoncées à l'annexe 3 de l'instruction générale interministérielle

n° 1300/SGDSN/PSE/PSD (IGI 1300) du 9 août 2021 [1] et à l’II 901 [28]. Les recommandations de ce guide sont donc applicables aux SI manipulant des informations de cette nature sans préjudice d’éventuelles mesures de sécurité complémentaires précisées par l’État étranger ou l’organisation internationale.

Les problématiques liées aux informations classifiées de défense et à l’interconnexion des SI sensibles avec des SI classifiés sont hors du périmètre du présent guide.

Une version anglaise de ce guide est disponible sur le site Web de l’ANSSI [31].

## 1.2 Organisation du guide


Après avoir défini les notions de système d’information sensible et de système d’information usuel (chapitre 2), le chapitre 3 présente les différentes architectures acceptables pour un SI sensible. Dans les schémas d’architecture de ce chapitre, les SI sensibles sont représentés de façon macroscopique et monolithique : le but à ce stade est de comprendre comment, globalement, ils se positionnent par rapport à d’autres SI.

Le chapitre 4 décrit les moyens devant être mis en place pour qu’un SI sensible puisse être interconnecté avec un autre SI, qu’il s’agisse d’un SI de sensibilité moindre (p. ex. Internet) ou d’un autre SI sensible.

Les chapitres 5 et 6 apportent des recommandations pour la sécurisation *interne* des SI sensibles, en traitant respectivement des aspects généralistes liés au principe de défense en profondeur et des aspects relatifs aux postes de travail.

Enfin, le chapitre 7 présente les bonnes pratiques d’administration des SI sensibles.

## 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’II 901 [28]. 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.

La liste récapitulative des recommandations est disponible en page 105.



# 2

## Systèmes d'information (SI) non classifiés



### Objectif

Ce chapitre a pour but d'expliquer ce que sont les différents SI non classifiés de défense et d'introduire les notions de SI sensibles et de SI usuels, concepts clés du présent guide.

### 2.1 Besoins de protection en confidentialité des informations

L'II 901, le texte de référence régissant en France la protection des systèmes d'information sensibles, donne cette définition des informations sensibles <sup>1</sup> :



### Informations sensibles

*Les informations sensibles sont celles dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre.*

Cette définition est volontairement très ouverte : il appartient à toute entité de recenser les informations sensibles dont elle a la responsabilité et d'apprécier, pour chacune, quels sont les besoins en matière de sécurité.



### Information

Dans cette définition, une information *sensible* peut avoir des besoins de protection en confidentialité, en intégrité ou en disponibilité. Un parti pris de ce guide est de considérer la confidentialité comme le critère de sécurité primordial pour protéger une information sensible. Les recommandations qu'il contient ont été rédigées dans cet esprit, néanmoins, la plupart d'entre elles sont également pertinentes pour la protection en intégrité ou en disponibilité des informations (p. ex. prévenir un risque d'atteinte en disponibilité qui résulterait d'une attaque du SI au moyen d'un rançongiciel).

1. Se reporter à l'article 1<sup>er</sup> de l'II 901.

Les SI qui vont héberger les informations de l'entité peuvent garantir un niveau de protection plus ou moins important en fonction des mesures de sécurité qu'ils mettent en œuvre. Afin de pouvoir déterminer sur quel SI il sera le plus pertinent de traiter une information, il est préalablement nécessaire d'identifier le besoin de protection en confidentialité de cette information.

Pour une entité publique ou privée, l'identification de ce besoin de protection en confidentialité est une action éminemment subjective et relative. Subjective car il est très difficile de quantifier ce besoin de manière scientifique. Relative car ce besoin doit nécessairement être cohérent par rapport aux besoins en confidentialité de toutes les autres informations traitées par l'entité.

Une approche pour parvenir à classer les informations en fonction de leurs besoins en confidentialité consiste à se doter de deux outils : d'une part, une « échelle des besoins en confidentialité », d'autre part, une analyse des risques.

L'échelle des besoins en confidentialité est un référentiel arbitraire permettant d'exprimer le fait que certaines informations ont des besoins de protection *faibles* tandis que d'autres ont des besoins *forts*. Par exemple, une échelle des besoins en confidentialité peut prendre la forme d'un repère gradué où des valeurs numériques faibles traduisent des besoins de protection en confidentialité *faibles* tandis que des valeurs numériques élevées traduisent des besoins de protection en confidentialité *forts*.

Cette échelle étant établie, une analyse des risques va permettre à l'entité d'identifier, au sein de son patrimoine informationnel, les informations vraiment importantes, vraiment *sensibles*, par opposition à celles qui le sont « moins ». L'entité va devoir affecter, à chacune de ses informations, une « valeur numérique de confidentialité » de manière à pouvoir, dans un second temps, positionner cette information sur l'échelle des besoins en confidentialité. Cette valeur numérique est à la fois arbitraire (c'est-à-dire définie par une convention propre à l'entité) et relative (à deux informations ayant des besoins de confidentialité différents correspondent deux valeurs numériques différentes). Par exemple, il est possible d'arrêter une convention stipulant qu'une information publique ayant vocation à être largement accessible se voit attribuer une valeur nulle (p. ex. un catalogue publicitaire), tandis qu'une information très importante pour l'entité (p. ex. un secret de fabrication) se voit attribuer une valeur élevée (p. ex. la valeur 100).



### Attention

La valeur de confidentialité d'une information est susceptible d'évoluer tout au long de son cycle de vie. En particulier, il est parfois très difficile de prévoir l'évolution future de cette valeur, notamment si elle se retrouve agrégée avec d'autres informations.



### Information

Par convention, dans ce guide, les informations « moins » sensibles, mais dont le besoin de protection en confidentialité n'est pas nul pour autant, sont appelées *informations usuelles*.

La figure 1 est une illustration du concept d'échelle des besoins en confidentialité.

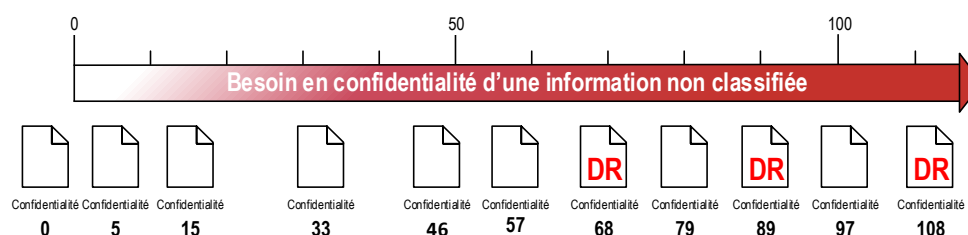


FIGURE 1 – Echelle des besoins de protection en confidentialité d'une information non classifiée

Un sous-ensemble des informations sensibles sont les informations Diffusion Restreinte (DR). La notion d'information DR est définie par la réglementation<sup>2</sup>, qui impose des mesures de sécurité spécifiques pour leur protection.



## Informations Diffusion Restreinte

*Les informations Diffusion Restreinte sont celles qui portent la mention Diffusion Restreinte ou ses équivalentes européennes ou internationales.*

L'intérêt de qualifier une information Diffusion Restreinte est de soumettre l'ensemble des personnes amenées à la manipuler à une restriction de diffusion. Ainsi, l'accès à une information DR est régi par le principe de restriction du *besoin d'en connaître* : seules les personnes ayant une nécessité impérieuse d'en prendre connaissance dans le cadre de leur fonction et pour une mission précise sont autorisées à y accéder. Cette restriction de diffusion s'applique en cas de transfert de l'information vers une autre entité juridique. Cette dernière doit traiter les données DR conformément à la réglementation, sur un SI où les mesures de sécurité propres à la protection des informations DR sont mises en œuvre.



## Attention

Contrairement aux informations DR, les informations sensibles non DR ne bénéficient pas par défaut d'une protection juridique lorsqu'elles sont transférées à une entité tierce. Il existe toutefois des solutions permettant de dépasser cette limitation. Le *secret des affaires* créé par la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires est un exemple de réponse à ce besoin.

R1

## Trier le patrimoine informationnel par niveau de sensibilité

Une entité publique ou privée doit trier son patrimoine informationnel. Pour ce faire, elle conduit une analyse des risques visant à exprimer les besoins de protection en confidentialité des informations<sup>3</sup>. Ces besoins peuvent être positionnés sur une échelle croissante de protection en confidentialité allant d'un besoin faible pour des informations publiques à un besoin fort pour des informations sensibles ou DR.

2. Se reporter à l'annexe 3 de l'IGI 1300 et à l'II 901.



## Information

L'expression « informations non protégées » (« informations NP ») est parfois rencontrée pour désigner les « informations non classifiées ». L'emploi de ce qualificatif « NP » est malheureusement impropre.

D'une part, les informations NP (ou au minimum les SI qui hébergent les informations NP) font toujours, en pratique, l'objet de mesures de protection et ne sont donc jamais véritablement *non protégées*.

Ensuite, ce qualificatif est ambigu car, en fonction de son contexte d'emploi, il désigne des réalités différentes. Le qualificatif « NP » est fréquemment utilisé lorsqu'il s'agit de désigner le *complément inverse* d'un ensemble d'informations pris comme référence. À titre d'illustration, si dans un contexte particulier, les informations de référence sont les informations classifiées, alors le terme « informations NP » désignera les informations « non classifiées » ; si, dans un autre contexte, les informations de référence sont les informations sensibles (au sens de l'II 901), alors le terme « informations NP » désignera les informations non sensibles (au sens de l'II 901) et non classifiées.

Aussi, par souci de clarté du propos, le qualificatif « non protégé » n'est pas utilisé dans ce guide. Les termes non ambigus « informations publiques », « informations usuelles », « informations sensibles » ou « informations DR » sont préférés.

Pour en savoir plus sur les différences entre les informations publiques, usuelles, sensibles et DR, se reporter à l'annexe A.

## 2.2 Définition des SI sensibles et des SI usuels

Le patrimoine informationnel étant trié, il devient possible de déterminer sur quel SI une information peut être hébergée ; le niveau de protection apporté par le SI doit être cohérent avec le besoin de protection en confidentialité des données hébergées. Mais, contrairement à l'échelle des besoins en confidentialité qui couvre une large gamme de nuances, le nombre de SI qu'une entité va pouvoir mettre en œuvre est nécessairement limité.

Les SI peuvent être vus comme des réceptacles des informations : en fonction des besoins de sécurité d'une information, celle-ci est hébergée sur l'un ou l'autre de ces SI. Les informations pour lesquelles le besoin de confidentialité est fort sont placées sur un SI ayant un niveau de protection « supérieur ». Inversement, les informations pour lesquelles le besoin de confidentialité est jugé plus faible sont placées sur un SI ayant un niveau de protection « inférieur ».

Dans le cadre de ce guide portant sur les architectures des SI sensibles, il est pris pour hypothèse qu'une entité désireuse de protéger des informations sensibles crée deux SI distincts. Le premier, appelé *SI sensible*, présente un niveau de protection « supérieur », par opposition au second, appelé *SI usuel*, lequel présente un niveau de protection « inférieur » que celui du SI sensible. Les données hébergées sur le SI usuel ont un besoin en confidentialité moindre que celles hébergées sur le SI sensible. À titre d'illustration, le SI sensible est le réceptacle des informations vitales d'une entité (brevets, secrets de fabrication...). Par opposition, le SI usuel est le réceptacle des informations « moins sensibles ». À noter que, ni les informations sensibles, ni les informations usuelles, n'ont vocation à être rendues publiques.

---

3. Se reporter à la mesure II 901 GDB-QUALIF-SENSI.

Le fait de considérer qu'une entité ne met en œuvre que deux SI (SI sensible et SI usuel) est un parti pris à vocation pédagogique. La réalité est souvent plus complexe. Une entité peut être amenée à mettre en œuvre non pas un mais plusieurs SI usuels, sensibles ou DR en fonction de ses besoins de cloisonnement de l'information.

Le SI sensible est caractérisé par la mise en œuvre de mesures de sécurité techniques et organisationnelles plus exigeantes que celles mises en œuvre sur un SI usuel. Par opposition au SI usuel, le SI sensible doit être moins exposé aux réseaux publics (typiquement Internet) et le nombre d'utilisateurs de ce SI doit être limité au strict besoin.



### SI sensible

Un *SI sensible* est un SI susceptible d'héberger ou de traiter des données sensibles. Il est le réceptacle technique de toutes les données ayant une importance « forte » pour l'entité qui le met en œuvre. Un cas particulier de SI sensible est un SI qui héberge des données DR. Un tel SI est désigné *SI DR*.



### Attention

Dans ce guide, l'utilisation du terme *SI sensible* s'applique à tous les SI sensibles (aussi bien les SI DR que les SI non DR) tandis que l'utilisation du terme *SI DR* est réservé aux SI sensibles homologués au niveau DR<sup>4</sup>.



### SI usuel

Un *SI usuel* désigne un SI présentant un niveau de protection moindre que le SI sensible. Il est le réceptacle technique de toutes les données ayant une importance « moindre » pour l'entité qui le met en œuvre. Ces données sont qualifiées d'*usuelles* dans ce document.

R2

### ⚖️ Identifier les types de SI nécessaires

Après avoir trié son patrimoine informationnel non classifié, une entité doit identifier les types de SI (usuels, sensibles voire DR) qu'elle va devoir mettre en œuvre pour répondre à ses besoins de sécurité.



### Information

Par défaut, les informations d'un niveau de sensibilité donné doivent être traitées sur un SI à ce même niveau de sensibilité et non sur un SI de niveau supérieur (p. ex. des informations usuelles doivent, par défaut, être traitées sur un SI usuel et non sur un SI sensible ; des informations DR doivent, par défaut, être traitées sur un SI DR et non sur un SI classifié). Le non-respect de ce principe pourrait amener, au fil du temps, à devoir traiter la problématique d'extraction d'informations « moins sensibles » hébergées sur un SI « plus sensible ». Or, le traitement de cette problématique peut s'avérer complexe car il n'est pas trivial de garantir que ces extractions d'informations n'induisent pas des sorties incontrôlées de données.

4. Se reporter à la section 2.4 pour plus d'informations sur l'homologation de sécurité.

L'entité mettant en œuvre un ou plusieurs SI sensibles doit ensuite choisir la *classe* de ces SI<sup>5</sup>. L'II 901 définit trois classes de SI<sup>6</sup> :

- SI de classe 0 : SI public (p. ex. Internet) ou SI connecté à un SI public (p. ex. SI usuel) qui ne respecte pas les exigences de la classe 1 ;
- SI de classe 1 : SI sensible (ou DR) connecté à Internet au travers d'une passerelle sécurisée satisfaisant les exigences de sécurité définies dans l'II 901 ;
- SI de classe 2 : SI sensible (ou DR) physiquement isolé d'Internet.

Cette notion de classe de SI est détaillée à la section 3.1.2 où sont décrits les différents type d'architectures de SI sensibles.



### Information

Au sens strict, l'annexe 2 de l'II 901 où est défini le concept de SI de classe 1 ou de classe 2, ne concerne que les SI homologués au niveau DR. Toutefois, dans le cadre de ce guide, le parti-pris est d'étendre ce concept à l'ensemble des SI sensibles.

Par ailleurs, sauf mention explicite contraire, les recommandations formulées s'appliquent indifféremment aux SI sensibles de classe 1 ou de classe 2.

La figure 2 donne une représentation de l'articulation entre les classes de SI non classifiés (classe 0, classe 1 ou classe 2) et les niveaux de sensibilité de ces SI (public, usuel, sensible, DR). Les notions de « SI homologué sensible » et de « SI homologué DR » présentes sur cette figure sont expliquées à la section 2.3.

La figure 2 montre différentes interconnexions possibles entre les SI. Pour en savoir plus sur les interconnexions de SI, se reporter au chapitre 4.

5. Se reporter à l'article 14 de l'II 901.

6. En réalité, dans son annexe 2, l'II 901 définit le concept de *classe de réseau* et non de *classe de SI*. Le mot *réseau* étant utilisé dans l'expression *classe de réseau* pour désigner un système d'information, c'est cette appellation qui est préférée dans ce guide. On parle ainsi de « SI de classe 2 » et de « SI de classe 1 ». Le terme *réseau* est quant à lui réservé pour désigner l'ensemble des équipements permettant de matérialiser le réseau de communication qui interconnecte plusieurs systèmes informatiques.

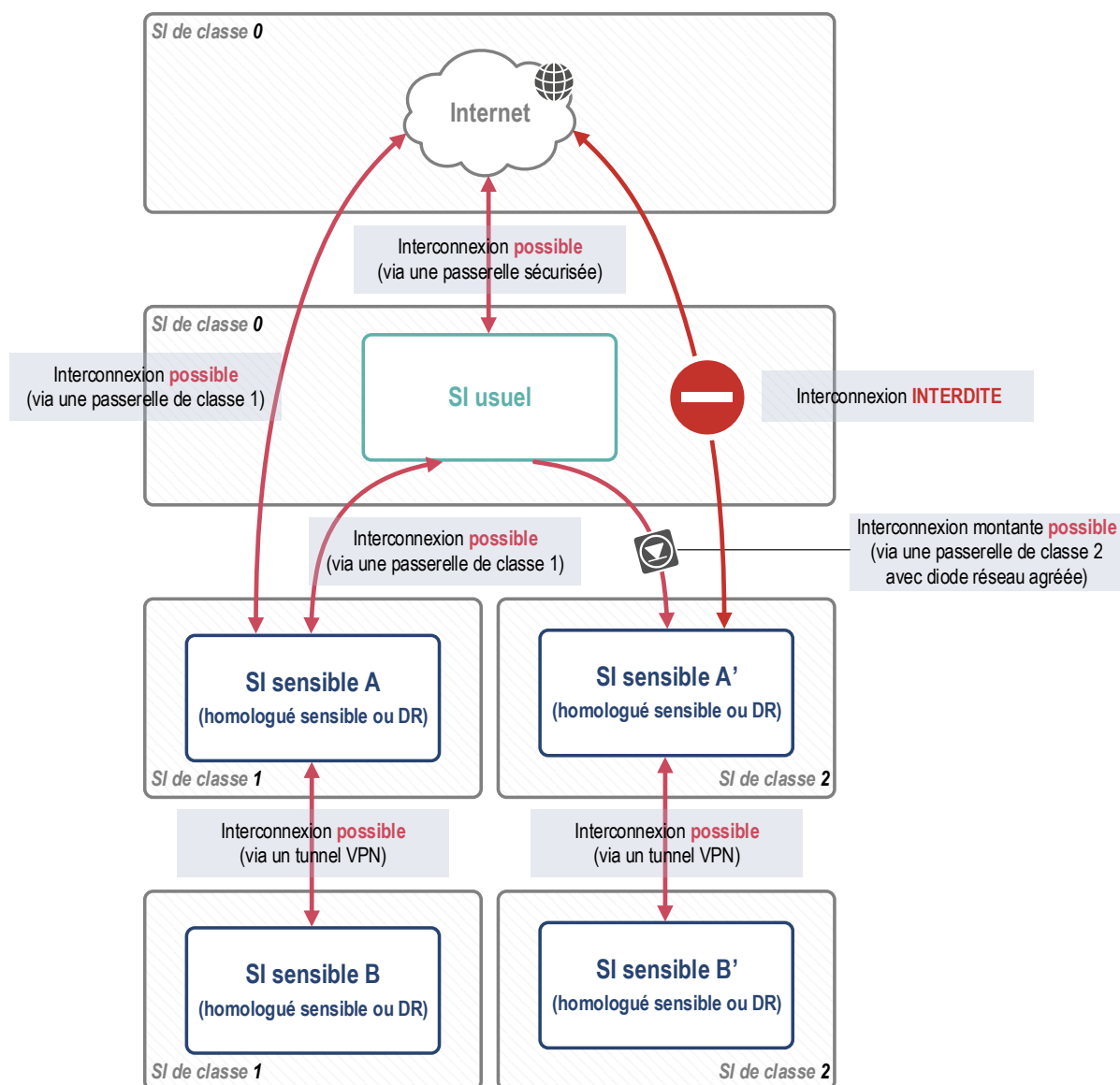


FIGURE 2 – Mise en correspondance des classes de SI (0, 1 ou 2) avec les niveaux de sensibilité des SI (public, usuel, sensible, DR)

Le patrimoine informationnel étant trié (recommandation R1) et la nature des SI (usuel, sensible, DR) étant identifiée (recommandation R2), il devient possible de répartir les informations au sein de ces différents SI, en fonction de leur positionnement sur l'échelle des besoins en confidentialité. La figure 3 illustre cette idée.

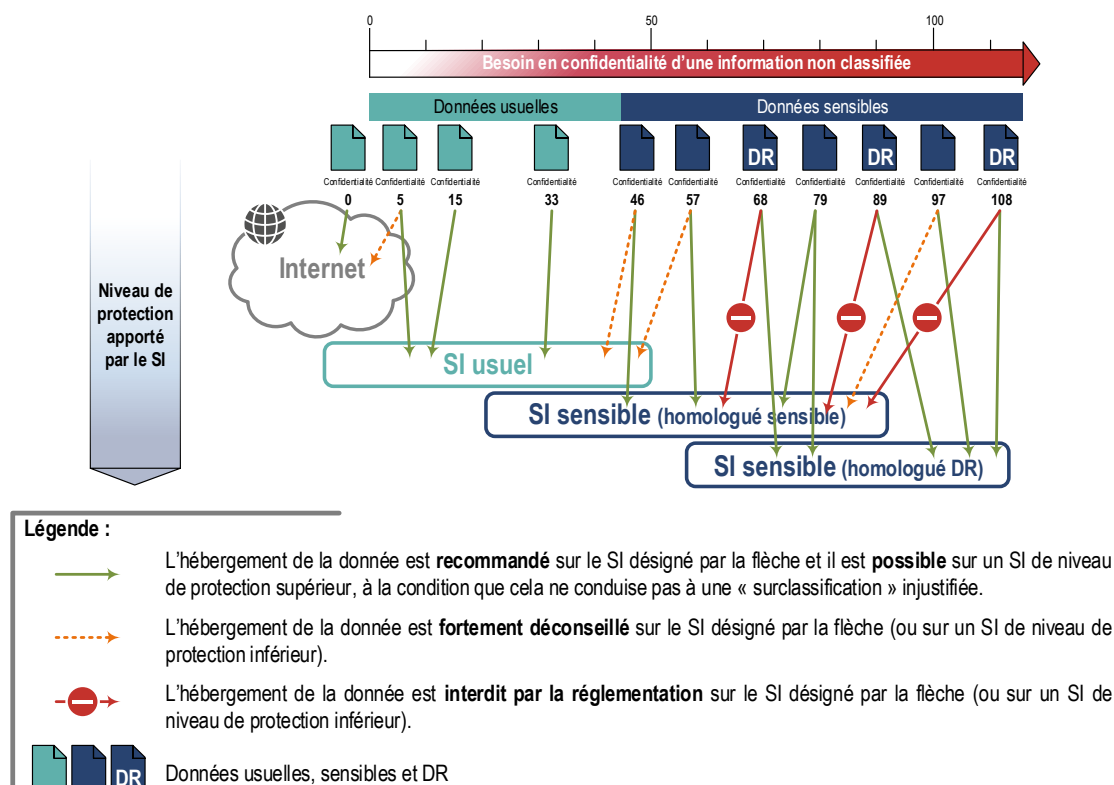


FIGURE 3 – Choix d'un SI adapté au besoin de protection en confidentialité d'une information

L'observation de l'exemple donné à la figure 3 conduit à plusieurs constats :

- seules des informations de niveau de confidentialité nulle (C0) peuvent être placées sur des SI publics tels qu'Internet ;
- une valeur arbitraire de confidentialité (C45 dans cet exemple) permet de distinguer les informations usuelles et les informations sensibles : au dessus de C45, l'information est considérée comme sensible (ou DR, si elle est marquée DR) ; au dessous de C45, l'information est considérée comme usuelle ;
- dans certains cas, le choix du SI d'hébergement d'une information est arbitraire. C'est par exemple le cas avec l'information C79 qui est une information sensible non DR pouvant être hébergée soit sur un SI sensible homologué sensible, soit sur un SI sensible homologué DR ;
- les informations DR ne peuvent être traitées que sur un SI homologué DR ;
- des informations ayant un besoin de protection en confidentialité particulièrement important (C97), sans pour autant être des informations DR, peuvent être traitées sur un SI homologué DR<sup>7</sup> ;
- la valeur de confidentialité maximale est ici C108, illustration que l'échelle des besoins en confidentialité est, par définition, ouverte et relative.

7. Ce raisonnement, poussé à l'extrême, peut amener à concevoir qu'une entité protège ses informations les plus sensibles sur un SI répondant aux exigences de sécurisation demandées pour un SI homologué DR, quand bien même aucune desdites informations ne seraient des informations DR.



## 2.3 Détermination du régime de protection des informations sensibles

Après avoir identifié qu'une information doit être hébergée sur un SI sensible, l'entité mettant en œuvre ce SI sensible doit déterminer le régime de protection de cette information. Il s'agit soit du régime de protection sensible (et, dans ce cas, l'information doit être hébergée sur un SI sensible), soit du régime de protection DR (et, dans ce cas, l'information doit être hébergée sur un SI DR).

Deux cas de figure peuvent se présenter :

- le régime de protection DR est imposé par l'État au travers de la réglementation<sup>8</sup> ou par un commanditaire au travers d'un marché public ou d'un contrat entre entités privées ;
- pour les informations ne relevant pas du cas précédent, c'est à l'entité qui met en œuvre le SI sensible de choisir le régime de protection adapté à ses besoins.

L'application de la mention Diffusion Restreinte relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient :

- conduire à la découverte d'une information classifiée ;
- porter atteinte à la sécurité ou à l'ordre public, au renom des institutions, à la vie privée de leurs membres ;
- porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d'établissements publics.

Un point de vigilance concerne l'agrégation d'informations usuelles. Une information considérée unitairement peut être vue comme usuelle mais *l'agrégation* de ces multiples informations unitaires peut avoir pour conséquence d'augmenter le niveau de sensibilité de l'agrégat résultant.

R3

### Déterminer le régime de protection des informations sensibles

Une entité qui met en œuvre un SI sensible doit déterminer le régime de protection à appliquer aux informations qu'elle va manipuler. En fonction des cas, ce régime de protection est soit imposé par la réglementation (ou par une entité tierce), soit laissé à la discrétion de l'entité. *In fine*, les informations sensibles sont hébergées sur des SI sensibles ou DR et les informations DR sont obligatoirement hébergées sur des SI DR.

Une fois le régime de protection des informations sensibles déterminé, la lecture de l'article 2 de l'II 901 permet de déduire quelles mesures de sécurité de l'II 901 sont obligatoires et lesquelles sont recommandées. En complément, l'annexe B de ce guide présente les différents niveaux de sensibilité des informations en France et précise pour quels niveaux les mesures de sécurité de l'II 901 sont imposées et pour lesquels elles sont recommandées.

8. L'article 2 de l'II 901 liste les cas pour lesquels l'entité a l'obligation d'appliquer un régime de protection DR.

## 2.4 Homologation d'un SI sensible

Après avoir défini le régime de protection des informations sensibles (régime sensible ou régime DR), l'entité mettant en œuvre un ou plusieurs SI sensibles doit appliquer des mesures de sécurité visant à atteindre un niveau de sécurité suffisant et à le maintenir pendant la durée de leur exploitation et jusqu'à leur démantèlement. De manière à formaliser l'atteinte d'un niveau de sécurité réel satisfaisant, une procédure organisationnelle dite d'homologation de sécurité doit être conduite.

Dans le cadre de cette procédure, un responsable de l'entité est désigné autorité d'homologation (AH) par l'autorité qualifiée en sécurité des systèmes d'information (AQSSI) de cette même entité <sup>9</sup>.

La démarche d'homologation, appliquée à un SI sensible, vise à faire accepter formellement par l'AH les risques résiduels pesant sur ce SI au regard de sa contribution aux missions de l'entité. Pour ce faire, un dossier d'homologation est constitué afin d'éclairer l'AH sur la méthode d'appréciation des risques et sur leur traitement (acceptation, refus, transfert, réduction). En particulier, il détaille les mesures de sécurité retenues pour réduire les risques. Ces mesures de sécurité sont de nature technique ou organisationnelle. Elles s'appliquent à l'entité ou aux parties prenantes de son écosystème (par exemple au moyen de clauses contractuelles). Le dossier d'homologation apporte également des éléments d'appréciation du niveau de sécurité réel du SI sensible (p. ex. rapports d'audits, attestations de qualification, de certification ou d'agrément des versions de produits déployées sur le SI...).

À l'issue de la présentation de ces éléments, l'AH peut, en connaissance de cause, prendre la décision formelle d'homologation. Par cet acte, elle atteste que les risques pesant sur les informations, les traitements et les services du SI sensible sont connus, maîtrisés et que les risques résiduels sont acceptés, compte tenu de la contribution du SI aux missions de l'entité. Le SI sensible est alors déclaré homologué, pour une durée déterminée. En fonction de sa finalité et de son régime (sensible ou DR), un SI sensible est dit « homologué au niveau sensible » ou « homologué au niveau DR ».

Pour plus d'informations concernant l'homologation de sécurité, il est conseillé de se reporter au guide publié par l'ANSSI portant sur ce sujet [16].

R4

### Homologuer tout SI sensible avant sa mise en production

Tout SI sensible doit être homologué. Toutes les interconnexions de ce SI doivent également être homologuées.

Les risques pesant sur un SI sensible doivent, en outre, être périodiquement réévalués dans une démarche d'amélioration continue et d'adaptation permanente à l'évolution de la menace <sup>10</sup>.

La démarche d'homologation des SI sensibles va conduire à définir un *périmètre d'homologation II 901*.

9. Se reporter à l'article 86 de l'IGI 1300.

10. Se reporter à l'article 3 de l'II 901 et à la mesure de sécurité II 901 EXP-CI-AUDIT.



## Périmètre d'homologation II 901

Le périmètre d'homologation II 901 délimite l'ensemble des systèmes qui, dans une démarche d'homologation, doivent être conformes aux mesures de sécurité décrites dans l'II 901 et dans le présent guide. Tous les matériels concourant au traitement ou au stockage des informations sensibles (y compris les matériels mobiles comme les supports amovibles) doivent être inclus dans le périmètre d'homologation.



### Information

L'II 901 précise que les homologations des interconnexions de SI sensibles font l'objet d'homologations distinctes de celle des SI interconnectés <sup>11</sup>.

---

11. Se reporter à l'II 901, annexe 2.

# 3

## Typologies de SI sensibles



### Objectif

Le chapitre 2 a permis de comprendre en quoi la création d'un (et potentiellement plusieurs) SI sensible(s) est la réponse au besoin d'une entité de protéger son patrimoine informationnel non classifié de défense. Ce chapitre a pour objectif de présenter les grandes typologies d'architectures envisageables pour ces SI.

## 3.1 Représentation des typologies d'architecture

L'architecture d'un SI est définie par l'organisation et les interactions des composants informatiques matériels et logiciels qui le constituent. Ce chapitre a pour ambition de présenter au lecteur trois grands types d'architecture de SI sensibles. Ces types d'architecture sont acceptables d'un point de vue réglementaire, bien que non équivalents du point de vue du niveau de leur sécurité.

Pour la bonne compréhension des architectures décrites dans ce chapitre, il est nécessaire d'expliquer préalablement les conventions de représentation utilisées dans les schémas d'architecture de ce guide.

### 3.1.1 Conventions graphiques pour les schémas d'architecture

Sur les schémas d'architecture présentés dans ce guide, le SI sensible et le SI usuel sont volontairement représentés de manière symbolique par des rectangles « monolithiques » (de couleur bleue pour le SI sensible et de couleur verte pour le SI usuel). Chaque rectangle contient implicitement l'ensemble des composants matériels et logiciels d'un SI (serveurs, postes de travail, équipements réseau...).

Cette représentation au moyen de rectangles ne signifie pas que le SI soit décroisé et que toutes les communications entre tous les systèmes qui le constituent soient possibles. Bien au contraire, dans le cas d'un SI sensible, les mesures de cloisonnement et de durcissement des systèmes sont plus strictes que pour un SI usuel. Ces mesures, relatives à la sécurisation interne d'un SI sensible, sont décrites aux chapitres 5 (principe de défense en profondeur) et 6 (sécurisation des postes de travail).



### Attention

Dans les schémas d'architecture de ce document, sauf indication contraire explicite, tous les composants des SI sensibles et des SI usuels sont supposés être physiquement distincts. Autrement dit, aucune mutualisation n'est envisagée entre les

SI sensibles et les SI usuels, que ce soit au niveau système (machines physiques, hyperviseurs...), au niveau réseau (routeurs, commutateurs...) ou au niveau stockage (baies de disques, commutateurs de *fabric*...).

Par ailleurs, sur les schémas d'architecture, le *périmètre d'homologation II 901* (concept défini à la fin de la section 2.4) est représenté par des pointillés de couleur orange.

Enfin, le terme *passerelle Internet sécurisée* est utilisé sur les schémas pour représenter l'ensemble des moyens de protection recommandés pour sécuriser l'interconnexion d'un SI quelconque (typiquement un SI usuel) avec Internet. Ce concept de *passerelle Internet sécurisée* est expliqué dans le guide de l'ANSSI relatif à l'interconnexion d'un SI à Internet [23].

### 3.1.2 Les classes de SI

L'II 901 définit dans son annexe 2 un concept de classe de réseau. Ce concept, déjà évoqué à la section 2.2, est utilisé dans ce guide pour expliquer les différentes architectures de SI sensibles. Chaque fois que cela est pertinent, les périmètres des classes de SI (classe 1 ou classe 2) sont représentées sur les schémas d'architecture au moyen de surfaces hachurées grises.

Les définitions des classes de SI sont données dans l'II 901 <sup>12</sup> et rappelées ci-après.



#### SI de classe 0

*Un SI de classe 0 est un SI public (Internet, SI usuel...) ou un SI connecté à un SI public qui ne respecte pas les exigences de la classe 1 ci-dessous.*



#### SI de classe 1

*Un SI de classe 1 est un SI qui est interconnecté<sup>13</sup> à des SI de classe 0 à l'aide de dispositifs de filtrage et de rupture de flux de la façon suivante :*

- *au moins un dispositif de filtrage qualifié au niveau standard est mis en coupure de tous les flux depuis et vers le SI de classe 0<sup>14</sup> ;*
- *un dispositif de rupture de tous les flux (proxy) depuis et vers le SI de classe 0, si possible qualifié au niveau élémentaire, est positionné entre deux dispositifs de filtrage ;*
- *une sonde de détection qualifiée au moins au niveau élémentaire contrôle l'ensemble des flux échangés avec le SI de classe 0.*

*L'interconnexion de réseaux de classe 1 entre eux est autorisée sous certaines conditions (lire section 4.2).*

Les dispositifs de sécurité exigés par la réglementation pour interconnecter un SI sensible de classe 1 et un SI de classe 0 sont regroupés dans une passerelle qui est appelée *passerelle de classe 1*

12. Se reporter à l'annexe 2 de l'II 901.

13. La formulation exacte dans l'II 901 est *SI qui est isolé*. Pour plus de clarté, dans ce guide, le terme *isolé* est réservé aux SI de classe 2.

14. Cette formulation suggère que ce dispositif de filtrage est unique. Il s'agit d'un abus de langage. Au contraire, il est recommandé que plusieurs dispositifs de ruptures de flux soient mis en œuvre en fonction de la nature des protocoles et de manière à réduire la surface d'attaque.

dans ce guide. Une *passerelle de classe 1* est donc composée de deux dispositifs de filtrage (dont au moins un qualifié au niveau standard) encadrant un *proxy* et une sonde qualifiée. Cette passerelle est décrite en détail à la section 4.3.1.

La figure 4 donne la représentation de ce segment d'interface dans les schémas d'architecture de ce guide. À noter que, sur certains schémas, par souci de lisibilité, tous les dispositifs de sécurité (pare-feux, *proxy* et sonde) ne seront pas systématiquement dessinés. Pour autant, chaque fois que le terme *passerelle de classe 1* sera utilisé dans les schémas, il sera sous-entendu que ces dispositifs doivent être présents, même si ils ne sont pas représentés.

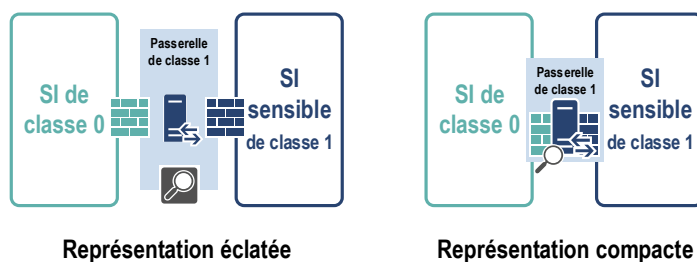


FIGURE 4 – Représentations d'une *passerelle de classe 1* dans ce guide. Les deux représentations (étlatée et compacte) ont des significations strictement équivalentes.



## SI de classe 2

Un SI de classe 2 est un SI qui :

- est isolé, c'est-à-dire non connecté, même indirectement, à Internet ;
- ne comprend aucune interconnexion « descendante » permettant l'envoi de flux en clair ou chiffrés à destination des SI de classe 0 ou 1, sauf à utiliser des dispositifs agréés spécifiquement pour cet usage (notion de « passerelle descendante ») ;
- comprend éventuellement des interconnexions « montantes » permettant la réception de flux en provenance des SI de classe 0 ou 1 au travers d'une diode agréée par l'ANSSI pour de tels usages (notion de « passerelle montante »).

L'interconnexion de réseaux de classe 2 entre eux est autorisée sous certaines conditions (lire section 4.2).

## 3.2 Différentes architectures de SI sensibles

### 3.2.1 SI sensible physiquement isolé

Par définition, les architectures de SI sensibles de classe 2 sont des SI « physiquement isolés ». Dans un tel SI, aucun composant de stockage ou de traitement de données (serveurs, postes de travail, baies de stockage...) n'est partagé avec un autre SI de classe 1 ou de classe 0.

En outre, ce type de SI est dépourvu d'interconnexion avec un SI de classe 0, sauf à satisfaire des conditions spéciales (se reporter à la section relative au systèmes d'échanges sécurisés pour les utilisateurs). La connexion à des ressources hébergées sur Internet n'est pas autorisée depuis un SI sensible de classe 2.

Du fait de leur forte isolation réseau, les architectures de SI sensibles de classe 2 présentent un faible niveau d'exposition aux menaces issues d'autres SI. Le recours à ces architectures est obligatoire lorsque les risques pesant sur le SI sensible sont élevés.

Faire le choix d'un SI sensible de classe 2, physiquement isolé de tout autre SI, est d'autant plus pertinent que la taille du SI est réduite (typiquement, un SI sensible constitué de quelques postes de travail destinés à consulter des informations sensibles).



### Attention

Un SI de classe 2, physiquement isolé de tout autre SI, ne doit pas être considéré trop rapidement comme étant un *SI sécurisé*. En effet, l'absence d'interconnexion, bien qu'étant de nature à réduire l'exposition du SI aux menaces, peut aussi complexifier l'administration, le maintien en conditions de sécurité et la supervision du SI, ce qui peut s'avérer problématique pour les SI sensibles les plus étendus.



### Attention

L'absence totale d'interconnexion ne signifie pas que des données ne puissent pas être introduites ou extraites d'un SI de classe 2. Des besoins métier peuvent justifier que l'insertion ou l'extraction de données au moyen de supports amovibles soient autorisées par la politique de sécurité. Dans ce cas, la gestion de ces supports doit être encadrée avec la plus grande rigueur, faute de quoi les bénéfices escomptés de la stratégie d'isolation pourraient être réduits à néant. La section 5.7 donne plus d'informations concernant les supports amovibles.

R5 +

### Isoler physiquement le SI sensible et le SI usuel

Il est recommandé que les entités ayant des besoins de confidentialité importants mettent en place au minimum deux SI (un SI usuel et un SI sensible) physiquement isolés. Dans ce cas, le SI sensible est un SI de classe 2 dépourvu d'interconnexion, même indirecte, avec Internet.

Les figures 5 et 6 donnent deux représentations fonctionnelles simplifiées d'architectures possibles pour des SI sensibles de classe 2. Le premier exemple d'architecture (figure 5) met en œuvre une passerelle montante depuis un SI de moindre confiance (en l'occurrence un SI usuel) vers un SI de classe 2. Le second exemple (figure 6) montre un SI sensible de classe 2 dépourvu d'interconnexion directe, totalement isolé.

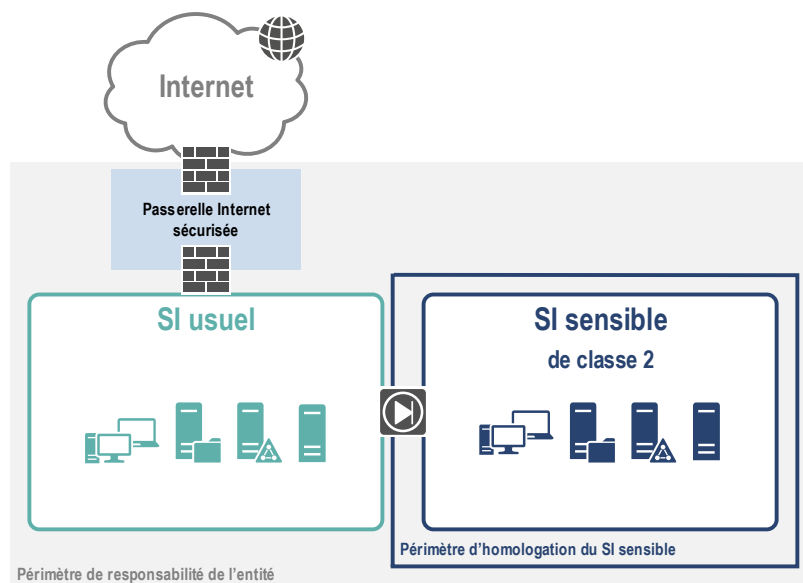


FIGURE 5 – SI sensible de classe 2 - Exemple d’une architecture avec une interconnexion directe unidirectionnelle par le biais d’une passerelle montante

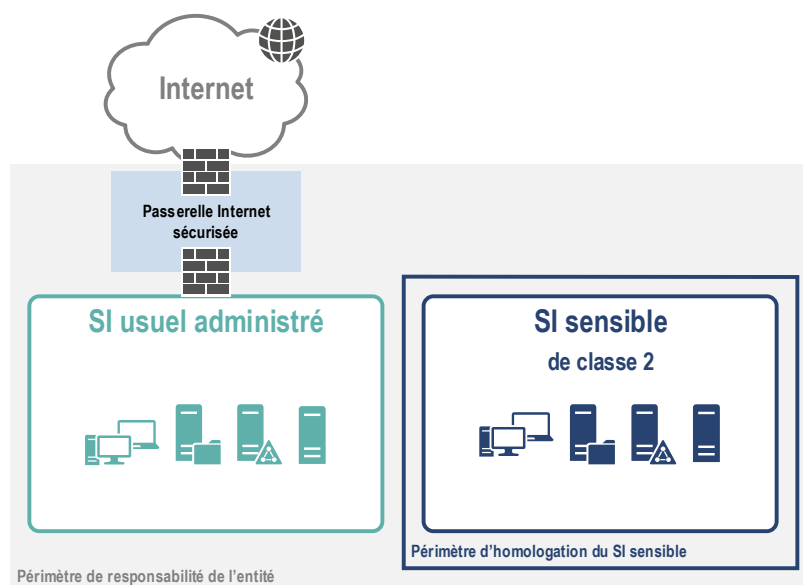


FIGURE 6 – SI sensible de classe 2 - Exemple d’une architecture sans interconnexion directe

### 3.2.2 SI sensible physiquement cloisonné

Lorsque les besoins métier ne sont pas compatibles avec une architecture « SI sensible physiquement isolé » et que les besoins de sécurité le permettent, il est possible d’opter pour une architecture de SI sensible de classe 1 : un « SI physiquement cloisonné ».

Ce type de SI se rapproche d’un « SI sensible physiquement isolé » car aucun composant de stockage



ou de traitement de données (serveurs, postes de travail, baies de stockage...) n'est partagé avec un autre SI. Mais il s'en distingue car une ou plusieurs passerelles d'interconnexion rendent possibles le transfert bidirectionnel de données, au travers du réseau, avec un ou plusieurs autres SI et, potentiellement, avec Internet.

Ce type d'architecture rend possible la fourniture de services qui sont difficiles ou impossibles à mettre en œuvre dans le cas des réseaux de classe 2, en particulier des services nécessitant des interactions entre le SI sensible et des SI tiers, en particulier Internet.

Cette architecture peut être pertinente pour les entités mettant en œuvre des processus métier où l'élaboration, le traitement et le stockage de données sensibles ne constituent pas une part dominante de l'activité.

Le segment d'interface entre SI de classe 0 et SI de classe 1 héberge au minimum les composants de sécurité listés dans la réglementation, à savoir des dispositifs de filtrage, des dispositifs de rupture protocolaire et des dispositifs de détection d'intrusion (voir la définition d'un SI de classe 1 rappelée à la section 3.1.2).

R5

### Cloisonner physiquement le SI sensible et le SI usuel

À défaut de mettre en œuvre un SI physiquement isolé, il est possible de construire deux SI (un SI sensible et un SI usuel) physiquement cloisonnés et interconnectés par une passerelle bidirectionnelle conforme à l'II 901. Dans ce cas, le SI sensible est un SI de classe 1 interconnecté indirectement à Internet.

La figure 7 donne une représentation fonctionnelle simplifiée d'architecture possible d'un « SI sensible physiquement cloisonné ».

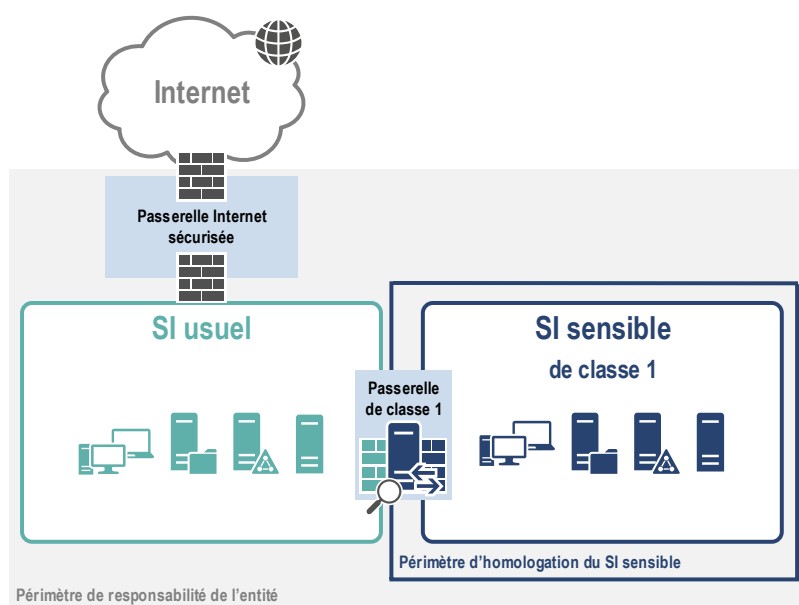


FIGURE 7 – SI sensible de classe 1 - Exemple d'architecture d'un SI physiquement cloisonné

### 3.2.3 SI sensible sans SI usuel

Lorsque les besoins métier ne sont pas compatibles avec une architecture « SI sensible physiquement cloisonné » et que les besoins de sécurité le permettent, il peut être envisagé une version dégradée de l'architecture de SI sensible de classe 1 présentée à la section précédente. Dans cette architecture, les données usuelles et les données sensibles sont hébergées au sein d'un même SI. Pour autant, cela ne signifie pas que ces deux ensembles soient fusionnés du point de vue de leur architecture. Au contraire, des mécanismes de cloisonnement logique doivent être mis en œuvre, tant au niveau réseau (segmentation des réseaux et filtrage strict des flux entre ces segments), qu'aux niveaux système et applicatif, pour séparer les données et traitements sensibles des données et traitements usuels.

Contrairement aux architectures présentées aux sections précédentes, avec un « SI sensible sans SI usuel », certains des composants (hyperviseurs, serveurs, baies de stockage, équipements réseau...) sont mutualisés pour le « sous-ensemble des données usuelles » et pour le « sous-ensemble des données sensibles ».

Le transfert bidirectionnel de données, au travers du réseau, avec un ou plusieurs SI de classe 0 (donc, potentiellement, avec Internet) n'est possible qu'au travers d'une ou plusieurs passerelles d'interconnexion.

Cette architecture peut être pertinente pour les entités mettant en œuvre des processus métier où l'élaboration, le traitement et le stockage de données sensibles constituent une part dominante de l'activité.

Avec cette architecture, le *périmètre d'homologation II 901* inclut non seulement les ressources sensibles mais également les ressources usuels. Les moyens usuels, hébergés *de facto* sur un SI sensible, doivent être protégés comme s'ils étaient des moyens sensibles et doivent par conséquent être conformes aux mesures de sécurité de l'II 901. Elle oblige le responsable du SI sensible à une grande rigueur dans les actions de maintien en conditions de sécurité et de maintien en conditions opérationnelles de *l'ensemble* des ressources du SI.



#### Attention

Cette architecture est par nature beaucoup plus difficile à sécuriser que celles présentées aux sections 3.2.1 et 3.2.2. En effet, non seulement le *périmètre d'homologation II 901* du SI est étendu, mais un cloisonnement logique (entre le sous-ensemble des données sensibles et le sous-ensemble des données usuels) apporte un niveau de robustesse inférieur à celui d'un cloisonnement physique. Un cloisonnement logique augmente la surface d'attaque et suppose en conséquence une maîtrise très forte de la configuration des systèmes et un maintien dans la durée de cette maîtrise. Cette architecture ne doit être envisagée qu'en ultime recours et est réservée aux entités ayant un fort degré de maturité SSI.



#### Attention

Avec cette architecture, si le service de navigation Web est requis, l'application de la recommandation R18- (postes de rebond) est fortement recommandée.

## Cloisonner logiquement les données sensibles au sein d'un SI sensible

À défaut de mettre en œuvre un SI sensible physiquement isolé ou physiquement cloisonné, les entités ayant un niveau de maturité SSI élevé peuvent envisager de mettre en place un SI sensible et de ne pas créer de SI usuel<sup>15</sup>. Les ressources usuelles doivent alors être incluses dans le *périmètre d'homologation II 901* du SI sensible.

Au sein de ce SI sensible, les données sensibles doivent être cloisonnées logiquement des données usuelles.

Dans cette architecture, le SI unique est un SI de classe 1 interconnecté à Internet au moyen d'une *passerelle Internet sécurisée* qui intègre l'ensemble des dispositifs de sécurité définissant une *passerelle de classe 1*.

Si le service de navigation Web est nécessaire, il est fortement recommandé qu'il soit rendu au travers d'une infrastructure de postes utilisateur de rebond (voir la recommandation R18-).

La figure 8 donne une représentation fonctionnelle simplifiée de l'architecture d'un SI avec cloisonnement logique des données sensibles et des données usuelles.

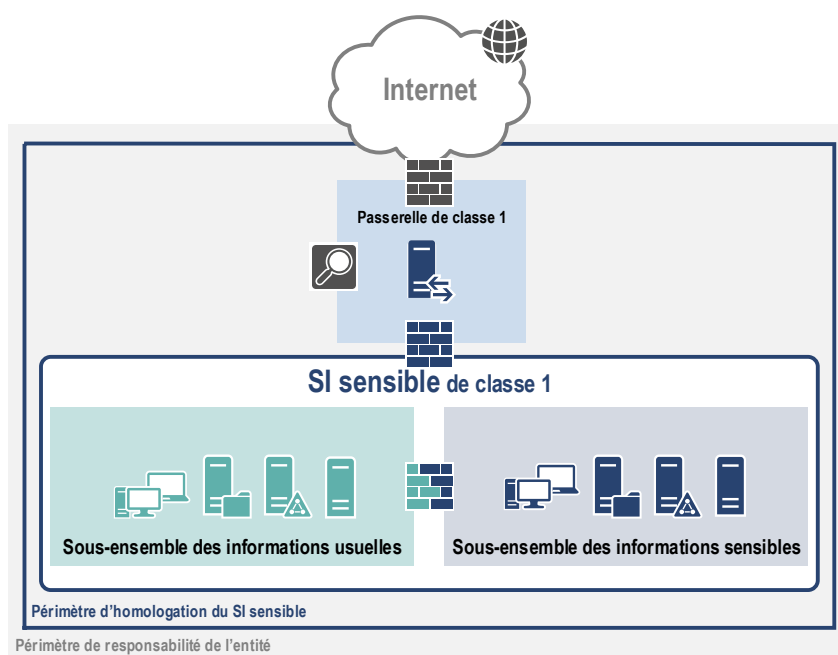


FIGURE 8 – SI sensible de classe 1 - Exemple d'architecture avec cloisonnement logique des données sensibles et usuelles

## Considérations relatives à la mutualisation des moyens

Dans cette architecture « SI sensible sans SI usuel », le *périmètre d'homologation II 901* n'est pas réduit aux moyens sensibles mais étendu aux moyens usuels. Par voie de conséquence, les coûts de

15. Le lien de causalité doit ici être bien compris : c'est bien parce qu'elle possède des compétences techniques élevées en matière de SSI et qu'elle entend les maintenir dans la durée (cause), qu'une entité peut envisager de faire le choix d'une telle architecture (conséquence). Le raisonnement inverse serait erroné : ce n'est pas parce qu'une entité fait le choix de cette architecture, qu'elle peut s'estimer mature en SSI. Cette architecture ne doit être envisagée qu'en ultime recours.

sécurisation augmentent. L'entité mettant en oeuvre cette architecture est amenée, pour répondre au besoin de cloisonnement des données usuelles et sensibles, à s'interroger sur le niveau de mutualisation acceptable des composants du SI sensible. Cette étude doit prendre en compte tous les composants du SI (réseau, systèmes, stockage...).

Les exigences de sécurité qui visent à réduire le risque induit par le recours à la mutualisation des moyens entre le « sous-ensemble des données usuelles » et le « sous-ensemble des données sensibles » doivent faire l'objet d'études spécifiques conduites par l'entité et être intégrées à la démarche d'homologation.

Il est hors du périmètre de ce guide de se prononcer sur les cas de mutualisation acceptables ou non. La réponse à cette question est en effet dépendante des choix technologiques faits par l'entité et l'offre technologique est beaucoup trop vaste et évolutive pour pouvoir en dégager des règles précises.

Quelques principes directeurs peuvent néanmoins être énoncés.

Si un composant est mutualisé pour traiter des données usuelles et des données sensibles, il faut s'efforcer de mettre en oeuvre au moins deux barrières logiques, robustes et complémentaires, pour protéger l'accès aux données. Cette double protection a pour but d'améliorer le cloisonnement : la compromission d'une barrière (malveillance ou erreur humaine) n'expose ainsi pas les données sensibles <sup>16</sup>.

R6

### Appliquer le principe de défense en profondeur en cas de mutualisation de ressources

Le concept de défense en profondeur est un principe stratégique de l'II 901 <sup>17</sup>. En particulier, quand la mutualisation de ressources d'un SI sensible avec un autre SI est envisagée, l'entité doit systématiquement mettre en oeuvre le concept de défense en profondeur pour réduire les risques induits par cette mutualisation.

Les postes de travail peuvent constituer un autre exemple d'équipements pouvant être mutualisés. Cette mutualisation peut être envisagée dans le respect strict des recommandations R52- (poste de travail multiniveau) ou R52-- (poste de travail sensible avec accès distant au SI usuel) détaillées à la section 6.3 consacrée aux aspects postes de travail.

La mutualisation des postes d'administration pour l'administration de ressources sensibles et de ressources usuelles est envisageable. En revanche, il est recommandé de dédier les outils d'administration par niveau de sensibilité (des outils pour l'administration des ressources sensibles et des outils distincts pour l'administration des ressources usuelles). Pour plus d'informations, se reporter à la section 7.2 relative au SI d'administration.

Dans le cas des recommandations R5+ et R5, le service d'annuaire des utilisateurs est, par hypothèse, nécessairement constitué d'annuaires distincts (l'un usuel et l'autre sensible). La question de leur

16. À titre d'illustration, si une baie de stockage est utilisée pour stocker les deux types de données, il est judicieux de définir des volumes de données logiques distincts pour chacune d'entre elles et de compléter cette mesure par un chiffrement des données sensibles (chiffrement au niveau du système de fichiers ou chiffrement au niveau de la donnée).

17. Se reporter à l'article 3 de l'II 901.

mutualisation ne se pose donc pas. En revanche, une entité qui mettrait en œuvre l'architecture faisant l'objet de la recommandation dégradée R5- (« SI sensible sans SI usuel »), pourrait avoir la tentation de créer un annuaire unique : cette mutualisation est fortement déconseillée.

R7

### Cloisonner les annuaires sensible et usuel

Dans le contexte de la recommandation dégradée R5-, il est fortement recommandé que l'entité mette en œuvre des annuaires distincts : au minimum, un annuaire est déployé pour les utilisateurs et ressources sensibles et un deuxième pour les utilisateurs et ressources usuelles.

## 3.3 Critères influençant les choix d'architecture des SI sensibles

La section 3.2 donne trois exemples d'architectures de SI sensibles acceptables du point de vue réglementaire. L'entité qui souhaite déployer un SI sensible doit choisir parmi ces trois architectures laquelle, ou lesquelles, sont les plus adaptées à son contexte métier et à sa stratégie. À ce titre, il lui appartient de réfléchir, en phase amont du projet de mise en œuvre d'un SI sensible, aux critères métier et réglementaires qui vont orienter ce choix.

Seule l'entité peut mener cette analyse et il serait vain de présenter dans ce guide un arbre de décision conduisant à préférer une architecture à une autre. En revanche, cette section a pour objet d'explicitier les principaux critères à considérer pour faire un choix éclairé.

### Niveau de protection visé pour la protection en confidentialité des informations sensibles

Dans le cas des SI sensibles tels qu'ils sont définis dans l'II 901, un des principaux objectifs de sécurité visé est la protection en *confidentialité* des *informations* hébergées sur ces SI.

De manière à atteindre cet objectif, une protection en intégrité du *SI sensible* est également recherchée. En effet, une dégradation de l'intégrité du SI pourrait *in fine* conduire à une divulgation d'informations ayant un haut niveau de confidentialité<sup>18</sup>.

Or, les niveaux de protection des informations sensibles ne sont pas équivalents pour les trois grands types d'architectures présentées à la section précédente. L'architecture associée à la recommandation R5+ (« SI sensible physiquement isolé ») apporte un niveau de protection supérieur à l'architecture associée à la recommandation R5 (« SI sensible physiquement cloisonné du SI usuel »), elle-même d'un niveau supérieur à l'architecture associée à la recommandation R5- (« SI sensible sans SI usuel »).

18. Apporter une protection optimale de la confidentialité des *informations* hébergées sur un SI sensible est une caractéristique des SI sensibles relevant de l'II 901. En ce sens, ces SI se distinguent des SI pour lesquels l'objectif principal recherché est d'assurer un bon niveau de protection en intégrité et en disponibilité des *traitements* qu'ils opèrent. Des exemples de tels SI sont certains systèmes d'information d'importance vitale (SIIV) et certains systèmes d'information essentiels (SIE).

Ainsi, le critère principal à prendre en compte pour la mise en œuvre d'un SI sensible est le niveau de protection que l'entité responsable du SI cherche à atteindre pour la protection des informations sensibles dont elle a la responsabilité.

## Niveau de maturité SSI de l'entité responsable du SI sensible

Les trois grands types d'architectures présentés à la section précédente ne se distinguent pas seulement par le niveau de protection qu'elles confèrent aux données sensibles hébergées mais aussi par des complexités de mise en œuvre inégales. Ainsi, un « SI sensible physiquement isolé », s'il est dépourvu de passerelle descendante agréée, est nettement plus simple à concevoir que les autres types de SI sensibles : l'absence d'interconnexion descendante réduit nettement les risques d'exfiltration de données. Sans pour autant résoudre tous les problèmes (la problématique de gestion des supports amovibles demeure), une telle architecture permet de s'affranchir de nombreuses difficultés et de réduire les risques.

De manière générale, la mise en œuvre d'un SI de classe 1 génère de fortes contraintes sur les interconnexions de ce SI (se reporter au chapitre 4) et sur la maîtrise des postes de travail des utilisateurs (se reporter au chapitre 6).

Un SI de classe 1 implique également une forte maturité SSI des personnes chargées de sa conception et de son exploitation. Par conséquent, les architectures de SI sensibles de classe 1 sont peu adaptées aux entités ayant un nombre réduit de personnes qualifiées en SSI. Les architectures de SI sensibles de classe 2 doivent être préférées dans ce cas.

La maturité SSI d'une entité dépend aussi fortement du niveau d'appropriation des règles d'hygiène<sup>19</sup> informatique par les utilisateurs. Les utilisateurs portent en effet la responsabilité de la bonne manipulation des informations (usuelles ou sensibles) qu'ils élaborent ou qui leurs sont confiées<sup>20</sup>. Or, les règles afférentes à ces traitements seront d'autant plus simples à appréhender que l'architecture retenue pour le SI sensible explicitera, par construction, les cloisonnements existant entre les différents SI. Ainsi, les architectures « SI sensible physiquement isolé » et « SI sensible physiquement cloisonné » seront plus intuitives pour leurs utilisateurs. La nécessité de s'authentifier avec des authentifiants distincts, de préférence depuis des postes de travail distincts, permettra aux utilisateurs de travailler sans ambiguïté sur les SI usuels et sensibles.

Dans le cas de l'architecture « SI sensible sans SI usuel », il est à noter que les mesures de sécurité II 901, exigées pour atteindre le niveau de protection d'un SI sensible, et qui s'appliquent à tous les utilisateurs de l'entité, pourraient être perçues comme des contraintes par ceux qui n'ont besoin d'accéder qu'aux seules ressources usuelles.

## Besoins en matière d'interconnexions d'un SI sensible

Des raisons métier peuvent justifier des besoins plus ou moins importants de connexion d'un SI sensible avec d'autres SI, que ces derniers soient de niveau de sensibilité inférieur, égal ou supérieur à celui du SI sensible. Ces besoins de connexions avec d'autres SI influencent le choix d'architecture

---

19. Pour plus d'information concernant les règles élémentaires de sécurité recommandées par l'ANSSI, se reporter au guide d'hygiène informatique [11].

20. Se reporter à la mesure II 901 GDB-PROT-IS.

d'un SI sensible. Par exemple, la création d'un SI sensible de classe 2 pourra être imposée par un besoin métier nécessitant l'interconnexion avec un partenaire qui a lui-même mis en œuvre un SI de classe 2.

Quels que soient leur nombre, leur sens (montant ou descendant) et leur nature (interconnexions de réseaux ou transferts de données à l'aide de supports amovibles), les échanges de données avec un SI sensible doivent être justifiés par des besoins métier et être limités au strict nécessaire (principe de minimalité). Créer et tenir à jour la cartographie exhaustive des échanges nécessaires sera très utile pour la détection d'échanges anormaux ou inhabituels, et, dans le cas d'une passerelle descendante, pour la définition d'une éventuelle liste d'autorisations.

## Quantité d'informations sensibles

Toutes les informations manipulées par une entité ne sont pas sensibles. En fonction des besoins métier, le ratio entre les informations sensibles et les informations usuelles est différent. La méthode d'évaluation de la quantité et de l'importance des données sensibles par rapport aux données usuelles dépend de la stratégie de développement de l'entité concernée. Cette appréciation quantitative et qualitative pourra prendre en compte des éléments tels que le nombre d'utilisateurs de l'entité amenés à consulter ou élaborer des informations sensibles, le volume total de données sensibles placées sous la responsabilité de l'entité (de son propre fait ou confiées par des tiers) ou encore l'importance stratégique de ces informations en comparaison des autres informations dont elle a la responsabilité.

## Autres critères

D'autres facteurs doivent être pris en compte par l'entité pour l'élaboration de l'architecture d'un SI sensible : les implications sur les méthodes de travail des utilisateurs et des administrateurs des SI, les autres obligations réglementaires auxquelles elle est soumise<sup>21</sup>, les perspectives d'extension du SI sensible pour répondre à des enjeux métier futurs...

---

21. Par exemple, le respect de réglementations financières.

# 4

## Interconnexions directes de SI sensibles



### Objectif

Ce chapitre présente les recommandations relatives à la sécurisation des interconnexions directes d'un SI sensible avec d'autres SI. Le terme « interconnexion directe » désigne les interconnexions réalisées au moyen de dispositifs permettant l'échange d'informations par transfert de signaux électromagnétiques entre les SI interconnectés. Ces interconnexions directes s'opposent aux interconnexions réalisées indirectement, au moyen de supports amovibles (pour plus d'informations sur ces interconnexions indirectes, se reporter à la section 5.7).

### 4.1 Généralités

Un SI sensible peut avoir des interconnexions avec d'autres SI. Afin de prévenir les intrusions et les exfiltrations de données, l'entité doit maîtriser ces interconnexions. Cette maîtrise nécessite notamment la prise en compte des éléments suivants :

- toute interconnexion avec des SI internes à l'entité ou avec des SI tiers (p. ex. Internet) doit être inventoriée et homologuée (voir la section 2.4 relative à l'homologation de sécurité). Une attention particulière doit être portée sur toutes les interconnexions spécifiques (p. ex. liaisons de télémaintenance pour des moyens industriels, voir section 7.3), ainsi qu'à toutes les interconnexions non contrôlées qui pourraient être introduites par la mise en œuvre de composants connectés au SI (p. ex. les capacités de communication des dispositifs d'impression multifonction doivent être désactivées<sup>22</sup>);
- les accès nomades sont possibles mais doivent faire l'objet d'une justification métier et être intégrés à l'analyse des risques conduite dans le cadre de la démarche d'homologation. Si le service de nomadisme est autorisé, sa mise en œuvre technique et organisationnelle doit être conforme aux mesures de sécurité de l'II 901 (voir la section 6.4 relative au nomadisme numérique);
- le SI sensible doit faire l'objet d'une supervision de sécurité permanente, permettant notamment de détecter des canaux de communication susceptibles d'exfiltrer des données via le réseau (ces canaux peuvent être créés à l'insu de l'utilisateur dans le cas d'une attaque ou par une action délibérément déviante de l'utilisateur). Cette supervision de sécurité constante du SI sensible doit être conforme aux mesures de sécurité de l'II 901 (voir la section 7.5 relative à la journalisation et à la supervision de sécurité).

---

22. Se reporter à la mesure II 901 EXP-IMP-2.



## 4.2 Interconnexion d'un SI sensible avec un second SI sensible

Les interconnexions de deux SI sensibles (classe 1 ou classe 2) sont possibles, y compris au travers de réseaux qui ne sont pas de confiance (classe 0). Elles doivent toutefois satisfaire certains prérequis.

Toute interconnexion de SI sensibles doit être homologuée avant sa mise en production et faire l'objet d'une homologation distincte de celle des SI<sup>23</sup>. Si les deux SI sensibles à interconnecter ne sont pas placés sous l'autorité de la même entité juridique, les deux parties doivent commencer par définir une stratégie d'homologation commune et préciser leurs périmètres de responsabilité respectifs<sup>24</sup>.

Dans le cadre de cette homologation, une analyse des risques doit conduire les deux entités à déterminer les fonctions de sécurité qui seront portées par la passerelle d'interconnexion et à préciser les flux autorisés à la traverser.

Lors de l'instruction du dossier d'homologation, chaque entité doit être attentive à la qualité du dossier d'homologation du SI sensible de l'autre partie, et, en particulier, aux points suivants :

- la typologie d'architecture de SI mise en œuvre par l'autre partie car, comme expliqué au chapitre 3, toutes les architectures de SI sensibles ne sont pas équivalentes du point de vue de leur sécurité ;
- pour l'interconnexion de SI DR, le strict respect des spécificités techniques obligatoires (en particulier les recommandations de ce guide portant sur l'usage de moyens de chiffrement agréés DR) ;
- la liste des risques résiduels identifiés à l'issue de la démarche d'homologation du SI de l'entité.

R8

### Définir une stratégie d'homologation pour chaque interconnexion de SI sensible

L'interconnexion de deux SI sensibles doit faire l'objet d'une homologation spécifique où chacune des parties s'assure que l'impact sur la sécurité de l'interconnexion est compatible avec les besoins de sécurité exprimés dans le dossier d'homologation du SI dont elle a la responsabilité.

Les interconnexions entre SI sensibles doivent mettre en œuvre des équipements de chiffrement, placés en coupure de tous les flux et agréés par l'ANSSI (s'agissant de la protection d'informations DR) ou disposant d'un visa de sécurité<sup>25</sup> (s'agissant de la protection d'informations sensibles). Si le protocole IPsec est utilisé, les équipements de chiffrement doivent être configurés suivant les recommandations de l'ANSSI [17].

23. Se reporter à l'II 901, annexe 2.

24. La stratégie d'homologation correspond aux étapes 1 à 4 de la démarche d'homologation en 9 étapes qui est décrite dans le guide ANSSI relatif à l'homologation de sécurité [16].

25. Se reporter à l'annexe C pour plus d'informations concernant les visas de sécurité et les agréments de sécurité.

**R9**

## ⚖️ Sécuriser les interconnexions de SI DR

Les interconnexions de SI DR doivent être sécurisées au moyen de tunnels VPN garantissant la protection de tous les flux échangés (confidentialité, intégrité, anti-rejeu, authentification mutuelle des extrémités). Les équipements permettant d'établir ces tunnels VPN doivent être agréés par l'ANSSI.

**R10**

## ⚖️ Sécuriser les interconnexions de SI sensibles

Il est fortement recommandé que les interconnexions de SI sensibles soient sécurisées au moyen de tunnels VPN garantissant la protection de tous les flux échangés (confidentialité, intégrité, anti-rejeu, authentification mutuelle des extrémités). Il est également recommandé que les équipements permettant d'établir ces tunnels VPN disposent d'un visa de sécurité ANSSI.

*i*

## Information

Dans le cas particulier où les deux SI sensibles sont physiquement colocalisés<sup>26</sup>, si les résultats de l'analyse des risques démontrent que le risque de compromission des données transmises via l'interconnexion est acceptable compte tenu des mesures techniques et organisationnelles mises en place, il est envisageable de ne pas chiffrer l'interconnexion des deux SI sensibles<sup>27</sup>.

Dans le cas d'une interconnexion de deux SI sensibles, placés sous la responsabilité de deux entités juridiques distinctes, il est également recommandé que chacune des parties mette en œuvre des équipements de filtrage qualifiés, en limite de son périmètre de responsabilité propre.

La figure 9 précise le positionnement des fonctions de filtrage et de chiffrement d'une interconnexion de SI sensibles.

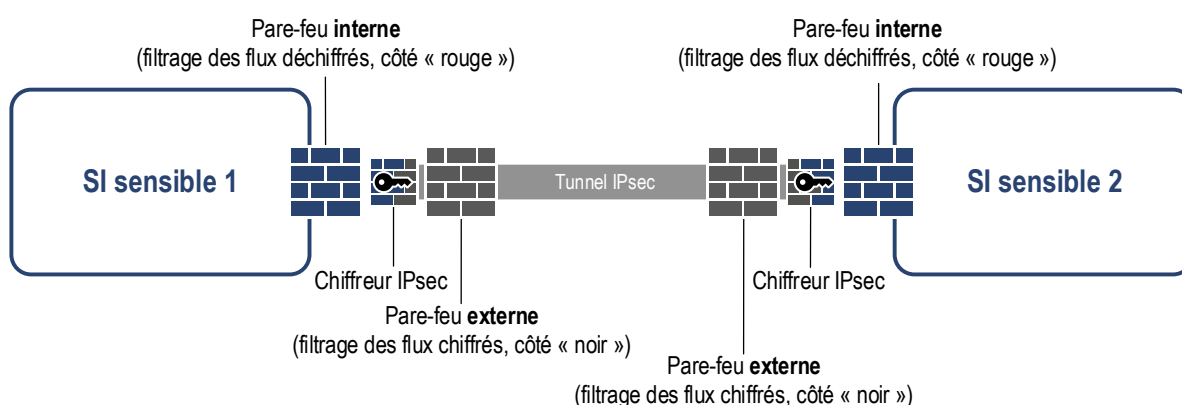


FIGURE 9 – Architecture d'une interconnexion de SI sensibles

26. Le terme « colocalisé » signifie que les deux SI ont des emprises physiques contiguës. À titre d'exemple, il peut s'agir de deux entités juridiques distinctes situées au même étage d'un immeuble et dont les locaux sont adjacents.

27. Se reporter à la mesure de sécurité II 901 RES-INTERCOGEO.

Il est recommandé de filtrer les flux en amont du chiffreur (au moyen des pare-feux externes représentés sur la figure 9) mais également en aval (au moyen des pare-feux internes). Le but du filtrage côté noir<sup>28</sup> (pare-feu externe) est de protéger le chiffreur sur son côté noir en réduisant son exposition et de prévenir toute fuite d'information qui serait consécutive à une erreur de configuration du chiffreur. Le but du filtrage côté rouge est de donner au responsable du SI sensible, le contrôle des flux « hors tunnel » entrants ou sortants de ce SI. En particulier, si les deux SI sensibles sont de classe 1, il est recommandé que chaque entité bloque les accès à des SI de classe 0 au travers de l'interconnexion, de manière à ne pas reposer sur un filtrage qu'elle ne maîtrise pas, car réalisé par l'autre entité.

R11

### Filtrer les flux des interconnexions de SI sensibles

Il est recommandé que deux entités juridiques souhaitant interconnecter leurs SI sensibles mettent chacune en œuvre, sous leur contrôle respectif, des dispositifs de filtrage, en amont et en aval des chiffreurs. Il est recommandé que ces dispositifs soient qualifiés.



### Information

La fonction de filtrage assurée par le pare-feu côté noir et la fonction de chiffrement peuvent être mutualisées, sous réserve que l'équipement unique assurant ces deux fonctions soit adapté à la protection d'informations sensibles<sup>29</sup> et que le filtrage soit configuré pour prévenir tout risque de fuite de données<sup>30</sup>.

## 4.3 Interconnexion d'un SI sensible de classe 1 avec un SI de classe 0

Atteindre un bon niveau de sécurisation des passerelles d'accès à Internet est difficile. Non seulement la conception et la mise en œuvre initiales doivent être à l'état de l'art, mais il faut ensuite maintenir dans la durée un niveau élevé de sécurité. L'ANSSI a publié le guide [23] qui liste des mesures de sécurité visant à sécuriser une interconnexion au réseau Internet. Son application est particulièrement recommandée dans le cas des SI sensibles.

R12

### Appliquer les recommandations de l'ANSSI relatives à l'interconnexion d'un SI à Internet

Il est fortement recommandé que l'interconnexion d'un SI sensible de classe 1 avec Internet respecte au minimum les bonnes pratiques de l'ANSSI, en particulier celles listées dans le guide relatif aux architectures d'interconnexion à Internet [23].

28. Le côté noir est celui des flux encapsulés et chiffrés du tunnel créé par le chiffreur, par opposition au côté rouge où les flux sont « hors tunnel ».

29. En pratique, il s'agit de vérifier que les deux fonctions sont bien agréées (cas des SI DR) ou qualifiées (cas des SI sensibles) et que leur utilisation concomitante sur un même équipement est bien autorisée dans les conditions d'emploi attachées à l'agrément ou à la qualification.

30. Par exemple, si l'équipement unique est un pare-feu Stormshield SNS, le lecteur est invité à se reporter au chapitre 7 du guide [5] relatif à la configuration des VPN IPsec.

L'interconnexion d'un SI sensible de classe 1 avec un SI de classe 0 suppose la mise en œuvre d'une *passerelle de classe 1* telle que définie à la section 3.2.2.

### 4.3.1 Nature des dispositifs de sécurité de la passerelle de classe 1

La définition d'une passerelle de classe 1 (voir la section 3.1.2) implique la mise en œuvre, sous la maîtrise de l'entité responsable du SI sensible à interconnecter<sup>31</sup>, de plusieurs dispositifs de sécurité. Ces dispositifs font l'objet de recommandations publiées dans le guide [23], qui porte sur l'interconnexion d'un SI à Internet. Cette section a pour but d'apporter des compléments d'informations s'agissant de leur mise en œuvre dans le cas d'un SI sensible de classe 1.

#### Pare-feux qualifiés

Pour l'interconnexion d'un SI sensible avec un SI de classe 0, il est nécessaire de mettre en œuvre une zone démilitarisée (DMZ<sup>32</sup>) encadrée par deux pare-feux, dont l'un, au moins, est qualifié au niveau standard. L'un des pare-feux, dit « pare-feu externe », est connecté au SI de classe 0 ; l'autre, dit « pare-feu interne », est connecté au SI sensible (se reporter à la section 3.2.2). Pour plus d'informations concernant les pare-feux dans les zones exposées à Internet, en particulier leur positionnement et leur diversification technologique, l'ANSSI a publié le guide [21]. Sa section 4.2 traite plus particulièrement du cas d'une passerelle Internet sécurisée assurant la protection d'un SI DR.

R13

#### **Passerelle de classe 1 : mettre en œuvre au moins un pare-feu qualifié**

L'entité responsable d'un SI DR doit mettre en œuvre un dispositif de filtrage qualifié au niveau standard en coupure de tous les flux depuis et vers le SI de classe 0. Il est fortement conseillé d'appliquer cette recommandation aux SI sensibles.

#### Dispositif de rupture des flux

La rupture protocolaire consiste à interrompre une session qui a été établie, au moyen d'un protocole de communication, entre deux parties. Elle peut être effectuée avec ou sans changement de protocole.

Les dispositifs de rupture protocolaire peuvent être de natures extrêmement diverses. Suivant le contexte, il peut s'agir d'un serveur de partage de fichiers, d'une passerelle d'échange inter-applications, d'un serveur mandataire...

Des dispositifs de rupture des flux en provenance ou à destination des SI de classe 0 doivent être mis en œuvre. Ces relais doivent être positionnés dans la DMZ, entre les deux pare-feux mentionnés au paragraphe précédent.

En aucun cas des flux sortants ne doivent être initiés depuis le SI sensible vers des SI de moindre niveau de sensibilité sans transiter par un serveur relais. En effet, des flux directs de ce type, parce qu'ils échappent à la politique de journalisation mise en œuvre au niveau des serveurs relais,

31. Se reporter à la mesure de sécurité II 901 RES-INTERCO.

32. *Demilitarized zone*, en anglais.

peuvent être mis à profit par un attaquant ayant compromis une ressource d'un SI sensible pour établir des communications furtives sortantes. De tels canaux peuvent être utilisés pour exfiltrer des données, télécharger des outils d'attaque...

Une analyse des risques spécifique doit être réalisée pour déterminer la nature des dispositifs de rupture de flux à mettre en œuvre et identifier les fonctions de sécurité recherchées, dans le contexte d'usage de l'entité : filtrage d'accès aux ressources, analyse protocolaire, détection de fuites de données, imputabilité des actions, journalisation... Au minimum, pour les flux incluant des fichiers, une fonction de détection des codes malveillants est mise en œuvre.



### Attention

La rupture protocolaire s'applique également à des flux sécurisés. L'inspection de flux sécurisés (p. ex. TLS) a pour effet d'augmenter le risque d'atteinte à la confidentialité des échanges, le flux étant déchiffré puis rechiffré lors de l'inspection. Les équipements mettant en œuvre ces inspections doivent par conséquent être sélectionnés avec une grande attention et la configuration des paramètres cryptographiques doit être faite de telle sorte que le niveau de protection du flux avant inspection ne soit pas dégradé par l'équipement d'inspection<sup>33</sup>. Une attention doit également être portée à la partie organisationnelle, des personnes tierces ayant potentiellement accès au flux clair lors de l'inspection alors qu'elles n'y auraient pas eu accès en absence d'inspection (p. ex. administrateur de l'équipement d'inspection, gestion des supports physiques de l'équipement en cas de maintenance...).

R14

### Passerelle de classe 1 : mettre en œuvre au moins un dispositif de rupture de flux

L'entité responsable d'un SI DR doit mettre en œuvre un ou plusieurs dispositifs de rupture des flux depuis et vers le SI de classe 0, si possible qualifiés. Ces dispositifs doivent être positionnés entre deux dispositifs de filtrage.

Il est conseillé d'appliquer cette recommandation aux SI sensibles.

## Système de détection qualifié

Pour améliorer la détection des attaques informatiques, le déploiement d'un système de détection (incluant une sonde) au niveau de toute passerelle de classe 1 est obligatoire. L'efficacité de ces équipements tient en grande partie à la qualité des indicateurs de compromission<sup>34</sup> qu'ils utilisent.

R15

### Passerelle de classe 1 : mettre en œuvre un système de détection

L'entité responsable d'un SI DR doit mettre en œuvre un système de détection, incluant une sonde qualifiée, au sein de chacune des *passerelles de classe 1* de manière à contrôler l'ensemble des flux entrants et sortants du SI DR.

33. Pour plus d'informations concernant l'inspection TLS, se reporter au paragraphe 4.3 du guide [23] dans sa version 3 de juin 2020.

34. Les indicateurs de compromission ou marqueurs techniques désignent l'ensemble des méta-données permettant de caractériser techniquement des attaques informatiques passées. Il peut s'agir d'adresses IP ou de noms de domaines DNS de serveurs malveillants, d'adresse Web de sites piégés, d'empreintes de fichiers... La supervision et le déclenchement d'alertes lors de la détection de ces IOC (*Indicators of compromise*) permet de réagir au plus tôt à une potentielle attaque.

Il est conseillé d'appliquer cette recommandation aux SI sensibles. Au minimum, un système de détection doit être mis en place sur les SI sensibles, même s'il n'est pas qualifié.

Il est essentiel que la fonctionnalité de capture du trafic réseau ne puisse pas être détournée pour compromettre le SI. Pour réduire ce risque de détournement, il est conseillé de connecter la sonde de détection aux points d'écoute du réseau à l'aide d'équipements spécifiques (*tap*). Il est en outre recommandé que ces équipements soient totalement passifs, non administrables à distance et qualifiés par l'ANSSI. La capture du trafic réseau par recopie de flux au niveau des commutateurs réseau<sup>35</sup> est déconseillée.

R16

### Passerelle de classe 1 : mettre en œuvre des taps qualifiés passifs

Il est recommandé que l'entité responsable d'un SI DR mette en œuvre des *taps* passifs pour alimenter en flux réseau la ou les sondes de détection. Il est recommandé que ces équipements soient qualifiés par l'ANSSI.

Pour plus d'informations concernant la détection des incidents de sécurité, se reporter à la section 7.5.

## 4.3.2 Positionnement des dispositifs de sécurité de la passerelle de classe 1

Cette section a pour but de détailler le positionnement des dispositifs de sécurité, décrits à la section précédente, les uns par rapport aux autres, en fonction des différentes architectures décrites à la section 3.2.2.

Les figures 10 et 11 reprennent les deux exemples d'architecture de SI sensible de classe 1 présentés à la section 3.2, à savoir le « SI sensible physiquement cloisonné » et le « SI sensible sans SI usuel ». Ces figures précisent les exigences réglementaires concernant la nature des certifications, qualifications ou agrément de sécurité des principaux dispositifs de sécurité (pare-feux, serveurs mandataires et sondes) énumérés à la section précédente. Elles donnent en outre des recommandations concernant la diversification technologique des pare-feux.

35. Fonctionnalité dite de « miroir de port » ou *port mirroring* en anglais.

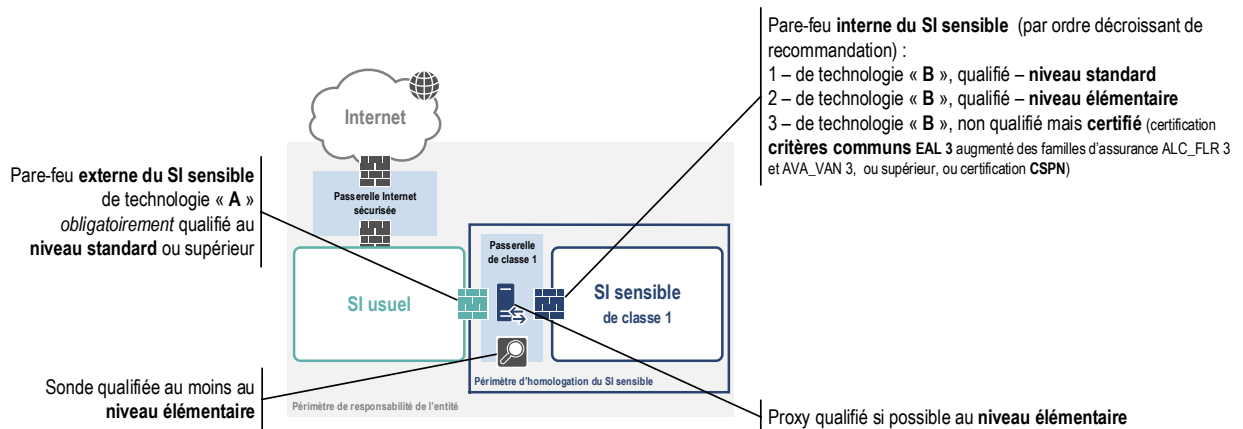


FIGURE 10 – SI sensible de classe 1 - Exemple d'architecture d'un SI physiquement cloisonné : positionnement des dispositifs de sécurité

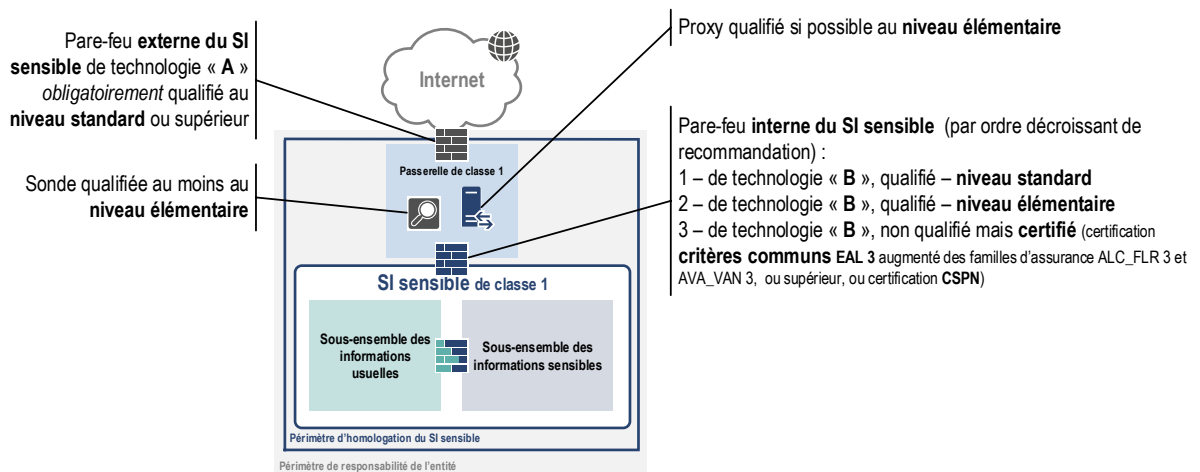


FIGURE 11 – SI sensible de classe 1 - Exemple d'architecture avec cloisonnement logique des informations sensibles et usuelles : positionnement des dispositifs de sécurité

R17

## Passerelle de classe 1 : faire porter les fonctions de sécurité par des dispositifs distincts

Il est recommandé que les fonctions de sécurité des pare-feux, des dispositifs de rupture de flux et des sondes de la passerelle de classe 1 soient portées par des matériels physiquement distincts.

### 4.3.3 Navigation Web

La navigation Web représente une source de menace importante pour la compromission d'un SI. L'approche la plus sécurisée consiste à interdire ce service depuis les SI sensibles<sup>36</sup> et à mettre en

36. Par définition des SI sensibles de classe 2, la navigation Web est impossible depuis ce type de SI.

place une infrastructure dédiée, depuis des postes physiquement distincts<sup>37</sup>.

R18

## Interdire la navigation Web depuis les SI sensibles

La navigation Web est impossible depuis les SI sensibles de classe 2. Pour les SI sensibles de classe 1, il est recommandé d'interdire l'accès au service de navigation Web. Si le service de navigation est nécessaire, il doit être mis à disposition des utilisateurs depuis un SI dédié à cet usage.

Si des impératifs métier amènent à autoriser la navigation Web depuis des SI sensibles de classe 1, il est possible de déployer des postes de rebond dont la configuration a été durcie<sup>38</sup>. Pour plus de sécurité, il est en outre recommandé que ces postes de rebond soient non persistants et réinitialisés régulièrement voire à chaque nouvelle utilisation du service de navigation Web. La figure 12 donne la représentation d'architectures de navigation Web mettant en œuvre des postes de rebond.

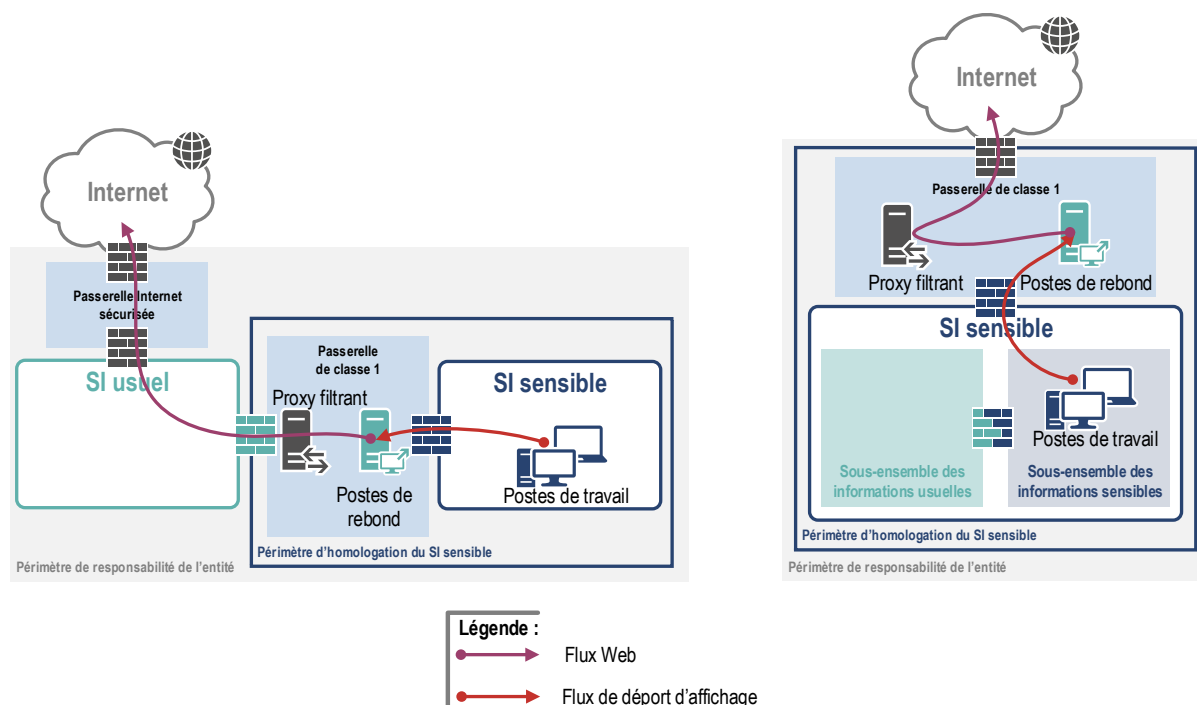


FIGURE 12 – Navigation Web : exemples d'architectures pour un SI de classe 1, avec postes de rebond (à gauche : cas d'une architecture physiquement cloisonnée ; à droite : cas d'une architecture avec cloisonnement logique des informations sensibles et usuelles)

R18 -

## Permettre la navigation Web depuis des postes de rebond

Pour les SI sensibles de classe 1, il est fortement recommandé de déployer une infrastructure de postes de rebond dédiés à la navigation Web. Cette infrastructure est cloisonnée du SI sensible. Les utilisateurs se connectent par accès à distance depuis leurs postes de travail sensibles à cette infrastructure. Seuls ces postes de rebond permettent la navigation Web depuis le SI sensible et les autorisations d'accès au

37. Se reporter à la mesure de sécurité II 901 RES-INTERNET-SPECIFIQUE.

38. Se reporter à la section 4.5 et à la recommandation R27+ du guide [23].



service sont limitées au strict besoin opérationnel.

Une recommandation alternative à la recommandation R18- consiste à faire transiter les flux Web entre les postes de travail sensibles et les serveurs Web au travers de serveurs mandataires (*proxy*) maîtrisés par le responsable du SI sensible. En comparaison de la recommandation R18-, cette solution est plus risquée. En effet, dans cette architecture, le poste de travail utilisé pour la navigation est directement connecté au SI sensible : si le poste de travail est compromis, l'attaque n'est pas contenue et c'est l'ensemble du SI sensible qui est susceptible d'être compromis. La figure 13 donne la représentation d'architectures de navigation Web mettant en œuvre des serveurs mandataires.

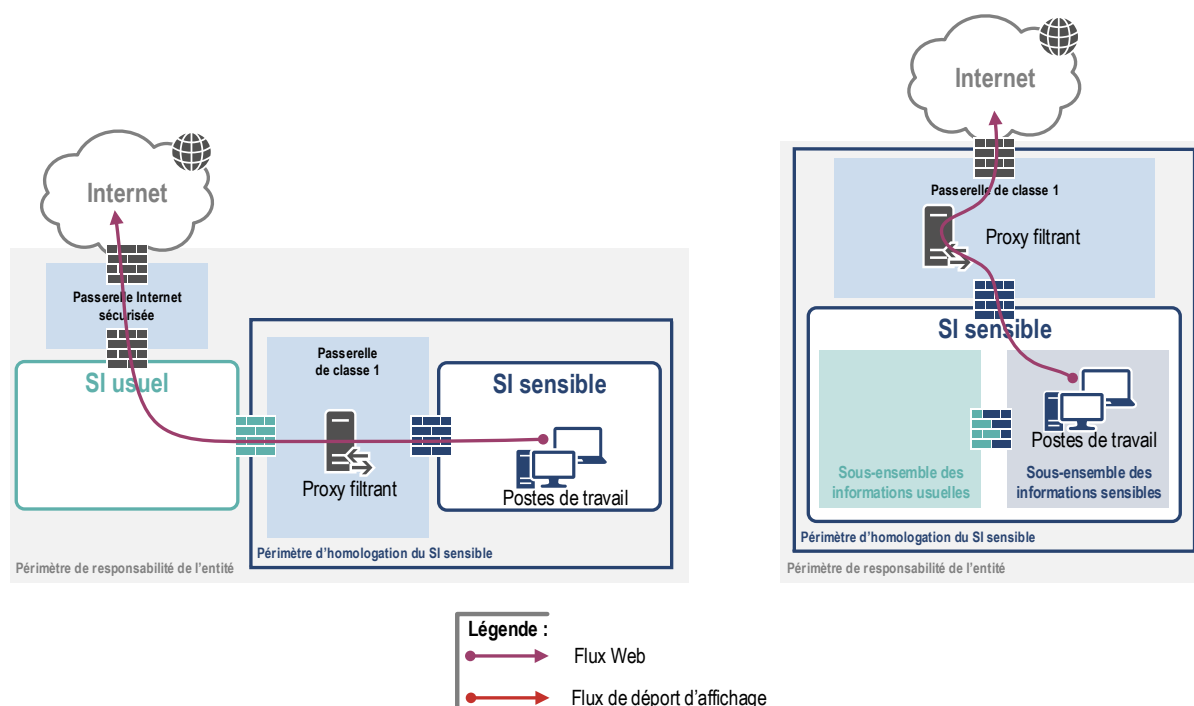


FIGURE 13 – Navigation Web : exemple d'architecture d'un SI de classe 1, sans postes de rebond (à gauche : cas d'une architecture physiquement cloisonnée; à droite : cas d'une architecture avec cloisonnement logique des informations sensibles et usuelles)

R18 --

## Permettre la navigation Web sans postes de rebond

Pour les SI sensibles de classe 1, si le déploiement d'une infrastructure de postes de rebond dédiés à la navigation Web n'est pas possible, l'accès à Internet peut être autorisé depuis les postes de travail sensibles au moyen de serveurs mandataires cloisonnés du SI sensible. Cette solution n'est pas optimale d'un point de vue sécurité et il est fortement recommandé de la mettre en œuvre avec des serveurs mandataires qualifiés (se reporter à la recommandation R14). Les autorisations d'accès au service de navigation sont limitées au strict besoin opérationnel.

## 4.3.4 Transfert via Internet de documents sensibles chiffrés

Des fichiers sensibles ayant vocation à être rendus accessibles depuis Internet et donc à transiter par un réseau qui n'est pas de confiance doivent être chiffrés au moyen de solutions disposant d'un agrément de sécurité (informations DR) ou disposant d'un visa de sécurité<sup>39</sup> ANSSI (informations sensibles).

R19

### Chiffrer les informations DR transférées via des SI de classe 0

Les informations DR échangées entre deux SI DR au travers d'un SI de classe 0 doivent être chiffrées au moyen de produits de sécurité agréés DR.

R20

### Chiffrer les informations sensibles transférées via des SI de classe 0

Les informations sensibles échangées entre deux SI sensibles au travers d'un SI de classe 0 doivent être chiffrées. Il est recommandé pour ce faire d'utiliser un produit disposant d'un visa de sécurité.



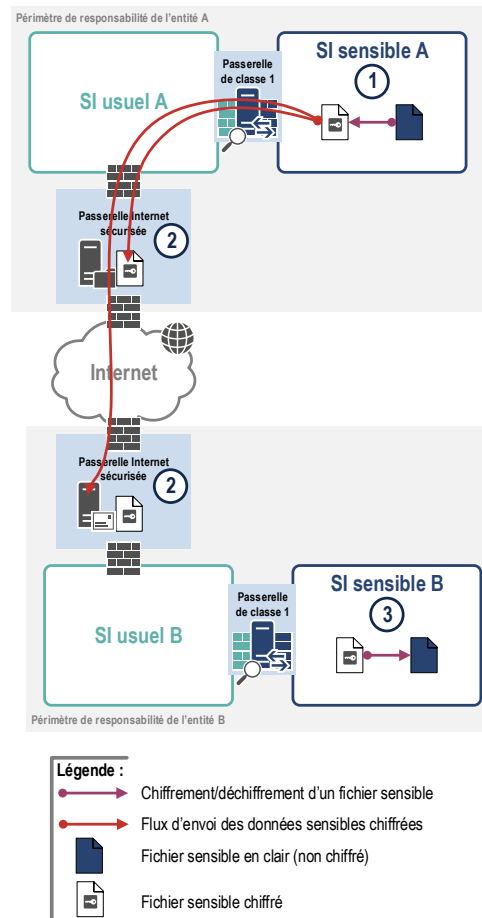
### Attention

Dans le contexte des recommandations R19 et R20, les informations sensibles transférées sur un SI de classe 0 doivent impérativement être chiffrées et déchiffrées sur un SI sensible.

Conformément aux recommandations du guide ANSSI relatif à l'interconnexion d'un SI à Internet [23], si des ressources de la passerelle Internet sécurisée doivent être mises à disposition de clients connectés à Internet, elles doivent être hébergées dans une zone dédiée (appelée *zone de services exposés*). Les informations sensibles, chiffrées au moyen de l'outil *ad hoc*, peuvent donc être publiées sur Internet dans cette zone.

La figure 14 illustre une architecture de partage de fichiers sensibles conforme à la réglementation. Les informations à partager sont chiffrées à l'aide d'un outil *ad hoc* sur le SI sensible de l'entité. Elles sont ensuite transférées vers le destinataire (p. ex. transfert par courrier électronique) ou mises à disposition de cette entité tierce sur un serveur accessible depuis Internet. Les fichiers chiffrés doivent être transférés sur un SI homologué sensible avant de pouvoir être déchiffrés.

39. Se reporter à l'annexe C pour plus d'informations concernant les visas de sécurité.



- ① Sur le SI sensible « émetteur » (SI sensible A), les fichiers DR sont chiffrés à l'aide d'un outil agréé DR (ou les fichiers sensibles sont chiffrés à l'aide d'un outil disposant d'un visa de sécurité);
- ② Les fichiers sensibles, chiffrés à l'étape 1, sont mis à disposition dans la *zone de services exposés* pour les destinataires sur Internet ou leur sont transférés (par courrier électronique par exemple);
- ③ Les fichiers sensibles sont réceptionnés ou téléchargés par les destinataires soit sur un SI usuel (puis transférés sur un SI sensible homologué), soit directement depuis le SI sensible destinataire (SI sensible B). Dans les deux cas, le déchiffrement des fichiers est fait exclusivement sur un SI sensible homologué.

FIGURE 14 – SI sensible de classe 1 - Exemple d'architecture de partage de fichiers avec une entité tierce

### 4.3.5 Accès via Internet à des informations issues d'une application sensible

Dans ce cas, les données sensibles ne se présentent pas sous forme de fichiers mais sont stockées dans une base de données.

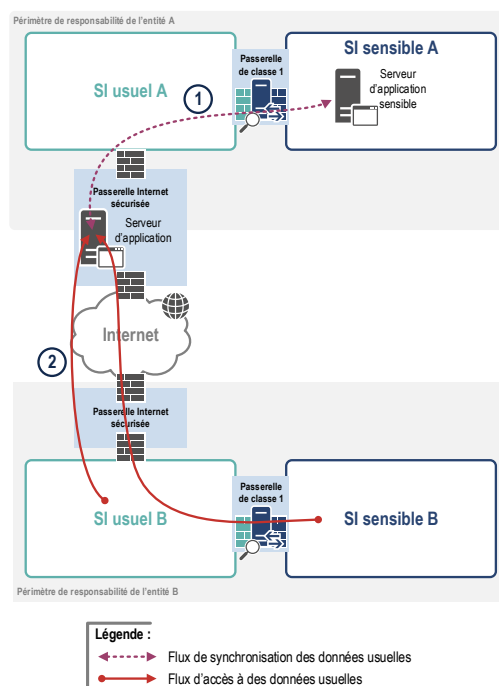
## ⚖️ Interdire l'accès aux applications sensibles depuis les SI non homologués

L'accès à toute application sensible (ou DR) depuis un SI non homologué au niveau sensible (respectivement depuis un SI non homologué au niveau DR) est interdit.

Si l'entité tierce dispose bien d'un SI sensible homologué au bon niveau (sensible ou DR), il est nécessaire de bien définir le besoin réel : le besoin est-il de partager avec l'entité tierce uniquement des informations non sensibles ou bien de partager des informations, dont certaines sont sensibles ?

### Architecture avec réplication des informations non sensibles

Si le besoin est de partager avec l'entité tierce uniquement des informations non sensibles, il convient d'étudier la faisabilité technique de diviser l'application en deux instances : l'une, expurgée de toute information sensible est hébergée sur le SI usuel et est exposée sur Internet ; l'autre, qui contient l'ensemble des informations (sensibles et non sensibles) est hébergée sur le SI sensible sans être exposée sur Internet. Dans cette architecture, un système d'échanges sécurisés est mis en place entre le SI usuel et le SI sensible (voir la section 4.4 pour plus d'informations). La figure 15 donne une représentation de cette architecture.



- ① Sur le SI sensible « émetteur » (SI sensible A), un mécanisme permet la synchronisation des seules données usuelles entre un serveur hébergé sur le SI sensible et un serveur placé dans la zone de services exposés ;
- ② Des clients accèdent depuis des SI usuels ou depuis des SI sensibles aux données ainsi exposées.

FIGURE 15 – SI sensible de classe 1 - Exemple d'architecture de partage d'une application avec une entité tierce



## Information

Cette architecture doit être adaptée aux besoins de protection en intégrité et disponibilité des données exposées.

### Architecture sans réplication des informations

Si la division de l'application en deux instances est impossible ou que le besoin fonctionnel est de donner accès à l'entité tierce à des données sensibles stockées dans la base de données, une interconnexion du SI sensible avec le SI sensible de l'entité tierce doit être envisagée. Cela revient à créer une interconnexion de SI sensibles (voir la section 4.2 pour plus d'informations).

Dans cette architecture, il convient de protéger le service applicatif, qui est nécessairement hébergé sur le SI sensible, en ne l'exposant pas directement sur Internet. Il s'agit, soit d'établir une interconnexion de réseaux sensibles « point à point », telle que décrite à la section 4.2, soit de fournir aux utilisateurs distants des moyens d'accès nomades s'appuyant sur des VPN (se reporter à la section 6.4). Dans les deux cas, le point de terminaison VPN est placé au sein de la *passerelle de classe 1*.

De même, l'hébergement du serveur applicatif sensible doit être cloisonné logiquement des autres ressources du SI sensible, qui n'ont pas vocation à être rendues accessibles depuis Internet. Il doit être placé au sein d'une *passerelle de classe 1*.

R22

### Cloisonner l'infrastructure de mise à disposition sur Internet d'informations sensibles

L'infrastructure de mise à disposition d'informations sensibles, accessibles depuis Internet, doit être cloisonnée dans une DMZ, au sein d'une *passerelle de classe 1*. Elle est accessible soit depuis un autre SI sensible via une interconnexion « point à point » telle que décrite à la section 4.2, soit depuis un équipement d'accès nomade attaché au SI sensible.

## 4.4 Échanges sécurisés pour les utilisateurs

Les différentes architectures présentées à la section 3.2 prévoient toutes un cloisonnement (physique ou logique) des ressources sensibles (dans une « zone » sensible) et usuelles (dans une « zone » usuelle). Toutefois, il est vraisemblable que les utilisateurs aient besoin d'échanger des informations entre ces différentes zones.

De manière générale, lorsque le SI sensible est étendu ou lorsque les flux d'échange entre les zones sensibles et les zones usuelles sont importants, il est recommandé de réaliser les échanges de données au travers du réseau et à l'aide de systèmes d'échanges *ad hoc*. Cette section a pour objectif d'apporter des recommandations propres à ces systèmes d'échanges sécurisés à la disposition des utilisateurs.



## Information

Il est préférable de ne pas réaliser ces échanges de données au moyen de supports amovibles. En effet, la multiplication des supports augmente les risques d'atteinte en confidentialité des données qui y sont stockées (voir la section 5.7 pour plus d'informations concernant les supports amovibles). Quand l'utilisation de supports amovibles est quasiment incontournable (notamment pour les SI sensibles de petite taille ou pour les « flux descendants » des SI de classe 2), des mesures techniques et organisationnelles encadrent les échanges de données et permettent notamment d'en assurer la traçabilité.

### 4.4.1 Cas des SI de classe 2

Pour l'architecture dite « SI sensible physiquement isolé » (voir la section 3.2.1), la réglementation prévoit que des flux issus d'un SI usuel puissent entrer dans le SI sensible (notion de « flux montants »). De manière à assurer un niveau de sécurité optimal, cette interconnexion de SI doit obligatoirement être sécurisée à l'aide de dispositifs agréés, garantissant le caractère strictement unidirectionnel des flux de données. Le plus souvent, ils comportent une diode optique et des systèmes spécifiques, lesquels ont pour fonction de transférer des données du niveau dit « bas » vers le niveau dit « haut », au moyen de protocoles ne nécessitant pas d'acquittements de transmission.

Les interconnexions « descendantes »<sup>40</sup>, via le réseau, sont également prévues par la réglementation (voir la définition d'un SI de classe 2 rappelée à la section 3.1.2). Toutefois, la complexité de leur mise en œuvre les rend hors de portée des entités ne présentant pas un très haut niveau de maîtrise de la sécurité des systèmes d'information. Dans ce cas particulier, une utilisation strictement encadrée de supports amovibles est préférable à une interconnexion descendante fragile, qui n'implémenterait pas les fonctions de sécurité permettant, notamment, de gérer les risques de canaux cachés dans les flux descendants.

R23

## Maîtriser les interconnexions descendantes des SI de classe 2

Dans un SI de classe 2, il est recommandé de préférer une interconnexion « descendante » mettant en œuvre des supports amovibles plutôt qu'une interconnexion via le réseau. Les conditions d'emploi de ces supports amovibles doivent être strictement définies.

### 4.4.2 Cas des SI de classe 1

Dans l'architecture dite « SI sensible physiquement cloisonné » (voir la section 3.2.2), mais aussi dans le cas de l'architecture « SI sensible sans SI usuel » (voir la section 3.2.3), il est recommandé d'installer un *système d'échanges sécurisés* respectant les principes détaillés dans cette section.

Dans la mesure du possible, les flux doivent être autorisés de la façon suivante :

- depuis un poste sensible (client) vers le système d'échanges sécurisés (serveur);
- depuis un poste usuel (client) vers le système d'échanges sécurisés (serveur).

40. Il s'agit des interconnexions permettant que des flux issus du SI sensible puissent entrer dans le SI usuel.

La figure 16 précise les sens recommandés d'initialisation des flux dans un système d'échanges sécurisés.

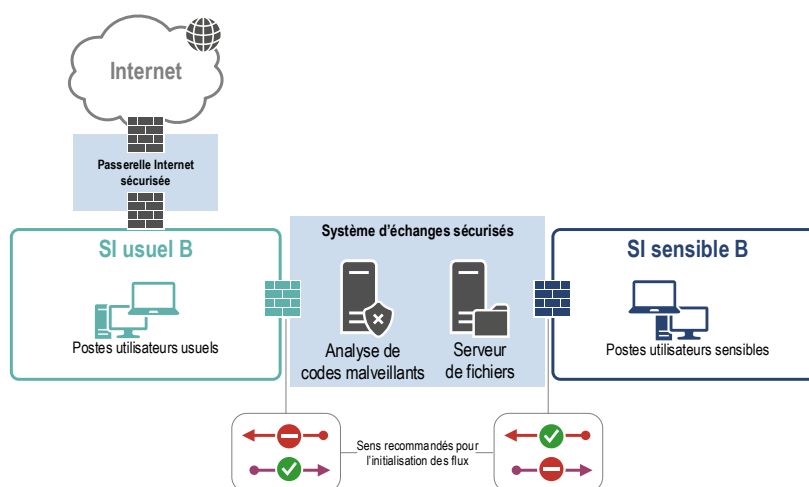


FIGURE 16 – SI sensible de classe 1 - Représentation fonctionnelle d'un système d'échanges sécurisés

Un système d'échanges sécurisés doit, idéalement, autoriser seulement les protocoles de transfert de données. Par exemple, le service SSH doit être configuré pour n'autoriser que les commandes de transferts de fichiers de type SCP (*Secure Copy*) ou SFTP (*SSH File Transfer Protocol*). Les recommandations de l'ANSSI pour la sécurisation du protocole SSH sont applicables [4].

R24

### N'autoriser que des protocoles de transfert vers le système d'échanges sécurisés

Seuls les services et les protocoles permettant le transfert de données vers le système d'échanges sécurisés doivent être autorisés ; les flux doivent toujours être à l'initiative des clients situés en dehors du système d'échanges.

L'accès à un système d'échanges sécurisés depuis le SI usuel doit être strictement réservé aux postes et aux utilisateurs ayant le besoin d'échanger des informations avec le SI sensible. Ces restrictions peuvent être réalisées par la mise en œuvre d'un filtrage réseau ou d'un contrôle d'accès logique au système d'échanges sécurisés.

R25

### Système d'échanges sécurisés : restreindre les accès aux seuls utilisateurs autorisés

Il est recommandé de restreindre l'accès au système d'échanges sécurisés uniquement aux postes et aux utilisateurs qui en ont le besoin.

Afin de ne pas compromettre les secrets d'authentification d'un SI sensible, il est essentiel qu'un utilisateur de ce SI s'authentifie sur le système d'échanges sécurisés avec un compte utilisateur référencé dans un annuaire dédié de la passerelle de classe 1 ou positionné dans le SI usuel et, en aucun cas, avec un compte référencé dans un annuaire du SI sensible.

**R26**

### **Système d'échanges sécurisés : authentifier les utilisateurs avec un compte non sensible**

Les utilisateurs ne doivent pas s'authentifier avec un compte du SI sensible sur le système d'échanges sécurisés, considéré comme de moindre confiance. Si l'authentification de l'utilisateur s'appuie sur un mot de passe, il doit être différent des autres mots de passe utilisés par l'utilisateur sur d'autres SI, y compris le SI sensible. De plus, le mot de passe ne doit pas pouvoir être déduit de la connaissance d'autres mots de passe de l'utilisateur.

Des mécanismes de filtrage de contenu et de protection contre les codes malveillants doivent être systématiquement déployés. Cette mesure vise à protéger les ressources d'un SI sensible des risques de compromission par exécution de code malveillant, qui aurait été véhiculé par des fichiers ou des binaires dont l'origine n'est pas de confiance <sup>41</sup>.

**R27**

### **Système d'échanges sécurisés : analyser le contenu des données échangées**

Toutes les données transitant par le système d'échanges sécurisés doivent être soumises systématiquement à une analyse de contenu pour la recherche de codes malveillants.

Enfin, tout échange de données doit être journalisé et imputé à un utilisateur. L'exploitation de ces journaux doit être intégrée à la stratégie de journalisation et de supervision de la sécurité (voir la section 7.5).

**R28**

### **Système d'échanges sécurisés : journaliser et imputer les données échangées**

Toutes les données transitant par le système d'échanges sécurisés doivent être tracées et imputables à un utilisateur identifié.

---

41. Voir aussi la section 5.6 pour plus d'informations concernant la protection contre les codes malveillants.



# 5

## Sécurisation au sein des SI sensibles



### Objectif

Le principe de défense en profondeur consiste à faire reposer la protection d'une information sur des mesures complémentaires pouvant se compenser mutuellement en cas de défaillance de l'une d'entre elles. Ce chapitre énonce quelques bonnes pratiques traduisant la déclinaison de ce principe au cas des SI sensibles, dans le but principal d'assurer l'accès aux informations sensibles sur la base du *besoin d'en connaître* et dans le but secondaire de préserver l'intégrité du SI et des informations.

### 5.1 Produits et prestataires de service de confiance

Le principe de défense en profondeur est un concept général qui se traduit par l'application de mesures de sécurité globales, mais également par l'utilisation de briques de confiance que sont les produits qualifiés et certifiés. Le responsable d'un SI est dans ce cas dispensé de devoir supporter la charge de leur évaluation dans le cadre de la démarche d'homologation.

De même, utiliser des prestataires de services de confiance peut permettre de soutenir voire de compenser le manque de compétences internes de l'entité responsable d'un SI sensible.

En pratique, les produits et les prestataires de service de confiance sont ceux pour lesquels l'ANSSI a délivré une qualification de sécurité et, dans une moindre mesure, ceux pour lesquels l'ANSSI a délivré une certification. Ces solutions éprouvées et approuvées par l'ANSSI (produits et prestataires de service) sont regroupées sous une bannière unique : les visas de sécurité. Pour le responsable d'un SI sensible, l'intérêt principal de ces visas est de repérer facilement les produits et prestataires de service fiables et adaptés à l'état de la menace, sur le marché de la sécurité informatique. Pour en savoir plus sur les visas de sécurité, et en particulier, sur les différences entre certification, qualification et agrément, se reporter à l'annexe C.

R29

#### Recourir à des prestataires de services SSI disposant d'un visa de sécurité ANSSI

Il est fortement recommandé de recourir à des prestataires de sécurité disposant d'un visa de sécurité ANSSI<sup>42</sup>. Dans le cas où les prestations externalisées concernent des SI DR, le contrat liant le commanditaire au prestataire de services doit garantir l'obligation pour le prestataire de respecter les mesures de sécurité de l'II 901. Il est fortement recommandé que la prestation s'effectue depuis le territoire national<sup>43</sup>.

42. Se reporter à l'article 3 de l'II 901.

43. Se reporter à l'article 16 de l'II 901.



## Attention

Pour l'hébergement de données dans un *cloud* public, l'ANSSI recommande de recourir au service d'un prestataire qualifié *SecNumCloud*. L'hébergement de données sensibles dans un *cloud* public est théoriquement possible sous réserve que le fournisseur de service soit qualifié *SecNumCloud* et qu'il se conforme aux mesures de sécurité de l'II 901 et du présent guide.

### R30

## ⚖️ Acquérir des produits de sécurité disposant d'un visa de sécurité ANSSI

Dès qu'ils existent, les produits de sécurité qualifiés doivent être utilisés<sup>44</sup>. Un produit qualifié par l'ANSSI doit être préféré à un produit certifié. Cette mesure s'applique aussi bien aux produits de sécurisation d'un SI sensible, qu'aux moyens mis en œuvre pour le contrôle d'accès physique aux éléments dont il est constitué<sup>45</sup>. Les qualifications ayant toujours une durée de validité, il appartient au responsable d'un SI de veiller à ce que les qualifications des versions déployées des produits de sécurité soient toujours valides<sup>46</sup>. Enfin, l'usage d'un produit qualifié doit être compatible du périmètre d'évaluation ayant conduit à délivrer la qualification<sup>47</sup>.

Pour la protection d'un SI DR, certains produits de sécurité doivent disposer d'un agrément de sécurité. Cela concerne essentiellement les produits de chiffrement, mais aussi les diodes mises en œuvre dans les passerelles montantes dans le cas des architectures « SI sensible physiquement isolé » (voir la section 3.2.1)<sup>48</sup>.

Une décision d'agrément DR de l'ANSSI, délivrée pour un produit de sécurité, est accompagnée d'un document listant les conditions d'emploi de ce produit. Ces règles d'utilisation rassemblent des mesures organisationnelles ou techniques complémentaires qui ont pour but de traiter des risques identifiés au regard du niveau de sécurité DR visé par l'agrément. Typiquement, pour certains équipements de sécurité agréés par l'ANSSI pour la protection d'informations DR, l'éditeur de la solution n'active pas nécessairement par défaut certains mécanismes techniques permettant d'atteindre un niveau de protection dit « Diffusion Restreinte ». Dès lors que ces équipements sont utilisés dans un contexte DR, ces options techniques doivent être activées par l'administrateur de l'équipement de sécurité.

### R31

## ⚖️ Respecter les conditions d'emploi des équipements de sécurité agréés

Lorsqu'un produit de sécurité agréé DR est mis en œuvre sur un SI DR, les conditions d'emploi accompagnant ce produit doivent être mises en œuvre par le responsable de ce SI. Les preuves de conformité doivent être versées au dossier d'homologation du SI ou de l'interconnexion.

44. Se reporter à l'article 3 de l'II 901 et à la mesure de sécurité II 901 INT-AQ-PSL.

45. Se reporter à la mesure de sécurité II 901 PHY-CI-CTRLACC.

46. À noter que cette remarque s'applique également aux prestataires de service qualifiés.

47. L'utilisation d'un produit qualifié qui est faite en dehors du périmètre défini lors de l'évaluation de sécurité équivaut à utiliser un produit non qualifié. Le périmètre d'évaluation est précisé dans la cible de sécurité du produit qualifié.

48. Se reporter à la mesure de sécurité II 901 INT-AQ-PSL, ainsi qu'aux articles 3, 14, 17 et à l'annexe 2 de l'II 901.

## 5.2 Chiffrement

Le fait de chiffrer une information sensible avec un moyen adapté au niveau de sensibilité permet de la protéger (en confidentialité et en intégrité) et, en fonction des conditions d'emploi qui accompagnent la décision de qualification ou d'agrément, de la stocker, ou de la faire transiter, par des ressources qui ne sont pas nécessairement homologuées au niveau sensible ou DR<sup>49</sup>. De nombreuses illustrations de ce cas d'usage du chiffrement sont détaillées dans ce guide :

- la sécurisation des interconnexions de SI sensibles (voir les recommandations [R9](#) et [R10](#));
- la sécurisation des canaux d'interconnexion nomades (voir les recommandations [R55](#) et [R56](#));
- la protection des données transitant par des SI de classe 0 (voir les recommandations [R19](#) et [R20](#));
- la protection des données stockées sur des supports de données nomades (voir les recommandations [R57](#) et [R58](#)).

De manière générale, l'II 901 impose l'utilisation de moyens de chiffrement *agréés* pour la protection d'informations Diffusion Restreinte dès lors que des informations DR transitent ou sont stockées dans une zone dont la protection physique n'est pas conforme aux exigences de l'II 901<sup>50</sup>.

Un autre cas d'usage du chiffrement est l'application du principe de défense en profondeur. À titre d'illustration, le chiffrement peut être une solution dans certains cas de mutualisation de ressources entre SI de niveaux de sensibilité différents (voir la section [3.2.3](#)). De même, l'II 901 demande qu'un outil de chiffrement soit mis à la disposition des utilisateurs et des administrateurs pour chiffrer les données sensibles stockées sur les postes de travail, les serveurs ou les supports amovibles<sup>51</sup>.



### Attention

L'utilisation du chiffrement a de fortes implications organisationnelles pour l'entité qui le met en œuvre. De nombreuses procédures doivent être créées pour gérer le cycle de vie des secrets cryptographiques : procédures de création et de stockage sécurisés des secrets maîtres, procédures de renouvellement des clés, procédure de séquestre des clés ou encore, procédure de recouvrement des données. L'absence de maîtrise de ces mécanismes peut avoir des conséquences dévastatrices pour l'entité (déni de service, atteinte majeure à la confidentialité des informations par la capacité illégitime d'un utilisateur malveillant à recouvrer toutes les données chiffrées, incapacité à recouvrer des données exigées dans le cadre d'une réquisition judiciaire...).

## 5.3 Cloisonnement interne du SI sensible et durcissement des systèmes

Un SI sensible doit être cloisonné en zones présentant des besoins de sécurité homogènes<sup>52</sup>. Pour atteindre cet objectif, il est nécessaire de segmenter le réseau puis de mettre en place un filtrage

49. Se reporter à la mesure de sécurité II 901 EXP-PROT-INF.

50. Se reporter à l'article 14 de l'II 901.

51. Se reporter à la mesure de sécurité II 901 PDT-CHIFF-SENS.

52. Se reporter aux mesures de sécurité II 901 RES-CLOIS, ARCHI-HEBERG et EXP-CI-FILT.

des flux entre ces différents segments. La segmentation du réseau peut être physique (équipements dédiés) ou logique (VPN, VLAN...).

Les exemples ci-dessous illustrent cette idée :

- un filtrage réseau doit être mis en œuvre entre les postes de travail et les ressources serveurs du centre de données ;
- les serveurs applicatifs peuvent faire l'objet d'un cloisonnement (p. ex. cloisonnement de serveurs affectés à des projets distincts ; cloisonnement des composants serveurs dans une architecture n-tiers).

R32

### Cloisonner le SI sensible en zones ayant des niveaux de sécurité homogènes

Un SI sensible doit être cloisonné en différentes zones de confiance, homogènes du point de vue de leurs besoins de sécurité et de leur exposition. Ce cloisonnement doit faire l'objet d'une segmentation réfléchie du réseau, complétée par un filtrage fin des flux au niveau des pare-feux.

R33

### Éviter l'installation de moyens informatiques sensibles dans les zones ouvertes au public

S'il existe un besoin métier justifiant l'extension du réseau sensible dans une zone ouverte au public, cette extension doit être cloisonnée du reste du SI sensible<sup>53</sup>. De manière générale, le traitement de données sensibles en zone d'accueil du public doit rester ponctuel et exceptionnel et s'accompagner de mesures de protection spécifiques<sup>54</sup>.

Au sein d'une zone ayant des besoins de sécurité homogènes, le responsable d'un SI sensible doit définir une stratégie de blocage des communications entre les différents systèmes de la zone considérée. Par exemple, le blocage des communications, dites « latérales », entre les moyens distribués (postes de travail, moyens d'impression...) est de nature à réduire les risques de propagation d'une attaque, en complexifiant la tâche d'un attaquant cherchant à élever ses privilèges. Dans une approche de défense en profondeur, les mesures techniques, issues de cette stratégie de blocage des flux latéraux, doivent être variées et complémentaires. Elles sont appliquées aussi bien au niveau des réseaux qu'au niveau des systèmes. Pour ce qui relève du réseau, il peut s'agir de mettre en place un mécanisme de micro-segmentation avec filtrage intra-VLAN (p. ex. *Private VLAN*<sup>55</sup>). Pour ce qui relève du système, il peut s'agir d'activer et configurer le pare-feu local sur chaque poste de travail<sup>56</sup>, de manière à bloquer les communications directes entre les systèmes.

Cette stratégie de cloisonnement doit être étendue aux serveurs. Par exemple, pour les services réseaux inutiles qui ne peuvent pas être durcis<sup>57</sup>, les règles de filtrage du pare-feu local doivent

53. Se reporter à la mesure de sécurité II 901 PHY-PUBL.

54. Se reporter à la mesure de sécurité II 901 PHY-SENS.

55. Voir le guide de l'ANSSI portant sur les recommandations pour la sécurisation d'un commutateur de desserte [6].

56. Se reporter à la mesure de sécurité II 901 PDT-NOMAD-PAREFEU.

57. Le durcissement peut consister en la désinstallation du service ou, à défaut, en sa configuration pour être rendu inutilisable.

bloquer toutes les connexions non nécessaires de manière à réduire la surface d'attaque en minimisant l'exposition des services en écoute.

R34

### Bloquer les communications latérales

Afin de limiter les risques de propagation latérale d'une attaque, le responsable d'un SI sensible doit définir et mettre en œuvre une stratégie de blocage des communications latérales. Cette stratégie concerne en premier lieu les moyens distribués mais aussi les serveurs.

L'installation de tout matériel, de tout micrologiciel<sup>58</sup>, ou de tout logiciel (p. ex. systèmes d'exploitation, hyperviseurs, systèmes d'exploitation virtualisés, applications) doit être conditionnée à l'authentification préalable de son origine et à la vérification de son intégrité.

En outre, la configuration des systèmes d'exploitation et autres logiciels, doit être durcie de manière à complexifier la tâche d'un attaquant cherchant à exploiter des vulnérabilités (connues ou non encore révélées).

Il est recommandé de réaliser une configuration, notamment des fonctionnalités de sécurité, à l'état de l'art afin de réduire le risque de compromission : activation des mécanismes de protection<sup>59</sup> ou mise en application de bonnes pratiques d'installation des systèmes (p. ex. désactivation des services inutiles, changement des mots de passe par défaut, désactivation de l'*autorun*, désactivation du routage réseau...). Pour le durcissement d'un système Linux, se reporter au guide ANSSI [9].

R35

### Durcir la configuration des matériels et des logiciels utilisés sur les SI sensibles

Avant leur mise en exploitation, l'intégrité des matériels et des logiciels d'un SI sensible doit être vérifiée et leur configuration doit être durcie<sup>60</sup>. Cette recommandation s'applique à chacun des composants du SI sensible : serveurs, postes de travail, équipements réseau (commutateurs, routeurs...<sup>61</sup>) et matériels<sup>62</sup>. Une attention particulière doit être apportée aux postes de travail qui constituent souvent le point d'entrée privilégié pour compromettre un SI.

## 5.4 Marquage

### Marquage des informations et des applications

Il est fortement recommandé que les informations sensibles soient marquées par des moyens laissés à la discrétion du responsable d'un SI sensible<sup>63</sup>. La vertu de ce marquage est d'attirer l'attention

58. *Firmware*, en anglais.

59. Exemples : *Data execution prevention* (DEP), *Address space layout randomization* (ASLR), *Security-enhanced Linux* (SELinux), *AppArmor*.

60. Se reporter à la mesure de sécurité II 901 EXP-CONFIG.

61. Se reporter à la mesure de sécurité II 901 RES-DURCI.

62. Se reporter aux mesures de sécurité II 901 PDT-MUL-DURCISS et PDT-TEL-MINIM.

63. Se reporter à l'article 5 de l'II 901 et à la mesure de sécurité II 901 GDB-QUALIF-SENSI.

de l'ensemble des intervenants du SI sensible (utilisateurs, administrateurs, exploitants, mainteneurs...) sur le niveau de sensibilité des informations manipulées, afin de les inciter au respect des règles de manipulation afférentes.

Dans le cas des données non structurées (typiquement, les fichiers bureautiques), le marquage consiste à insérer le timbre de la mention de protection au milieu en haut et en bas de chaque page. La figure 17 donne la représentation du timbre DIFFUSION RESTREINTE.



FIGURE 17 – Timbre DIFFUSION RESTREINTE

Dans le cas des données structurées (typiquement des données accessibles au travers d'une application), le marquage peut consister en l'ajout d'une bannière à l'ouverture de chaque session applicative ou encore en un rappel permanent du niveau de sensibilité des informations dans l'interface homme-machine de l'application.

R36

### Marquer les informations sensibles

Il est fortement recommandé que l'entité mettant en œuvre un SI sensible se dote des moyens permettant le marquage des fichiers sensibles (tampons, conventions de nommage...) et des applications sensibles (bannières, adaptation de l'interface homme-machine...). Elle doit en outre sensibiliser les utilisateurs du SI sensible à l'importance de marquer les informations dès leur création. Les informations DR doivent être marquées avec la mention DIFFUSION RESTREINTE.



### Information

Le marquage ne doit pas être confondu avec la labellisation. De manière simplifiée, dans le premier cas, il s'agit d'apposer à une information un marqueur visuel exploitable par un être humain; dans le second cas, il s'agit d'ajouter des données techniques (méta-données) à une information, de manière à pouvoir automatiser ultérieurement la détermination de son niveau de sensibilité. La fonction de labellisation a plutôt vocation à être utilisée dans les architectures de SI classifiés, quand des problématiques d'échanges d'informations entre des SI de niveaux de sensibilité différents sont rencontrées.

## Marquage des matériels

En pratique, il n'est pas toujours possible de réaliser le marquage des informations. Dans ce cas, c'est le support physique utilisé pour le stockage de ces informations qu'il convient de marquer. Le marquage des supports, comme le marquage des données, permet d'attirer l'attention sur l'importance de leur manipulation pour protéger la confidentialité des données qui y sont stockées. En particulier, lorsque les supports sont réaffectés à d'autres usages, envoyés en maintenance à l'extérieur

63. Sigle anglais pour *Data loss prevention* ou *Data leakage prevention*.

de l'entité ou lorsqu'ils sont désengagés, des mesures d'effacement sécurisé voire de destruction s'appliquent <sup>64</sup>.

Le marquage cumulatif des informations et des supports doit être recherché.

R37

### Marquer les supports stockant des informations sensibles

Il est fortement recommandé de marquer les supports physiques de stockage de ces informations.

Dans le but de réduire les erreurs de branchement et, surtout, de faciliter la détection visuelle de branchements illégitimes, il est pertinent de définir un code couleur pour le câblage des équipements sur les différents réseaux, en fonction de leur niveau de sensibilité. Cette recommandation s'applique aussi bien dans les centres de données, que dans les locaux techniques de distribution du réseau ou dans les bureaux, au plus près des utilisateurs non techniques du SI.

R38

### Adopter un code couleur pour le câblage des équipements

Il est recommandé de distinguer visuellement les câbles réseaux ayant des niveaux de sensibilité différents, par exemple par l'utilisation de câbles de différentes couleurs.

## 5.5 Gestion des authentifiants et des droits d'accès

Toute personne accédant à une ressource d'un SI sensible doit obligatoirement être identifiée et authentifiée au moyen d'un compte individuel. En outre, plusieurs comptes individuels doivent être créés pour une même personne dont le métier justifie qu'elle ait des rôles distincts sur le SI (typiquement un compte utilisateur et un compte administrateur).

Il convient de distinguer l'authentification initiale (ou « primaire ») qui est un prérequis pour pouvoir accéder au SI et les authentifications ultérieures. Ces authentifications (dites « secondaires ») ont pour objectif de conditionner l'accès de certaines ressources aux seuls utilisateurs du SI ayant le besoin d'en connaître. Elles permettent d'apporter, dans une approche de défense en profondeur, une protection supplémentaire vis-à-vis d'agents malveillants qui auraient compromis le SI.

### Authentification initiale

L'authentification initiale permettant à un utilisateur d'accéder à un SI sensible doit être une authentification forte <sup>65</sup>. Une authentification est dite « forte » si elle est implémentée à l'état de l'art et si elle est « multifacteur ». Une authentification est dite multifacteur si elle s'appuie sur, au moins, deux des trois types d'authentifiants disponibles : quelque chose que l'utilisateur sait (un mot de passe, une *passphrase*, une code PIN...), quelque chose que l'utilisateur possède (une carte à puce, un jeton d'authentification...), ce que l'utilisateur est (présentation d'une caractéristique qui lui est propre telle que iris, visage, empreinte digitale...).

64. Se reporter aux mesures de sécurité II 901 EXP-CI-EFFAC, EXP-MAINT-EXT et EXP-MIS-REB.

65. Se reporter à la mesure de sécurité II 901 EXP-ID-AUTH.



Si des secrets d'authentification sont associés à cette authentification initiale, ils doivent être mémorisés par le détenteur du compte utilisateur et en aucun cas être stockés ailleurs (ni sur un papier, ni dans un fichier, même chiffré, qui serait stocké sur un SI...).

**R39**

### Activer une authentification initiale forte

L'authentification initiale d'un utilisateur sur un SI sensible doit être une authentification multifacteur à l'état de l'art.

## Authentifications secondaires

Si l'authentification initiale doit nécessairement requérir une action de l'utilisateur, il est au contraire recommandé de rendre les authentifications ultérieures transparentes. Ainsi il est recommandé au responsable d'un SI sensible de déployer des solutions d'authentification unique<sup>66</sup>. Ces solutions ont différentes architectures dont la description sort du périmètre de ce guide. De manière générale, il faut retenir que les architectures mettant en œuvre des protocoles d'authentification centralisés, à base de jeton d'authentification, ou de fédération d'identité (architectures dites « SSO serveur »<sup>67</sup>) doivent être préférées aux architectures dites « SSO client » ou « SSO entreprise »<sup>68</sup>.



### Information

En fonction des contextes, l'accès à des applications particulièrement critiques pourra être conditionné par une ré-authentification régulière de l'utilisateur avec ses informations d'authentification utilisées lors de l'authentification initiale.

Il peut être fastidieux pour les utilisateurs de gérer les secrets d'authentification qui ne peuvent pas être pris en charge par les systèmes d'authentification unique. Pour protéger ces secrets d'authentification, il est recommandé de former les utilisateurs à l'usage d'un coffre-fort de mots de passe<sup>69</sup>. Conformément à la recommandation R30, l'utilisation d'un coffre-fort de mots de passe disposant d'un visa de sécurité délivré par l'ANSSI doit être privilégiée.

Les services d'authentification reposant sur des mots de passe doivent être en mesure d'imposer techniquement des règles de complexité. À défaut, une procédure formelle doit encadrer la vérification périodique de la force des mots de passe<sup>70</sup>. De manière générale, les règles de gestion des mots de passe doivent suivre les recommandations de l'ANSSI [3]<sup>71</sup>.

**R40**

### Protéger les secrets d'authentification

Il est recommandé que les secrets d'authentification secondaires soient protégés à l'aide d'un système d'authentification unique (SSO). Il est en outre recommandé que les secrets d'authentification qui ne pourraient pas être pris en charge par le système d'authentification unique, soient protégés à l'aide d'un coffre-fort de mots de passe,

66. *Single Sign On* (SSO), en anglais.

67. Exemples : Kerberos, CAS, protocoles de fédération d'identité comme SAML ou *WS-Federation*...

68. Ces solutions, qui présentent l'avantage de ne nécessiter aucune adaptation des applications, automatisent la saisie des identifiants et les secrets d'authentification dans les fenêtres d'authentification applicatives.

69. Se reporter aux mesures de sécurité II 901 EXP-CONF-AUTH, EXP-GEST-PASS et EXP-INIT-PASS.

70. Se reporter à la mesure de sécurité II 901 EXP-QUAL-PASS.

71. Se reporter à la mesure de sécurité II 901 EXP-POL-PASS.



disposant si possible d'un visa de sécurité délivré par l'ANSSI.

## Autorisations

Pour imposer le respect du besoin d'en connaître, l'entité responsable d'un SI sensible doit mettre en place une procédure par laquelle toute affectation de droit d'accès logique à une ressource sensible est conditionnée à une autorisation formelle<sup>72</sup>. Les rôles des personnes impliquées dans le circuit d'approbation de ces demandes de modification de droits d'accès logiques doivent être clairement définis. Les demandes d'ouverture, de modification ou de suppression des autorisations doivent être archivées à des fins d'audits ou d'investigations consécutives à des incidents de sécurité.

L'octroi des autorisations d'accès aux ressources doit préférentiellement être réalisé par affectation des comptes utilisateurs à des groupes d'utilisateurs<sup>73</sup>.

Les droits d'accès logiques associés à un compte utilisateur doivent refléter le poste occupé par l'utilisateur au sein de l'entité et être régis par le principe de moindre privilège. À cette fin, les affectations, modifications et suppressions de droits doivent être réalisées en fonction des changements de poste ou de fonction de l'utilisateur. À la fin de son cycle de vie, le compte utilisateur doit être neutralisé<sup>74</sup> mais pas supprimé.

Les conséquences de la compromission d'un compte utilisateur sont d'autant plus réduites que les droits qui lui sont attachés sont faibles. Une revue des droits d'accès affectés aux comptes utilisateurs (privilèges et autorisations d'accès) doit être réalisée annuellement au minimum<sup>75</sup>, de manière à détecter et corriger d'éventuelles dérives. Pour être efficaces, ces revues doivent être conduites par les personnes de l'entité ayant une très bonne connaissance de la nature des informations, ainsi que des utilisateurs ayant un besoin d'accès légitime. Ces revues sont donc réalisées par des responsables métier plutôt que par des administrateurs de l'infrastructure.

Toutes les tâches énumérées précédemment peuvent s'avérer particulièrement lourdes et complexes. Pour les entités de taille importante, il est fortement recommandé d'outiller ces procédures grâce à des plateformes de gestion des identités et des accès (IAM<sup>76</sup>).

R41

### Gérer avec rigueur l'affectation des droits d'accès logiques des comptes informatiques

La gestion des droits sur un SI sensible doit faire l'objet d'une procédure permettant d'imputer les affectations, les modifications et les suppressions de droits, tout au long du cycle de vie des comptes informatiques. Une revue périodique des droits logiques doit en outre être réalisée annuellement. Pour les SI sensibles très étendus, l'utilisation d'outils de gestion des identités, de l'authentification unique et des autorisations est fortement recommandée.

72. Se reporter aux mesures de sécurité II 901 RH-MOUV, EXP-DROITS, EXP-PROFILS, EXP-PROC-AUTH.

73. Il n'est pas recommandé d'affecter des autorisations directement à un compte utilisateur car cela complexifie les procédures d'octroi et, surtout, de retrait des droits logiques.

74. La neutralisation d'un compte utilisateur dépend des possibilités du système d'exploitation ou de l'application. Elle peut consister, par exemple, en une configuration particulière des paramètres du compte ou en une suppression des privilèges associés au compte.

75. Se reporter à la mesure de sécurité II 901 EXP-REVUE-AUTH.

76. *Identity and Access Management*, en anglais.

## 5.6 Protection contre les codes malveillants

L'II 901 demande une diversification des technologies antivirales mises en œuvre pour détecter les codes malveillants<sup>77</sup>. À ce titre, il est recommandé que les logiciels antivirus soient différents sur les serveurs applicatifs, sur les postes de travail et sur les moyens d'interconnexion.

Cette diversification technologique ne doit toutefois pas être recherchée à tout prix, en particulier si le niveau de sécurité intrinsèque des produits n'a pas été évalué, ou si la diversification technologique est réalisée au détriment de la maîtrise des différentes solutions par le personnel en charge de leur administration.

R42

### Protéger le SI sensible des codes malveillants

Des logiciels antivirus doivent être installés sur l'ensemble des serveurs applicatifs, sur les postes de travail et sur les moyens permettant l'interconnexion du SI sensible avec d'autres SI. Dans la mesure du possible, il est recommandé de diversifier les technologies de protection contre les codes malveillants sur ces différents systèmes.

Par ailleurs, bien que non spécifiques aux SI sensibles, certains points d'attention sont particulièrement importants pour les SI sensibles :

- Les supports amovibles destinés à être connectés à un SI sensible doivent être fournis par l'entité responsable du SI et faire l'objet d'une analyse avant d'être connectés au SI (voir la section 5.7 relative aux périphériques et aux supports amovibles).
- Les fonctionnalités d'évaluation dynamique de la réputation d'un contenu doivent être désactivées lorsque ces évaluations ne sont pas réalisées localement (p. ex. évaluation faite dans le *cloud* ou référentiels hébergés dans le *cloud*).
- Dans le cas particulier des systèmes dont la criticité est élevée et dont la surface d'attaque a été strictement réduite, l'installation d'un logiciel antivirus, potentiellement vulnérable, peut aller à l'encontre du but recherché et est donc déconseillée (p. ex. serveur d'annuaire).
- Les privilèges des comptes de service utilisés par les agents logiciels antivirus installés sur les systèmes sont souvent élevés par défaut ; il est nécessaire de passer en revue ces droits et de les réduire autant que possible (principe du moindre privilège)<sup>78</sup>.
- Les mises à jour antivirales doivent être déployées rapidement après leur mise à disposition par les éditeurs de logiciels de protection. Un délai maximal de 24 heures est recommandé.

R43

### Adapter la politique de protection contre les codes malveillants

Des solutions de protection contre les codes malveillants sont indispensables, mais leur déploiement doit être réfléchi, de sorte qu'elles ne soient pas à l'origine d'un affaiblissement du niveau de sécurité (augmentation de la surface d'attaque, source d'exfiltration de données...).

77. Se reporter à la mesure de sécurité II 901 EXP-PROT-MALV.

78. Se reporter à la mesure de sécurité II 901 EXP-DOM-LIMITSERV.

En fonction des résultats de l'analyse des risques et de la stratégie de supervision de l'entité mettant en œuvre un SI sensible, il est recommandé de déployer des solutions permettant de révéler des comportements potentiellement suspects (p. ex. outils de contrôle d'intégrité des fichiers d'un système d'exploitation, HIDS<sup>79</sup>, outils de restrictions logicielles pour limiter l'exécution des programmes...).

R44

### Déployer des outils révélant des activités suspectes

Il est recommandé d'installer des outils de détection des comportements suspects et que les journaux qu'ils génèrent alimentent le système de supervision mis en œuvre sur le SI sensible. Cette recommandation concerne en premier lieu les postes de travail.

## 5.7 Gestion des périphériques et des supports amovibles

### Limitation du nombre de périphériques et de supports amovibles

Tout périphérique amené à être connecté à un SI sensible peut être le vecteur d'une attaque informatique<sup>80</sup>. Il est essentiel que le responsable d'un SI sensible approuve les équipements utilisables sur le SI sensible et en gère la configuration et l'exploitation. La mise en œuvre de mesures techniques ou organisationnelles permettant de contrôler les périphériques autorisés sur le SI sensible est recommandée (voir la recommandation R49).

Parmi tous les périphériques, les supports amovibles permettant le stockage de données<sup>81</sup> (clés USB, disques durs externes, appareils photo, cartes mémoires, CD-ROM...) doivent faire l'objet d'une attention particulière.

Les échanges au moyen de supports amovibles peuvent être vus comme une forme particulière d'interconnexion de SI, qu'il est possible de qualifier d'« interconnexion indirecte », par opposition aux interconnexions directes vues au chapitre 4. Comme les interconnexions directes, les supports amovibles constituent un vecteur potentiel de propagation de codes malveillants ou d'exfiltration de données. Leur dangerosité provient de leur facilité à être transportés et échangés.

Par conséquent, une mesure de réduction des risques consiste à trouver des moyens de substitution aux supports amovibles. Cela signifie par exemple que les échanges de données doivent, chaque fois que cela est envisageable, être réalisés au travers du réseau. Par ailleurs, les échanges de données entre le SI sensible et les SI usuels de la même entité doivent préférentiellement être effectués au moyen de systèmes d'échanges pour les utilisateurs (voir la section 4.4).

R45

### Supports amovibles : limiter leur usage au strict besoin opérationnel

Il est fortement recommandé que l'entité mettant en œuvre un SI sensible réduise le nombre de supports amovibles au strict besoin opérationnel et préfère des solutions d'échange via le réseau.

79. *Host-based intrusion detection system*, en anglais.

80. À titre d'exemple, des souris ou des claviers peuvent être piégés à des fins de collecte de données.

81. Dans ce guide, le terme *support amovible* est utilisé pour désigner les *supports amovibles de stockage de données*.

Il peut toutefois exister des cas d'usage pour lesquels l'utilisation de supports amovibles s'avère incontournable. C'est par exemple le cas lorsqu'un SI sensible a une taille très réduite. Il n'est alors pas pertinent de mettre en œuvre un système d'échanges pour les utilisateurs de ce SI. D'autres exemples concernent des besoins d'échanges avec des SI isolés (c.-à-d. sans interconnexion directe), ou avec des SI d'autres entités pour lesquels il n'est pas possible de réaliser une interconnexion.

## Gestion et contrôle des supports amovibles

Si une entité responsable d'un SI sensible autorise l'utilisation de supports amovibles, elle doit se doter d'une politique définissant les règles de gestion et les conditions d'usage. Cette politique relative aux supports amovibles intègre au minimum les éléments listés ci-après.

Les supports amovibles :

- sont fournis par l'entité responsable d'un SI sensible <sup>82</sup> ;
- sont affectés à un seul utilisateur, et leur réaffectation est encadrée par une procédure validée par le RSSI <sup>83</sup> ;
- sont préférentiellement marqués (voir la recommandation R37) ;
- sont chiffrés suivant les recommandations R57 et R58 ;
- s'ils contiennent des données sensibles, doivent être stockés, en dehors de leurs périodes d'utilisation, dans des meubles fermant à clé <sup>84</sup> ;
- en cas de perte ou de vol, font l'objet d'une déclaration auprès du RSSI <sup>85</sup>.

R46

### Supports amovibles : maîtriser leur gestion et leurs conditions d'usage

Une entité qui autorise l'utilisation de supports de stockage amovibles sur un SI sensible doit se doter d'une politique, conforme aux mesures de sécurité de l'II 901, précisant leurs règles de gestion et leurs conditions d'usage. En particulier, cette politique doit interdire la connexion sur le SI sensible de tout support amovible personnel et de tout support amovible fourni par une entité tierce. Seuls les supports amovibles fournis et administrés par le responsable du SI sensible, et explicitement autorisés pour une utilisation sur le SI sensible, peuvent être connectés sur le SI sensible.

Il est recommandé d'installer sur les postes de travail des utilisateurs et sur les postes de travail des administrateurs du SI sensible, des moyens techniques permettant de garantir que seuls des supports amovibles explicitement autorisés peuvent être connectés.

La stricte application de la recommandation R46 est d'autant plus critique que les supports amovibles permettent l'exportation de données du SI sensible. Une mesure de réduction du risque

82. En aucun cas les supports amovibles personnels ne sont autorisés à être connectés sur un SI sensible (se reporter à la mesure de sécurité II 901 PDT-AMOV). De même, l'II 901 interdit la connexion sur un SI sensible de tout support amovible qui n'est pas sous maîtrise directe du responsable du SI sensible (se reporter à la mesure de sécurité II 901 EXP-MAIT-MAT). Les échanges de données mettant en œuvre des supports amovibles fournis par des entités tierces doivent être réalisés suivant la recommandation R48.

83. Se reporter à la mesure de sécurité II 901 EXP-REAFECT.

84. Se reporter à la mesure de sécurité II 901 EXP-PROT-VOL.

85. Se reporter à la mesure de sécurité II 901 EXP-DECLAR-VOL.

de sortie incontrôlée de données du SI sensible, consiste à préférer l'utilisation de supports amovibles qui, lorsqu'ils sont utilisés sur un poste de travail sensible, restreignent les échanges aux seules importations de données sur le SI sensible. En pratique, il s'agit d'utiliser des supports non réinscriptibles (p. ex. CD-ROM) ou des dispositifs interdisant l'écriture de données lorsqu'ils sont connectés au SI sensible (p. ex. bloqueurs USB). De tels supports, en « lecture seule », permettent uniquement l'importation de données sur le SI sensible mais en interdisent l'exportation.

R47

### Supports amovibles : privilégier l'utilisation de supports en lecture seule

Dans la mesure du possible, il est recommandé de privilégier l'usage de supports amovibles ou de dispositifs permettant de garantir que seule l'importation de données est possible sur le SI sensible.

## Dépollution des supports amovibles

Les supports amovibles doivent être dépollués avant tout échange de données avec un SI sensible. La règle générale est d'effectuer cette dépollution à l'aide de moyens dédiés à cet usage : *sas* ou *station blanche*. Cette règle doit être strictement respectée dans le cas des supports amovibles qui ne sont ni fournis ni administrés directement par l'entité responsable du SI sensible<sup>86</sup> (p. ex. support fourni par un tiers) ou quand l'innocuité des données stockées sur le support amovible n'est pas garantie.

Il est envisageable de réaliser la dépollution d'un support amovible directement sur le SI sensible, sans qu'il soit nécessaire de le connecter préalablement sur un *sas* ou sur une station blanche. Toute dérogation à la règle générale doit être explicitement autorisée par le responsable du SI sensible et strictement encadrée :

- le risque supplémentaire induit par une dérogation doit avoir été évalué dans l'analyse des risques et être intégré aux risques résiduels lors de l'homologation du SI sensible ;
- le support amovible utilisé doit être nécessairement fourni et administré par l'entité responsable du SI sensible (voir la recommandation R46) ;
- le niveau de confiance de l'utilisateur concernant l'innocuité du support doit être fort (p. ex. l'utilisateur connaît l'historique d'utilisation du support).

Dans tous les autres cas (utilisation d'un support fourni par un tiers, utilisation d'un support fourni et administré par le responsable du SI sensible mais dont l'innocuité n'est pas garantie...), le recours à des moyens dédiés à la dépollution des supports de stockage est obligatoire.

R48

### Supports amovibles : utiliser des solutions de dépollution des supports de stockage

Il est fortement recommandé d'utiliser une solution dédiée à la dépollution (p. ex. *sas*, station blanche...) pour les échanges de données avec un SI sensible réalisés au moyen de supports amovibles qui ne sont ni fournis ni administrés directement par l'entité (supports gérés par une entité tierce), ou pour lesquels il

86. L'II 901 interdit la connexion sur un SI sensible de tout support amovible qui n'est pas sous maîtrise directe du responsable du SI sensible. Se reporter à la mesure de sécurité II 901 EXP-MAIT-MAT.

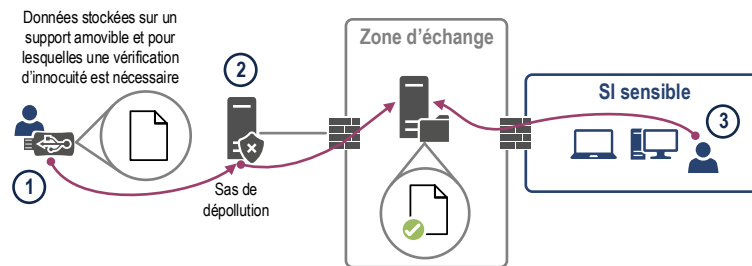
existe des doutes quant à l'innocuité de leur contenu. Si cette solution met elle-même en œuvre des supports amovibles, il est recommandé que ceux-ci soient dédiés à cet usage et que des mesures techniques ou organisationnelles permettent d'assurer leur innocuité au cours du temps.

Voici des exemples de fonctions de sécurité qui peuvent être intégrées dans les solutions de type sas ou station blanche :

- analyse antivirus à partir d'une base de connaissances ou d'heuristiques ;
- blocage des formats de fichiers non explicitement autorisés ;
- vérification de la conformité de la structure des fichiers par rapport à des formats de référence ;
- analyse comportementale par ouverture du document ou du code exécutable à analyser dans un environnement virtualisé (« bac à sable ») ;
- transformation des documents, depuis un format de fichier bureautique éditable vers un format image, afin d'éviter qu'un éventuel code intégré puisse être exécuté ;
- protection des équipements contre les attaques visant la destruction physique de matériels (p. ex. surcharge électrique) ;
- protection contre les micrologiciels USB malveillants.

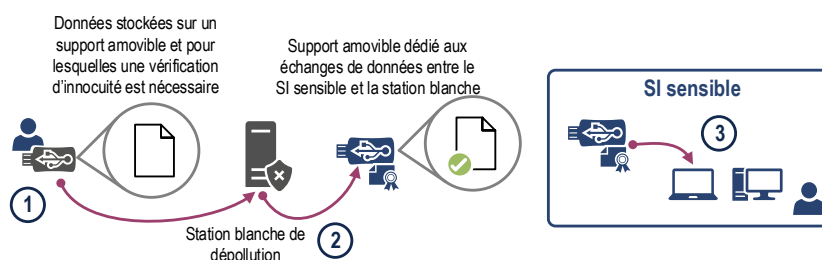
Les figures 18 et 19 donnent deux exemples d'architecture acceptables pour des solutions de dépollution de supports amovibles. Sur ces deux figures, seul le cas du transfert de données stockées sur le support amovible vers le SI sensible est présenté. Pour l'exportation de données du SI sensible au moyen de supports amovibles, l'analyse d'innocuité avec un sas ou une station blanche est obligatoire si le support amovible est fourni par une entité tierce, ou si le support utilisé pour cette exportation de données est fourni et administré par le responsable du SI sensible mais que son innocuité n'est pas garantie.

Pour en savoir plus sur les sas et les stations blanches, se reporter au document ANSSI [30].



- ① L'utilisateur connecte le support de données à analyser sur le sas et sélectionne les fichiers qu'il souhaite transférer sur le SI sensible.
- ② Le sas de dépollution analyse les fichiers et copie les fichiers sains dans la zone d'échange, dans un espace accessible uniquement de l'utilisateur ayant initié le transfert.
- ③ L'utilisateur, authentifié sur le SI sensible, télécharge les fichiers depuis la zone d'échange. Cette action d'importation de données est journalisée et imputée à l'utilisateur. De manière à limiter l'impact en cas de compromission du sas, un mécanisme automatique supprime les données de la zone d'échange. Cette suppression est faite préférentiellement à l'issue de l'importation des données sur le SI sensible ou, à défaut, périodiquement (p. ex. quotidiennement).

FIGURE 18 – Illustration du concept de sas de dépollution et explication de son utilisation dans le cas d'une importation de données sur le SI sensible



- ① L'utilisateur connecte le support amovible à analyser à la station blanche et sélectionne les fichiers qu'il souhaite transférer sur le SI sensible.
- ② La station blanche analyse les fichiers et copie les fichiers sains sur un support amovible maîtrisé et dédié à l'importation et à l'exportation de données entre le SI sensible et la station blanche. De manière à limiter l'impact en cas de compromission de la station blanche, les transferts de données entre les deux supports de données sont réalisés en minimisant autant que possible les données temporaires. Si ces données temporaires sont inévitables, un mécanisme automatique les supprime périodiquement (p. ex. quotidiennement).
- ③ L'utilisateur, authentifié sur le SI sensible, connecte le support amovible maîtrisé sur un point d'insertion de données, lequel vérifie qu'il s'agit d'un support maîtrisé et que l'analyse de sécurité a bien été faite par la station blanche. Cette action d'importation de données est journalisée et imputée à l'utilisateur.

FIGURE 19 – Illustration du concept de station blanche de dépollution et explication de son utilisation dans le cas d'une importation de données sur le SI sensible



# 6

## Sécurisation des postes de travail sensibles



### Objectif

Les postes de travail constituent des points d'entrée souvent privilégiés pour compromettre un SI. En fonction des choix d'architecture, ils peuvent être situés à la confluence de SI ayant des niveaux d'exposition aux menaces différents et constituent, à ce titre, des systèmes de rebond particulièrement attractifs du point de vue d'un attaquant. Mais surtout, les postes de travail sont le siège des interactions homme-machine entre le SI et les utilisateurs. Ces derniers peuvent être abusés et devenir les vecteurs involontaires d'actions malveillantes. La sensibilisation des utilisateurs joue donc un rôle primordial pour prévenir la compromission des postes de travail. Cette sensibilisation doit être complétée par des mesures de sécurité techniques et organisationnelles visant à réduire la probabilité de compromission des postes de travail. L'objet de ce chapitre est de présenter ces mesures.

### 6.1 Maîtrise des postes de travail des SI sensibles

L'entité mettant en œuvre un SI sensible doit maîtriser la sécurité des postes de travail utilisés pour l'accès aux informations sensibles. À ce titre, différentes mesures doivent être prises :

- les logiciels installés sur les postes de travail, et leur configuration, sont sous le contrôle exclusif du responsable du SI sensible<sup>87</sup>. En particulier, l'utilisation d'hyperviseurs de type 2<sup>88</sup> est interdite sauf accord du responsable du SI sensible et uniquement pour des cas d'usage particuliers ;
- tous les équipements connectés à un SI sensible sont administrés et mis à jour sous la responsabilité du responsable du SI sensible<sup>89</sup> ;
- les mouvements latéraux d'un attaquant qui aurait compromis un poste de travail<sup>90</sup> sont bloqués par différentes techniques complémentaires : diversifier les moyens d'authentification des comptes administrateurs locaux<sup>91</sup>, interdire la connexion distante à ces comptes, configurer un pare-feu local...<sup>92</sup> (se reporter aussi à la recommandation R34) ;

87. Se reporter à la mesure de sécurité II 901 PDT-CONFIG et à la recommandation R35 relative au durcissement des systèmes.

88. Par opposition à un hyperviseur de type 1 qui s'exécute directement sur la couche matérielle d'un ordinateur, un hyperviseur de type 2 s'exécute sur un système d'exploitation préinstallé sur l'ordinateur. Utilisé de manière non contrôlée, un hyperviseur de type 2 représente un risque pour la sécurité du SI sensible par sa capacité à contourner la politique de sécurité mise en œuvre sur l'ordinateur où il s'exécute.

89. Se reporter à la mesure de sécurité II 901 EXP-MAIT-MAT.

90. Se reporter à la mesure de sécurité II 901 EXP-DOM-ADMINLOC et à la recommandation R34.

91. Si le système d'exploitation est Windows, l'outil *Local admin password solution* (LAPS) est à considérer.

92. À noter que cette dernière technique peut permettre de répondre en outre à la mesure de sécurité PDT-PART-FIC de l'II 901 qui vise à interdire le partage de données hébergées localement sur les postes de travail.



- les postes fixes peu volumineux sont protégés contre le vol par un système d'attache sécurisé<sup>93</sup> ;
- la réaffectation d'un poste de travail sensible à un autre utilisateur fait l'objet d'une procédure spécifique permettant de garantir le respect du besoin d'en connaître<sup>94</sup>.



### Attention

L'II 901 interdit la connexion de moyens informatiques personnels sur les SI sensibles<sup>95</sup>. L'utilisation de moyens personnels, utilisés pour des usages professionnels<sup>96</sup>, est par conséquent également interdit.

R49

### Maîtriser les moyens informatiques affectés aux utilisateurs d'un SI sensible

Des mesures techniques et organisationnelles permettent à l'entité responsable d'un SI sensible de maîtriser les moyens informatiques mis à la disposition des utilisateurs, de façon à notamment réduire le risque d'atteinte à l'intégrité des postes de travail sensibles. En particulier, les utilisateurs ne disposent pas de droits d'administration locaux et ceux-ci sont réservés aux administrateurs en charge de l'exploitation et du support des postes de travail<sup>97</sup>.

Les moyens informatiques confiés aux utilisateurs sont réservés à un usage professionnel.



### Information

Les dispositifs électroniques personnels dotés d'une connectique USB doivent être rechargés électriquement au moyen de chargeurs dédiés à cet usage. En aucun cas, ils ne doivent être connectés à des moyens informatiques professionnels appartenant à un SI sensible<sup>98</sup>.

## 6.2 Connexion des postes de travail au réseau

Concernant la connexion des moyens distribués (postes de travail, moyens d'impressions...) aux réseaux locaux, le meilleur niveau de sécurité est atteint par la mise en œuvre d'un réseau physique dédié au SI sensible.

R50

### Connecter les ressources sensibles sur un réseau physique dédié

Il est fortement recommandé de déployer les ressources d'un SI sensible sur un réseau physique dédié à cet usage.

93. Se reporter à la mesure de sécurité II 901 PDT-VEROUIL-FIXE.

94. Se reporter aux mesures de sécurité II 901 EXP-CI-EFFAC et PDT-REAFFECT.

95. Se reporter à l'article 17 de l'II 901 et à la mesure de sécurité II 901 PDT-GEST.

96. Concept désigné par l'acronyme anglais BYOD pour *Bring Your Own Device*.

97. Se reporter aux mesures de sécurité II 901 EXP-RESTR-DROITS et PDT-ADM-LOCAL.

98. L'application de cette mesure d'hygiène informatique est recommandée sur tout type de SI et pas seulement sur les SI sensibles.

Le SI sensible pouvant potentiellement être très étendu, la mise en œuvre d'un réseau physique dédié ne sera pas toujours possible. Dans ce cas, le déploiement d'un réseau logique dédié mettant en œuvre des mécanismes de chiffrement et d'authentification de réseau (protocole IPsec) est envisageable.

#### R50 -

### Connecter les ressources sensibles sur un réseau logique dédié

Une mesure de sécurité dégradée de la recommandation R50 consiste à déployer les ressources sensibles sur un réseau logique dédié à cet usage et protégé à l'aide du protocole IPsec. En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l'exposition du concentrateur VPN IPsec aux seuls moyens distribués sensibles.

Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [17] doivent être appliquées.



### Information

La recommandation R50- n'est pas applicable aux architectures de type « SI sensible physiquement isolé » (voir la section 3.2.1) et de type « SI sensible physiquement cloisonné » (voir la section 3.2.2) puisque dans ces cas le SI usuel et le SI sensibles sont, par définition, totalement séparés.

De manière à éviter à des composants non explicitement autorisés de bénéficier d'une connectivité réseau s'ils venaient à être branchés sur le réseau local, les accès à un réseau sensible doivent être contrôlés<sup>99</sup>. Il est fortement recommandé de mettre en place un service d'authentification des ressources sensibles vis-à-vis du réseau. Par exemple, il peut s'agir d'établir un tunnel VPN IPsec (voir la recommandation R50-) ou de mettre en œuvre le protocole 802.1X, avec authentification des équipements demandeurs (*supplicants*) par certificat électronique.



### Attention

Concernant l'utilisation du protocole 802.1X, le service d'authentification au réseau ne doit pas affaiblir le niveau de sécurité du SI sensible. Une vigilance particulière doit être portée sur le cloisonnement du serveur d'authentification, d'autorisation et de traçabilité<sup>100</sup>, à plus forte raison si des accès Wi-Fi au réseau sont autorisés par le responsable du SI sensible (voir aussi la recommandation R60 relative aux réseaux sans fil). Le guide de l'ANSSI consacré au déploiement du protocole 802.1X [8] explique dans quels cas l'utilisation de cette solution technique est conseillée.

#### R51

### Authentifier les ressources sensibles vis-à-vis du réseau

Il est fortement recommandé que les ressources d'un SI sensible, et en premier lieu les moyens distribués, soient authentifiés, avant de pouvoir bénéficier d'une connectivité sur le réseau local sensible.

99. Se reporter à la mesure de sécurité II 901 EXP-CI-ACCRES.

100. Ce serveur est appelé serveur AAA pour *Authentication, Authorization and Accounting*. Le serveur AAA le plus fréquemment utilisé met en œuvre le protocole RADIUS. Il est généralement qualifié de « serveur RADIUS » par métonymie.

## 6.3 Architecture des postes de travail

Pour permettre aux utilisateurs d'accéder à un SI usuel, d'une part, et à un SI sensible, d'autre part, trois solutions d'architecture de poste de travail sensibles sont envisageables. Elles sont présentées ci-après par niveau de sécurité décroissant au regard des objectifs de sécurité visés :

- un poste utilisateur dédié au SI sensible ;
- un poste utilisateur multiniveau connecté au SI usuel et au SI sensible ;
- un poste utilisateur sensible avec accès distant au SI usuel.

### Poste utilisateur sensible dédié

La solution qui offre la meilleure garantie du point de vue sécurité consiste à utiliser deux postes physiquement distincts (voir la figure 20) : l'un permet l'accès au SI usuel et le second l'accès au SI sensible.

**R52**

**Utiliser un poste utilisateur sensible dédié**  
Il est recommandé de mettre en œuvre des postes de travail sensibles physiquement distincts de tout autre SI.

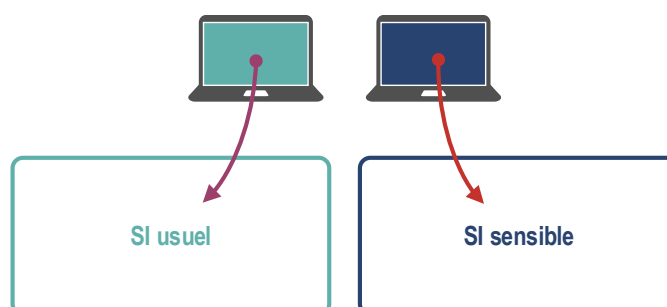


FIGURE 20 – Architecture recommandée : poste utilisateur sensible dédié



#### Information

Dans le cas des architectures de SI sensibles, où le poste de travail utilisateur sensible est physiquement dédié, la question d'utiliser des KVM <sup>101</sup> peut se poser. Idéalement, si des KVM sont mis en œuvre, ceux-ci devraient être qualifiés par l'ANSSI. Cependant, à la date de publication de ce guide, il n'existe pas de KVM qualifié. Les KVM certifiés Critères Communs, avec le profil de protection *Peripheral Sharing Switch* version 3.0 et antérieures, ne présentent pas de garanties quant à l'isolation des différents équipements qui y sont raccordés. L'utilisation d'un tel dispositif, entre deux postes de travail raccordés à des réseaux différents (p. ex. un poste de travail usuel et un poste de travail sensible), doit faire l'objet d'une analyse des risques adaptée au cas d'usage.

<sup>101</sup>. Commutateur écran-clavier-souris ou *keyboard-video-mouse switch*. Il s'agit d'un dispositif électronique matériel permettant de partager un écran, un clavier et une souris entre deux systèmes.

## Poste utilisateur multiniveau

Le principe d'un poste multiniveau consiste à disposer de plusieurs environnements logiciels (généralement deux) sur un même poste physique, grâce à l'emploi des technologies de virtualisation ou de conteneurisation.

Des mécanismes de durcissement du noyau, et de cloisonnement, permettent d'isoler ces environnements pour réduire les risques de compromission du niveau de sensibilité haute, ou de fuite d'informations depuis le niveau de sensibilité haute (ici, un SI sensible), vers le niveau de sensibilité basse (ici, un SI usuel). Un exemple de mise en œuvre concrète d'un poste multiniveau est le projet *CLIP OS* porté par l'ANSSI <sup>102</sup>.

Cette solution (voir la figure 21) offre un niveau de sécurité moindre qu'une séparation physique. Elle doit impérativement faire l'objet d'une évaluation de confiance des mécanismes d'isolation et de cloisonnement. En effet, l'emploi de cette solution, si elle n'est pas de confiance, peut donner un faux sentiment de sécurité. Il est par ailleurs préférable que ces mécanismes soient gérés au niveau du système, et non par une application utilisateur (voir les figures 22 et 23).

R52 -

### Utiliser un poste utilisateur multiniveau

À défaut d'un poste utilisateur sensible physiquement dédié, l'emploi de technologies de virtualisation ou de conteneurisation pour obtenir un système multiniveau, peut être envisagé, dans la mesure où le cloisonnement des environnements est réalisé par des mécanismes au niveau système évalués comme étant de confiance.

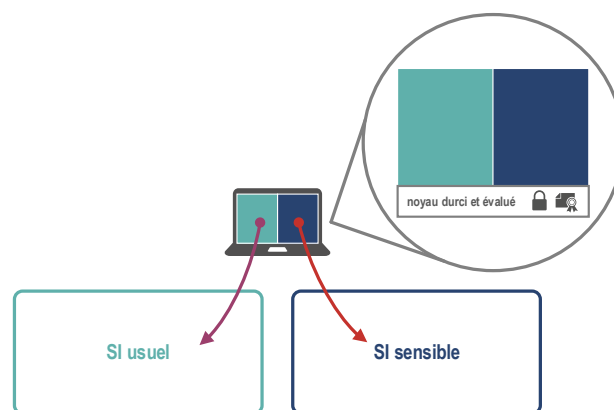


FIGURE 21 – Architecture recommandée : poste utilisateur multiniveau

102. Se reporter au site officiel du projet pour plus d'informations : <https://clip-os.org/>.

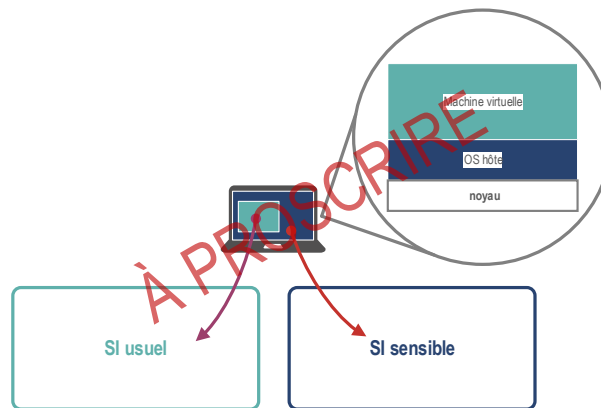


FIGURE 22 – Architecture interdite : poste utilisateur sensible hébergeant une machine virtuelle usuelle

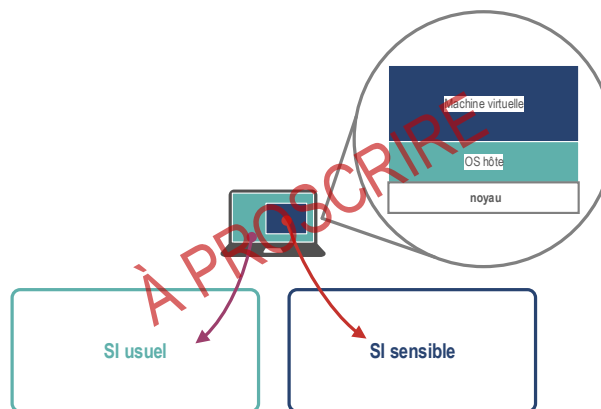


FIGURE 23 – Architecture interdite : poste utilisateur usuel hébergeant une machine virtuelle sensible

## Poste utilisateur sensible avec accès distant au SI usuel

Une dernière solution consiste en l'emploi d'un poste utilisateur physique connecté au réseau sensible et permettant un accès au SI usuel par connexion à distance (voir la figure 24).

Dans cette architecture, le niveau de sécurité est encore moindre. En effet, la surface d'attaque du SI sensible est augmentée par l'exécution du code d'un client de connexion à distance, sur le poste sensible.



### Attention

Il est à noter que la solution inverse, qui consiste à accéder depuis un poste usuel à un poste sensible par connexion à distance, est à proscrire (voir la figure 25).

En effet, le niveau de protection d'un poste usuel étant inférieur à celui d'un poste sensible, sa compromission pourrait notamment permettre à un attaquant d'espionner les actions effectuées depuis ce poste (frappes clavier, copies d'écran,...), en particulier les connexions initiées vers le poste sensible (p. ex. adresse IP, mot de

— passe).

Un attaquant pourrait alors, par rebond, accéder illégitimement au SI sensible.

Si cette solution est mise en œuvre, l'utilisation d'un logiciel de connexion à distance nécessite des précautions de configuration qui visent à restreindre les fonctions d'échange entre le système local (sensible) et le système distant (usuel). En effet, en cas de compromission du serveur de connexion à distance, un attaquant pourrait alors remonter le canal de communication établi dans le but de compromettre le poste sensible. Faute d'évaluation à la date de rédaction de ce document, les mécanismes d'échange des logiciels de connexion à distance ne peuvent pas être, *a priori*, considérés comme étant de confiance.

De manière non exhaustive, les fonctions d'échange d'informations à désactiver sont :

- les fonctions avancées de copier-coller ;
- le partage d'écran ;
- la fonction de prise en charge des périphériques (USB, imprimantes, etc.) ;
- les partages réseaux.

La désactivation de ces fonctions est généralement effectuée au niveau des serveurs *Virtual Desktop Infrastructure* (VDI). Pour améliorer le niveau d'intégrité de ces serveurs et réduire leur exposition aux menaces, il est recommandé de les héberger au sein d'une *passerelle de classe 1*.

Dès lors, la mise en place d'un système d'échanges sécurisés peut être nécessaire. Le concept de système d'échanges sécurisés est détaillé à la section 4.4.

R52 --

### Utiliser un poste utilisateur sensible avec accès distant au SI usuel

À défaut d'un poste sensible physiquement distinct du poste usuel ou d'un poste utilisateur multiniveau de confiance, une solution d'un niveau de sécurité moindre peut consister à ce que les utilisateurs du SI sensible :

- disposent d'un poste de travail physique pour accéder au SI sensible ;
- accèdent, par connexion à distance uniquement, à un poste usuel (physique ou virtuel, par exemple : *Virtual Desktop Infrastructure*) depuis le poste sensible.

Dans tous les cas, les fonctions permettant un échange d'informations entre les deux SI doivent être désactivées.

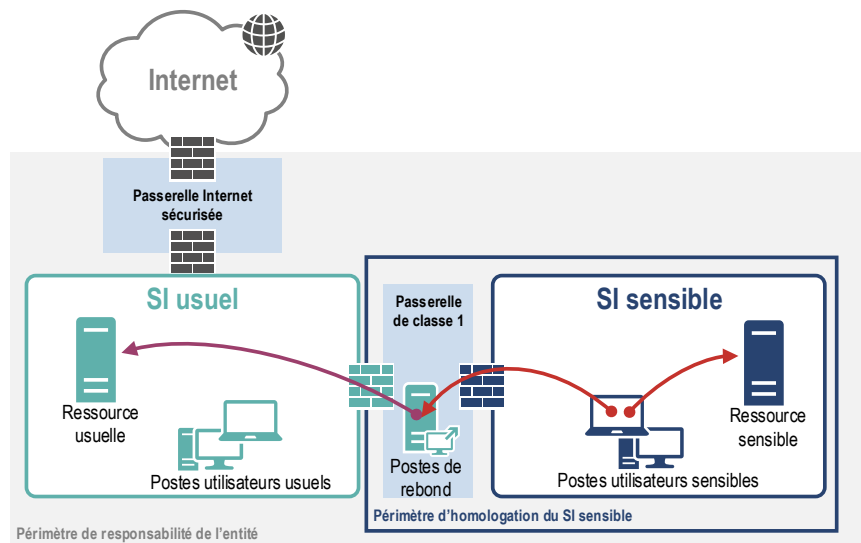


FIGURE 24 – Architecture recommandée : poste sensible physique avec accès distant à un environnement usuel virtualisé

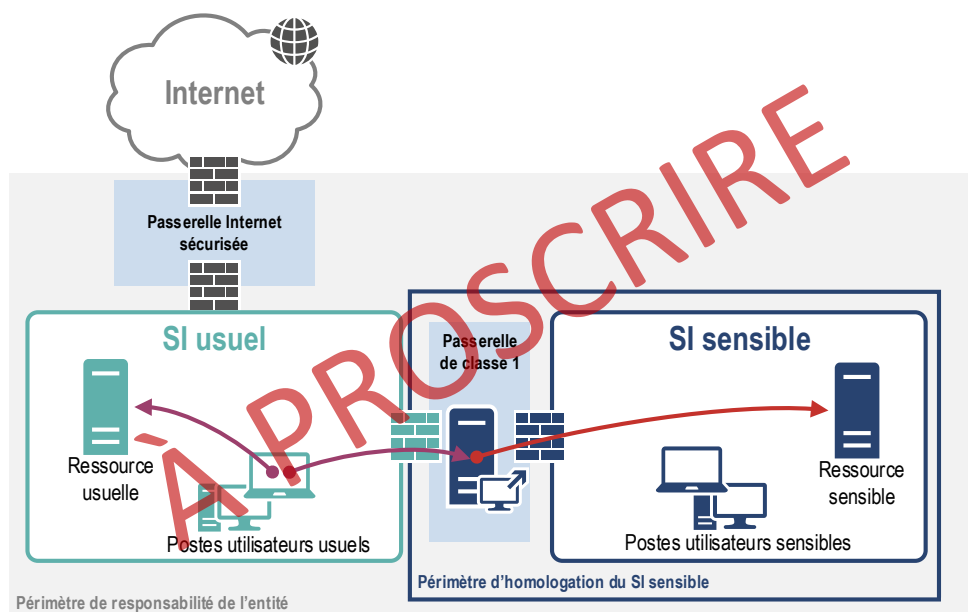


FIGURE 25 – Architecture interdite : poste usuel physique avec accès distant à un environnement sensible virtualisé

Dans le cas des deux recommandations dégradées R52- et R52--, les exigences suivantes s'appliquent :

- un filtrage des flux de connexion à distance vers le SI usuel doit être réalisé au moyen d'un pare-feu ;
- l'authentification de l'utilisateur sur le poste sensible doit être réalisée au moyen de l'annuaire dédié au SI sensible ;

- l'authentification de l'utilisateur sur le poste usuel doit être réalisée au moyen de l'annuaire dédié au SI usuel (voir la recommandation R7).

## 6.4 Nomadisme



### Information

Cette section concerne les accès nomades des utilisateurs à un SI sensible. Pour les accès nomades des administrateurs à un SI sensible, se reporter à la section 7.3 du chapitre 7 relatif aux bonnes pratiques d'administration d'un SI sensible.

Il peut être envisagé de mettre en œuvre un service de nomadisme sur un SI sensible, que celui-ci soit de classe 1 ou de classe 2.

Une première recommandation consiste à mettre en œuvre les bonnes pratiques relatives au nomadisme numérique détaillées dans le guide de l'ANSSI [22].

R53

### Appliquer les recommandations de l'ANSSI relatives au nomadisme numérique

Les recommandations publiées par l'ANSSI dans son guide relatif au nomadisme numérique [22] doivent être appliquées dès qu'un service de nomadisme est mis en production pour l'accès à distance à un SI sensible.



### Information

Le tableau de l'annexe D du présent guide met en correspondance les mesures de sécurité de l'II 901 relatives au nomadisme et les recommandations du guide ANSSI [22] dans sa version 1 d'octobre 2018.

Les paragraphes suivants ont pour but d'attirer l'attention du lecteur sur certaines recommandations du guide [22] particulièrement importantes dans un contexte d'usage sensible.

## Positionnement des concentrateurs VPN

Dans le cas d'un SI de classe 2 ou d'un SI de classe 1, il est nécessaire de mettre en place une architecture d'accès nomade suivant les recommandations du guide [22].

Dans le cas d'une architecture de classe 1, le concentrateur VPN des utilisateurs du SI sensible est hébergé au sein d'une *passerelle de classe 1*. Si l'entité a également la responsabilité d'un SI usuel, et qu'un service de nomadisme est mis en place sur ce SI, l'équipement de terminaison VPN des utilisateurs du SI usuel est obligatoirement distinct de l'équipement équivalent sur le SI sensible.



## Protection physique de l'équipement d'accès nomade

Par définition, un équipement d'accès nomade en situation de nomadisme ne bénéficie pas d'une protection physique équivalente à celle des équipements fixes. Pour réduire les risques d'atteinte à la confidentialité des données, des mesures physiques doivent être prises. Ainsi, un câble antivol et un filtre de confidentialité doivent être fournis avec chaque équipement d'accès nomade et les utilisateurs doivent être sensibilisés à leur utilisation <sup>103</sup>.

**R54**

### Protéger physiquement les équipements d'accès nomade

Les équipements d'accès nomade sensibles doivent être dotés de dispositifs physiques de protection (câble antivol, filtre de confidentialité). Ils ne doivent pas être laissés sans surveillance en dehors de leur période d'utilisation.

## Authentification des utilisateurs nomades

En plus de l'authentification forte de utilisateur (voir la recommandation R39), une authentification de l'équipement d'accès est recommandée. L'annexe D du guide [22] dans sa version 1.0 apporte des compléments d'informations sur les architectures d'authentification possibles.

## Protection du canal d'interconnexion nomade

Suivant le cas d'usage, SI de niveau DR ou de niveau sensible, les moyens de chiffrement mis en œuvre dans une infrastructure nomade (clients VPN et concentrateurs VPN) doivent être agréés DR (cas des SI DR) ou disposer d'un visa de sécurité (cas des SI sensibles) <sup>104</sup>.

**R55**

### Sécuriser les canaux d'interconnexion nomades des SI DR

Le canal d'interconnexion entre un équipement d'accès nomade DR, et une passerelle d'interconnexion permettant l'accès au SI DR, doit être sécurisé au moyen de produits de sécurité agréés DR.

**R56**

### Sécuriser les canaux d'interconnexion nomades des SI sensibles

Il est recommandé de sécuriser le canal d'interconnexion entre un équipement d'accès nomade sensible, et une passerelle d'interconnexion permettant l'accès au SI sensible, au moyen de produits de sécurité disposant d'un visa de sécurité.

103. Se reporter aux mesures de sécurité II 901 PDT-VEROUIL-PORT et PDT-NOMAD-FILT.

104. Se reporter à la mesure de sécurité II 901 PDT-NOMAD-ACCESS.

## Chiffrement des dispositifs de stockage nomades sensibles

Tous les dispositifs de stockage de données nomades sensibles (disques durs, clés USB, téléphones multifonctions...) doivent être chiffrés par des moyens de chiffrement agréés (s'agissant des données DR) ou disposant d'un visa de sécurité (s'agissant des données sensibles) <sup>105</sup>.



### Information

Les données stockées sur les disques durs des équipements d'accès nomade peuvent être chiffrées de deux manières, non exclusives l'une de l'autre. Il peut s'agir, d'une part, du chiffrement complet du disque dur <sup>106</sup> et, d'autre part, du chiffrement sélectif de certains fichiers <sup>107</sup>. Ces deux solutions techniques sont des réponses à des menaces différentes (protection en cas de perte ou vol, dans un cas ; protection du besoin d'en connaître dans l'autre). Une analyse des risques permet de déterminer laquelle de ces deux techniques (potentiellement les deux) doit être déployée.

R57

### Chiffrer les données DR stockées sur des supports amovibles

Les données DR stockées sur un support amovible doivent être chiffrées au moyen de produits de sécurité agréés DR.

R58

### Chiffrer les données sensibles stockées sur des supports amovibles

Les données sensibles stockées sur un support amovible doivent être chiffrées au moyen de produits de sécurité disposant d'un visa de sécurité.

Pour en savoir plus sur le sécurisation des supports de stockage amovibles, se reporter à la section 5.7.

## Blocage des flux locaux et mécanisme de détection de posture

Un équipement d'accès nomade sensible ne peut être attaché qu'à un seul SI sensible et peut être vu comme une extension de ce dernier. Pour ne pas devenir un pont incontrôlé entre le SI sensible et des SI non maîtrisés, il doit être, à tout instant, dans l'un ou l'autre de ces états : soit déconnecté de tout réseau, soit connecté à son SI sensible de rattachement. L'accès à des services hébergés par un SI tiers (typiquement la navigation Web) n'est possible que si les flux de communication transitent par la passerelle d'interconnexion du SI sensible avec le SI tiers.

<sup>105</sup>. Se reporter à l'article 17 de l'II 901 et aux mesures de sécurité II 901 PDT-NOMAD-STOCK et PDT-CHIFF-SENS.

<sup>106</sup>. Dans ce cas, la granularité de chiffrement est le volume logique. La saisie d'un secret est obligatoire pour pouvoir accéder au contenu du disque dur mais il est important de noter que toutes les données sont déchiffrables dès lors que ce secret a été fourni au système d'exploitation, rendant de fait possible l'accès potentiel d'un attaquant à l'ensemble des données du disque dur.

<sup>107</sup>. Dans ce cas, la granularité de chiffrement est le répertoire ou le fichier d'un système de fichiers. Les données chiffrées ne seront accessibles qu'après ouverture d'une session utilisateur et authentification de l'utilisateur auprès d'un logiciel tiers de chiffrement de données.

Les équipements nomades sont parfois configurés pour déterminer dynamiquement la nature des réseaux auxquels ils sont connectés, de manière à ensuite auto-adapter leur comportement (établir ou non un tunnel VPN avec leur SI d'appartenance, bénéficier de règles de flux du pare-feu local plus ou moins permissives...). Ces mécanismes dits de *détection de posture* ne peuvent pas être considérés comme suffisamment fiables pour en permettre l'usage dans un contexte sensible. Ils sont donc fortement déconseillés et la recommandation est de mettre en place deux concentrateurs VPN distincts : un pour les accès externes, l'autre pour les accès internes.

R59

### Chiffrer les flux réseau d'un équipement d'accès nomade sensible en toute circonstance

Il est fortement recommandé que tous les flux réseau nomades d'un SI sensible transitent par des concentrateurs VPN dédiés et soient encapsulés dans un tunnel VPN agréé DR (cas des SI DR) ou disposant d'un visa de sécurité ANSSI (cas des SI sensibles), que l'équipement d'accès nomade soit connecté directement au réseau local de son SI sensible d'appartenance ou indirectement, à distance. Le pare-feu local de l'équipement d'accès nomade doit bloquer tous les flux, à l'exception des flux nécessaires à l'établissement du tunnel<sup>108</sup>, et la fonctionnalité *split-tunneling* doit être désactivée par configuration des concentrateurs VPN sensibles.

Pour plus d'informations concernant les mécanismes de détection de posture, se reporter à la section 3.4.5 du guide [22] dans sa version 1.

## 6.5 Réseaux sans fil

Dans le cas des réseaux sensibles filaires, un utilisateur ne peut généralement accéder au SI sensible qu'après franchissement de barrières de protection physiques constituées de divers dispositifs (contrôle d'accès, vidéosurveillance, détection d'intrusion...). Ce principe de protection physique est invalidé dans le cas des réseaux sans fil, car les ondes radio peuvent se propager au-delà des barrières de protection physique.

Les risques induits par la mise en œuvre des réseaux sans fil s'en trouvent démultipliés : atteinte à la confidentialité des données sensibles transmises par écoute du réseau, déni de service, création de points d'accès sans fil pirates...

108. Se reporter à la mesure de sécurité II 901 PDT-NOMAD-PAREFEU.

Si la mise en œuvre d'un réseau sans fil s'avère nécessaire pour répondre aux impératifs opérationnels d'un SI sensible, l'approche la plus sécurisée consiste à considérer le réseau sans fil comme un réseau de transport qui n'est pas de confiance <sup>109</sup>. À ce titre, l'équipement d'accès sensible utilisant le réseau sans fil est considéré comme un poste nomade et respecte la recommandation R59 qui conseille de toujours faire transiter les flux par un tunnel VPN agréé DR (cas des SI DR) ou disposant d'un visa de sécurité ANSSI (cas des SI sensibles).

R60

### Mettre en place une architecture de réseau sans fil cloisonnée du SI sensible

La mise en œuvre des technologies de réseaux sans fil doit être justifiée par des impératifs opérationnels. Les flux sans fil doivent être sécurisés à l'aide d'un tunnel disposant d'un visa de sécurité ANSSI (cas des SI sensibles), ou d'un agrément ANSSI (cas des SI DR), et doivent transiter par une passerelle nomade suivant les recommandations de l'ANSSI portant sur le nomadisme numérique [22].

Le point d'accès sans fil peut être de nature diverse : une box ADSL, un point d'accès Wi-Fi public ou encore un réseau Wi-Fi déployé par l'entité pour fournir un accès à Internet à ses visiteurs, et dont un SSID peut être réservé pour ses propres utilisateurs nomades. Quelle que soit la nature du point d'accès sans fil, seuls les flux nécessaires à l'établissement du tunnel doivent être autorisés (voir l'explication sur le blocage des flux locaux détaillée à la section précédente). Cette restriction a pour conséquence de rendre impossible l'usage des portails captifs publics <sup>110</sup> (p. ex. accès sans fil proposé aux résidents d'un hôtel). Pour plus d'informations concernant les solutions sécurisées alternatives aux portails captifs publics, se reporter au chapitre 3.4.4 de la version 1 du guide ANSSI consacré au nomadisme numérique [22].

R61

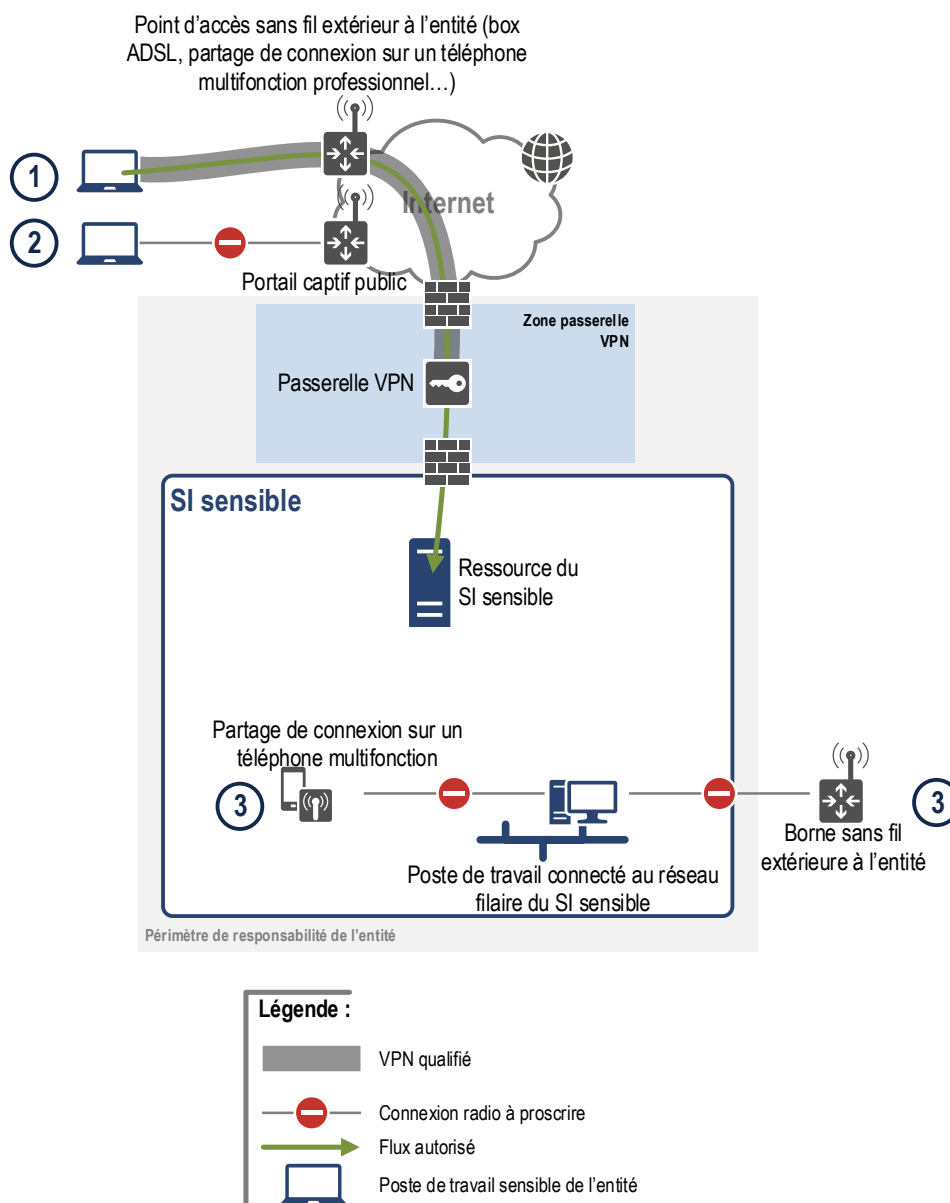
### Bloquer l'accès aux portails captifs depuis des équipements d'accès nomades sensibles

L'accès aux portails captifs publics doit être bloqué sur tout équipement d'accès nomade appartenant à un SI sensible.

Les figures 26 et 27 donnent des cas d'usage où la mise en œuvre de réseaux sans fil est envisageable pour des flux sensibles et des cas d'usage pour lesquels cette mise en œuvre est proscrite.

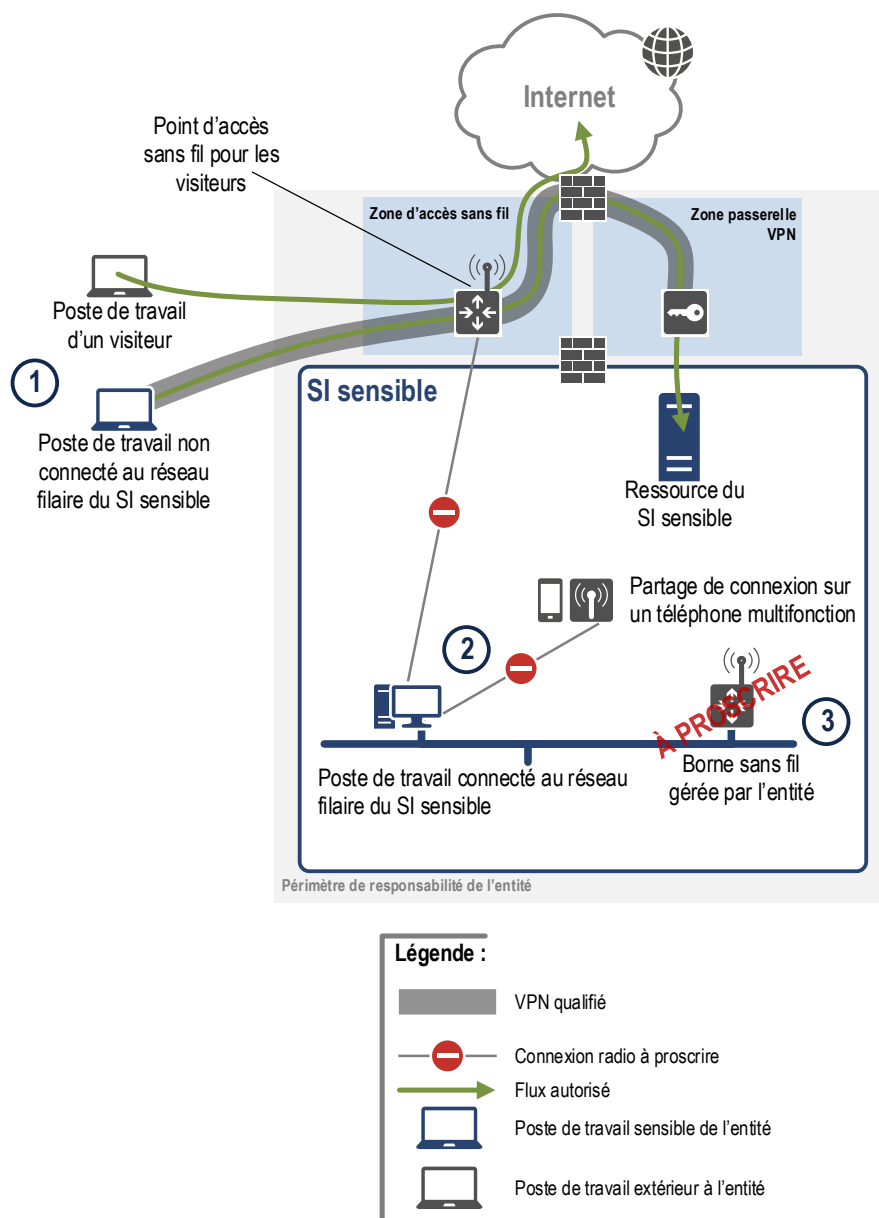
109. Se reporter à la mesure de sécurité II 901 RES-SSFIL.

110. Se reporter à la mesure de sécurité II 901 PDT-NOMAD-CONNEX.



- ① Cas nominal autorisé où le poste nomade établit une connexion sans fil avec un point d'accès sans fil extérieur à l'entité puis accède à des ressources du SI sensible exclusivement au travers d'un tunnel VPN disposant d'un visa de sécurité ANSSI (cas des SI sensibles) ou d'un agrément ANSSI (cas des SI DR).
- ② Les flux nécessaires pour l'établissement d'une connexion sans fil au travers d'un portail captif public sont bloqués rendant impossible ce cas d'usage.
- ③ Les postes sensibles (fixes ou portables) connectés par câble réseau au SI sensible ne doivent pas pouvoir établir de connexion sans fil (ni avec un téléphone multifonction ni avec une box sans fil extérieure à l'entité, dans l'exemple ci-dessus).

FIGURE 26 – Architecture de réseau sans fil : les points d'accès sans fil ne sont pas maîtrisés par l'entité responsable du SI sensible



- ① Si l'entité met en œuvre une zone d'accès sans fil (typiquement pour fournir un accès Internet à ses visiteurs), il est possible de dédier un SSID pour les utilisateurs nomades du SI sensible. Ce cas d'usage est comparable au cas 1 de la figure 26 et les mêmes prérequis techniques de sécurisation s'appliquent.
- ② Comme dans le cas 3 de la figure 26, les postes sensibles connectés au réseau filaire ne doivent pas pouvoir établir une bi-connexion avec un point d'accès sans fil, même si celui-ci est mis en œuvre par l'entité responsable du SI sensible (ni avec un téléphone multifonction ni avec le point d'accès Internet pour les visiteurs, dans l'exemple ci-dessus).
- ③ L'entité responsable d'un SI sensible ne doit pas mettre en œuvre de point d'accès sans fil qui serait connecté directement au réseau sensible, sans filtrage.

FIGURE 27 – Architecture de réseau sans fil : les points d'accès sans fil sont maîtrisés par l'entité responsable du SI sensible

# 7

## Administration des SI sensibles



### Objectif

Ce chapitre présente les bonnes pratiques d'administration applicables à tout SI sensible. Ces bonnes pratiques ne sont pas spécifiques aux SI sensibles, mais correspondent à celles attendues pour la protection de tout SI administré à l'état de l'art.

### 7.1 Généralités

Le respect des bonnes pratiques d'administration est un point très important pour tout SI, à plus forte raison si celui-ci est sensible <sup>111</sup>. Les actions d'administration doivent être réservées au personnel dûment autorisé et depuis des moyens dédiés. L'ANSSI a publié un guide [25] indiquant les bonnes pratiques applicables à l'administration sécurisée d'un SI.

R62

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

Le responsable d'un SI sensible doit respecter les recommandations du guide relatif à l'administration sécurisée des SI [25].



### Information

Le tableau de l'annexe E du présent guide met en correspondance les mesures de sécurité de l'II 901 relatives à l'administration des systèmes et les recommandations du guide de bonnes pratiques publié par l'ANSSI [25] dans sa version 2 d'avril 2018.



### Information

Le SI d'administration d'un SI sensible constitue un sous-ensemble du SI sensible. Il doit de fait être homologué au même niveau que le SI sensible.

Les administrateurs ayant des droits étendus, ils ont un accès potentiel à un nombre important de données sensibles ou DR. L'obtention, pour chacun d'entre eux, d'une habilitation individuelle d'un niveau permettant l'accès à des informations relevant du secret de la défense nationale peut être requise par le responsable du SI sensible.

L'habilitation des administrateurs concerne en premier lieu les administrateurs des composants de l'infrastructure, et non les administrateurs fonctionnels ou « métier ». En outre, parmi les

<sup>111</sup>. Se reporter à l'objectif 22 de l'II 901.

administrateurs d'infrastructure, il est fortement recommandé d'exiger une habilitation pour ceux disposant des plus hauts niveaux de privilèges. Cela concerne deux grandes familles d'administrateurs :

- les administrateurs disposant de privilèges sur l'ensemble du SI, et ayant une capacité à outrepasser leurs droits et à effacer les traces de leurs actions ;
- les administrateurs disposant de privilèges sur de nombreuses ressources centrales (serveurs, moyens de stockage...) ou de sécurité.

R63

### Gérer les administrateurs d'un SI sensible

La liste des administrateurs autorisés à opérer sur un SI sensible doit être limitée au juste besoin, connue et validée par l'autorité d'homologation <sup>112</sup>. Il est en outre recommandé que les administrateurs d'un SI DR soient détenteurs d'une habilitation individuelle, d'un niveau permettant l'accès à des informations relevant du secret de la défense nationale, en particulier si leurs privilèges sur le SI sont étendus.

## 7.2 SI d'administration

Cette section donne le positionnement des SI d'administration pour les trois architectures présentées au chapitre 3 relatif aux typologies de SI sensibles.

---

112. Se reporter à la mesure de sécurité II 901 EXP-HABILIT-ADMIN.



## 7.2.1 Cas des SI sensibles physiquement isolés

Dans le cas de l'architecture « SI sensible physiquement isolé » (voir la section 3.2.1), deux SI d'administration distincts sont déployés pour permettre l'administration du SI sensible, d'une part, et du SI usuel, d'autre part. Les postes d'administration et les serveurs outils d'administration<sup>113</sup> utilisés pour l'administration du SI sensible sont physiquement distincts de ceux utilisés pour l'administration du SI usuel.

La figure 28 donne le positionnement des SI d'administration dans le cas d'une architecture « SI sensible physiquement isolé ».

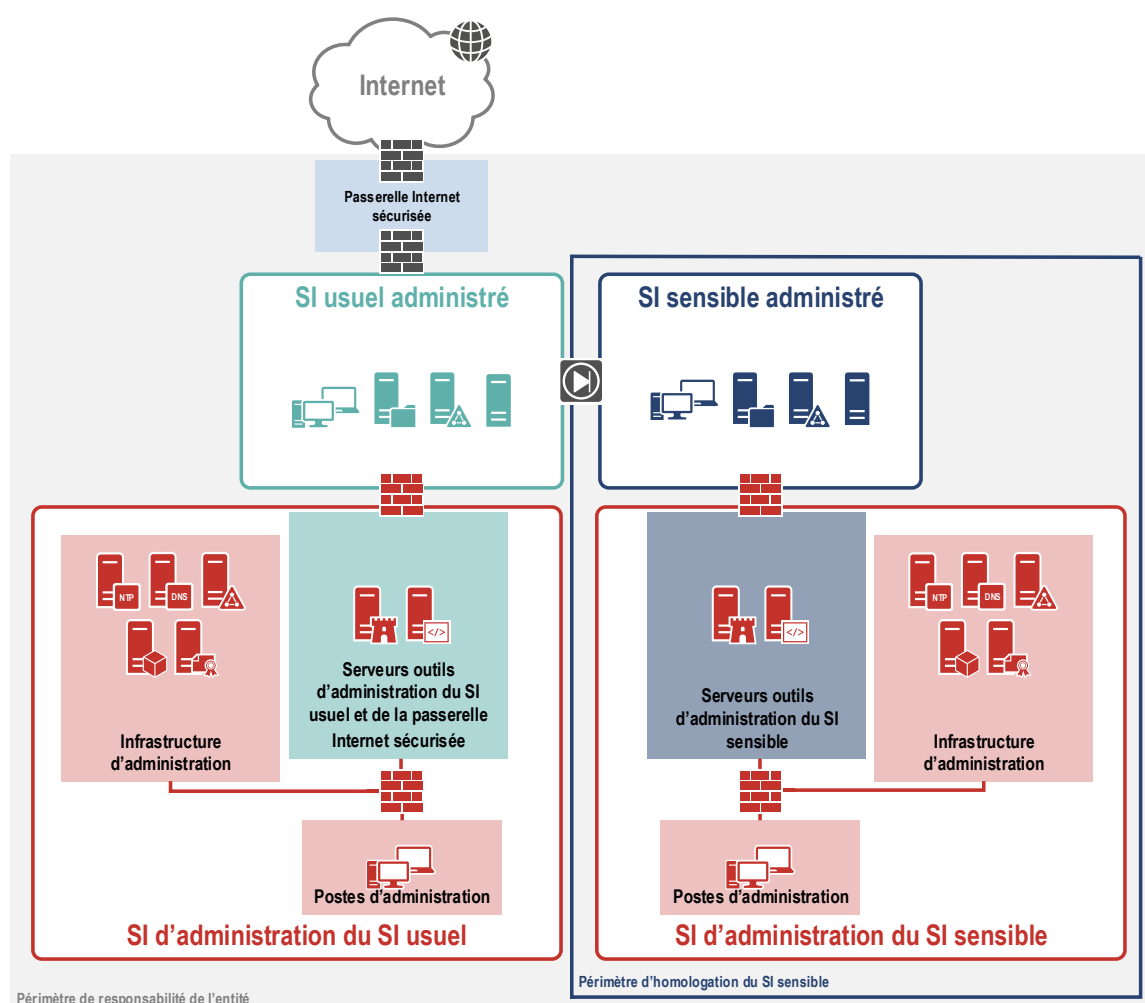


FIGURE 28 – SI sensible de classe 2 - Positionnement du SI d'administration dans le cas d'un « SI sensible physiquement isolé »

113. Les *serveurs outils d'administration* désignent les serveurs dédiés à l'exécution des outils d'administration proposés par des éditeurs ou des équipementiers (p. ex. client lourd ou service Web interagissant avec les ressources administrées). Pour en savoir plus sur les *serveurs outils d'administration*, se reporter à la section 6.1 du guide de l'ANSSI relatif aux pratiques d'administration sécurisée [25] dans sa version 2.

## 7.2.2 Cas des SI sensibles physiquement cloisonnés

Dans le cas de l'architecture « SI sensible physiquement cloisonné » (voir la section 3.2.2), deux SI d'administration distincts sont déployés pour permettre l'administration du SI sensible, d'une part, et du SI usuel, d'autre part. Les postes d'administration et les outils d'administration utilisés pour l'administration du SI sensible sont physiquement distincts de ceux utilisés pour l'administration du SI usuel.

La figure 29 donne le positionnement du SI d'administration dans le cas d'une architecture « SI sensible physiquement cloisonné ».

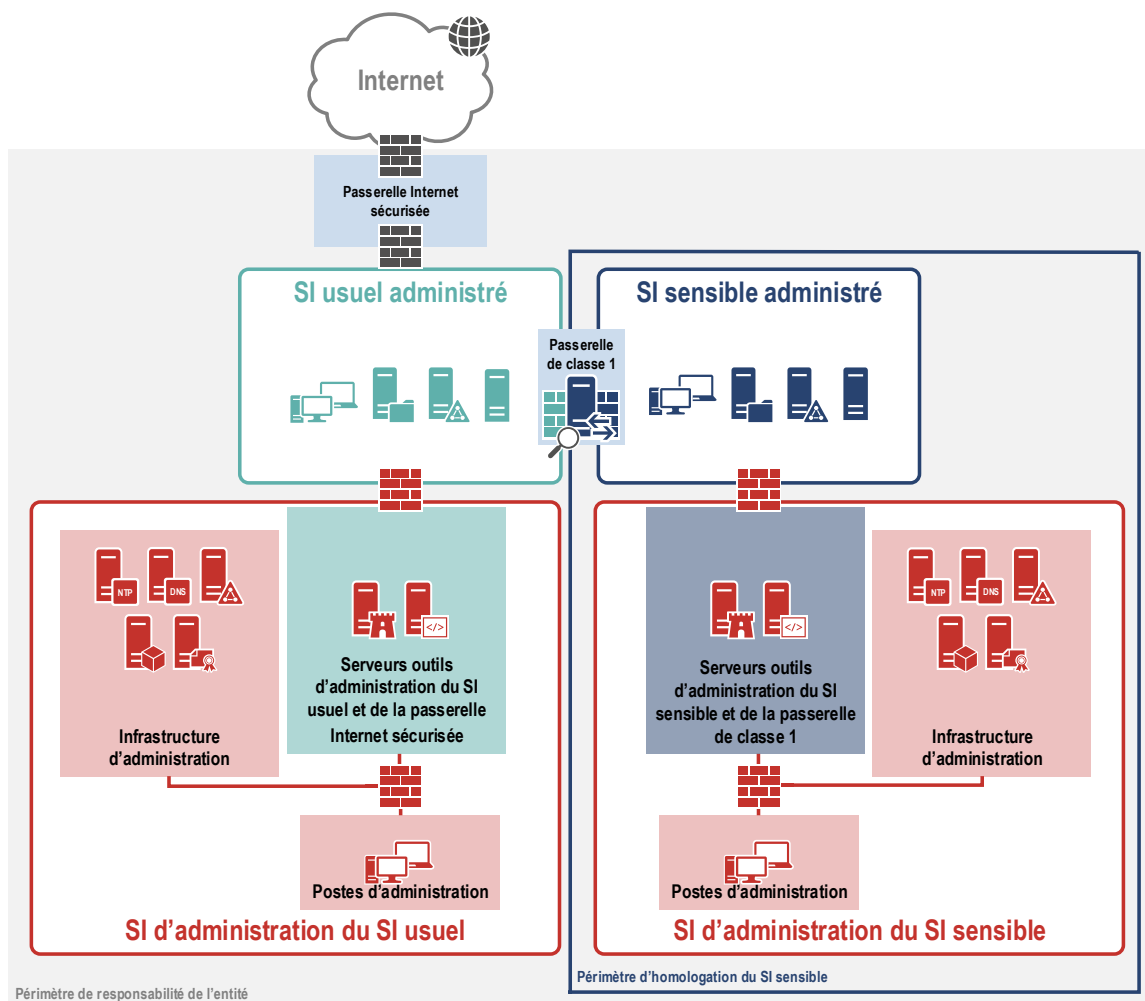


FIGURE 29 – SI sensible de classe 1 - Positionnement du SI d'administration dans le cas d'un « SI sensible physiquement cloisonné »

Il est possible d'utiliser un poste d'administration unique pour administrer des ressources d'un SI sensible de classe 1 et des ressources d'un SI usuel (voir la figure 30). Les conditions de cette mutualisation sont explicitées à la section 12.2 du guide [25] dans sa version 2. Ces conditions imposent en particulier que les serveurs outils mis en œuvre pour l'administration de SI de niveaux de

sensibilité différents (typiquement niveau sensible et niveau usuel) doivent être dédiés par niveau de sensibilité et cloisonnés entre eux.

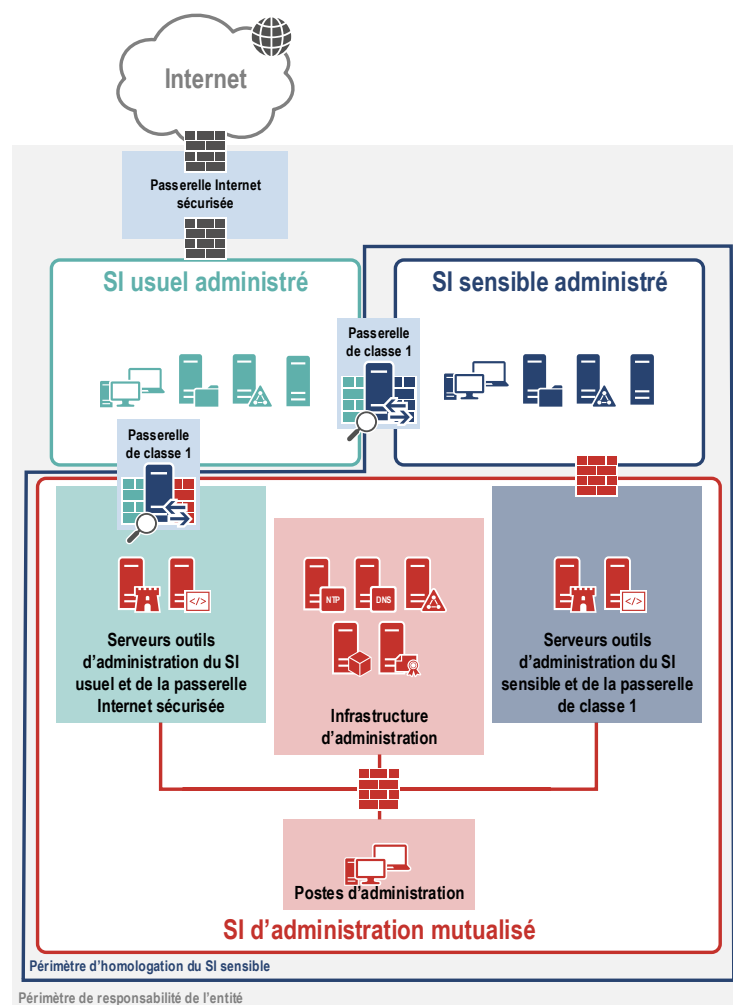


FIGURE 30 – SI sensible de classe 1 - Exemple de mutualisation du SI d'administration dans le cas d'un « SI sensible physiquement cloisonné »

### 7.2.3 Cas des SI sensibles sans SI usuel

Dans le cas de l'architecture « SI sensible sans SI usuel » (voir la section 3.2.3), la mutualisation des postes d'administration est possible. En revanche, les outils d'administration doivent être dédiés par SI : des outils d'administration pour le SI usuel et d'autres outils d'administration pour le SI sensible.

La figure 31 donne le positionnement du SI d'administration dans le cas d'une architecture « SI sensible sans SI usuel ».

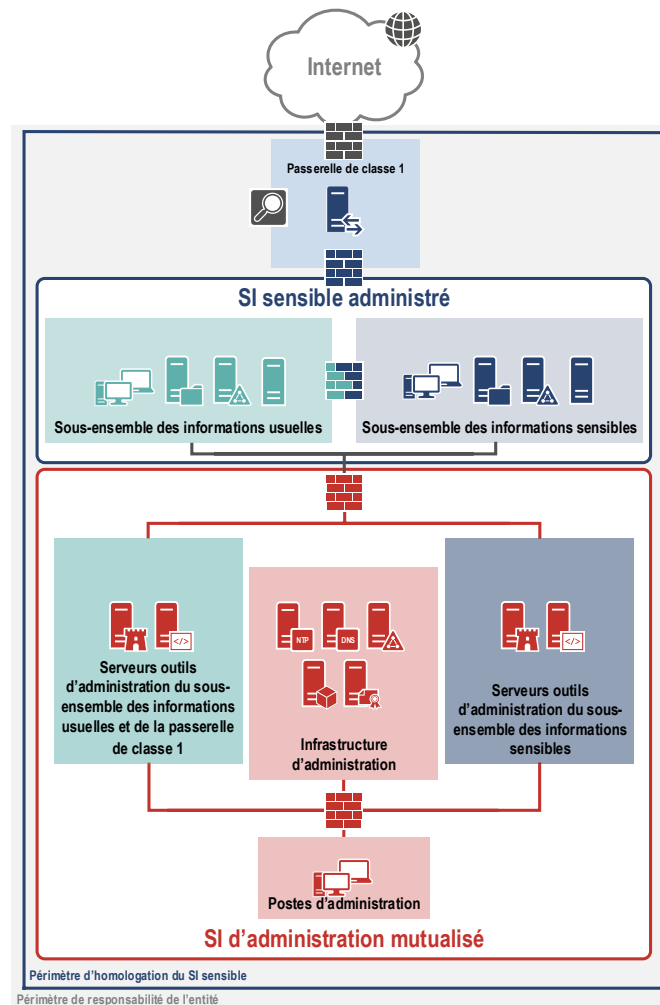


FIGURE 31 – SI sensible de classe 1 - Positionnement du SI d'administration dans le cas d'un « SI sensible sans SI usuel »

## 7.3 Administration à distance

Conformément aux recommandations du guide [25], les postes d'administration utilisés pour ces accès à distance doivent être gérés et sécurisés par l'entité responsable du SI sensible. En outre, le concentrateur VPN IPsec doit être dédié à l'administration à distance et placé au plus près du SI d'administration. Il est hébergé au sein d'une *passerelle de classe 1* et l'architecture permet de garantir que les flux d'administration déchiffrés au niveau de cette passerelle restent cloisonnés des flux de production du SI sensible <sup>114</sup>.

R64

### Sécuriser la chaîne de connexion pour l'administration à distance

Si un service d'administration à distance est autorisé pour un SI sensible, les accès doivent être effectués depuis des postes d'administration maîtrisés et les flux doivent être sécurisés au moyen d'un tunnel VPN IPsec. Le concentrateur VPN, dédié au service d'administration à distance, doit être agréé (cas des SI DR) ou disposer d'un visa de sécurité (cas des SI sensibles). Le protocole IPsec doit être configuré suivant les recommandations du guide de l'ANSSI [17]. Le pare-feu local d'un poste d'administration doit bloquer tous les flux, à l'exception des flux nécessaires à l'établissement du tunnel, et la fonctionnalité *split-tunneling* doit être désactivée par configuration du concentrateur VPN.

Un cas particulier de l'administration à distance est la télémaintenance. La télémaintenance concerne les accès à distance d'une personne à des moyens métier, avec un compte doté de privilèges élevés sur ces moyens (p. ex. accès à des logiciels métier spécifiques par des experts de l'éditeur). Dans certains cas de télémaintenance, il peut être difficile pour l'entité responsable d'un SI sensible de maîtriser le poste d'administration utilisé pour cet accès à distance. En conséquence, tout accès de ce type doit faire l'objet d'une analyse des risques spécifique et des mesures techniques ou organisationnelles doivent être mises en œuvre pour réduire le risque d'intrusion ou d'exfiltration (p. ex. absence de connexion permanente mais ouverture ponctuelle de l'accès, obligation pour l'administrateur de se connecter à une machine temporaire intermédiaire qui est réinitialisée après toute utilisation...).

Les procédures de télémaintenance doivent toujours être établies sous contrôle de l'entité responsable (directement ou indirectement par la mise en place de clauses contractuelles). L'ANSSI a publié un guide [13] portant sur la maîtrise des risques liés à l'infogérance.

R64 -

### Maîtriser les systèmes de télémaintenance connectés à des SI sensibles

Les interconnexions de télémaintenance font l'objet d'une analyse des risques spécifique et des mesures de réduction des risques sont mises en œuvre.

## 7.4 Maintien en condition de sécurité (MCS)

Les composants d'un SI sensible doivent être régulièrement mis à jour pour corriger les vulnérabilités qui les affectent. L'entité mettant en œuvre un SI sensible doit formaliser une politique de

<sup>114</sup>. Se reporter à la mesure de sécurité II 901 EXP-SEC-FLUXADMIN.

MCS qui précise, pour chaque composant, les modalités de déploiement des mises à jour de sécurité <sup>115</sup> (fréquence, dépendances systèmes, tests de non régression...). Ces modalités sont notamment dépendantes de l'exposition du composant, de sa criticité métier et de ses contraintes de disponibilité opérationnelle.

**R65**

### Définir et appliquer une politique de MCS

Le responsable d'un SI sensible établit une politique permettant le maintien en condition de sécurité des composants du SI et de son SI d'administration. Cette politique précise notamment les fréquences de déploiement et les procédures de test des mises à jour de sécurité. Il est recommandé de déployer les mises à jour de sécurité critiques sous un délai d'une semaine et les autres mises à jour de sécurité sous un délai de quatre semaines.

Cette politique, pour être efficace, suppose que l'entité responsable du SI sensible en maintienne à jour la cartographie, incluant l'inventaire des ressources mises en œuvre <sup>116</sup>.

Il est recommandé de structurer un SI sensible en zones de confiance d'un niveau de sécurité homogène (voir la recommandation [R32](#)). Un des critères d'homogénéité concerne la capacité de l'entité à maintenir à jour les composants de cette zone. Pour y parvenir, le recours à des outils centralisés est recommandé <sup>117</sup>.

Toute action permettant de réduire la probabilité de devoir gérer des systèmes obsolètes doit être recherchée. En particulier, l'entité responsable d'un SI sensible doit être particulièrement vigilante à intégrer, dans les contrats qui la lient avec des éditeurs de solutions matérielles ou logicielles, des clauses de maintien en condition de sécurité <sup>118</sup>.

Malgré les efforts déployés par l'entité, des systèmes obsolètes peuvent subsister. Ces systèmes, qui ne sont plus maintenus en condition de sécurité, doivent être isolés du SI sensible et ne partager aucune ressource avec lui <sup>119</sup>.

Il n'est pas possible de donner ici de recommandations génériques concernant la mise en pratique de cette isolation. La réponse technique est en effet différente suivant la portée de l'obsolescence (concerne-t-elle uniquement des composants serveur ou bien également des composants clients?), le niveau d'intégration des systèmes obsolètes (couplage fort ou faible avec d'autres composants du SI?), le nombre d'utilisateurs concernés et leur répartition géographique...

**R66**

### Isoler les systèmes obsolètes

Les systèmes obsolètes conservés en production pour répondre à des besoins métier justifiés doivent être isolés du SI sensible. La manière de réaliser cette isolation doit faire l'objet d'une étude spécifique.

<sup>115</sup>. Se reporter à la mesure de sécurité II 901 EXP-POL-COR.

<sup>116</sup>. Se reporter à l'article 9 de l'II 901 et aux mesures de sécurité II 901 GDB-INVENT, GDB-CARTO et RES-CARTO.

<sup>117</sup>. Se reporter à la mesure de sécurité II 901 EXP-CENTRAL.

<sup>118</sup>. Se reporter à la mesure de sécurité II 901 INT-REX-HS.

<sup>119</sup>. Se reporter aux mesures de sécurité II 901 EXP-OBSOLETE et EXP-ISOL.

## 7.5 Journalisation et supervision de sécurité

La collecte des journaux, et la mise en œuvre d'un système de détection qualifié (voir la section 4.3.1), ne présentent que peu d'intérêt si elle ne s'accompagne pas d'une supervision active et permanente, réalisée par des professionnels de la détection d'incidents de sécurité. Aussi, la politique de journalisation doit être intimement liée à la stratégie de supervision.

Venant compléter le guide relatif aux bonnes pratiques d'administration [25], l'ANSSI a publié un guide de bonnes pratiques concernant la journalisation des systèmes informatisés [26] dont l'application est nécessaire dans le cadre de la mise en œuvre d'un SI sensible.

R67



### Appliquer les recommandations de l'ANSSI relatives à la journalisation

Les bonnes pratiques d'architecture et de configuration des fonctionnalités de journalisation des événements de sécurité formulées par l'ANSSI [26] doivent être appliquées.

Les journaux système et de sécurité d'un SI sensible doivent être conservés pendant une durée de douze mois glissants<sup>120</sup>. Leur collecte et leur conservation sur cette durée visent à accroître l'efficacité de détection du SOC<sup>121</sup> pour :

- déclencher des alertes de sécurité en cas de mise en correspondance d'événements de sécurité avec des règles de détection définies par la supervision de sécurité;
- améliorer la capacité à qualifier les alertes levées (distinguer les faux positifs des vrais positifs) par analyse d'événements bruts (événements n'ayant pas nécessairement été corrélés par des règles de détection);
- rechercher des événements suspects *a posteriori* (p. ex. recherche de nouveaux marqueurs de compromission<sup>122</sup> dans des données passées; application de nouvelles règles dans les journaux archivés...).

R68



### Conserver les journaux d'un SI sensible pendant 12 mois

Les journaux des événements de sécurité doivent être conservés pendant douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Les journaux étant collectés, la supervision de sécurité a pour objet de déclencher des alertes en réponse à la détection de scénarios de menace pré-établis, qu'il s'agisse d'attaques non ciblées et opportunistes ou d'événements redoutés dans un contexte métier particulier.

Dans ce processus d'élaboration de la stratégie de supervision, le responsable du SI s'assure que les données nécessaires à la détection sont bien générées, collectées et centralisées. Si ce n'est pas le cas, un processus d'amélioration doit être mis en place afin de pallier ces lacunes. Seule une logique itérative de ce type permet d'augmenter dans le temps la couverture de détection.

120. Se reporter à la mesure de sécurité II 901 EXP-CONS-JOUR.

121. *Security operation center*, en anglais.

122. Plus d'informations concernant les indicateurs de compromission sont disponibles à la section 4.3.1.

Il est recommandé à une entité mettant en œuvre un SI sensible de recourir aux services d'un prestataire de détection des incidents de sécurité (PDIS) qualifié par l'ANSSI <sup>123</sup>.

Le service de détection peut-être assuré par l'entité responsable du SI sensible à superviser ou bien par une société externe <sup>124</sup>.

À défaut de faire appel aux services d'un prestataire qualifié, il est recommandé au responsable d'un SI sensible de s'inspirer des bonnes pratiques décrites dans le référentiel d'exigences PDIS [29] pour la conception, le déploiement et l'exploitation du système de supervision.

**R69**

## Recourir aux services d'un prestataire qualifié pour la supervision de sécurité

Il est fortement recommandé que le responsable d'un SI sensible fasse appel à un prestataire de détection des incidents de sécurité (PDIS) qualifié par l'ANSSI pour mettre en place une supervision de sécurité. À défaut de souscrire aux services d'un prestataire externe, un service de supervision interne doit être mis en place par l'entité et ce service doit être conçu en s'inspirant des bonnes pratiques décrites dans le référentiel d'exigences PDIS.



## Information

Le référentiel d'exigences pour la qualification d'un PDIS impose que les données manipulées par le prestataire soient protégées au niveau Diffusion Restreinte <sup>125</sup>. En conséquence, l'architecture de détection mise en œuvre par le prestataire constitue un SI homologué de niveau DR <sup>126</sup>.

Que le SI sensible fasse l'objet d'une supervision de sécurité par un prestataire qualifié ou par l'entité responsable du SI sensible, les incidents de sécurité doivent être signalés à l'ANSSI dès leur survenue <sup>127</sup>.

**R70**

## Formaliser une procédure de déclaration des incidents de sécurité à l'ANSSI

Le responsable d'un SI sensible doit formaliser une procédure de déclaration des incidents de sécurité à l'ANSSI. Ces déclarations concernent en particulier les incidents dépassant ou susceptibles de dépasser le périmètre du SI sensible et ceux relatifs à des alertes de sécurité (notamment les alertes émises par le CERT-FR <sup>128</sup>).

123. Se reporter à l'article 16 de l'II 901.

124. Se reporter au chapitre III.1 du référentiel d'exigences des PDIS [29] dans sa version 2.0 de décembre 2017. La liste des PDIS qualifiés ou en cours de qualification est disponible sur le site Web de l'ANSSI [32].

125. Ces données intègrent notamment les documents transmis par le commanditaire, les informations collectées, les indicateurs de compromission, les constats, les mains courantes, les différents registres, la feuille de route et les rapports d'analyse.

126. Se reporter au référentiel d'exigences relatif aux PDIS [29] dans sa version 2.0 de décembre 2017 : IV.3.2. c) *Le SI du service de détection doit être homologué au minimum au niveau Diffusion Restreinte pour superviser les systèmes d'information non classifiés de défense du commanditaire.*

127. Se reporter à la mesure de sécurité II 901 TI-INC-REM.

128. Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. Site Web : <https://www.cert.ssi.gouv.fr/>.



# Annexe A

## Informations sensibles, DR et usuelles - Explications détaillées

Cette annexe est un complément au chapitre 2 où sont définis les SI sensibles et les SI usuels. Elle est structurée en deux parties. Dans une première section, les termes « informations sensibles », « informations DR » et « informations usuelles » sont définis. Puis une seconde section permet de comprendre quelles sont les différences d'ordre juridique entre ces types d'informations.

### A.1 Définitions

#### Patrimoine informationnel numérique

Toute personne morale, publique ou privée, est responsable d'un ensemble d'informations numériques, qu'il est possible de qualifier *patrimoine informationnel numérique*. Ces informations sont traitées sur un ou plusieurs systèmes d'information (SI). Un sous-ensemble de ce patrimoine est constitué d'informations publiques : il s'agit des informations pour lesquelles le besoin de sécurité en confidentialité est, par définition, nul <sup>129</sup>.

La figure 32 donne une représentation symbolique du patrimoine informationnel et des informations publiques.

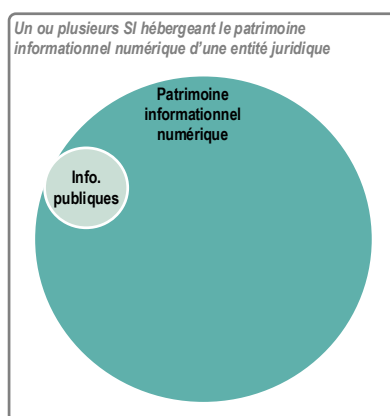


FIGURE 32 – Représentation symbolique du patrimoine informationnel d'une entité juridique

129. Si le besoin de sécurité en confidentialité est nul pour les informations publiques, ce n'est pas la cas pour les besoins de sécurité en intégrité et en disponibilité de ces données ou des SI qui les hébergent.

Cette représentation va être utilisée dans cette annexe comme un fil conducteur pour expliquer l'imbrication des niveaux de sensibilité des informations.

## Informations sensibles

L'II 901, le texte de référence régissant en France la protection des systèmes d'information sensibles, donne cette définition des informations sensibles <sup>130</sup> :



### Informations sensibles

*Les informations sensibles sont celles dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en œuvre.*



### Information

En ayant comme objectif principal de définir les règles de gestion et de protection en *confidentialité* de certaines *informations*, l'II 901 se distingue en cela d'autres réglementations qui visent en premier lieu à assurer que les *traitements* opérés sur un SI soient *intègres* et *disponibles*. Des exemples de ces réglementations sont la loi de programmation militaire 2014-2019 (qui définit la notion de système d'information d'importance vitale ou SIIV) ou encore la directive européenne sur la sécurité des réseaux et des systèmes d'information, dite « directive NIS » (qui définit la notion de système d'information essentiel ou SIE).

Les informations sensibles constituent un sous-ensemble du patrimoine informationnel numérique. La figure 33 illustre ce point.

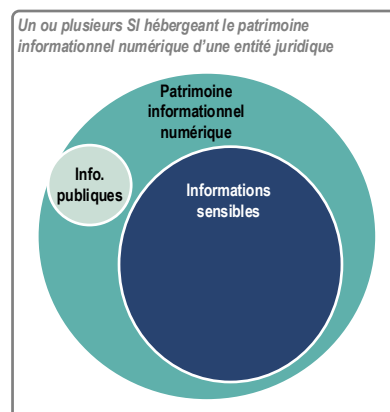


FIGURE 33 – Représentation symbolique des informations sensibles, sous-ensemble du patrimoine informationnel d'une entité juridique

## Informations Diffusion Restreinte (DR)

La notion d'information Diffusion Restreinte est introduite dans l'annexe 3 de l'IGI 1300 [1]. Ce texte précise que les règles applicables aux SI ayant ce niveau de sensibilité sont définies dans

130. Se reporter à l'article 1<sup>er</sup> de l'II 901.

l’II 901 [28]. Ces règles de protection ne sont pas limitées à une communauté d’intérêt mais applicables à toute entité publique ou privée française <sup>131</sup>.



## Informations Diffusion Restreinte (définition de l’II 901)

*Les informations Diffusion Restreinte (DR) sont les informations sensibles (telles que définies précédemment) portant la mention Diffusion Restreinte ou ses équivalences européennes ou internationales <sup>132</sup>.*

Dans l’II 901, l’objectif de protection de la confidentialité des informations est exacerbé dans le cas des informations marquées Diffusion Restreinte. L’utilisation de ce qualificatif explicite la nécessaire restriction de diffusion de ces informations. Les informations DR ne doivent pas être rendues publiques. Elles peuvent être communiquées aux seules personnes ayant le *besoin d’en connaître*, c’est-à-dire aux personnes ayant une nécessité impérieuse d’accéder aux informations pour mener à bien des missions qui leur sont confiées dans le cadre de leurs fonctions.

En France, contrairement à certaines réglementations internationales, la mention Diffusion Restreinte n’est pas un niveau de classification du secret de la défense nationale, mais une mention de protection. Elle ne confère pas à l’information la protection pénale propre aux informations classifiées relevant du secret de la défense nationale. Néanmoins, une personne divulguant des informations Diffusion Restreinte s’expose à des sanctions disciplinaires <sup>133</sup>, voire à l’engagement de sa responsabilité financière.

Les informations Diffusion Restreinte (DR) sont un sous-ensemble des informations sensibles. La figure 34 illustre ce point.

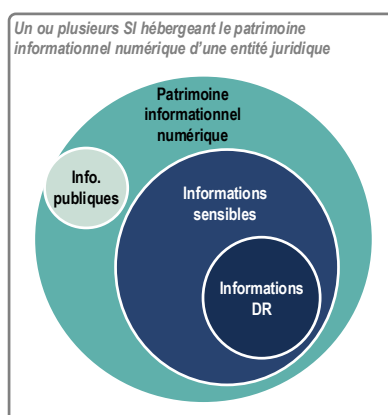


FIGURE 34 – Représentation symbolique des informations DR au sein du patrimoine informationnel d’une entité juridique

131. Les mentions de restriction de diffusion équivalentes à Diffusion Restreinte attribuées à des documents par des États étrangers ou des organisations internationales ont pour effet de soumettre ces documents aux règles de protection décrites à l’article 5 et à l’annexe 3 de l’IGI 1300 et dans l’II 901. À noter que l’équivalent des informations DR dans certaines réglementations (p. ex. *EU Restricted*, *NATO Restricted*) constituent des informations classifiées.

132. Se reporter à l’article 1<sup>er</sup> de l’II 901.

133. Par exemple, se reporter à l’article L. 4121-2 du code de la défense pour les militaires et à l’article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.

Les informations (et, le plus souvent, les supports physiques de ces informations) sont explicitement marquées DIFFUSION RESTREINTE. L'intérêt de ce marquage est de transférer la responsabilité de la gestion et de la protection de ces informations sensibles particulières à l'entité juridique réceptrice de telles informations, sous réserve des éventuelles dispositions contractuelles applicables entre l'entité émettrice et l'entité réceptrice. Pour plus d'informations concernant le marquage des informations et des supports de données, se reporter à la section 5.4.

Les utilisateurs d'un SI sensible, ayant un besoin justifié de traiter des informations sensibles voire Diffusion Restreinte, doivent être informés par l'entité responsable du SI du besoin de confidentialité de ces informations. Ils doivent en outre être sensibilisés aux obligations applicables pour le traitement de ces informations et à la déclinaison pratique de ces obligations au sein de l'entité.

En cas de transmission de données Diffusion Restreinte à un tiers, il convient de préciser les règles de sécurité devant être appliquées par celui-ci pour protéger ces données, notamment dans le cadre d'une convention. Une telle convention peut se contenter de lui imposer le respect de l'II 901, ou être plus détaillée et contraignante.

Enfin, certaines informations DR peuvent en outre être marquées Spécial France (SF). Dans ce cas, l'entité responsable d'un SI DR hébergeant des données DR SF doit mettre en œuvre les moyens de contrôle d'accès logique et les moyens organisationnels permettant de garantir que celles-ci ne soient rendues accessibles qu'aux seuls ressortissants français <sup>134</sup>.

## Informations usuelles

Une difficulté est de pouvoir nommer le sous-ensemble des informations qui ne sont ni des informations sensibles au sens de l'II 901 ni des informations publiques (librement accessibles à tous, sans authentification préalable). Une tentation pourrait être de désigner ce sous-ensemble par l'expression « informations non sensibles ». Mais ces informations présentent néanmoins un certain niveau de sensibilité et demandent donc un niveau de protection : l'entité qui en est responsable ne concevrait pas de les laisser accessibles sans aucune protection.

En conséquence, l'expression « informations non sensibles » n'est pas utilisée dans ce guide. Les informations qui ne sont ni sensibles au sens de l'II 901, ni publiques sont désignées « informations usuelles » et ce sous-ensemble d'informations est représenté par la surface de couleur rouge sur la figure 35.

---

134. Se reporter à l'article 65 de l'IGI 1300.

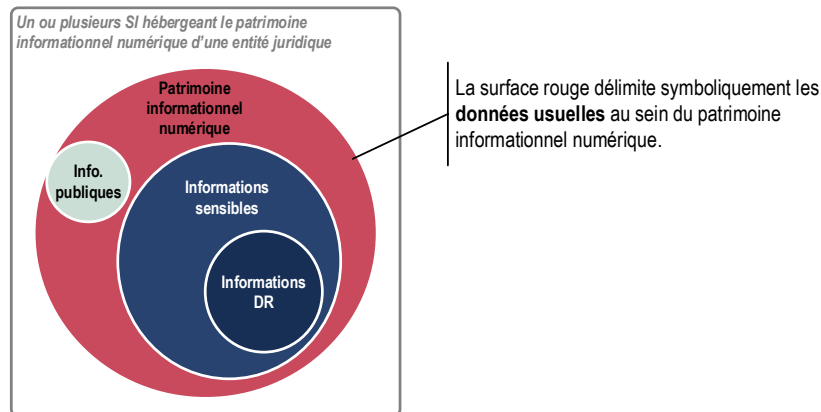


FIGURE 35 – Représentation symbolique des informations usuelles : informations ni sensibles, ni publiques

## A.2 Différences d'ordre juridique entre les informations DR et les informations non DR

L'intérêt, pour le créateur d'une information, de la qualifier Diffusion Restreinte est de soumettre l'ensemble des personnes amenées à la manipuler à une restriction de diffusion (voir la définition des informations DR en A.1). Cette qualification permet en outre de propager cette restriction de diffusion lors du transfert de l'information vers une autre entité juridique. Cette dernière doit assurer la continuité de la protection des informations DR reçues en traitant les informations DR déchiffrées sur un SI où les mesures de sécurité propres à la protection des informations DR sont mises en œuvre.

Les informations sensibles, qui ne sont pas des informations DR, sont des informations protégées par un régime propre à l'entité qui les élabore. Le choix des termes utilisés pour qualifier ces informations est laissé libre à l'entité mettant en œuvre ce régime de protection. À titre d'illustration, les désignations suivantes sont des exemples de mentions de protection des informations qui peuvent être choisies par une entité pour protéger ses données sensibles non DR : DIFFUSION LIMITÉE, LIMITÉ SOCIÉTÉ, RESTREINT SOCIÉTÉ, CONFIDENTIEL INDUSTRIE.

Ces informations sensibles non DR peuvent toutefois bénéficier d'une protection juridique au travers de réglementations spécifiques (protection du secret des affaires<sup>135</sup>, informations couvertes par le secret professionnel<sup>136</sup>, réglementation propre aux données de santé...).

135. Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. D'après l'article L. 151-1 du code du commerce, est protégée au titre du secret des affaires toute information répondant aux critères suivants : 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret.

136. Loi n° 78-754 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif.

Les différences d'ordre juridique concernant les transferts d'informations sensibles sont illustrées par les figures 36 (transferts d'informations sensibles non DR) et 37 (transferts d'informations DR).

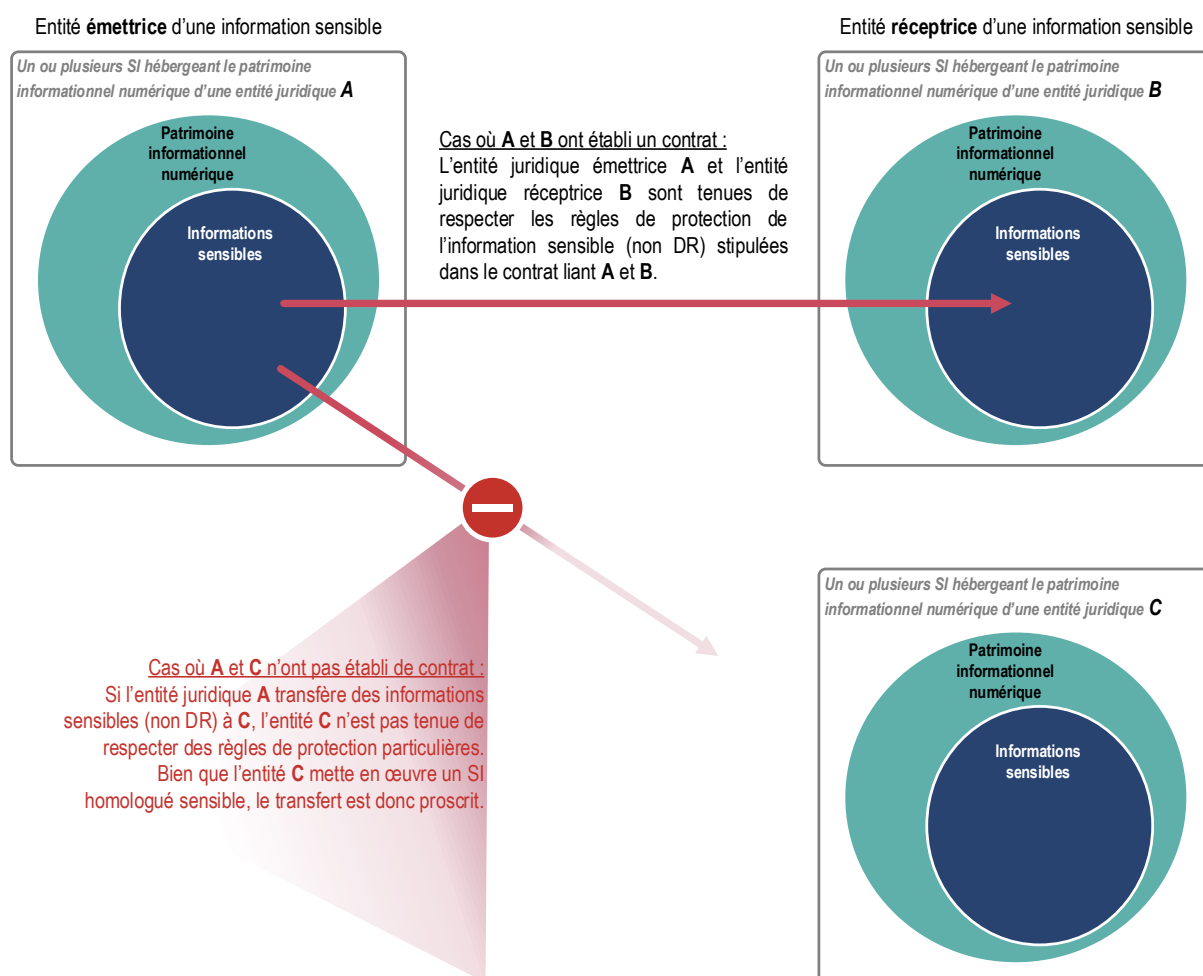


FIGURE 36 – Illustration du transfert d'informations sensibles (non DR) d'une entité juridique vers une autre entité juridique

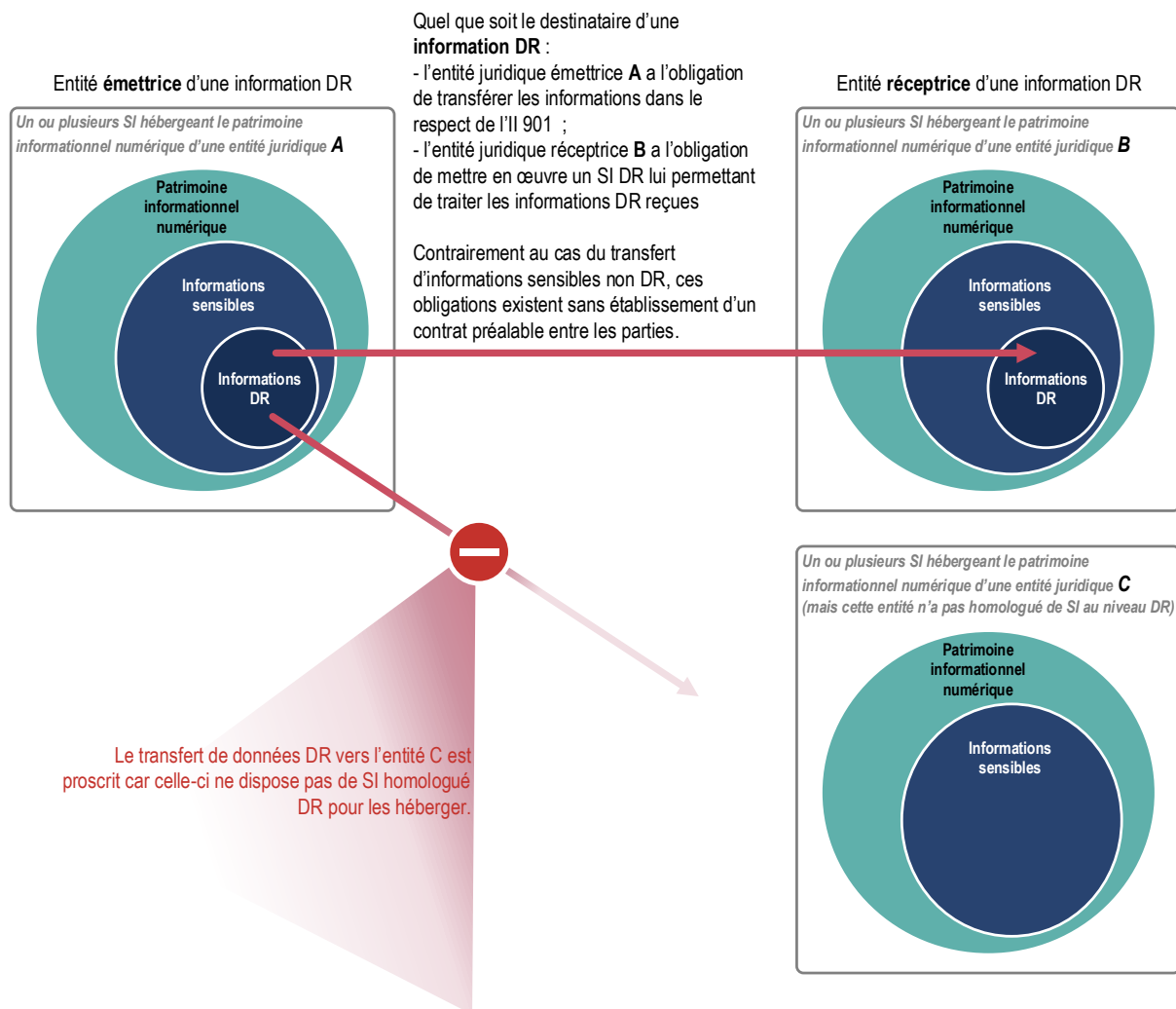


FIGURE 37 – Illustration du transfert d'informations DR d'une entité juridique vers une autre entité juridique

# Annexe B

## Niveaux de sensibilité des informations

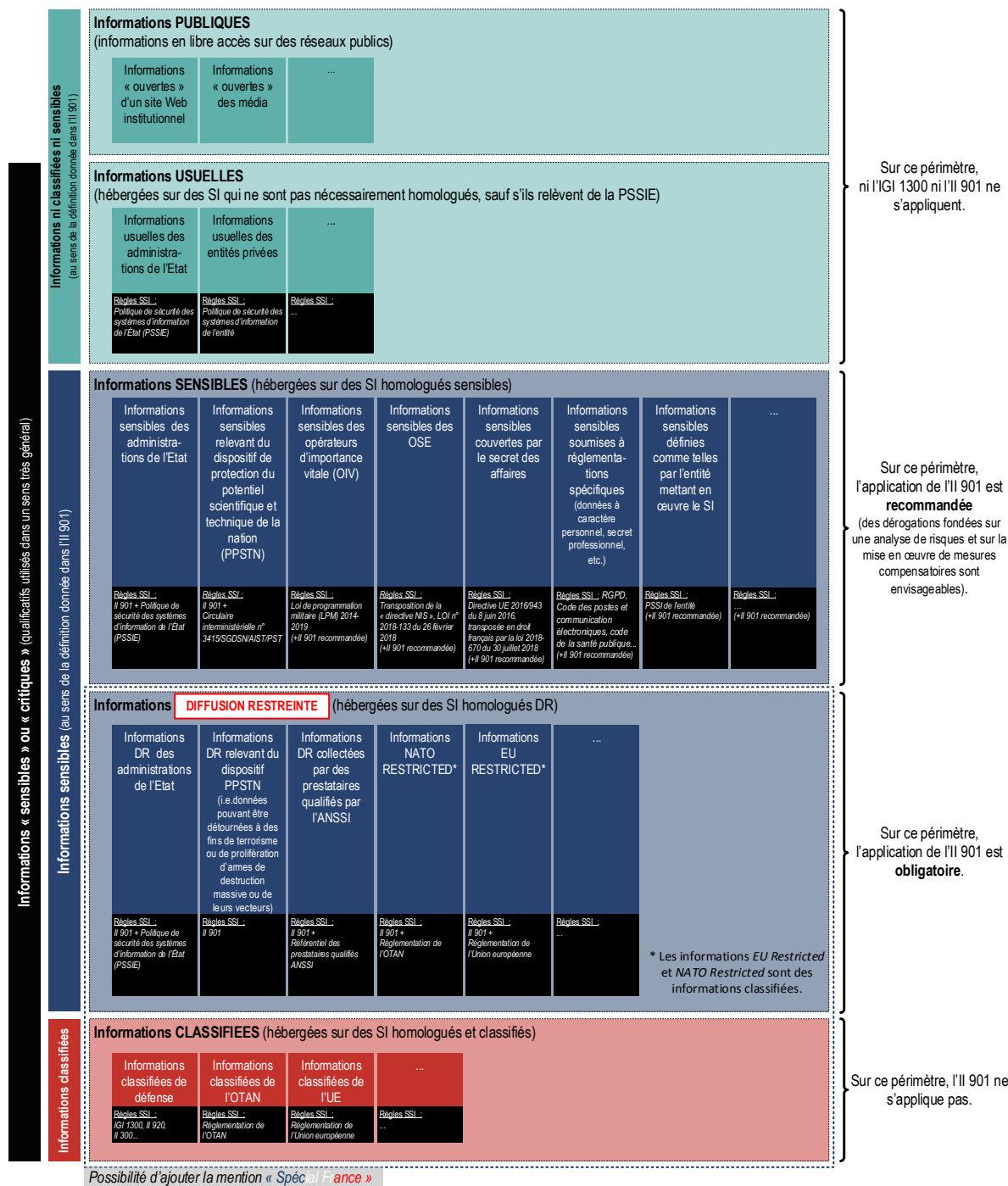


FIGURE 38 – Niveaux de sensibilité des informations en France et référentiels SSI associés



# Annexe C

## Visas de sécurité

Un visa de sécurité est une attestation de l'atteinte d'un niveau de sécurité. Il peut concerner un produit de sécurité ou un prestataire de service en sécurité.

La certification, la qualification et l'agrément sont des notions distinctes qui ne doivent pas être confondues. Ces trois termes sont pertinents pour les produits de sécurité. Pour les prestataires de service de confiance, seul le terme qualification est utilisé.

### Certification de sécurité d'un produit

La certification de sécurité délivrée par l'ANSSI est la reconnaissance de la robustesse d'un produit, c'est-à-dire de sa capacité à résister à des attaques informatiques. Cette robustesse est éprouvée à travers une évaluation par un tiers, dont la compétence est garantie par l'ANSSI. Ces laboratoires indépendants sont appelés centres d'évaluation de la sécurité des technologies de l'information (CESTI).

La certification apporte également l'assurance de la conformité des fonctions de sécurité au regard de celles attendues, décrites dans la cible de sécurité, ainsi que l'assurance de la conformité aux référentiels et critères d'évaluation.

Les objectifs de sécurité et les cas d'usage d'une solution certifiée sont définis par le donneur d'ordre qui peut être le fournisseur de la solution, l'ANSSI, ou une tierce partie (typiquement intéressée par l'acquisition de la solution). L'ANSSI n'intervient pas dans la définition de la cible de sécurité<sup>137</sup> : la certification de sécurité ne constitue pas une recommandation par l'État français pour une utilisation dans un cadre déterminé.

L'évaluation conduisant à la certification peut être menée selon deux types de méthodologies :

- la certification de sécurité de premier niveau (CSPN), méthodologie nationale focalisée sur l'analyse de vulnérabilité (robustesse) et qui se déroule en temps et en charge contraints ;
- les Critères Communs (CC), méthodologie internationale normalisée qui permet l'évaluation de la robustesse d'un produit et atteste d'un niveau d'assurance (plusieurs niveaux d'assurance sont définis, de EAL<sup>138</sup> 1 (niveau le plus bas) à EAL 7 (niveau le plus élevé).

---

137. Dans une procédure de certification, l'ANSSI n'intervient que pour dénoncer les cibles de sécurité qui auraient un caractère mensonger.

138. *Evaluation Assurance Level*, en anglais.

# Qualification de sécurité d'un produit ou d'un service

Pour les produits comme pour les services, la confiance est évaluée dans le cadre du processus de qualification et de son suivi. L'évaluation de la confiance consiste à éprouver la capacité du fournisseur à respecter sur le long terme un ensemble d'engagements pris auprès de l'ANSSI :

- pour les produits : confidentialité et protection des données confiées par l'utilisateur du produit, correction des failles et vulnérabilités...
- pour les services : aptitude à identifier et maîtriser les menaces et risques pour satisfaire les exigences inscrites dans des référentiels métiers, maintien des compétences...

La procédure de qualification d'un produit de sécurité s'appuie sur une ou plusieurs certifications de sécurité (CSPN ou certification CC). Mais contrairement à la procédure de certification décrite au paragraphe précédent, l'ANSSI peut corriger la définition des exigences de sécurité explicitées dans la cible de sécurité. En outre, l'ANSSI analyse et oriente, en sa qualité d'autorité nationale de sécurité, les travaux menés par les centres d'évaluation.

Pour un usage donné, la qualification est la recommandation par l'État français d'un produit ou d'un service. Elle atteste à la fois de la qualité de la solution (robustesse d'un produit ou compétence d'un prestataire), de la confiance qu'a l'État envers le fournisseur et de la pertinence de la solution au regard d'un besoin identifié par l'État, qu'il s'agisse de son besoin propre, du besoin des opérateurs d'importance vitale (OIV) ou de celui de tout autre acteur identifié dans un cadre réglementaire.

La qualification d'un produit (ou d'un service) peut être assortie d'un niveau de recommandation d'utilisation, qui évolue en fonction du suivi dans le temps de la qualification, et est matérialisé par un code couleur :

- Catégorie verte : solution recommandée sans réserve, y compris pour les nouveaux usages (nouveau déploiement de produit, nouveau contrat de service);
- Catégorie orange : solution recommandée uniquement pour les usages existants, à ne pas privilégier pour les nouveaux usages (p. ex. produit pour lequel une nouvelle version qualifiée, plus performante, est disponible et à privilégier pour les nouveaux déploiements);
- Catégorie rouge : solution dont la qualification sera révoquée prochainement et dont le remplacement ou retrait de service doit être planifié (produit plus maintenu par son développeur, service prochainement interrompu).

La liste de produits et services qualifiés est régulièrement mise à jour et disponible sur le site Web de l'ANSSI : <https://www.ssi.gouv.fr/liste-produits-et-services-qualifies/>.

## Agrément de sécurité d'un produit

Un agrément de sécurité est associé à un niveau de sensibilité des informations à protéger. Ainsi, l'agrément de sécurité de niveau DR délivré par l'ANSSI atteste de l'aptitude d'un produit à protéger des informations DR.

Lorsqu'un produit est agréé DR, une mention explicite figure sur le certificat de qualification du produit.

## Pour en savoir plus

La liste des produits qualifiés est disponible sur le site Web de l'ANSSI :

<https://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/>

Pour plus d'informations concernant les visas de sécurité :

<https://www.ssi.gouv.fr/visa-de-securite/>

# Annexe D

## Nomadisme - Mesures de sécurité

### II 901 et guide ANSSI

TABLE 1 – Table de correspondance entre les mesures de sécurité de l’II 901 relatives au nomadisme et les « Recommandations sur le nomadisme numérique » [22] de l’ANSSI (version 1, octobre 2018)

Réf. II 901	Description de la mesure de sécurité	Recommandation(s) du guide ANSSI portant sur le nomadisme numérique (version 1, octobre 2018)
EXP-NOMAD-SENS	Déclaration des équipements nomades aptes à traiter des informations sensibles	R2, R3
EXP-ACC-DIST	Accès à distance au système d’information de l’organisme	R21, R22
PDT-VEROUIL-PORT	Verrouillage des postes portables	R7 - L’utilisation d’un câble antivol est fortement recommandée pour les équipements d’accès sensible.
PDT-NOMAD-ACCESS	Accès à distance aux SI de l’entité	R16, R17, R18, R19, R20
PDT-NOMAD-PAREFEU	Pare-feu local	R11, R17
PDT-NOMAD-STOCK	Stockage local d’information sur les postes nomades	R9 - Une solution de chiffrement agréée pour la protection d’informations DR est obligatoire pour protéger des données DR présentent sur l’équipement d’accès nomade.
PDT-NOMAD-FILT	Filtre de confidentialité	R7
PDT-NOMAD-CONNEX	Configuration des interfaces de connexion sans fil	R12, [14]
PDT-NOMAD-DESACTIV	Désactivation des interfaces de connexion sans fil	R12

# Annexe E

## Administration des SI - Mesures de sécurité II 901 et guide ANSSI

TABLE 2 – Table de correspondance entre les mesures de sécurité de l’II 901 relatives à l’administration et les « Recommandations relatives à l’administration sécurisée des systèmes d’information V2 » de l’ANSSI [25] (version 2, avril 2018)

Réf.II 901	Description de la mesure de sécurité	Recommandation(s) du guide ANSSI portant sur l’administration sécurisée (version 2, avril 2018)
EXP-RESTR-DROITS	Restriction des droits	R27
EXP-PROT-ADMIN	Protection des accès aux outils d’administration	R1, R2, R15/R15-, R16, R18/R18-, R22, R23, R32
EXP-HABILIT-ADMIN	Habilitation des administrateurs	R39, R40, R41
EXP-GEST-ADMIN	Gestion des actions d’administration	R45, R46, R47
EXP-SEC-FLUXADMIN	Sécurisation des flux d’administration	R8, R9/R9-/R9- -, R10, R11, R12, R13, R15, R15-, R18, R18-, R19, R20, R21, R23, R24, R24-
EXP-CENTRAL	Gestion des actions d’administration	R22
EXP-CI-MESSTECH	Messagerie technique	R53
PDT-PRIV	Utilisation des privilèges d’accès des administrateurs	R29
PDT-ADM-LOCAL	Gestion du compte de l’administrateur local	R1

# Annexe F

## Mesures de sécurité II 901

TABLE 3 – Liste exhaustive des mesures de sécurité de l’II 901 avec, en regard, les renvois vers les sections de ce guide où ces mesures sont mentionnées ou, le cas échéant, des références vers d’autres publications de l’ANSSI

Réf. II 901	Description de la mesure de sécurité	Réf. dans ce guide (ou autre réf. ANSSI)
Article 1 <sup>er</sup>	Définitions	2.1, A.1
Article 2	Champ d’application	R3
Article 3	Principes stratégiques appliqués	R4 (amélioration continue); 5, R6 (défense en profondeur); R62 (administration sécurisée); R29, R30 (produits et prestations de sécurité qualifiées)
Article 4	Application des règles	
Article 5	Détermination de la sensibilité des informations	R1, R36
Article 6	Gouvernance de la protection des systèmes d’information	
Article 7	Maîtrise des risques	2.1,
Article 8	Homologation des systèmes d’information sensibles	2.4
Article 9	Protection des systèmes d’information	R65 (cartographie); [24] (protection physique); 5, 6 (protection logique)
Article 10	Gestion des incidents de sécurité des systèmes d’information	7.5
Article 11	Évaluation du niveau de sécurité	R4
Article 12	Relation avec les autorités de l’État	
Article 13	Homologation des systèmes d’information <i>Diffusion Restreinte</i>	2.4
Article 14	Traitement des informations portant la mention <i>Diffusion Restreinte</i>	2.2 (classes de SI); R19, R9, R55 (chiffrement des informations DR)
Article 15	Protection physique des locaux	[24]
Article 16	Externalisation	5.1, 7.3, [10]
Article 17	Utilisation en milieu non maîtrisé	R19 (chiffrement des informations DR); 6.4 (précautions particulières en situation de nomadisme)
Article 18	Supports audiovisuels	
Article 19	Autorisations de dérogations	
Article 20	Dispositions transitoires	
Article 21	Abrogation	
ORG-SSI	Organisation de la SSI	
ORG-ACT-SSI	Identification des acteurs de la SSI	
ORG-RSSI	Désignation du responsable de la SSI	

Suite page suivante...

Réf.	Description de la mesure de sécurité	Réf. dans ce guide (ou autre réf. ANSSI)
ORG-RESP	Formalisation des responsabilités	
ORG-TIERS	Gestion contractuelle des tiers	5.1, 7.3, [10]
ORG-PIL-PSSI	Définition et pilotage de la PSSI	[12]
ORG-APP-INSTR	Application de l'instruction dans l'entité	
ORG-APP-DOCS	Formalisation de documents d'application	
RH-SSI	Charte d'application de la SSI	
RH-MOTIV	Choix et sensibilisation des personnes tenant les postes clés de la SSI	
RH-CONF	Personnels de confiance	
RH-UTIL	Sensibilisation des utilisateurs des systèmes d'information	
RH-MOUV	Gestion des arrivées, des mutations et des départs	5.5
RH-NPERM	Gestion du personnel non permanent (stagiaires, intérimaires, prestataires)	
GDB-INVENT	Inventaire des ressources informatiques	7.4
GDB-CARTO	Cartographie	7.4
GDB-QUALIF-SENSI	Qualification des informations	5.4, 2.1
GDB-PROT-IS	Protection des informations	3.3
INT-HOMOLOG-SSI	Homologation de sécurité des systèmes d'information	2.4, 4.2, [16]
INT-SSI	Intégration de la sécurité dans les projets	7.4
INT-QUOT-SSI	Mise en œuvre au quotidien de la SSI	7.4
INT-TDB	Créer un tableau de bord SSI	
INT-AQ-PSL	Acquisition de produits de sécurité et de services de confiance	5.1
INT-PRES-CS	Clauses de sécurité	5.1, 7.3, [10]
INT-PRES-CNTRL	Suivi et contrôle des prestations fournies	[10]
INT-REX-AR	Analyse des risques	2.4, [16]
INT-REX-HB	Hébergement	
INT-REX-HS	Hébergement et clauses de sécurité	5.1, 7.4, [10]
PHY-ZONES	Découpage des sites en zones de sécurité	
PHY-PUBL	Accès réseau en zone d'accueil du public	5.3
PHY-SENS	Protection des informations sensibles au sein des zones d'accueil	5.3
PHY-TECH	Sécurité physique des locaux techniques	
PHY-TELECOM	Protection des câbles électriques et de télécommunications	
PHY-CTRL	Contrôles anti-piégeages	
PHY-CI-LOC	Découpage des locaux en zones de sécurité	
PHY-CI-HEBERG	Convention de service en cas d'hébergement tiers	[10]
PHY-CI-CTRLACC	Contrôle d'accès physique	5.1
PHY-CI-MOYENS	Délivrance des moyens d'accès physique	
PHY-CI-TRACE	Traçabilité des accès	
PHY-CI-ENERGIE	Local énergie	
PHY-CI-CLIM	Climatisation	
PHY-CI-INC	Lutte contre l'incendie	
PHY-CI-EAU	Lutte contre les voies d'eau	
PHY-SI-SUR	Sécurisation du SI de sûreté	[24]
RES-MAITRISE	Systèmes autorisés sur le réseau	6.1
RES-INTERCO	Interconnexion avec des réseaux externes	4.2, 4.3, [23]
RES-ENTSOR	Mettre en place un filtrage réseau pour les flux sortants et entrants	4.2, 4.3, [21], [5], [15], [18], [23]
RES-PROT	Protection des informations	4.2, 4.3, [23]
RES-CLOIS	Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes	5.3
RES-INTERCOGEO	Interconnexion des sites géographiques locaux d'une entité	4.2
RES-RESS	Cloisonnement des ressources en cas de partage de locaux	
RES-INTERNET-SPECIFIQUE	Cas particulier des accès spécifiques dans une entité	4.3.3
RES-SSFIL	Mise en place de réseaux sans fil	6.5
RES-COUCHBAS	Implanter des mécanismes de protection contre les attaques sur les couches basses	[6]
RES-ROUTDYN	Surveiller les annonces de routage	
RES-ROUTDYN-IGP	Configurer le protocole IGP de manière sécurisée	
RES-ROUTDYN-EGP	Sécuriser les sessions EGP	
RES-SECRET	Modifier systématiquement les éléments d'authentification par défaut des équipements et services	5.3
RES-DURCI	Durcir les configurations des équipements de réseaux	5.3, [6]
RES-CARTO	Élaborer les documents d'architecture technique et fonctionnelle	7.4
ARCHI-HEBERG	Principes d'architecture de la zone d'hébergement	5.3
ARCHI-STOCKCI	Architecture de stockage et de sauvegarde	
ARCHI-PASS	Passerelle Internet	4.3, [23]
EXP-PROT-INF	Protection des informations sensibles en confidentialité et en intégrité	5.2
EXP-TRAC	Traçabilité des interventions sur le système	
EXP-CONFIG	Configuration des ressources informatiques	5.3

Suite page suivante...

Réf.	Description de la mesure de sécurité	Réf. dans ce guide (ou autre réf. ANSSI)
EXP-DOC-CONFIG	Documentation des configurations	
EXP-ID-AUTH	Identification, authentification et contrôle d'accès logique	5.5
EXP-DROITS	Droits d'accès aux ressources	5.5
EXP-PROFILS	Gestion des profils d'accès aux applications	5.5
EXP-PROC-AUTH	Autorisations d'accès des utilisateurs	5.5
EXP-REVUE-AUTH	Revue des autorisations d'accès	5.5
EXP-CONF-AUTH	Confidentialité des informations d'authentification	5.5
EXP-GEST-PASS	Gestion des mots de passe	5.5
EXP-INIT-PASS	Initialisation des mots de passe	5.5
EXP-POL-PASS	Politiques de mots de passe	5.5
EXP-CERTIFS	Utilisation de certificats électroniques	[27]
EXP-QUAL-PASS	Contrôle systématique de la qualité des mots de passe	5.5
EXP-SEQ-ADMIN	Séquestre des authentifiants des administrateurs	7, [25]
EXP-POL-ADMIN	Politique des mots de passe des administrateurs	7, [25]
EXP-DEP-ADMIN	Gestion du départ d'un administrateur des SI	7, [25]
EXP-RESTR-DROITS	Restriction des droits	6.1
EXP-PROT-ADMIN	Protection des accès aux outils d'administration	7, [25]
EXP-HABILIT-ADMIN	Habilitation des administrateurs	7, [25]
EXP-GEST-ADMIN	Gestion des actions d'administration	7, [25]
EXP-SEC-FLUXADMIN	Sécurisation des flux d'administration	7, [25]
EXP-CENTRAL	Centraliser la gestion du système d'information	7.4
EXP-SECX-DIST	Sécurisation des outils de prise de main à distance	[19]
EXP-DOM-POL	Définir une politique de gestion des comptes du domaine	
EXP-DOM-PASS	Configurer la stratégie des mots de passe des domaines	
EXP-DOM-NOMENCLAT	Définir et appliquer une nomenclature des comptes du domaine	[25]
EXP-DOM-RESTADMIN	Restreindre au maximum l'appartenance aux groupes d'administration du domaine	
EXP-DOM-SERV	Maîtriser l'utilisation des comptes de service	
EXP-DOM-LIMITSERV	Limiter les droits des comptes de service	
EXP-DOM-OBSOLET	Désactiver les comptes du domaine obsolètes	
EXP-DOM-ADMINLOC	Améliorer la gestion des comptes d'administrateur locaux	6.1, [25]
EXP-MAINT-EXT	Maintenance externe	5.4
EXP-MIS-REB	Mise au rebut	5.4
EXP-PROT-MALV	Protection contre les codes malveillants	5.6
EXP-GES-ANTIVIR	Gestion des événements de sécurité de l'antivirus	5.6, 7.5
EXP-MAJ-ANTIVIR	Mise à jour de la base de signatures	5.6, 7.4
EXP-NAVIG	Configuration du navigateur Internet	5.3
EXP-POL-COR	Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité	7.4
EXP-COR-SEC	Déploiement des correctifs de sécurité	7.4
EXP-OBSOLET	Assurer la migration des systèmes obsolètes	7.4
EXP-ISOL	Isoler les systèmes obsolètes restants	7.4
EXP-JOUR-SUR	« Journalisation » des alertes	7.5
EXP-POL-JOUR	Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces	7.5
EXP-CONS-JOUR	Conservation des journaux	7.5
EXP-GES-DYN	Gestion dynamique de la sécurité	7.5
EXP-MAIT-MAT	Maîtrise des matériels	6
EXP-PROT-VOL	Rappel des mesures de protection contre le vol	6, 5.7
EXP-DECLAR-VOL	Déclarer les pertes et vols	5.7
EXP-REAFFECT	Réaffectation de matériels informatiques	5.7
EXP-NOMAD-SENS	Déclaration des équipements nomades aptes à traiter des informations sensibles	6.4
EXP-ACC-DIST	Accès à distance au système d'information de l'organisme	6.4
EXP-IMP-SENS	Impression des informations sensibles	
EXP-IMP-2	Sécurité des imprimantes et des copieurs multifonctions	4.1
EXP-CI-OS	Systèmes d'exploitation	5.3, 7.4, [2], [7]
EXP-CI-LTP	Logiciels en tiers présentation	
EXP-CI-LTA	Logiciels en tiers application	
EXP-CI-LTD	Logiciels en tiers données	
EXP-CI-PROTFIC	Passerelle d'échange de fichiers	4.4
EXP-CI-MESSTECH	Messagerie technique	[25]
EXP-CI-FILT	Filtrage des flux applicatifs	5.3
EXP-CI-ADMIN	Flux d'administration	
EXP-CI-DNS	Service de noms de domaine - DNS technique	
EXP-CI-EFFAC	Effacement de support	5.4, 6.1

Suite page suivante...



Réf.	Description de la mesure de sécurité	Réf. dans ce guide (ou autre réf. ANSSI)
EXP-CI-DESTR	Destruction de support	5.7
EXP-CI-TRAC	Traçabilité et imputabilité	7.5
EXP-CI-SUPERVIS	Supervision	7.5
EXP-CI-AMOV	Accès aux périphériques amovibles	5.7
EXP-CI-ACCRES	Accès aux réseaux	6.2
EXP-CI-AUDIT	Audit et contrôle	2.4
PDT-GEST	Fourniture et gestion des postes de travail	6
PDT-CONFIG	Formalisation de la configuration des postes de travail	6
PDT-VEROUIL-FIXE	Verrouillage de l'unité centrale des postes fixes	6
PDT-VEROUIL-PORT	Verrouillage des postes portables	6.4
PDT-REAFECT	Réaffectation du poste de travail	6.1
PDT-PRIVIL	Privilèges des utilisateurs sur les postes de travail	6
PDT-PRIV	Utilisation des privilèges d'accès des administrateurs	7, [25]
PDT-ADM-LOCAL	Gestion du compte de l'administrateur local	7, [25]
PDT-STOCK	Stockage des informations	6.4
PDT-SAUV-LOC	Sauvegarde et synchronisation des données locales	6
PDT-PART-FIC	Partage de fichiers	6
PDT-SUPPR-PART	Suppression des données sur les postes partagés	6
PDT-CHIFF-SENS	Chiffrement des données sensibles	5.2, 6.4
PDT-AMOV	Fourniture de supports de stockage amovibles	5.7
PDT-NOMAD-ACCESS	Accès à distance aux SI de l'entité	6.4
PDT-NOMAD-PAREFEU	Pare-feu local	6.4, 5.3
PDT-NOMAD-STOCK	Stockage local d'information sur les postes nomades	5.2, 6.4
PDT-NOMAD-FILT	Filtre de confidentialité	6.4
PDT-NOMAD-CONNEX	Configuration des interfaces de connexion sans fil	6.5
PDT-NOMAD-DESACTIV	Désactivation des interfaces de connexion sans fil	6.5
PDT-MUL-DURCISS	Durcissement des imprimantes et des copieurs multifonctions	
PDT-MUL-SECNUM	Sécurisation de la fonction de numérisation	
PDT-TEL-MINIM	Sécuriser la configuration des autocommutateurs	
PDT-TEL-CODES	Codes d'accès téléphoniques	
PDT-TEL-DECT	Limiter l'utilisation du DECT	
PDT-CONF-VERIF	Utiliser des outils de vérification automatique de la conformité	7.4
DEV-INTEGR-SECLOC	Intégrer la sécurité dans les développements locaux	
DEV-SOUS-TRAIT	Intégrer des clauses de SSI dans les contrats de sous-traitance de développement informatique	[10]
DEV-FUITES	Limiter les fuites d'information	
DEV-LOG-ADHER	Réduire l'adhérence des applications à des produits ou à technologies spécifiques	
DEV-LOG-CRIT	Instaurer des critères de développement sécurisé	
DEV-LOG-CYCLE	Intégrer la sécurité dans le cycle de vie du logiciel	
DEV-LOG-WEB	Améliorer la prise en compte de la sécurité dans les développements Web	
DEV-LOG-PASS	Calculer les empreintes de mots de passe de manière sécurisée	
DEV-FILT-APPL	Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque	
TI-OPS-SSI	Chaînes opérationnelles de la SSI	7.5
TI-MOB	Mobilisation en cas d'alerte	7.5
TI-QUAL-TRAIT	Qualification et traitement des incidents	7.5
TI-INC-REM	Remontée des incidents	7.5
PCA-MINIS	Définition du plan de continuité d'activité des SI	
PCA-LOCAL	Définition du plan local de continuité d'activité des systèmes d'information	
PCA-SUIVILOCAL	Suivi de la mise en œuvre du plan de continuité d'activité local des SI	
PCA-PROC	Mise en œuvre de dispositifs techniques et des procédures opérationnelles	7.4
PCA-SAUVE	Protection de la disponibilité des sauvegardes	
PCA-PROT	Protection de la confidentialité des sauvegardes	
PCA-EXERC	Exercice régulier du plan local de continuité d'activité des systèmes d'information	
PCA-MISAJOUR	Mise à jour du plan local de continuité d'activité des systèmes d'information	
CONTR-SSI	Contrôles locaux	

# Liste des recommandations

<b>R1</b>	☞ Trier le patrimoine informationnel par niveau de sensibilité	10
<b>R2</b>	☞ Identifier les types de SI nécessaires	11
<b>R3</b>	☞ Déterminer le régime de protection des informations sensibles	15
<b>R4</b>	☞ Homologuer tout SI sensible avant sa mise en production	16
<b>R5+</b>	Isoler physiquement le SI sensible et le SI usuel	21
<b>R5</b>	Cloisonner physiquement le SI sensible et le SI usuel	23
<b>R5-</b>	Cloisonner logiquement les données sensibles au sein d'un SI sensible	25
<b>R6</b>	☞ Appliquer le principe de défense en profondeur en cas de mutualisation de ressources	26
<b>R7</b>	Cloisonner les annuaires sensible et usuel	27
<b>R8</b>	☞ Définir une stratégie d'homologation pour chaque interconnexion de SI sensible	31
<b>R9</b>	☞ Sécuriser les interconnexions de SI DR	32
<b>R10</b>	☞ Sécuriser les interconnexions de SI sensibles	32
<b>R11</b>	Filtrer les flux des interconnexions de SI sensibles	33
<b>R12</b>	Appliquer les recommandations de l'ANSSI relatives à l'interconnexion d'un SI à Internet	33
<b>R13</b>	☞ Passerelle de classe 1 : mettre en œuvre au moins un pare-feu qualifié	34
<b>R14</b>	☞ Passerelle de classe 1 : mettre en œuvre au moins un dispositif de rupture de flux	35
<b>R15</b>	☞ Passerelle de classe 1 : mettre en œuvre un système de détection	36
<b>R16</b>	Passerelle de classe 1 : mettre en œuvre des <i>taps</i> qualifiés passifs	36
<b>R17</b>	Passerelle de classe 1 : faire porter les fonctions de sécurité par des dispositifs distincts	37
<b>R18</b>	Interdire la navigation Web depuis les SI sensibles	38
<b>R18-</b>	Permettre la navigation Web depuis des postes de rebond	39
<b>R18- -</b>	Permettre la navigation Web sans postes de rebond	39
<b>R19</b>	☞ Chiffrer les informations DR transférées via des SI de classe 0	40
<b>R20</b>	☞ Chiffrer les informations sensibles transférées via des SI de classe 0	40
<b>R21</b>	☞ Interdire l'accès aux applications sensibles depuis les SI non homologués	42
<b>R22</b>	☞ Cloisonner l'infrastructure de mise à disposition sur Internet d'informations sensibles	43
<b>R23</b>	Maîtriser les interconnexions descendantes des SI de classe 2	44
<b>R24</b>	☞ N'autoriser que des protocoles de transfert vers le système d'échanges sécurisés	45
<b>R25</b>	☞ Système d'échanges sécurisés : restreindre les accès aux seuls utilisateurs autorisés	45
<b>R26</b>	☞ Système d'échanges sécurisés : authentifier les utilisateurs avec un compte non sensible	46
<b>R27</b>	☞ Système d'échanges sécurisés : analyser le contenu des données échangées	46
<b>R28</b>	☞ Système d'échanges sécurisés : journaliser et imputer les données échangées	46
<b>R29</b>	☞ Recourir à des prestataires de services SSI disposant d'un visa de sécurité ANSSI	47
<b>R30</b>	☞ Acquérir des produits de sécurité disposant d'un visa de sécurité ANSSI	48
<b>R31</b>	☞ Respecter les conditions d'emploi des équipements de sécurité agréés	48
<b>R32</b>	☞ Cloisonner le SI sensible en zones ayant des niveaux de sécurité homogènes	50
<b>R33</b>	☞ Éviter l'installation de moyens informatiques sensibles dans les zones ouvertes au public	50
<b>R34</b>	☞ Bloquer les communications latérales	51

<b>R35</b>	☞ Durcir la configuration des matériels et des logiciels utilisés sur les SI sensibles	51
<b>R36</b>	☞ Marquer les informations sensibles	52
<b>R37</b>	Marquer les supports stockant des informations sensibles	53
<b>R38</b>	Adopter un code couleur pour le câblage des équipements	53
<b>R39</b>	☞ Activer une authentification initiale forte	54
<b>R40</b>	Protéger les secrets d'authentification	55
<b>R41</b>	☞ Gérer avec rigueur l'affectation des droits d'accès logiques des comptes informatiques	55
<b>R42</b>	☞ Protéger le SI sensible des codes malveillants	56
<b>R43</b>	Adapter la politique de protection contre les codes malveillants	56
<b>R44</b>	Déployer des outils révélant des activités suspectes	57
<b>R45</b>	Supports amovibles : limiter leur usage au strict besoin opérationnel	58
<b>R46</b>	☞ Supports amovibles : maîtriser leur gestion et leurs conditions d'usage	58
<b>R47</b>	Supports amovibles : privilégier l'utilisation de supports en lecture seule	59
<b>R48</b>	Supports amovibles : utiliser des solutions de dépollution des supports de stockage	60
<b>R49</b>	☞ Maîtriser les moyens informatiques affectés aux utilisateurs d'un SI sensible	63
<b>R50</b>	Connecter les ressources sensibles sur un réseau physique dédié	63
<b>R50-</b>	Connecter les ressources sensibles sur un réseau logique dédié	64
<b>R51</b>	Authentifier les ressources sensibles vis-à-vis du réseau	64
<b>R52</b>	Utiliser un poste utilisateur sensible dédié	65
<b>R52-</b>	Utiliser un poste utilisateur multiniveau	66
<b>R52- -</b>	Utiliser un poste utilisateur sensible avec accès distant au SI usuel	68
<b>R53</b>	☞ Appliquer les recommandations de l'ANSSI relatives au nomadisme numérique	70
<b>R54</b>	☞ Protéger physiquement les équipements d'accès nomade	71
<b>R55</b>	☞ Sécuriser les canaux d'interconnexion nomades des SI DR	71
<b>R56</b>	☞ Sécuriser les canaux d'interconnexion nomades des SI sensibles	71
<b>R57</b>	☞ Chiffrer les données DR stockées sur des supports amovibles	72
<b>R58</b>	☞ Chiffrer les données sensibles stockées sur des supports amovibles	72
<b>R59</b>	Chiffrer les flux réseau d'un équipement d'accès nomade sensible en toute circonstance	73
<b>R60</b>	☞ Mettre en place une architecture de réseau sans fil cloisonnée du SI sensible	74
<b>R61</b>	☞ Bloquer l'accès aux portails captifs depuis des équipements d'accès nomades sensibles	74
<b>R62</b>	☞ Appliquer les recommandations de l'ANSSI relatives à l'administration sécurisée des SI	77
<b>R63</b>	☞ Gérer les administrateurs d'un SI sensible	78
<b>R64</b>	☞ Sécuriser la chaîne de connexion pour l'administration à distance	83
<b>R64-</b>	☞ Maîtriser les systèmes de télémaintenance connectés à des SI sensibles	83
<b>R65</b>	☞ Définir et appliquer une politique de MCS	84
<b>R66</b>	☞ Isoler les systèmes obsolètes	84
<b>R67</b>	☞ Appliquer les recommandations de l'ANSSI relatives à la journalisation	85
<b>R68</b>	☞ Conserver les journaux d'un SI sensible pendant 12 mois	85
<b>R69</b>	Recourir aux services d'un prestataire qualifié pour la supervision de sécurité	86
<b>R70</b>	☞ Formaliser une procédure de déclaration des incidents de sécurité à l'ANSSI	86

# Bibliographie

- [1] *Instruction générale interministérielle n°1300.*  
Référentiel, SGDSN, août 2021.  
<https://www.ssi.gouv.fr/igi1300>.
- [2] *Recommandations de sécurité relatives à un système GNU/Linux.*  
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.  
<https://www.ssi.gouv.fr/reco-securite-systeme-linux>.
- [3] *Recommandations de sécurité relatives aux mots de passe.*  
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.  
<https://www.ssi.gouv.fr/mots-de-passe>.
- [4] *Recommandations pour un usage sécurisé d’(Open)SSH.*  
Note technique DAT-NT-007/ANSSI/SDE/NP v1.2, ANSSI, août 2015.  
<https://www.ssi.gouv.fr/nt-ssh>.
- [5] *Recommandations de sécurisation d’un pare-feu Stormshield Network Security (SNS) - Version 1.2.*  
Note technique DAT-NT-031/ANSSI/SDE/NP v1.2, ANSSI, avril 2016.  
<https://www.ssi.gouv.fr/recos-stormshield-fw>.
- [6] *Recommandations pour la sécurisation d’un commutateur de desserte.*  
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.  
<https://www.ssi.gouv.fr/nt-commutateurs>.
- [7] *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation.*  
Guide ANSSI-BP-039 v1.0, ANSSI, novembre 2017.  
<https://www.ssi.gouv.fr/windows10-vsm>.
- [8] *Recommandations de déploiement du protocole 802.1X pour le contrôle d’accès à des réseaux locaux.*  
Guide ANSSI-BP-043 v1.0, ANSSI, août 2018.  
<https://www.ssi.gouv.fr/guide-802-1X>.
- [9] *Recommandations de configuration d’un système GNU/Linux.*  
Guide ANSSI-BP-028 v1.2, ANSSI, février 2019.  
<https://www.ssi.gouv.fr/reco-securite-systeme-linux>.
- [10] *Maîtriser les risques de l’infogérance. Externalisation des systèmes d’information.*  
Guide Version 1.0, ANSSI, décembre 2010.  
<https://www.ssi.gouv.fr/infogerance>.
- [11] *Guide d’hygiène informatique : renforcer la sécurité de son système d’information en 42 mesures.*  
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.  
<https://www.ssi.gouv.fr/hygiene-informatique>.
- [12] *Guide pour l’élaboration d’une politique de sécurité des systèmes d’information.*  
Guide Version 1.0, ANSSI, mars 2004.  
<https://www.ssi.gouv.fr/pssi>.

- [13] *Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques.*  
Page Web Version 1.0, ANSSI, décembre 2010.  
<https://www.ssi.gouv.fr/infogerance>.
- [14] *Recommandations de sécurité relatives aux réseaux Wi-Fi.*  
Note technique DAT-NT-005/ANSSI/SDE/NP v1.0, ANSSI, septembre 2013.  
<https://www.ssi.gouv.fr/nt-wifi>.
- [15] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu.*  
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.  
<https://www.ssi.gouv.fr/politique-filtrage-parefeu>.
- [16] *L'homologation de sécurité en neuf étapes simples.*  
Guide Version 1.2, ANSSI, juin 2014.  
<https://www.ssi.gouv.fr/guide-homologation-securite>.
- [17] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.*  
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.  
<https://www.ssi.gouv.fr/ipsec>.
- [18] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu.*  
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.  
<https://www.ssi.gouv.fr/nettoyage-politique-fw>.
- [19] *Recommandations de sécurité relatives à la télé-assistance.*  
Note technique DAT-NT-004/ANSSI/SDE/NP v1.1, ANSSI, janvier 2017.  
<https://www.ssi.gouv.fr/teleassistance>.
- [20] *La méthode EBIOS Risk Manager - Le Guide.*  
Guide ANSSI-PA-048 v1.0, ANSSI, octobre 2018.  
<https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide>.
- [21] *Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à Internet.*  
Guide ANSSI-PA-044 v1.0, ANSSI, janvier 2018.  
<https://www.ssi.gouv.fr/guide-pare-feux-internet>.
- [22] *Recommandations sur le nomadisme numérique.*  
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.  
<https://ssi.gouv.fr/nomadisme-numerique>.
- [23] *Recommandations relatives à l'interconnexion d'un système d'information à Internet.*  
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.  
<https://www.ssi.gouv.fr/passerelle-interconnexion>.
- [24] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection.*  
Guide ANSSI-PA-072 v2.0, ANSSI, mars 2020.  
<https://www.ssi.gouv.fr/controle-acces-videoprotection>.
- [25] *Recommandations relatives à l'administration sécurisée des systèmes d'information.*  
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.  
<https://www.ssi.gouv.fr/securisation-admin-si>.

- [26] *Recommandations de sécurité pour l'architecture d'un système de journalisation.*  
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.  
<https://www.ssi.gouv.fr/journalisation>.
- [27] *Référentiel général de sécurité (RGS).*  
Référentiel Version 2.0, ANSSI, juin 2012.  
<https://www.ssi.gouv.fr/rgs>.
- [28] *Instruction interministérielle n°901.*  
Référentiel Version 1.0, ANSSI, janvier 2015.  
<https://www.ssi.gouv.fr/ii901>.
- [29] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences.*  
Référentiel Version 2.0, ANSSI, décembre 2017.  
[https://www.ssi.gouv.fr/uploads/2014/12/pdis\\_referentiel\\_v2.0.pdf](https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf).
- [30] *Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés).*  
Guide ANSSI-PG-076 v1.0, ANSSI, juillet 2020.  
<https://www.ssi.gouv.fr/guide/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies>.
- [31] *Recommendations for the architecture of sensitive or Restricted Distribution information systems.*  
Guide ANSSI-PG-075-EN v1.1, ANSSI, septembre 2021.  
<https://www.ssi.gouv.fr/en/guide/sensitive-information-systems>.
- [32] *Prestataires de services de confiance qualifiés et prestataires de détection d'incidents de sécurité (PDIS).*  
Page Web Version 1.0, ANSSI, décembre 2011.  
<https://www.ssi.gouv.fr/pdis>.
- [33] *Licence ouverte / Open Licence v2.0.*  
Page web, Mission Etalab, avril 2017.  
<https://www.etalab.gouv.fr/licence-ouverte-open-licence>.





Version 1.2 - 24/09/2021 - ANSSI-PG-075  
Licence ouverte / Open Licence (Étalab - v2.0)

## AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP  
[www.ssi.gouv.fr](http://www.ssi.gouv.fr) / [conseil.technique@ssi.gouv.fr](mailto:conseil.technique@ssi.gouv.fr)

