RECOMMENDATIONS FOR THE ARCHITECTURE OF SENSITIVE OR RESTRICTED DISTRIBUTION INFORMATION SYSTEMS

ANSSI GUIDELINES

ANSSI-PG-075-EN
24/09/2021

TARGETED AUDIENCE:

Developers **Administrators** **IT security managers** **IT managers** Users

Information

Warning

These recommendations are provided as is and are related to threats known at the publication time. Considering the information systems diversity, ANSSI cannot guarantee direct application of these recommendations on targeted information systems. Applying the following recommendations shall be, at first, validated by IT administrators and/or IT security managers.
This document is a courtesy translation of the initial French document **"Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte [31]"**, available at www.ssi.gouv.fr. In case of conflicts between these two documents, the latter is considered as the only reference.

Document changelog:

VERSION	DATE	CHANGELOG
1.0	28/08/2020	Initial version
1.1	28/12/2020	Minor changes
1.2	24/09/2021	Minor changes

Contents

1 Introduction

1.1 Purpose of the guide

The interministerial instruction no. 901/SGDSN/ANSSI (II 901) of 28 January 2015 [28] defines the objectives and minimum security measures for the protection of sensitive information, and in particular information at “Diffusion Restreinte” level. In this guide, the french expression “Diffusion Restreinte” is translated to “Restricted Distribution” (RD).

This guide provides recommendations for the design of the architecture of information systems (ISs) that host sensitive information. In general, it provides technical advice for implementing II 901.

The primary concern of this guide is the technical architecture of sensitive ISs (including RD ISs). The reader’s attention is drawn to the fact that some II 901 fields are not covered in this document (physical and environmental security, security related to IT developments…), or are only partially covered (governance of the security of information systems). In addition, some technical aspects are not covered in this version of the guide (telephony over IP, access control information system…). In order to implement an II 901-compliant IS, it is therefore necessary to apply additional measures beyond the recommendations detailed in this document.

It will be easier to understand this guide if you read II 901 beforehand.

The security measures described in II 901 are organised according to security objectives and identified by means of numbered items or unique ID codes (e.g. *INT-QUOT-SSI*). As this guide is intended to be a tool, references to these articles and ID codes are included infootnotes wherever relevant. Conversely, Annex F of this guide lists the security measures in II 901 and provides, for each, references to the sections of this guide where the measure in question is addressed (or cross-references to other ANSSI publications).

This guide presents recommendations relevant to the state of the art, threats and regulations. Its application, although not sufficient to achieve the required level of security, may nevertheless contribute to the specification of a security foundation for a sensitive IS. Creating this foundation of trust is the first step of the EBIOS *Risk Manager* [20] risk analysis method, which is recommended for use in assessing and handling the risks to an IS.

A distribution restriction equivalent to Restricted Distribution attributed to a piece of information by a foreign State or international organisation makes that information subject in France to the protection rules set out in Annex 3 of general interministerial instruction no. 1300/SGDSN/PSE/PSD (IGI 1300) of 30 November 2011 [1] and to II 901 [28]. The recommendations in this guide are therefore applicable to ISs handling such information without prejudice to any additional security measures specified by the foreign State or the international organisation.

Issues related to classified defence information and the interconnection of sensitive IS with classified ISs are outside the scope of this guide.

The french version of this guide is available on the ANSSI website [32].

1.2 Structure of the guide

After defining the concepts of sensitive and standard information systems (Chapter 2), Chapter 3 presents the various acceptable architectures for a sensitive IS. In the architecture diagrams of this chapter, the sensitive ISs are represented macroscopically and monolithically: the aim at this stage is to understand how, in general terms, they position themselves in relation to other ISs.

Chapter 4 describes the methods to be implemented for a sensitive IS to be interconnected with another IS, whether it is a less sensitive IS (e. g. the Internet) or another sensitive IS.

Chapters 5 and 6 provide recommendations for the *internal* security of sensitive ISs, dealing respectively with general aspects related to the principle of defence in depth and aspects relating to workstations.

Finally, the 7 chapter presents good practices for the administration of sensitive ISs.

1.3 Reading convention

For each recommendation in this guide, the use of the word *must* and the use of the icon ⚖ means that the recommendation is directly linked to a security measure from II 901 [28]. The wording *it is recommended* is used for all good practices, and complements the regulations.

For some of the recommendations in this guide, several solutions are proposed which differ in thelevel of security they provide. This gives the reader the opportunity to choose a solution that offers the best protection according to the context and their security objectives.

The recommendations are presented as follows:

R

State-of-the-art recommendation

This recommendation allows for the implementation of a state-of-the-art level of security.

R -

First alternate recommendation

This recommendation makes it possible to implement a first alternative, with a lower level of security than recommendation R.

R --

Second alternate recommendation

This recommendation allows for the implementation of a second alternative, with a lower level of security than the R and R - recommendations.

R +

Advanced recommendation

This recommendation allows for a higher level of security to be implemented. It is intended for entities that are mature in terms of information systems security.

The summary list of recommendations is available at page 104.

2

Unclassified information systems (ISs)

Objective

The purpose of this chapter is to explain what the different non-classified defence ISs are and to introduce the notions of sensitive and standard ISs, which are key concepts in this guide.

2.1 Information confidentiality protection requirements

II 901,the reference legislation governing the protection of sensitive information systems in France, provides the following definition of sensitive information [1].:

Sensitive information

Sensitive information is information whose disclosure to unauthorised persons, alteration or unavailability is likely to prejudice the achievement of the objectives of the entities that use it.

This definition is deliberately very open: it is up to each entity to identify the sensitiveinformation for which it is responsible and to assess, for each one, what sensitive information it is responsible for and to assess the security needs for each.

Information

In this definition, *sensitive* information may have protection needs in terms of confidentiality, integrity or availability. An assumption made by this guide is to consider confidentiality as the most important security criterion for protecting sensitive information. The recommendations it contains were drafted with this in mind; however, most of them are also relevant to the protection of the integrity or availability of the information (e. g. to prevent an availability risk resulting from an attack on the IS by means of ransomware).

1. See Article 1 of II 901

The ISs that will host the entity's information can guarantee a level of protection that is higher or lower depending on the security measures they implement. In order to determine on which IS it will be most appropriate to process an item of information, it is first necessary to identify the confidentiality protection requirement for this information.

For a public or private entity, identifying this confidentiality protection requirement is an eminently subjective and relative action. It is subjective because it is very difficult to quantify this need in a scientific way. And it is relative because this need must necessarily be consistent with the confidentiality needs of all other information handled by the entity.

One approach to achieving a classification of information according to its confidentiality requirements is to have two tools: a "confidentiality requirements scale" and a risk analysis.

The confidentiality needs scale is an arbitrary benchmark to express the fact that some information has a *low* protection requirement while other information has a *high* requirement. For example, a confidentiality needs scale may take the form of a graduated benchmark in which low numerical values reflect *low* privacy requirements, while high numerical values reflect *high* privacy requirements.

Once this scale has been established, a risk analysis will enable the entity to identify, within its information assets, information that is genuinely important and *sensitive*, as opposed to those that are "less" so. The entity must assign to each of its information items a "numerical confidentiality value" so that it can, in a second step, position this information on the scale of confidentiality requirements. This numerical value is both arbitrary (i.e. defined by an entity-specific convention) and relative (two pieces of information with different confidentiality needs correspond to two different numerical values). For example, it is possible to agree a convention whereby public information that is intended to be widely available is assigned a zero value (e. g. an advertising catalogue), while information that is very important to the entity (e. g. a trade secret) is assigned a high value (e. g. the value 100).

Warning

The confidentiality value of an item of information is likely to change throughout its life cycle. In particular, it is sometimes very difficult to predict future changes in this value, especially when aggregated with other information.

Information

By convention, in this guide, information that is "less" sensitive, but whose confidentiality protection requirement is not zero, is referred to as *standard* information.

Figure 1 is an illustration of the concept of a scale of confidentiality needs.

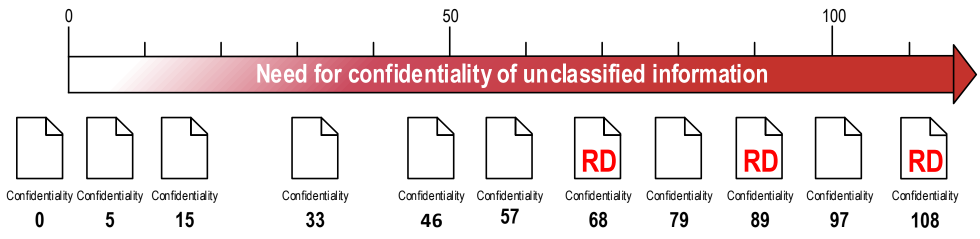


Figure 1 – Scale of confidentiality protection needs for unclassified information

A subset of sensitive information is Restricted Distribution (RD) information. The concept of RD information is defined by the regulations [2], which imposes specific security measures for their protection.

Restricted Distribution information

Restricted Distribution *information is information bearing the words* Restricted Distribution *or its European or international equivalents.*

The advantage of classifying information as Restricted Distribution is that it requires all those who handle it to comply with a restriction on distribution. Consequently, access to RD information is governed by the *need-to-know* restriction principle: only persons with a compelling need to know as part of their job role and for a specific purpose are allowed access. This restriction on distribution applies if the information is transferred to another legal entity. This entity must process the RD data in accordance with the regulations, on an IS which implements security measures specific to the protection of RD information.

Warning

Unlike RD information, sensitive non-RD information does not by default enjoy legal protection when transferred to a third party. However, there are solutions to overcome this limitation. The *business secret* created by Law no. 2018-670 of 30 July 2018 on the protection of business secrets is an example of a response to this need.

R1

Sorting information assets by sensitivity level

A public or private entity must sort its information assets. To do this, it conducts a risk analysis aimed at expressing the confidentiality protection requirements of the information [3]. These requirements can be positioned on an ascending scale of confidentiality protection, ranging from a low need for public information to a high need for sensitive or RD information.

2. See Annex 3 of IGI 1300 and II 901.
3. See measure II 901 GDB-QUALIF-SENSI.

Information

The term “non-protected information” (“NP information”) is sometimes encountered in reference to “unclassified information”. The use of this “NP” description is unfortunately inappropriate.
Firstly, NP information (or at least the ISs hosting NP information) is always, in practice, subject to protection measures and is therefore never truly *non-protected*.
Secondly, this description is ambiguous because, depending on the context in which it is used, it designates different realities. The “NP” description is frequently used when referring to the *inverse complement* of a set of information taken as a reference. For example, if in a particular context the reference information is classified information, then the term classified information, then the term “NP information” will refer to “unclassified” information; if in another context the reference information is the sensitive information (as defined in II 901), then the term “NP information” will refer to non-sensitive (as defined in II 901) and unclassified information.
Therefore, for the sake of clarity, the term “non-protected” is not used in this guide. The unambiguous terms “public information”, “standard information”, “sensitive information” and “RD information” are preferred.
For more information on the differences between public, standard, sensitive and RD information, see Annex A.

2.2 Definition of sensitive ISs and standard ISs

Once the information assets have been sorted, it becomes possible to determine which IS an item of information can be hosted on; the level of protection provided by the IS must be consistent with the need to protect the confidentiality of the hosted data. But, unlike the scale of confidentiality needs, which covers a wide range of nuances, the number of ISs that an entity will be able to implement is necessarily limited.

ISs can be seen as receptacles for information: depending on the security needs of an item of information, it is hosted on one or other of these ISs. Information for which there is a strong need for confidentiality is placed on an IS with a “higher” level of protection. Conversely, information for which the need for confidentiality is deemed to be lower is placed on an IS with a “lower” level of protection.

In the context of this guide on the architecture of sensitive ISs, it is assumed that an entity wishing to protect sensitive information will create two separate ISs. The first, called a *sensitive IS*, has a “higher” level of protection compared to the second, called a *standard IS*, which has a “lower” level of protection than the sensitive IS. Data hosted on the standard IS have a lower need for confidentiality requirements than those hosted on the sensitive IS. By way of illustration, the sensitive IS is the repository of an entity’s vital information (patents, trade secrets…). In contrast, the standard IS is the repository for “less sensitive” information. It should be noted that neither sensitive nor standard information is intended to be to be made public.

Considering that an entity implements only two IS (sensitive IS and standard IS) is an assumption of an educational nature. The reality is often more complex. An entity may be led to implement not one but several standard, sensitive or RD information systems, depending on its information partitioning needs.

The sensitive IS is characterised by the implementation of technical and organisational security measures that are more stringent than those implemented on a standard IS. Compared to the standard IS, the sensitive IS must be less exposed to public networks (typically the Internet) and the number of users of this IS must be limited to what is strictly necessary.

Sensitive IS

A *sensitive IS* is an IS that may host or process sensitive data. It is the technical repository for all data of "high" importance to the entity that implements it. A special case of a sensitive IS is an IS that hosts RD data. Such an IS is designated an *RD IS*.

Warning

In this guide, the use of the term *Sensitive IS* applies to all sensitive ISs (both RD and non-RD IS), while the use of the term *RD IS* is reserved for sensitive ISs accredited to RD level [4].

Standard IS

A *standard IS* means an IS with a lower level of protection than the sensitive IS. It is the technical repository for all data of "lesser" importance to the entity that implements it. These data are referred to as *standard* in this document.

R2

Identifying the types of IS needed

After sorting its unclassified information assets, an entity must identify the types of IS (standard, sensitive or even RD) that it will have to implement to meet its security needs.

Information

By default, information of a given sensitivity level must be processed on an IS at that same sensitivity level and not on a higher-level IS (e. g. standard information must, by default, be processed on a standard IS and not on a sensitive IS; RD information must, by default, be processed on an RD IS and not on a classified IS). Failure to comply with this principle could lead, over time, to having to deal with the problem of extracting "less sensitive" information hosted on a "more sensitive" IS . However, dealing with this issue can be complex as it is not trivial to ensure that such information extractions do not lead to uncontrolled data outputs.

4. See section 2.4 for more information on security accreditation.

An entity implementing one or more sensitive ISs must then choose the *class* of these ISs [5]. II 901 defines three classes of IS [6] :

- IS of class 0: Public IS (e.g. e.g. Internet) or IS connected to a public IS (e. g. standard IS) which does not meet the requirements of class 1;
- IS of class 1: Sensitive IS (or RD) connected to the Internet through a secure gateway meeting the security requirements defined in II 901;
- IS of class 2: Sensitive IS (or RD) physically isolated from the Internet.

This concept of IS class is detailed in section 3.1.2, where the different types of different types of sensitive IS architectures are described.

Information

Strictly speaking, Annex 2 of II 901, in which the concept of an IS of Class 1 or Class 2 is defined, only concerns ISs accredited to RD level. However, for the purposes of this guide, the assumption is to extend this concept to all sensitive ISs.
In addition, unless explicitly stated otherwise, the recommendations apply equally to sensitive ISs of class 1 and of class 2.

Figure 2 gives a representation of the link between the classes of unclassified ISs (class 0, class 1 or class 2) and the sensitivity levels of these ISs (public, standard, sensitive, RD). The concepts of an “accredited sensitive IS” and “an RD-accredited IS ” given in this figure are explained in section 2.3.

Figure 2 shows different possible interconnections between the ISs. For more information on IS interconnections, see chapter 4.

5. See Article 14 of II 901.
6. In fact, in its Annex 2, II 901 defines the concept of *network class* and not *IS class*. Because the word *network* is used in the expression *network class* to refer to an information system, this term is preferred in this guide. This is referred to as an “IS of class 2” and an “IS of class 1”. The term *network* is reserved for all the equipment used to physically create the communication network that interconnects several computer systems.

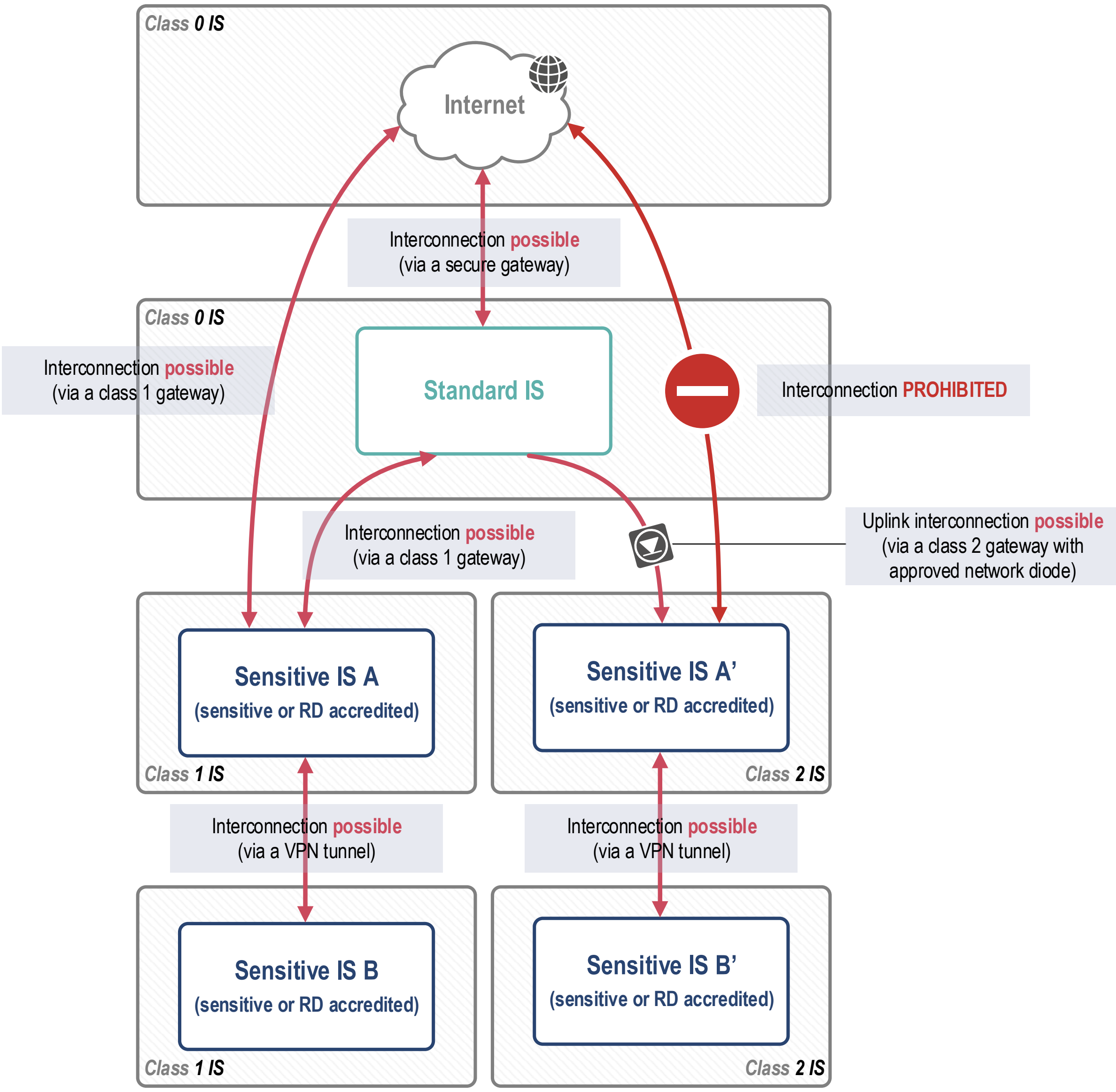


Figure 2 – Mapping of IS classes (0, 1 or 2) to the levels of sensitivity of the ISs (public, standard, sensitive, RD)

Once the information assets have been sorted (recommendation R1) and the nature of the ISs (standard, sensitive, RD) has been identified (recommendation R2), it is possible to distribute the information within these different ISs, according to their position on the scale of confidentiality needs. The figure 3 illustrates this idea.

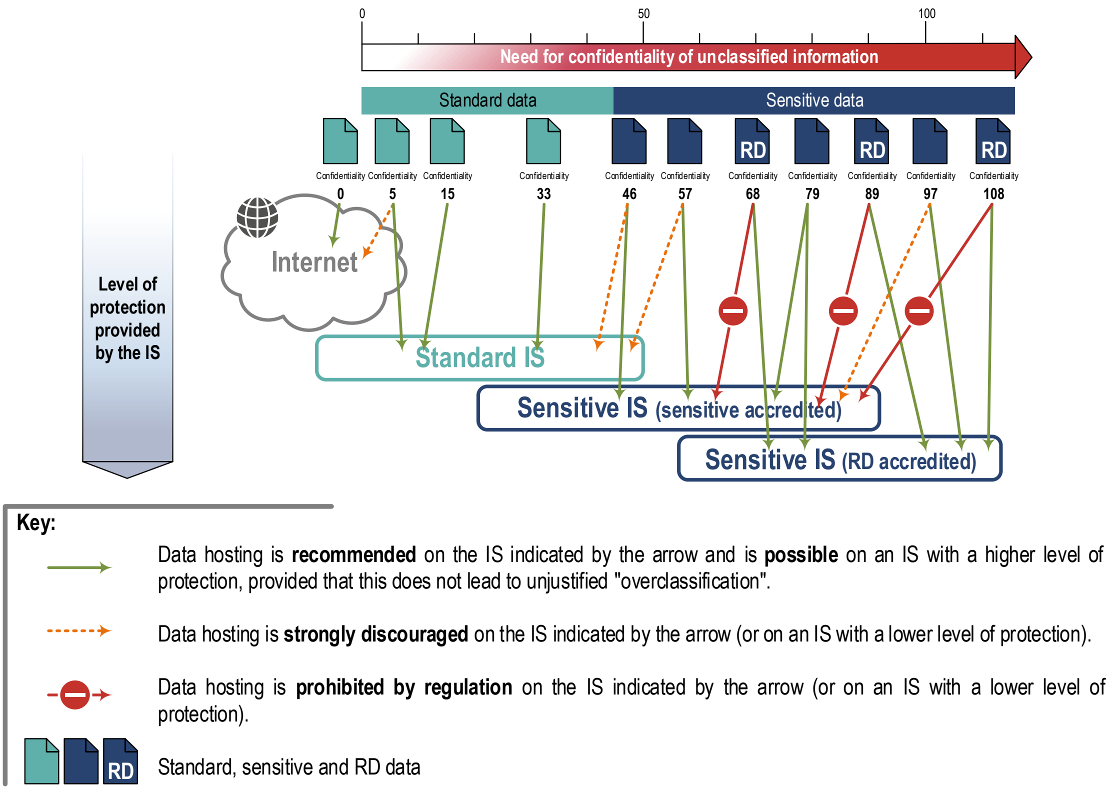


Figure 3 – Choice of an IS adapted to the need for confidentiality protection of information

Looking at the example given in Figure 3, several observations can be made:

- only information with a zero confidentiality level (C0) can be placed on public ISs such as the Internet;
- an arbitrary confidentiality value (C45 in this example) is used to distinguish standard information and sensitive information: above C45, the information is considered sensitive (or RD, if marked RD); below C45, the information is considered as standard;
- in some cases, the choice of IS for hosting information is arbitrary. This is for example the case with C79 information, which is sensitive non-RD information that can be hosted either on a sensitive IS that has been accredited as sensitive, or on a sensitive IS that has been accredited as RD;
- RD information can only be processed on an RD-accredited IS;
- information with a particularly high need for confidentiality protection(C97), but is not RD information, can be processed on a DR-accredited IS [7] ;
- The maximum confidentiality value here is C108, illustrating that the scale of confidentiality needs is, by definition, open and relative.

7. This reasoning, taken to the extreme, can lead to the idea that an entity protects its most sensitive information on an IS that meets the security requirements for an RD-accredited IS, even if none of this information is RD information.

2.3 Determining the protection regime for sensitive information

Having identified that information is to be hosted on a sensitive IS, the entity implementing the sensitive IS must determine the protection regime for that information. This is either the sensitive protection regime (in which case the information must be hosted on a sensitive IS) or the RD protection regime (in which case the information must be hosted on an RD IS).

There are two possible scenarios:

- the RD protection regime is imposed by the State through regulation [8] or by a sponsor through a public contract or contract between private entities;
- for information not covered by the previous case, it is the responsibility of the entity implementing the sensitive IS to choose the protection regime adapted to its needs.

Application of the Restricted Distribution label is based on the need to avoid the disclosure, in the public domain, of information whose aggregation or exploitation could:

- result in the discovery of classified information;
- undermine public security or order, the reputation of institutions, the private lives of their members;
- prejudice the economic or financial interests of private companies or public institutions.

Caution is required with regard to the aggregation of standard information. One piece of information considered on its own may be seen as standard, but *the aggregation* of multiple items of such individual information may result in an increase in the sensitivity of the resulting aggregation.

R3

Determining the protection regime for sensitive information

An entity that implements a sensitive IS must determine the protection regime to be applied to the information it will handle. Depending on the case, this protection regime is either imposed by regulation (or by a third party), or left to the discretion of the entity. *Ultimately*, sensitive information is hosted on sensitive or RD ISs, and RD information must be hosted on RD ISs.

Once the protection regime for sensitive information has been determined, a reading of Article 2 of II 901 makes it possible to deduce which security measures of II 901 are mandatory and which are which are recommended. In addition, annex B of this guide presents the different levels of levels of sensitivity of information in France and specifies the levels for which the security measures of II 901 are mandatory, and for which they are recommended.

8. Article 2 of II 901 lists the cases in which the entity has the obligation to apply an RD protection regime. to apply an RD protection regime.

2.4 Accreditation of a sensitive IS

After defining the protection regime for sensitive information (sensitive regime or RD regime), the entity implementing one or more sensitive ISs must apply security measures to achieve and maintain a sufficient level of security during their operation and until their dismantling. In order to formalise the attainment of a satisfactory level of security, an organisational procedure known as security accreditation must be conducted.

As part of this procedure, a manager of the entity is designated as the Accreditation Authority (AA) by the entity's Qualified Information Systems Security Authority (QISSA) of this same entity [9].

The accreditation process, applied to a sensitive IS, aims to have the AA formally accept the residual risks faced by this IS with regard to its contribution to the entity's missions. For this purpose, an accreditation file is compiled in order to inform the AA on the method of assessing and processing risks (acceptance, refusal, transfer, reduction). In particular, it details the security measures adopted to reduce risks. These security measures are of a technical or organisational nature. They apply to the entity or to stakeholders within its ecosystem (e.g. through contractual clauses). The accreditation file also provides elements for assessing the actual security level of the sensitive IS (e. g. audit reports, qualification, certification or accreditation of product versions deployed on the IS…).

Once these elements have been presented, the AA can make a formal accreditation decision based on its knowledge of the facts. In doing so, it certifies that the risks faced by the information, processing and services of the sensitive IS are known and controlled and that the residual risks have been accepted, taking into account the contribution of the IS to the entity's missions. The sensitive IS is then declared as accredited, for a specified period. Depending on its purpose and regime (sensitive or RD), a sensitive IS is said to be "accredited to sensitive level" or "accredited to RD level".

For more information on security accreditation, it is advisable to refer to the guide published by the ANSSI on this subject [16].

R4

Accrediting any sensitive IS before it goes into production

All sensitive ISs must be accredited. All interconnections for this IS must also be accredited.
The risks to a sensitive IS must also be periodically reassessed as part of a process of continuous improvement and permanent adaptation to the evolution of the threat [10].

The accreditation process for sensitive ISs will lead to the definition of a *II 901 accreditation scope*.

9. See article 86 of the IGI 1300.
10. Refer to Article 3 of II 901 and security measure II 901 EXP-CI-AUDIT.

II 901 accreditation scope

The II 901 accreditation scope delimits the set of systems which, in an accreditation process, must comply with the security measures described in II 901 and in this guide. All equipment involved in the processing or storage of sensitive information (including mobile equipment such as removable media) must be included in the accreditation scope.

Information

II 901 specifies that the accreditation of interconnections for sensitive ISs is subject to separate accreditations from that of interconnected ISs [11].

11. See II 901, annex 2.

3
Types of sensitive IS

Objective

Chapter 2 has explained how the creation of one (and potentiallyseveral) sensitive IS(s) is the answer to an entity's need to protect its unclassified IT defence assets. This chapter aims to present the main types of architecture that can be anticipated for these ISs.

3.1 Representation of architecture typologies

The architecture of an IS is defined by the structure and interactions of the hardware and software components it contains. This chapter aims to introduce the reader to three main types of sensitive IS architecture. These types of architecture are acceptable from a regulatory point of view, although not equivalent in terms of their level of security.

For a proper understanding of the architectures described in this chapter, it is necessary to explain the representation conventions used in the architecture diagrams in this guide.

3.1.1 Graphic conventions for architecture diagrams

In the architecture diagrams presented in this guide, sensitive ISs and standard ISs are intentionally represented symbolically by "monolithic" rectangles (blue for a sensitive IS and green for a standard IS). Each rectangle implicitly contains all the hardware and software components of an IS (servers, workstations, network equipment...).

This representation in the form of rectangles does not mean that the IS is partitioned and that all types of communications between all of the systems that it contains are possible. In fact, in the case of a sensitive IS, the measures for partitioning and hardening the systems are stricter than for a standard IS. These measures, relating to the internal security of a sensitive IS, are described in chapters 5 (principle of defence in depth) and 6 (securing workstations).

Warning

In the architecture diagrams in this document, unless explicitly stated otherwise, all components of sensitive ISs and standard ISs are assumed to be physically separate. In other words, there is no anticipation of mutualisation between sensitive ISs and standard ISs, whether at system level (physical machines, hypervisors...), at network level (routers, switches...) or at storage level (disk bays, *fabric*... switches).

In addition, in the architecture diagrams, the *II 901 accreditation scope* (a concept defined at the end of section 2.4) is represented by orange dotted lines.

Finally, the term *secure Internet gateway* is used on the diagrams to represent the set of protection means recommended to secure the interconnection of any IS (typically a standard IS) with the Internet. This concept of *secure Internet gateway* is explained in the ANSSI guide to the interconnection of an IS to the Internet [23].

3.1.2 IS classes

II 901 defines a concept of network class in its annex 2. This concept, already covered in section 2.2, is used in this guide to explain the various sensitive IS architectures. Wherever relevant, the scopes of the IS classes (Class 1 or Class 2) are represented on the architecture diagrams by means of grey hatched areas.

The definitions of the IS classes are given in II 901 [12], and are repeated below.

IS of class 0

An IS of class 0 is a public IS (Internet, standard IS…) or an IS connected to a public IS which does not meet the requirements of class 1 below.

IS of class 1

An IS of class 1 is an IS that is interconnected [13] to ISs of class 0 using filtering and flow-breaking devices in the following way:

- *at least one filtering device qualified to the standard level is set up to cut off all flows to and from ISs of class 0* [14] *;*
- *a device for breaking all flows (proxy) to and from ISs of class 0, qualified at elementary level if possible, is positioned between two filtering devices ;*
- *a detection sensor qualified at least at elementary level monitors all flows exchanged with ISs of class 0.*

The interconnection of networks of class 1 with each other is allowed under certain conditions (see section 4.2).

The security features required by the regulations to interconnect a sensitive IS of class 1 and an IS of class 0 are grouped in a gateway which is referred to as a *gateway of class 1* in this guide. A *gateway of class 1* is therefore composed of two filtering devices (at least one of which is qualified to the standard level) incorporating a *proxy* and a qualified sensor. This gateway is described in detail in section 4.3.1.

Figure 4 shows the representation of this interface segment in the architecture diagrams in this guide. Note that in some diagrams, for the sake of readability, not all security devices (firewalls,

12. See Annex 2 of II 901.
13. The exact formulation in II 901 is an *IS which is isolated*. For clarity, in this guide, the term *isolated* is reserved for ISs of Class 2.
14. This wording suggests that this filtering device is unique. This is terminologically incorrect. Rather, it is recommended that several flow breakers should be implemented depending on the nature of the protocols and in order to reduce the attack surface.

proxy and sensor) will always be systematically shown. However, wherever the term *gateway of class 1* is used in the diagrams, it will be implied that these devices must be present, even if they are not shown.

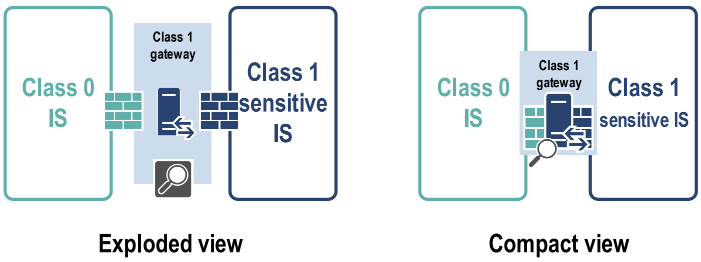


Figure 4 – Representations of a *gateway of class 1* in this guide. The two representations (exploded and compact) have strictly equivalent meanings.

IS of class 2

An IS of class 2 is an IS that :

- *is isolated, i.e. not connected, even indirectly, to the Internet;*
- *does not include any "downlink interconnection" enabling the sending of clear or encrypted flows to ISs of class 0 or 1, except by means of devices specifically approved for this purpose (concept of "downlink gateway") ;*
- *may include "uplink interconnections" allowing the reception of flows from ISs of class 0 or 1 through a diode approved by ANSSI for such uses (concept of an "uplink gateway").*

The interconnection of networks of class 2 with each other is allowed under certain conditions (see section 4.2).

3.2 Different sensitive IS architectures

3.2.1 Physically isolated sensitive IS

By definition, sensitive IS architectures of class 2 are "physically isolated" ISs. In such an IS, no storage or data processing components (servers, workstations, storage bays...) are shared with another IS of class 1 or of class 0.

In addition, this type of IS does not interconnect with an IS of class 0, unless special conditions are met (see section on section on secure exchange systems for users). Connection to resources hosted on the Internet is not allowed from a sensitive IS of class 2.

As a result of their strong network isolation, sensitive IS architectures of class 2 have a low level of exposure to threats from other ISs. The use of these architectures is mandatory in cases where the risks to the sensitive IS are high.

Choosing a sensitive IS of class 2, physically isolated from any other IS, is all the more important when the size of the IS is small (typically, a sensitive IS consisting of a few workstations for viewing sensitive information).

Warning

An IS of class 2, while physically isolated from any other IS, must not be automatically assumed to be a *secure IS*. Indeed, the absence of interconnection, while reducing the exposure of the IS to threats, can also make it more complex to administer, maintain in secure condition and monitor, which can be problematic for the most extensive and sensitive ISs.

Warning

The total absence of interconnection does not mean that data cannot be introduced into or extracted from an IS of class 2. Business needs may require that data insertion or extraction using removable media may be permitted by the security policy. In this case, the management of these media must be strictly controlled, or else the expected benefits of the isolation strategy could be lost. More information about removable media can be found in section 5.7.

R5 +

Physically isolating the sensitive IS and the standard IS

It is recommended that entities with significant confidentiality needs implement at least two physically isolated ISs (a standard IS and a sensitive IS). In this case, the sensitive IS is an IS of class 2 with no interconnection, even indirect, with the Internet.

Figures 5 and 6 give two simplified functional representations of possible architectures for sensitive ISs of class 2. The first architecture example (figure 5) implements an uplink gateway from a less trusted IS (in this case a standard IS) to an IS of class 2. The second example (figure 6) shows a totally isolated sensitive IS of class 2 without direct interconnection.

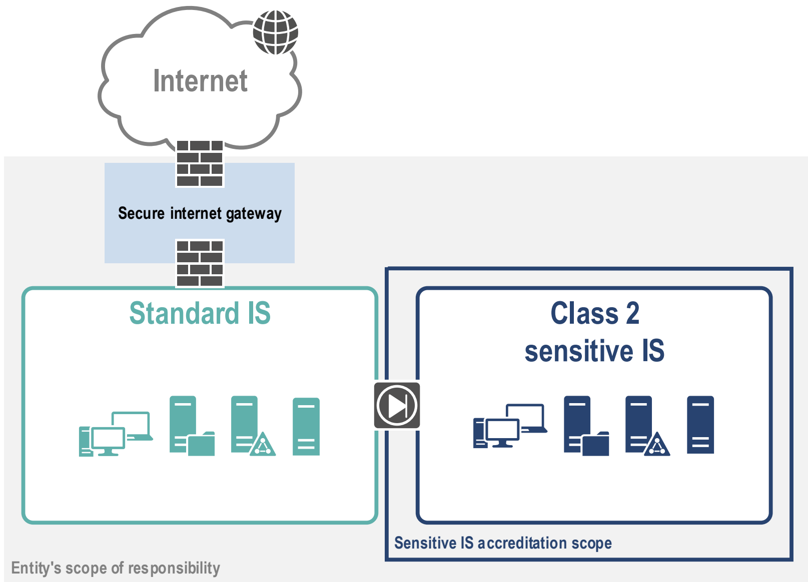


Figure 5 – Sensitive IS of class 2 - Example of an architecture with a direct one-way interconnection via an uplink gateway

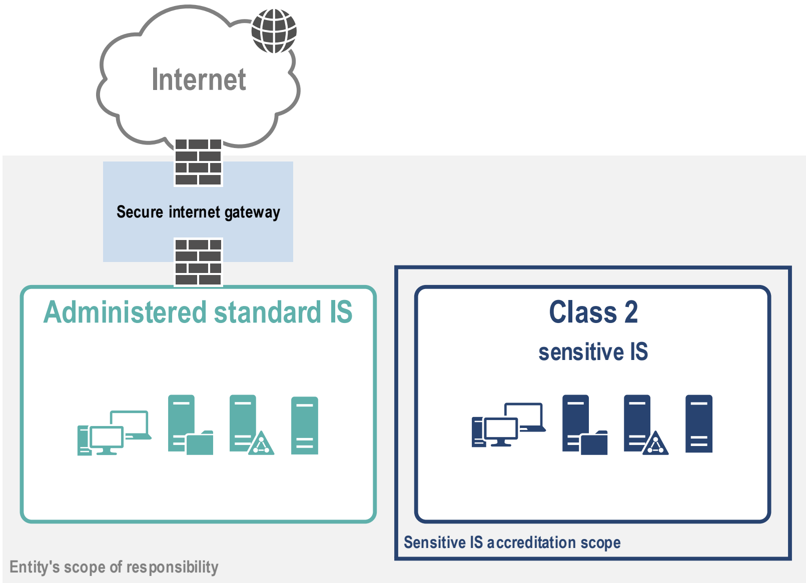


Figure 6 – Sensitive IS of class 2 - Example of an architecture without direct interconnection

3.2.2 Physically partitioned sensitive IS

Where business needs are not compatible with a "physically isolated sensitive IS architecture" and security requirements allow it, it is possible to opt for a sensitive IS architecture of class 1 : a "physically partitioned IS".

This type of IS is similar to a "physically isolated sensitive IS" as no storage or data processing (servers, workstations, storage bays…) components are shared with any other IS. But it differs in that one or more interconnection gateways provide the ability to transfer data bidirectionally through the network, with one or more other ISs and, potentially, with the Internet.

This type of architecture makes it possible to provide services that are difficult or impossible to implement in the case of networks of class 2, in particular services requiring interactions between the sensitive IS and third party ISs, e.g. the Internet.

This architecture may be relevant for entities with business processes for which the creation, processing and storage of sensitive data is not a major part of the business.

The interface segment between ISs of class 0 and ISs of class 1 shall host as a minimum the security components listed in the regulation, i.e. filtering devices, protocol breaking devices and intrusion detection devices (see the definition of an IS of class 1 recalled in section 3.1.2).

R5

Physically partitioning the sensitive IS and the standard IS

If it is not possible to implement a physically isolated IS, it is possible to build two ISs (a sensitive IS and a standard IS) which are physically partitioned and interconnected by a bidirectional gateway in accordance with II 901. In this case, the sensitive IS is an IS of class 1 indirectly interconnected to the Internet.

Figure 7 gives a simplified functional representation of the possible architecture of a physically partitioned, sensitive "IS".

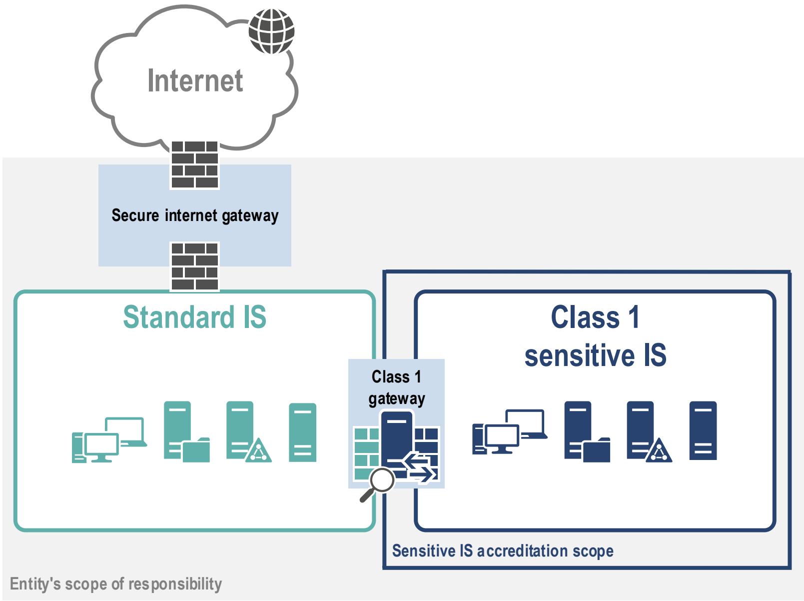


Figure 7 – Sensitive IS of class 1 - Example of a physically partitioned IS architecture

3.2.3 Sensitive IS without standard IS

Where business needs are not compatible with a "physically partitioned sensitive IS" architecture and security requirements permit, a degraded version of the sensitive IS architecture of class 1 presented in the previous section is feasible. In this architecture, standard data and sensitive data are hosted within the same IS. However, this does not mean that the two sets are merged in terms of their architecture. On the contrary, logical partitioning mechanisms must be implemented, both at network level (segmentation of networks and strict filtering of flows between these segments), and at system and application levels, to separate sensitive data and processing from standard data and processing.

Unlike the architectures presented in the previous sections, with a "sensitive IS without a standard IS", some of the components (hypervisors, servers, storage bays, network equipment…) are mutualised for the "subset of standard data" and for the "subset of sensitive data".

The bidirectional transfer of data, through the network, with one or more ISs of class 0 (and thus, potentially, with the Internet) is only possible through one or more interconnection gateways.

This architecture may be relevant for entities implementing business processes whereby the creation, processing and storage of sensitive data is a major part of the business activity.

With this architecture, the *II 901 accreditation scope* includes not only sensitive resources but also standard resources. The standard means, which are *de facto* hosted on a sensitive IS, must be protected as if they were sensitive means and must therefore comply with II 901 security measures. It obliges the person responsible for the sensitive IS to be very rigorous in the actions of maintaining *all* IS resources in secure and operational conditions.

Warning

This architecture is inherently much more difficult to secure than those presented in sections 3.2.1 and 3.2.2. Indeed, not only is the *II 901* accreditation scope of the IS extended, but a logical partitioning system (between the subset of sensitive data and the subset of standard data) provides a lower level of robustness than physical partitioning. Logical partitioning increases the attack surface consequently requires very strong control over the configuration of the systems and the ability to maintain this control over time. This architecture must only be considered as a last resort and is reserved for entities with a high degree of ISS maturity.

Warning

With this architecture, if the web browsing service is required, the application of the recommendation R18- (bounce servers) is strongly recommended.

R5 -

Logically partitioning sensitive data within a sensitive IS

In the absence of the implementation of a physically isolated or physically partitioned sensitive IS, entities with a high level of IS maturity may consider setting up a sensitive IS and not creating a standard IS [15]. Standard resources must then be included within the *II 901 accreditation scope* of the sensitive IS.
Within this sensitive IS, sensitive data must be logically partitioned from standard data.
In this architecture, the single IS is a class 1 IS interconnected to the Internet by means of a *secure Internet gateway* which integrates all the security features defining a *gateway of class 1*.
If the web browsing service is required, it is strongly recommended that it be delivered through a user workstation bounce infrastructure (see recommendation R18-).

Figure 8 gives a simplified functional representation of the architecture of an IS with logical partitioning of sensitive and standard data.

15. The causal link here must be clearly understood : it is precisely because an entity has high technical skills in the field of ISS and intends to maintain them over time (cause) that it may consider choosing such an architecture (consequence). The converse reasoning would be erroneous: the mere act of choosing this type of architecture does not mean that an entity can consider itself mature in terms of ISS. This architecture must be considered only as a last resort.

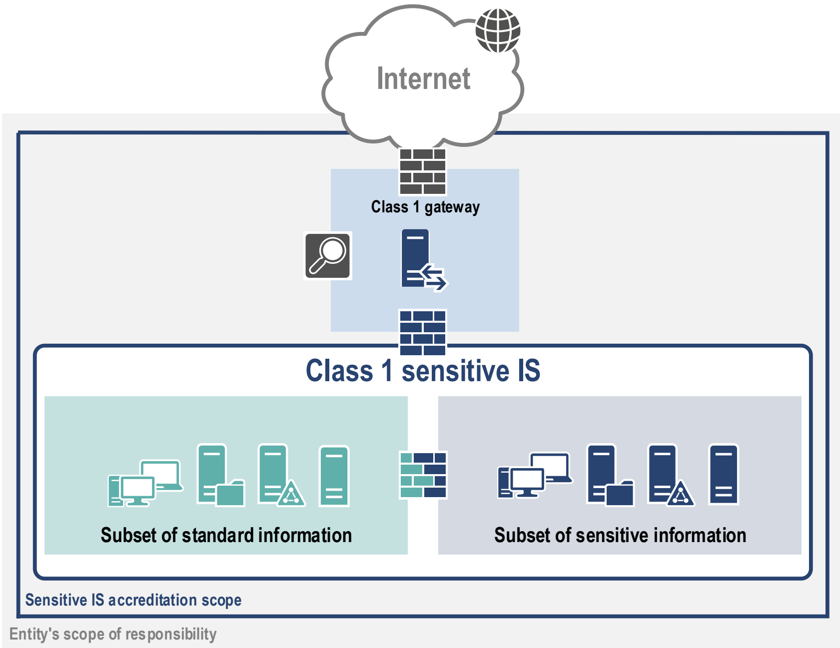


Figure 8 – Sensitive IS of class 1 - Example of architecture with logical partitioning of sensitive and standard data

Considerations on the mutualisation of resources

In this "sensitive IS without standard IS" architecture, the *II 901* scope of accreditation is not restricted to sensitive means but extended to standard means. As a result, security costs increase. The entity implementing this architecture is prompted, in order to respond to the need for partitioning of standard and sensitive data, to consider the level of mutualisation acceptable for sensitive IS components. This study must take into account all the components of the IS (network, systems, storage…).

Security requirements that aim to reduce the risk induced by the use of mutualisation between the "subset of standard data" and the "subset of sensitive data" must be the subject of specific studies conducted by the entity and be integrated into the accreditation process.

It is beyond the scope of this guide to comment on which cases of mutualisation are acceptable and which are not. The answer to this question depends on the technological choices made by the entity, and the technological offer is far too vast, and evolves too quickly, to be able to draw up precise rules.

Nevertheless, some guiding principles can be stated.

If a component is mutualised to process both standard and sensitive data, efforts should be made to implement at least two robust and complementary logical barriers, to protect access to the data. This double protection is intended to improve partitioning: the compromise of a barrier (whether malicious or through human error) does not expose sensitive data [16].

R6

Applying the principle of defence in depth when mutualising resources

The concept of defence in depth is a strategic principle of II 901 [17]. In particular, in cases where the mutualisation of resources of a sensitive IS with another IS is anticipated, the entity must systematically implement the concept of defence in depth to reduce the risks induced by such mutualisation.

Another example of equipment that can be mutualised is workstations. This mutualisation can be designed in strict compliance with the recommendations R52- (multi-level workstation) or R52-- (sensitive workstation with remote access to the standard IS) detailed in the section 6.3 on workstation aspects.

It is possible to mutualise administration workstations for the administration of sensitive resources and resources. On the other hand, recommended practice is to dedicate administration tools by level of sensitivity (tools for the administration of sensitive resources and separate tools for the administration of standard resources). For more information, refer to section 7.2 on IS administration.

In the case of the R5+ and R5recommendations, the directory service is, by assumption, necessarily made up of separate directories (one standard and one sensitive). Consequently, the question of their mutualisation does not arise. Conversely, an entity implementing the architecture covered by the degraded recommendation R5- ("sensitive IS without standard IS"), could be tempted to create a single directory: such mutualisation is strongly discouraged.

R7

Partitioning sensitive and standard directories

In the context of the degraded recommendation R5-, it is strongly recommended that the entity implements separate directories: at a minimum, one directory is deployed for sensitive users and resources and a second is for standard users and resources.

3.3 Criteria influencing the choice of architecture for sensitive ISs

Section 3.2 gives three examples of sensitive IS architectures that are acceptable from a regulatory perspective. An entity wishing to deploy a sensitive IS must choose which of these three architectures is/are the most suitable for its business environment and strategy. In this respect, it is the responsibility of the institution to consider, at the upstream stage of the project to implement a sensitive IS, the business and regulatory criteria that will inform this decision.

Only the entity itself can carry out this analysis, and it would be futile to present in this guide a decision tree to establish a preference for one architecture over another. Instead, this section aims to explain the main criteria to be considered when making an informed choice.

16. For example, if a storage array is used to store both types of data, it makes sense to define separate logical data volumes for each and complement this with encryption of sensitive data (file system level encryption or data level encryption).
17. See Article 3 of II 901.

Target level of protection for the confidentiality of sensitive information

In the case of sensitive IS as defined in II 901, one of the main security objectives is the protection of the *confidentiality* of the *information* hosted on these ISs.

In order to achieve this objective, it is also desirable to protect the integrity of the sensitive *IS*: a degradation of the integrity of the IS could *ultimately* lead to the disclosure of information with a high level of confidentiality [18].

However, the levels of protection for sensitive information are not equivalent for the three main types of architecture presented in the previous section. The architecture associated with the recommendation R5+ ("physically isolated sensitive IS") provides a higher level of protection than the architecture associated with the recommendation R5 ("Sensitive IS physically partitioned from the standard IS"), which is itself of a higher level than the architecture associated with the recommendation R5- ("IS without a standard IS").

Thus, the main criterion to be taken into account for the implementation of a sensitive IS is the level of protection that the entity responsible for the IS is seeking to achieve for the protection of sensitive information for which it is responsible.

ISS maturity level of the entity responsible for the sensitive IS

The three main types of architectures presented in the previous section differ not only in the level of protection they provide for sensitive data, but also in the complexity of their implementation. For example, a "physically isolated sensitive IS", if it lacks an approved downlink gateway, is much simpler to design than other types of sensitive IS : the absence of a downlink interconnection reduces the risk of data exfiltration. While not solving all the problems (the problem of management of removable media remains), such an architecture does remove many of the difficulties and reduce the risks.

In general, the implementation of an IS of class 1 generates strong constraints on the interconnections of this IS (see chapter 4) and on the control of users' workstations (see chapter 6).

An IS of class 1 also implies a high level of ISS maturity on the part of those responsible for its design and operation. Consequently, sensitive IS architectures of class 1 are not very suitable for entities with a small number of qualified ISS personnel. Architectures of class 2 should be used in preference in this case.

The ISS maturity of an entity also depends heavily on the level of appropriation of IT hygiene rules [19] by users. Users are responsible for the proper handling of the (standard or sensitive) information they produce or which is entrusted to them [20]. However, the rules relating to this processing will be easier to understand if the architecture chosen for the sensitive IS clearly demonstrates, by

18. The provision of optimal protection of the confidentiality of *information* hosted on a sensitive IS is a characteristic of sensitive ISs under the meaning of II 901. In this sense, these ISs are distinguished from ISs for which the main objective is to ensure a good level of protection in terms of integrity and availability of the *processing operations* they implement. Examples of such ISs are certain critical information systems (SIIVs) and certain essential information systems (SIEs).
19. For more information on the basic security rules recommended by ANSSI, see the IT hygiene guide [11].
20. See measure II 901 GDB-PROT-IS.

construction, the existing partitioning between the different ISs. This will make "physically isolated sensitive IS" and "physically partitioned Sensitive IS" architectures more intuitive for their users. The need to authenticate using separate authenticators, preferably from separate workstations, will enable users to work unambiguously on both standard and sensitive ISs.

In the case of the "Sensitive IS without standard IS" architecture, it should be noted that the II 901 security measures, which are required to achieve the level of protection of a sensitive IS, and which apply to all users of the entity, could be perceived as constraints by those who only need access to standard resources.

Interconnection needs for a sensitive IS

Business imperatives may inform more or less important needs to connect a sensitive IS with other IS, whether the latter are of a lower, equal or higher sensitivity level than the sensitive IS. These needs for connections with other ISs influence the choice of architecture for a sensitive IS. For example, the creation of a sensitive IS of class 2 may be imposed by a business need requiring interconnection with a partner that has itself implemented an IS of class 2.

Regardless of their number, direction (uplink or downlink) and nature (network interconnections or data transfers using removable media), data exchanges with a sensitive IS must be justified by business needs and limited to what is strictly necessary (principle of minimality). The creation and maintenance of a comprehensive map of exchanges will be very useful for the detection of abnormal or unusual exchanges, and, in the case of a downlink gateway, for the definition of a potential list of authorisations.

Quantity of sensitive information

Not all information handled by an entity is sensitive. The ratio between sensitive and standard information varies depending on business needs. The method of evaluating the quantity and importance of sensitive data in relation to standard data depends on the development strategy of the entity concerned. This quantitative and qualitative assessment may take into account elements such as the number of users of the entity who are required to consult or process sensitive information, the total volume of sensitive data under the entity's responsibility (whether by its own doing or entrusted by third parties) or the strategic importance of this information in comparison to the other information for which it is responsible.

Other criteria

Other factors must be taken into account by the entity when developing the architecture of a sensitive IS : the implications for the working methods of users and IS administrators, other regulatory obligations to which it is subject [21], the prospects of extending the sensitive IS to meet future business challenges, etc....

21. For example, compliance with financial regulations.

4

Direct interconnections of sensitive ISs

Objective

This chapter presents recommendations for securing direct interconnections of a sensitive IS with other ISs. The term “direct interconnection” refers to interconnections made by means of devices allowing the exchange of information by transfer of electromagnetic signals between interconnected ISs. These direct interconnections are in contrast to interconnections made indirectly, by means of removable media (for more information on such indirect interconnections, see section 5.7).

4.1 General

A sensitive IS may have interconnections with other ISs. In order to prevent intrusions and exfiltration, the entity must control these interconnections. This control requires consideration of the following elements, among others:

- any interconnection with the entity’s internal ISs or with third-party ISs (e. g. the Internet) must be inventorised and accredited (see section 2.4 on security accreditation). Particular attention must be paid to all specific interconnections (e. g. remote maintenance links for industrial facilities, see section 7.3), as well as any uncontrolled interconnections that could be introduced by the implementation of components connected to the IS (e. g. the communication capabilities of multifunction printing devices must be disabled [22]) ;
- mobile access is possible but must have business justification and integrated into the risk analysis conducted as part of the accreditation process. If the mobile service is authorised, its technical and organisational structure must comply with the security measures of II 901 (see section 6.4 on digital mobility) ;
- the sensitive IS must be subject to permanent security monitoring, enabling the detection of communication channels likely to exfiltrate data via the network (these channels can be created without the user’s knowledge in the case of an attack, or by deliberate unauthorised action on the part of the user). This constant security monitoring of the sensitive IS must comply with II 901 security measures (see section 7.5 on logging and security monitoring).

22. Refer to measure 901 EXP-IMP-2.

4.2 Interconnection of a sensitive IS with a second sensitive IS

Interconnections of two sensitive ISs (class 1 or class 2) are possible, including connections via networks that are not trusted (class 0). However, they must meet certain prerequisites.

Any interconnection of sensitive ISs must be accredited before it is put into production and be accredited separately from the ISs [23]. If the two sensitive IS to be interconnected are not under the authority of the same legal entity, the two parties must first define a legal entity, the two parties must begin by defining a common accreditation strategy and specify their respective areas of responsibility [24].

As part of this accreditation, a risk analysis must be conducted to enable the two entities to determine the security functions to be carried by the interconnection gateway and to specify the flows authorised to pass through it.

When examining the accreditation file, each entity must be alert to the quality of the other party's sensitive IS accreditation file, and, in particular, to the following points:

- the type of IS architecture implemented by the other party because, as explained in chapter 3, not all sensitive IS architectures are equivalent in terms of their security;
- for the interconnection of RD ISs, strict compliance with the mandatory technical specifications (in particular the recommendations of this guide concerning the use of RD-approved encryption means);
- the list of residual risks identified at the end of the accreditation process for the entity's IS.

R8

Defining an accreditation strategy for each sensitive IS interconnection

The interconnection of two sensitive ISs must be covered by a specific accreditation in which each of the parties ensures that the impact on security of the interconnection is compatible with the security needs expressed in the accreditation file of the IS for which it is responsible.

Interconnections between sensitive IS must implement encryption equipment, placed at the cut-off point of all flows and approved by the ANSSI (for the protection of RD information) or with a security visa [25] (with regard to the protection of sensitive information). If IPsec is used, the encryption devices must be configured according to the recommendations of ANSSI [17].

23. See II 901, annex 2.
24. The accreditation strategy corresponds to steps 1 to 4 of the 9 step accreditation process which is described in the ANSSI guide to security accreditation [16].
25. See annex C for more information on security visas and approvals.

R9

Securing RD IS interconnections

RD IS interconnections must be secured by means of VPN tunnels guaranteeing the protection of all exchanged flows (confidentiality, integrity, anti-playback, mutual authentication of endpoints). The equipment used to establish these VPN tunnels must be approved by ANSSI.

R10

Securing interconnections for sensitive ISs

It is strongly recommended that interconnections for sensitive ISs should be secured by means of VPN tunnels guaranteeing the protection of all exchanged flows (confidentiality, integrity, anti-replay, mutual authentication of endoints). It is also recommended that the equipment used to establish these VPN tunnels should have an ANSSI security visa.

Information

In the specific case where the two sensitive IS are physically co-located [26], if the results of the risk analysis reveal that the risk of compromise of the data transmitted via the interconnection is acceptable given the technical and organisational measures in place, it is possible to consider not encrypting the interconnection of the two sensitive ISs [27].

In the case of an interconnection of two sensitive ISs, placed under the responsibility of two separate legal entities, it is also recommended that each party implement qualified filtering equipment, within the limits of its own area of responsibility.

Figure 9 shows the positioning of the filtering and encryption functions of an interconnection between sensitive ISs.

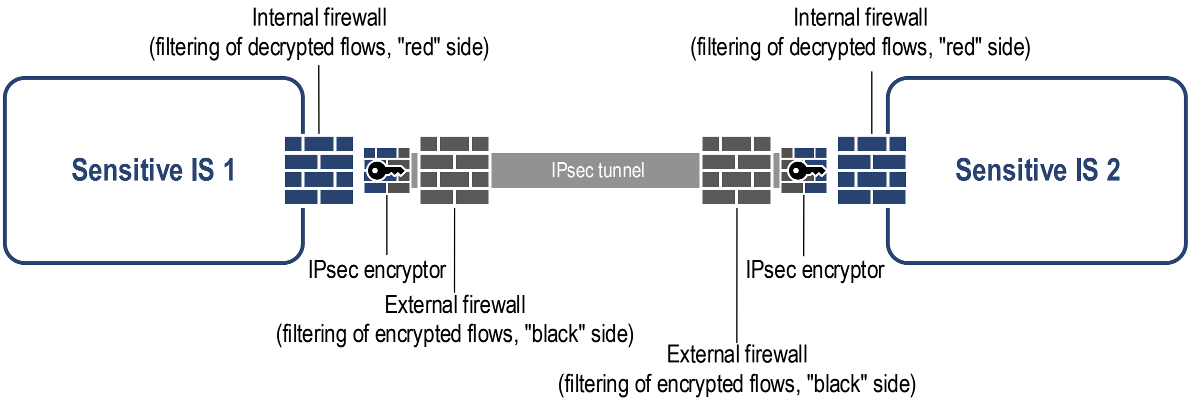


Figure 9 – Architecture of an interconnection between sensitive ISs

26. The term "co-located" means that the two IS have contiguous physical locations. For example, two separate legal entities located on the same floor of a building with whose premises are adjacent.
27. Refer to security measure II 901 RES-INTERCOGEO.

It is recommended to filter the flows upstream of the encryptor (using the external firewalls shown in Figure 9) but also downstream (using internal firewalls). The purpose of black-side filtering [28] (external firewall) is to protect the encryption device on its black side by reducing its exposure and to prevent any information leakage that might result from an configuration error of the encryptor. The purpose of red-side filtering is to give the party responsible for the sensitive IS control of the flows "outside the tunnel" entering or leaving this IS. In particular, if the two sensitive IS are of class 1, it is recommended that each entity blocks access to ISs of class 0 through the interconnection, so as not to rely on filtering that is carried out by the other entity and that it therefore does not control.

R11

Filtering the flows of sensitive IS interconnections

It is recommended that two legal entities wishing to interconnect their sensitive ISs should each implement, under their respective control, filtering devices, upstream and downstream of the encryptors. It is recommended that these devices should be qualified.

Information

The filtering function provided by the black-side firewall and the encryption function may be mutualised, provided that the single equipment providing both functions is suitable for the protection of sensitive information [29] and that the filtering is configured to prevent any risk of data leakage [30].

4.3 Interconnection of a sensitive IS of class 1 with an IS of class 0

It is difficult to achieve a good level of security for Internet access gateways. Not only must the initial design and implementation be state-of-the-art, but a high level of security must then be maintained over time. ANSSI has published the [23] guide which lists security measures for ensuring a secure interconnection to the Internet. Its application is especially recommended in the case of sensitive ISs.

R12

Applying ANSSI recommendations relating to the interconnection of an IS to the Internet

It is strongly recommended that the interconnection of a sensitive IS of class 1 with the Internet should at a minimum adhere to the best practices of the ANSSI, in particular those listed in the guide relating to Internet interconnection architectures [23].

28. The "black" side is the encapsulated and encrypted flows of the tunnel created by the encryptor, as opposed to the "red" side where the flows are "outside the tunnel".
29. In practice, it is a matter of checking that the two functions are approved (in the case of RD ISs) or qualified (in the case of sensitive ISs) and that their simultaneous use on the same equipment is authorised under the conditions of use attached to the approval or qualification.
30. For example, if the single device is a Stormshield SNS firewall, the reader is referred to chapter 7 of the [5] guide on IPsec VPN configuration.

The interconnection of a sensitive IS of class 1 with an IS of class 0 implies the implementation of a *gateway of class 1* as defined in section 3.2.2.

4.3.1 Nature of the security features of the gateway of class 1

The definition of a gateway of class 1 (see section 3.1.2) implies implementation under the control of the entity responsible for the sensitive IS to be interconnected [31], for several security devices. These devices are subject to recommendations published in the [23] guide, covering the interconnection of an IS to the Internet. This section aims to provide additional information regarding their implementation in the case of a sensitive IS of class 1.

Qualified firewalls

For the interconnection of a sensitive IS with an IS of class 0, it is necessary to implement a DMZ ([32]) contained within two firewalls, at least one of which is qualified to the standard level. One of the firewalls, known as an "external firewall", is connected to the IS of class 0 ; the other one, known as an "internal firewall", is connected to the sensitive IS (see section 3.2.2). For more information on firewalls in Internet-exposed zones, and in particular their positioning and technological diversification, ANSSI has published the [21] guide. Its section 4.2 deals specifically with the case of a secure Internet gateway protecting an RD IS.

R13

Gateway of class 1 : implement at least one qualified firewall

The entity responsible for an RD IS must implement a qualified filtering device at the standard level by cutting off all flows to and from the IS of Class 0.
It is strongly recommended that this recommendation be applied to sensitive ISs.

Flow-breaking device

A protocol break consists of interrupting a session that has been established, by means of a communication protocol, between two parties. It can be done with or without a change of protocol.

Protocol break devices can be extremely diverse in nature. Depending on the context, it may be a file-sharing server, an inter-application gateway, a proxy gateway, a proxy server, etc.

Flow breakers to and from ISs of Class 0 must be implemented. These relays must be positioned in the DMZ, between the two firewalls mentioned in the previous paragraph.

Under no circumstances should outgoing flows be initiated from the sensitive IS to ISs of a lesser sensitivity level without passing through a relay server. Indeed, direct flows of this type, because they avoid the logging policy implemented at the relay servers, can be used by an attacker who has compromised a resource on a sensitive IS to establish stealthy outbound communications. Such channels can be used to exfiltrate data, upload attack tools, etc.

A specific risk analysis must be carried out to determine the nature of the flow breakers to be implemented and to identify the security functions sought, within the context of the entity's use :

31. See security measure II 901 RES-INTERCO.
32. *Demilitarized zone*

access filtering to resources, protocol analysis, detection of data leaks, attributability of actions, logging, etc. At a minimum, for flows including files, a malware detection function is implemented.

Warning

Protocol breaking also applies to secure flows. The inspection of secure flows (e.g. TLS) increases the risk of compromising the confidentiality of the exchange, as the flow is decrypted and then re-encrypted during inspection. The equipment implementing these inspections must therefore be selected with great care, and the cryptographic parameters must be configured in such a way that the level of protection of the flow before inspection is not degraded by the inspection equipment [33]. Attention must also be paid to the organisational part, as third parties could potentially have access to the unencrypted data during the inspection, whereas they would not have had access to it in the absence of an inspection (e. g. administrator of the inspection equipment, management of the equipment's physical media in the event of maintenance...).

R14

Gateway of class 1 : implement at least one flow breaker

The entity responsible for an RD IS must implement one or more flow breakers from and to the IS of class 0; these should be qualified if possible. These devices should be positioned between two filtering devices.
It is advisable to apply this recommendation to sensitive ISs.

Qualified detection system

To improve the detection of computer attacks, the deployment of a detection system (including a sensor) at any gateway of class 1 is mandatory. The effectiveness of this equipment depends largely on the quality of the indicators of compromise [34] that they use.

R15

Gateway of class 1 : implement a detection system

The entity responsible for an RD IS must implement a detection system, including a qualified sensor, within each of the *gateways of class 1*, in order to control all incoming and outgoing flows for the RD IS.
It is advisable to apply this recommendation to sensitive ISs. At a minimum, a detection system must be implemented on sensitive ISs, even if it is not qualified.

It is essential that the network traffic capture functionality cannot be hijacked to compromise the IS. To reduce this risk of diversion, it is recommended to connect the detection sensor to the listening points of the network using specific equipment (*taps*). It is also recommended that this

33. For more information on TLS inspection, please refer to 4.3 of the [23] guide in its version 3 of June 2020.
34. Indicators of compromise or technical markers refer to the set of meta-data that enable the technical characterisation of past computer attacks. These can be IP addresses or DNS domain names of malicious servers, web addresses of booby-trapped sites, file fingerprints... Monitoring and triggering alerts when these IOCs (*Indicators of compromise*) are detected allows for an early reaction to a potential attack.

equipment be totally passive, not remotely administered, and qualified by ANSSI. Capturing network traffic by copying flow capture at network switches [35] not recommended.

R16

Gateway of class 1 : implement qualified passive taps

The entity responsible for an RD IS is advised to implement passive *taps* to supply the detection sensor(s) with a network flow. It is recommended for this equipment to be qualified by ANSSI.

For more information on security incident detection, see section 7.5.

4.3.2 Positioning of the security devices of the gateway of class 1

The purpose of this section is to detail the positioning of the security devices, described in the previous section, in relation to each other, according to the different architectures described in section 3.2.2.

Figures 10 and 11 show the two examples of sensitive IS architecture of class 1 presented in section 3.2, namely the "physically partitioned sensitive IS" and the "sensitive IS without a standard IS". These figures specify the regulatory requirements for the nature of the security certifications, qualifications or approval for the main security devices (firewalls, servers, proxies and sensors) listed in the previous section. In addition, they give recommendations regarding the technological diversification of firewalls.

35. A feature known as "port mirroring" is

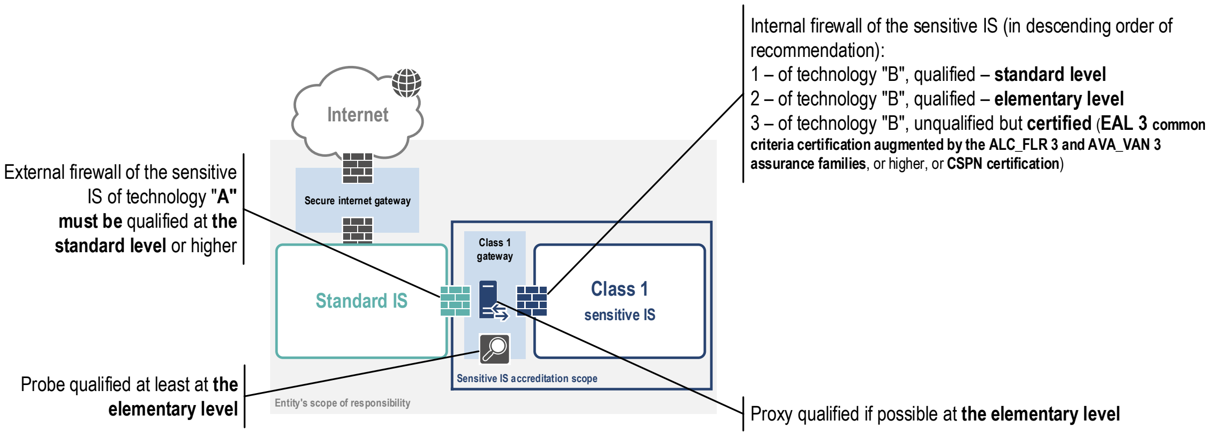


Figure 10 – Sensitive IS of class 1 - Example of a physically partitioned IS architecture : positioning of security devices

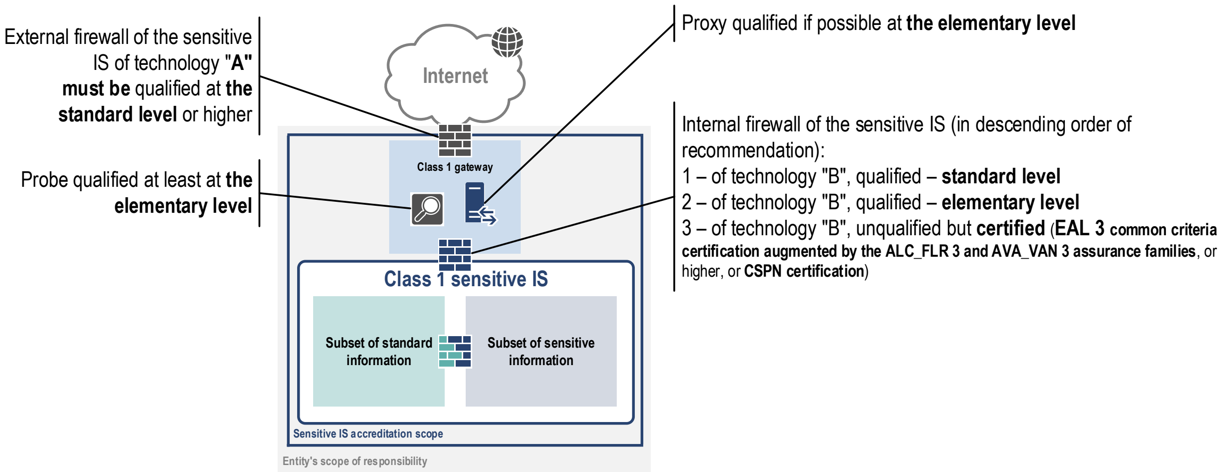


Figure 11 – Sensitive IS of class 1 - Example of an architecture with logical partitioning of sensitive and standard information : positioning of security devices

R17

Gateway of class 1 : have security functions provided by separate devices

It is recommended that the security functions of the firewalls, flow breakers and sensors of the Class 1 gateway should be provided by physically separate hardware devices.

4.3.3 Web browsing

Web browsing represents a significant source of threat for the compromise of an IS. The most secure approach is to prohibit this service from sensitive ISs [36], and to set up a dedicated infrastructure, from physically separate workstations [37].

36. Defining sensitive ISs of class 2 makes Web browsing impossible from this type of IS.
37. See security measure II 901 RES-INTERNET-SPECIFIC.

R18

Prohibiting web browsing from sensitive ISs

Web browsing is not possible from sensitive ISs of class 2. For sensitive ISs of class 1, it is recommended that access to the web browsing service be denied. If the browsing service is required, it must be made available to users from a dedicated IS.

If there are business requirements to allow web browsing from sensitive ISs of class 1, it is possible to deploy bounce servers with hardened configurations [38]. For added security, it is further recommended that these bounce servers be non-persistent and reset regularly or even each new time the web browsing service is used. Figure 12 illustrates web browsing architectures that use bounce servers.

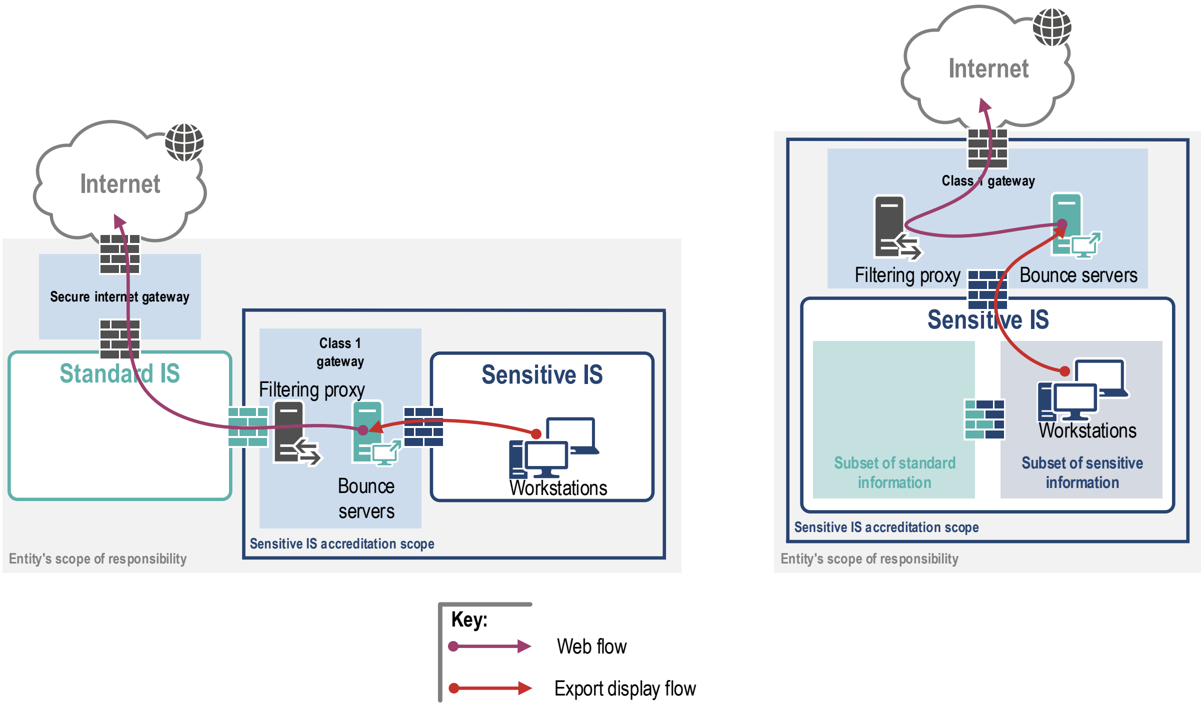


Figure 12 – Web browsing : examples of architectures for an IS of class 1, with bounce servers (left: case of a physically partitioned architecture; right: case of an architecture with logical partitioning of sensitive and standard information)

R18 -

Enabling web browsing from bounce servers

For sensitive ISs of class 1, it is strongly recommended to deploy an infrastructure of bounce servers dedicated to web browsing. This infrastructure is partitioned from the sensitive IS. Users connect via remote access from their sensitive workstations to this infrastructure. Only these bounce servers allow web browsing from the sensitive IS, and authorisations to access the service are strictly limited to operational needs.

An alternative recommendation to the R18- recommendation is to pass webflows between sensitive workstations and web servers through *proxy* servers controlled by the party responsible for the

38. See section 4.5 and recommendation R27+ of guide [23].

sensitive IS. Compared to the R18- recommendation , this solution is more risky. Indeed, in this architecture, the workstation used for browsing is directly connected to the sensitive IS : if the workstation is compromised, the attack is not contained and the entire sensitive IS is likely to be compromised. Figure 13 shows a representation of Web browsing architecture that use proxies.

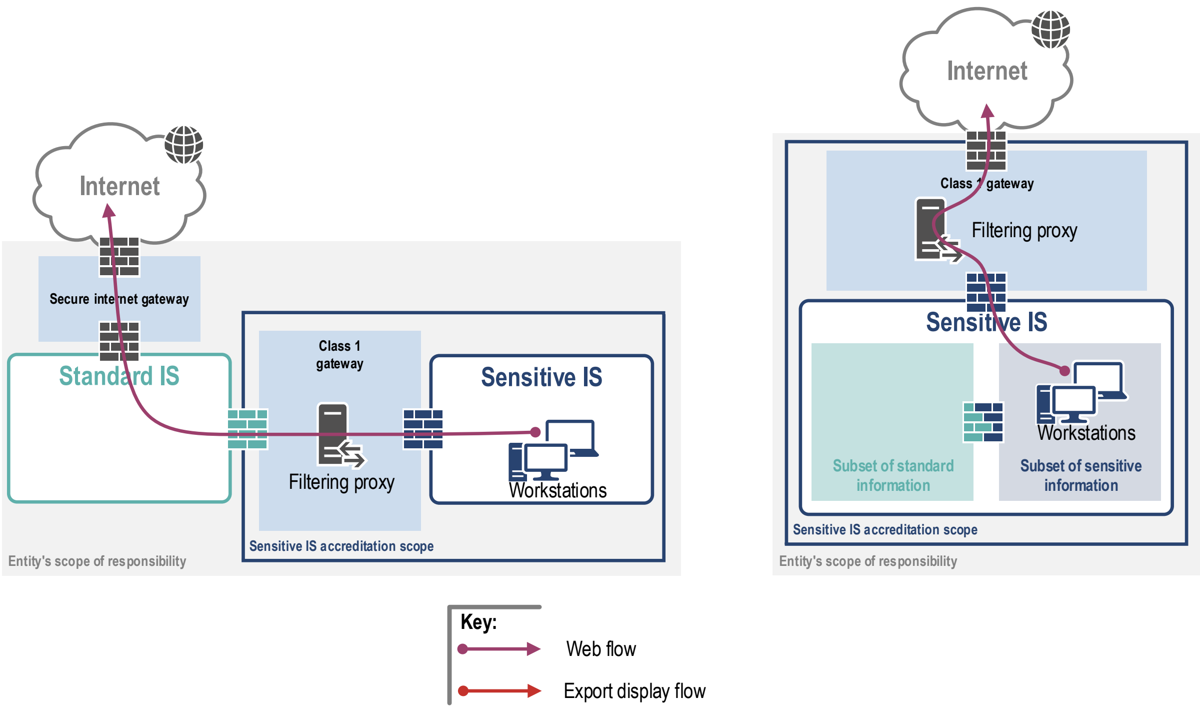


Figure 13 – Web browsing: example of an IS architecture of class 1, without bounce servers (left: case of a physically partitioned architecture; right: case of an architecture with logical partitioning of sensitive and standard information)

R18 - -

Enabling web browsing without bounce servers

For sensitive ISs of class 1, if the deployment of a dedicated web browsing infrastructure is not possible, access to the Internet can be authorised from sensitive workstations by means of proxy servers partitioned from the sensitive IS. This solution is not optimal from a security point of view and it is strongly recommended that it be implemented using qualified proxies (see recommendation R14). Access authorisations to the browsing service are limited to what is strictly operationally necessary.

4.3.4 Transfer of encrypted sensitive documents via the Internet

Sensitive files that are intended to be made accessible from the Internet and therefore transit through an untrusted network must be encrypted using solutions that have security approval (RD information) or a security visa [39] ANSSI (sensitive information).

39. See annex C for more information on security visas.

R19

Encrypting RD information transferred via ISs of Class 0

RD information exchanged between two RD ISs through an IS of Class 0 must be encrypted using RDapproved security products.

R20

Encrypting sensitive information transferred via ISs of class 0

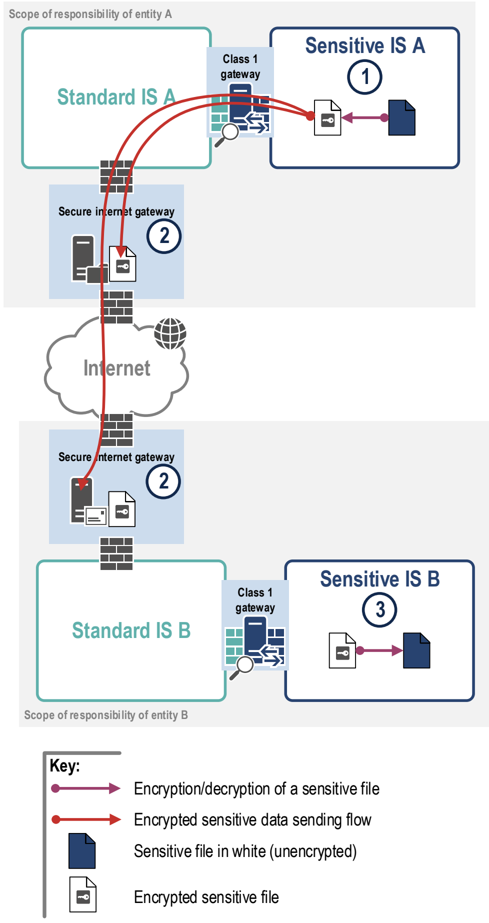
Sensitive information exchanged between two sensitive ISs via an IS of class 0 must be encrypted. It is recommended to use a product with a security visa for this purpose.

Warning

In the context of the R19 and R20 recommendations, sensitive information transferred to an IS of class 0 must be encrypted and decrypted on a sensitive IS.

In accordance with the recommendations of the ANSSI guide relating to the interconnection of an IS to the Internet [23], if the resources of the secure Internet gateway are to be made available to clients connected to the Internet, they must be hosted in a dedicated zone (referred to as an *exposed services zone*). Sensitive information, encrypted using the *ad hoc* tool, can therefore be published on the Internet in this zone.

Figure 14 illustrates an architecture for sharing sensitive files that complies with the regulations. The information to be shared is encrypted using an *ad hoc* tool on the entity's sensitive IS. It is then transferred to the recipient (e.g. e-mail transfer) or made available to that third-party entity on a server accessible from the Internet. Encrypted files must be transferred to a sensitive accredited IS before they can be decrypted.



① On the "sending" sensitive IS (sensitive IS A), RD files are encrypted using an RD-approved tool (or sensitive files are encrypted using a tool with a security visa);

② The sensitive files encrypted in step 1 are made available in the *exposed service zone* for recipients on the Internet, or are transferred to them (by e-mail, for example) ;

③ Sensitive files are received or downloaded by the recipients, either on a standard IS (and then transferred to an accredited sensitive IS), or directly from the receiving sensitive IS (sensitive IS B). In both cases, the decryption of the files is performed exclusively on an accredited sensitive IS.

Figure 14 – Sensitive IS of class 1 - Example of an architecture for sharing files with a third-party entity

4.3.5 Access via the Internet to information from a sensitive application

In this case, the sensitive data is not in the form of files, but is stored in a database.

R21

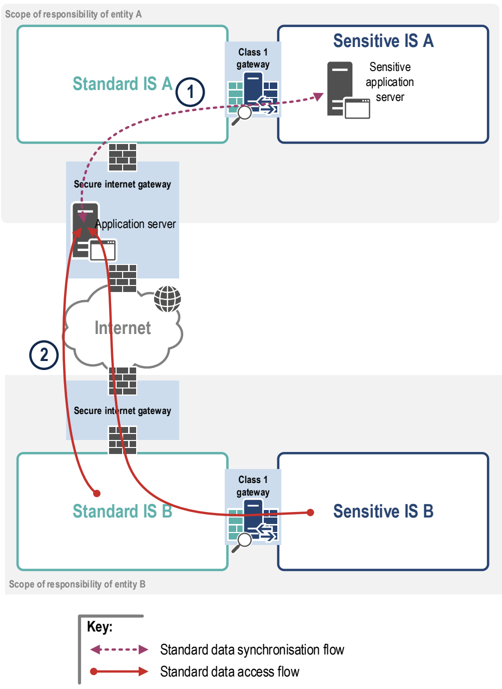
Prohibiting access to sensitive applications from non-accredited ISs

Access to any sensitive (or RD) application from an IS not accredited at sensitive level (and similarly from an IS not accredited at RD level) is prohibited.

If the third party entity does have a sensitive IS accredited to the right level (sensitive or RD), it is necessary to define the actual requirement: is the requirement to share only non-sensitive information with the third party, or to share information, some of which is sensitive?

Architecture with replication of non-sensitive information

If the need is to share only non-sensitive information with the third party entity, it is appropriate to consider the technical feasibility of splitting the application into two instances: one of these, redacted of all sensitive information, is hosted on the standard IS and is exposed on the Internet ; while the other, which contains all the information (both sensitive and non-sensitive), is hosted on the sensitive IS without being exposed on the Internet. In this architecture, a system of secure exchanges is set up between the standard IS and the sensitive IS (see section 4.4 for more information). Figure 15 gives a representation of this architecture.



① On the “sending” sensitive IS (sensitive IS A), a mechanism allows the synchronisation of only the standard data between a server hosted on the sensitive IS and a server located in the *exposed services zone* ;

② Customers access the data thus exposed from standard ISs or from sensitive ISs.

Figure 15 – Sensitive IS of class 1 - Example of an architecture for sharing an application with a third-party entity

Information

This architecture must be tailored to protecting the requirements of the integrity and availability of the exposed data.

Architecture without information replication

If splitting the application into two instances is not possible or the functional need is to give the third party access to sensitive data stored in the database, an interconnection of the sensitive IS with the sensitive IS of the third-party entity must be considered. This is to create an interconnection of sensitive ISs (see section 4.2 for more information).

In this architecture, the application service, which is necessarily hosted on the sensitive IS, is to be protected by not exposing it directly to the Internet. This involves either establishing a sensitive "point-to-point" network interconnection, as described in section 4.2, or providing remote users with mobile means of access based on VPNs (see section 6.4). In both cases, the VPN endpoint is placed within the *gateway of class 1*.

Similarly, the hosting of the sensitive application server must be logically partitioned from the other resources of the sensitive IS, which are not intended to be made accessible from the Internet. It must be placed within a *gateway of class 1*.

R22

Partitioning the infrastructure for making sensitive information

available on the Internet The infrastructure for making sensitive information available from the Internet must be partitioned in a DMZ, within a *gateway of class 1*. It is accessible either from another sensitive IS via a "point-to point" interconnection as described in section 4.2, or from a mobile access device attached to the sensitive IS.

4.4 Secure exchanges for users

The various architectures presented in section 3.2 all provide for partitioning (physical or logical) of sensitive resources (in a sensitive "zone") and standard resources (in a standard "zone"). However, it is likely that users will need to exchange information between these different zones.

In general, when the sensitive IS is extensive or when the exchange flows between the sensitive zones and the standard zones, it is recommended that exchanges of data should be made through the network, using *ad hoc*exchange systems. This section aims to provide recommendations specific to these secure exchange systems available to users.

Information

It is preferable not to carry out these data exchanges using removable media. This is because a proliferation of media increases the risk of confidentiality breaches of the data stored on them (see section 5.7 for more information about removable media). When the use of removable media is all but unavoidable (especially for small, sensitive ISs or for downlink flows from ISs"" of class 2), technical and organisational measures provide a framework for data exchanges and, in particular, ensure traceability.

4.4.1 Case of ISs of class 2

For so-called “physically isolated sensitive IS architecture” (see section 3.2.1), regulations provide that flows from a standard IS may enter the sensitive IS (concept of “uplink flows”). In order to ensure optimal security, this IS interconnection must be secured by means of approved devices, guaranteeing the strictly unidirectional nature of data flows. In most cases, they include an optical diode and specific systems , the function of which is to transfer data from the so-called “low” level to the so-called “high” level, using protocols that do not require transmission acknowledgements.

“Downlink interconnections” [40], via the network, are also provided for by the regulations (see the definition of an IS of class 2 given in section 3.1.2). However, the complexity of their implementation puts them beyond the reach of entities that do not have a very high level of control over the security of their information systems. In this particular case, a strictly controlled use of removable media is preferable to a fragile downlink interconnection, which would not implement security features that could manage risks such as concealed channels in downlink flows.

R23

Controlling downlink interconnections for ISs of class 2

In an IS of class 2, recommended practice is to favour a “downlink” interconnection using removable media rather than an interconnection via the network. The conditions for the use of these removable media must be strictly defined.

4.4.2 Case of ISs of class 1

In the architecture referred to as “physically partitioned sensitive IS” (see section 3.2.2), but also in the case of the “Sensitive IS without standard IS” architecture (see section 3.2.3), it is recommended to install a *secure exchange system* that complies with the principles detailed in this section.

Wherever possible, flows should be allowed as follows:

- from a sensitive workstation (client) to the secure exchange system (server);
- from a standard workstation (client) to the secure exchange system (server).

40. These are interconnections that allow flows from the sensitive IS to enter the standard IS.

Figure 16 shows the recommended directions for initiating flows in a secure exchange system.

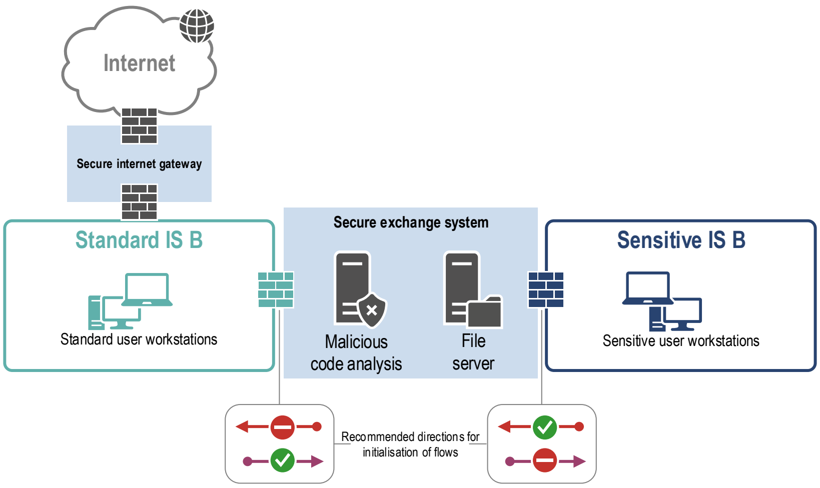


Figure 16 – Sensitive IS of class 1 - Functional representation of a secure exchange system

A secure exchange system must ideally allow only data transfer protocols. For example, the SSH service must be configured to allow only SCP (*Secure Copy*) or SFTP (*SSH File Transfer Protocol*)-type commands. The ANSSI recommendations for securing the SSH protocol apply [4].

R24

Allow only transfer protocols to the secure exchange system

Only services and protocols that allow data transfer to the secure exchange system must be authorised; flows must always be initiated by clients outside the exchange system.

Access to a secure exchange system from the standard IS must be strictly reserved for workstations and users who need to exchange information with the sensitive IS. These restrictions can be achieved through the implementation of network filtering or logical access control to the secure exchange system.

R25

Secure exchange system: restrict access to authorised users only

It is recommended that access to the secure exchange system be restricted to only those workstations and users who need it.

To avoid compromising the authentication secrets of a sensitive IS, it is essential that a user of this IS authenticates on the secure exchange system with a user account referenced in a dedicated directory of the *gateway of class 1* or positioned in the standard IS – but never with an account that is referenced in a directory of the sensitive IS.

R26

Secure exchange system: authenticate users with a non-sensitive account

Users must not authenticate with a sensitive IS account on the secure exchange system, which is considered less trustworthy. If user authentication is password-based, it must be different from other passwords used by the user on other ISs, including the sensitive IS. In addition, it must not be possible to deduce the password from a knowledge of the user's other passwords.

Content filtering and malware protection mechanisms should be systematically deployed. This measure aims to protect the resources of a sensitive IS from the risks of compromise by execution of malware, which could have been conveyed by files or binaries of untrusted origin [41].

R27

Secure exchange system: analysing the content of the data exchanged

The content of all data passing through the secure exchange system must be systematically analysed for malware.

Finally, all data exchanges must be logged and attributed to a user. The exploitation of these logs must be integrated into the logging and security monitoring strategy (see section 7.5).

R28

Secure exchange system : logging and attributing exchanged data

All data passing through the secure exchange system must be traced and attributable to an identified user.

41. See also section 5.6 for more information on protection against malware.

5
Security within sensitive ISs

Objective

The principle of defence in depth consists of basing the protection of an information-system on complementary measures that can compensate for each other in the event that one of them fails. This chapter sets out some good practices translating this principle into the case of sensitive ISs, with the main aim of ensuring access to sensitive information on the basis of *need-to-know* and with the secondary aim of preserving the integrity of the IS and the information.

5.1 Trusted products and service providers

The principle of defence in depth is a general concept that translates into the application of comprehensive security measures, but also into the use of trusted building blocks, such as qualified and certified products. In this case, the party responsible for an IS is exempted from having to bear the burden of evaluating them as part of the accreditation process.

Similarly, the use of trusted service providers can support or even compensate for the lack of internal skills in the entity responsible for a sensitive IS.

In practice, trusted products and service providers are those for which ANSSI has issued a security qualification and, to a lesser extent, those for which ANSSI has issued a certification. These proven solutions approved by ANSSI (products and service providers) are grouped under a single banner : security visas. For the party responsible for a sensitive IS, the main advantage of these visas is to easily identify reliable products and service providers on the IT security market that are reliable and appropriate for the state of the threat. For more information on security visas, and in particular the differences between certification, qualification and approval, see Annex C.

R29

Using ISS service providers with an ANSSI security visa

The use of security providers with an ANSSI security visa [42] is strongly recommended. In the case of outsourced services concerning RD ISs, the contract between the client and the service provider must enforce the service provider's obligation to comply with the security measures of II 901. It is strongly recommended that the service be provided from within the country [43].

42. See Article 3 of II 901.
43. See Article 16 of II 901.

Warning

For data hosting in a *public cloud*, ANSSI recommends the use of the services of a qualified *SecNumCloud* provider. The hosting of sensitive data in a *public cloud* is theoretically possible provided that the service provider is *SecNumCloud* qualified and complies with the security measures of II 901 and this guide.

R30

Acquiring security products with an ANSSI security visa

Wherever they exist, qualified security products must be used [44]. A product qualified by ANSSI must be selected ahead of a certified product. This measure applies both to products used to secure a sensitive IS and to the means used to control physical access to its components [45]. Because qualifications always have a period of validity, it is the responsibility of the party responsible for the IS to ensure that the qualifications of deployed versions of security products are still valid [46]. Finally, the use of a qualified product must be compatible with the scope of the evaluation that led to the issue of the qualification [47].

For the protection of an RD IS, certain security products must have security approval. This mainly concerns encryption products, but also diodes implemented in uplink gateways in the case of "physically isolated sensitive ISs" (see section 3.2.1) [48].

An ANSSI RD approval decision, issued for a security product, is accompanied by a document listing the terms of use of this product. These rules of use contain additional organisational or technical measures which are intended to address the risks identified in relation to the level of RD security targeted by the approval. Typically, for certain security equipment approved by the ANSSI for the protection of RD information, the publisher of the solution does not necessarily by default activate certain technical mechanisms that enable the attainment of a level of protection known as "Restricted Distribution". Wherever equipment is used in an RD context, these technical options must be activated by the administrator of the security equipment.

R31

Complying with the conditions of use of approved security equipment

In cases where an RD-approved security product is implemented on an RD IS, the conditions of use accompanying that product must be implemented by the party responsible for that IS. Evidence of compliance must be included in the IS or interconnection accreditation file.

44. Refer to Article 3 of II 901 and to the security measure 901 INT-AQ-PSL.
45. Refer to security measure II 901 PHY-CI-CTRLACC.
46. Note that this remark also applies to qualified service providers.
47. The use of a qualified product outside the scope of the security evaluation is equivalent to the use of an unqualified product. The evaluation scope is specified in the security target for the qualified product.
48. Refer to security measure II 901 INT-AQ-PSL, as well as sections 3, 14, 17 and Annex 2 of II 901.

5.2 Encryption

Encrypting sensitive information via a method appropriate for the level of sensitivity makes it possible to protect it (in terms of confidentiality and integrity) and, depending on the conditions of use that accompany the qualification or accreditation decision, to store it or to pass it via resources that are not necessarily accredited at the sensitive or RD level [49]. Numerous illustrations of this encryption use case are detailed in this guide:

- securing the interconnection of sensitive ISs (see recommendations R9 and R10);
- securing mobile interconnection channels (see recommendations R55 and R56);
- the protection of data passing through ISs of class 0 (see recommendations R19 and R20);
- the protection of data stored on mobile data media (see recommendations R57 and R58).

In general, II 901 requires the use of *approved* encryption methods for the protection of Restricted Distribution information where RD information is in transit via or stored in a zone where the physical protection does not comply with the requirements of II 901 [50].

Another use case for encryption is the application of the defence in depth principle. As an illustration, encryption can be a solution in certain cases of mutualisation of resources between ISs of different sensitivity levels (see 3.2.3 section). Similarly, II 901 requires an encryption tool to be made available to users and administrators to encrypt sensitive data stored on workstations, servers or removable media [51].

Warning

The use of encryption has strong organisational implications for the entity which implements it. Numerous procedures must be created to manage the life cycle of cryptographic secrets: procedures for securely creating and storing master secrets, key renewal procedures, key escrow procedures, and even data recovery procedures. The absence of control over these mechanisms can have devastating consequences for the entity (denial of service, major breach of confidentiality of information through the illegitimate ability of a malicious user to recover all encrypted data, inability to recover data required as part of a judicial requisition...).

5.3 Internal partitioning of the sensitive IS and hardening of systems

A sensitive IS must be partitioned into zones with homogeneous security needs [52]. To achieve this objective, it is necessary to segment the network and then to set up a means of filtering flows

49. See security measure II 901 EXP-PROT-INF.
50. See Article 14 of II 901.
51. Refer to security measure II 901 PDT-CHIFF-SENS.
52. See security measures II 901 RES-CLOIS, ARCHI-HEBERG and EXP-CI-FILT.

between these different segments. Network segmentation can be physical (dedicated equipment) or logical (VPN, VLAN…).

The following examples illustrate this idea:

- network filtering must be implemented between workstations and the data centre server resources;
- application servers can be partitioned (e. g. partitioning of servers assigned to separate projects; partitioning of server components in an n-tier architecture).

R32

Partitioning the sensitive IS into zones with homogeneous

security levels A sensitive IS must be partitioned into different trust zones, which are homogeneous in terms of their security needs and exposure. This partitioning must be the subject of a carefully-planned segmentation of the network, supplemented by fine filtering of flows at firewalls.

R33

Avoiding the installation of sensitive IT equipment in zones open to the public

If there is a business need to extend the sensitive network into a zone open to the public, this extension must be partitioned off from the rest of the sensitive IS [53]. In general, the processing of sensitive data in public reception areas must remain occasional and exceptional, and be accompanied by specific [54] protection measures.

Within a zone with homogeneous security needs, the party responsible for a sensitive IS must define a strategy for blocking communications between the various systems in the considered zone. For example, the blocking of so-called “lateral” communications between distributed resources (workstations, printing equipment…) is likely to reduce the risks of propagation of an attack, by making it more difficult for an attacker seeking to escalate their privileges. In a defence-in-depth approach, the technical measures resulting from this strategy of blocking lateral flows must be varied and complementary. They are applied at both network and system level. As far as the network is concerned, this may involve setting up a micro-segmentation mechanism with intra-VLAN filtering (e.g. *Private VLAN* [55]). On the system side, this may involve activating and configuring the local firewall on each workstation [56], so as to block direct communications between systems.

This partitioning strategy must be extended to servers. For example, for unnecessary network services that cannot be hardened [57], local firewall filtering rules must block all unnecessary connections to reduce the attack surface by minimising the exposure of listening services.

53. Refer to security measure II 901 PHY-PUBL.
54. Refer to security measure II 901 PHY-SENS.
55. See the ANSSI guide on recommendations for securing a service switch [6].
56. See security measure II 901 PDT-NOMAD-PAREFEU.
57. Hardening can consist of uninstalling the service or, alternatively, configuring it to be unusable.

R34

Blocking lateral communications

In order to limit the risks of lateral propagation of an attack, the party responsible for a sensitive IS must define and implement a strategy for blocking lateral communications. This strategy primarily concerns distributed resources, but also servers.

The installation of any hardware, firmware or software (e. g. operating systems, hypervisors, virtualised operating systems, applications) must be conditional on the prior authentication of its origin and verification of its integrity.

In addition, the configuration of operating systems and other software must be hardened to make it more difficult for an attacker to exploit (known or as yet undisclosed) vulnerabilities.

It is recommended that a configuration, including security features, be made using the state of the art in order to reduce the risk of compromise: activation of protection mechanisms [58] or implementation of good system installation practices (e. g. disabling unnecessary services, changing default passwords, disabling *autorun*, disabling network routing, etc.). For the hardening of a Linux system, refer to the ANSSI guide [9].

R35

Hardening the configuration of hardware and software used on sensitive ISs

Before they are put into operation, the integrity of the hardware and software of a sensitive IS must be checked and their configuration hardened [59]. This recommendation applies to each of the components of the sensitive IS : servers, workstations, network equipment (switches, routers... [60]) and hardware [61]. Particular attention must be paid to workstations, which are often the preferred point of entry for compromising an IS.

5.4 Marking

Marking of information and applications

It is strongly recommended that sensitive information be marked by means left to the discretion of the party responsible for a sensitive IS [62]. The benefit of this marking is to draw the attention of all those involved in the sensitive IS (users, administrators, operators, maintainers, etc.) to the level of sensitivity of the information handled, in order to encourage them to comply with the relevant handling rules.

In the case of unstructured data (typically office files), marking consists of inserting the protection notice stamp in the middle at the top and bottom of each page. Figure 17 shows the representation of the RESTRICTED DISTRIBUTION stamp.

58. Examples : *Data execution prevention* (DEP), *Address space layout randomization* (ASLR), *Security-enhanced Linux* (SELinux), *AppArmor*.
59. Refer to security measure II 901 EXP-CONFIG.
60. Refer to security measure II 901 RES-DURCI.
61. Refer to security measures II 901 PDT-MUL-DURCISS and PDT-TEL-MINIM.
62. Refer to article 5 of II 901 and to security measure II 901 GDB-QUALIF-SENSI.

Figure 17 – RESTRICTED DISTRIBUTION stamp

In the case of structured data (typically data accessible through an application), marking can consist of the addition of a banner when each application session is opened or as a permanent reminder of the sensitivity level of the information in the application's human-machine interface.

R36

Marking sensitive information

It is strongly recommended that the entity implementing a sensitive IS should equip itself with the means to mark sensitive files (buffers, naming conventions, etc.) and sensitive applications (banners, adaptation of the man-machine interface, etc.). It must also raise awareness of the IS's users to the importance of marking information as soon as it is created. RD information must be marked with the words RESTRICTED DISTRIBUTION.

Information

Marking must not be confused with labelling. In a simplified form, the first case involves tagging information with a visual marker that can be operated by a human being; in the second case, it involves adding technical data (metadata) to an item of information, so as to be able to automate the determination of its level of sensitivity at a later stage. The labelling function is intended to be used in classified IS architectures, when problems of information exchange between ISs of different levels of sensitivity are encountered.

Marking of materials

In practice, it is not always possible to mark information. In this case, the physical medium used to store the information should be marked instead. The marking of media, like the marking of data, draws attention to the importance of handling them to protect the confidentiality of the data stored on them. In particular, when media are reassigned to other uses, sent for maintenance outside the entity, or when they are decommissioned, secure erasure or even destruction measures apply [63].

Cumulative marking of information and media must be sought.

R37

Marking media that stores sensitive information

It is strongly recommended that the physical storage media for this information should be marked.

62. Acronym for *Data loss prevention* or *Data leakage prevention*.
63. See security measures II 901 EXP-CI-EFFAC, EXP-MAINT-EXT and EXP-MIS-REB.

In order to reduce connection errors and, above all, to facilitate the visual detection of illegitimate connections, it is appropriate to define a colour code for the wiring of equipment on the various networks, according to their level of sensitivity. This recommendation applies equally to data centres, technical network distribution premises and offices, as close as possible to the non-technical users of the IS.

R38

Adopting an equipment wiring colour code

It is recommended that network cables with different sensitivity levels should be visually distinguished, for example by using different coloured cables.

5.5 Managing authentication and access rights

Any person accessing a sensitive IS resource must be identified and authenticated by means of an individual account. In addition, several individual accounts must be created for an individual whose job justifies having distinct roles on the IS (typically a user account and an administrator account).

A distinction should be made in the case of initial (or “primary”) authentication, which is a prerequisitefor accessing the IS and subsequent authentications. These authentications (known as “secondary”) are designed to restrict access to certain resources to only those IS users who have a need to know. Using a defence-in-depth approach, they provide additional protection against malicious agents that may have compromised the IS.

Initial authentication

The initial authentication for a user to access a sensitive IS must be strong authentication [64]. An authentication is said to be “strong” if it is implemented in line with the state of the art and if it is “multifactor”. An authentication is multi-factor if it relies on at least two of the three types of authentication available: something the user knows (a password, a *passphrase*, a PIN code…), something the user has (a smart card, an authentication token, etc.), something the user is (presentation of a characteristic that is unique to the user such as iris, face, fingerprint, etc.).

If authentication secrets are associated with this initial authentication, they must be memorisedby the user account holder and under no circumstances be stored elsewhere (neither on paper nor in a file – even an encrypted one – that is stored on an IS…).

R39

Enabling strong initial authentication

The initial authentication of a user on a sensitive IS must be state-of-the-art multifactor authentication.

Secondary authentications

Although initial authentication necessarily requires user action, it is recommended that subsequent authentications should be made transparent. It is therefore recommended that the party

64. Refer to security measure II 901 EXP-ID-AUTH.

responsible for a sensitive IS should deploy SSO solutions [65]. These solutions have different architectures, a description of which is beyond the scope of this guide. In general, it is important to remember that architectures implementing centralised authentication protocols, based on authentication tokens or identity federations (so-called "SSO server architectures" [66]) should be preferred to so-called "SSO client" or "SSO enterprise architectures" [67].

Information

Depending on the context, access to particularly critical applications may be conditional upon regular re-authentication of the user with the authentication information used during the initial authentication.

It can be cumbersome for users to manage authentication secrets that cannot be handled by single sign-on systems. To protect these authentication secrets, it is recommended that users be trained in the use of a password manager [68]. According to the R30 recommendation, a password manager with a security visa issued by the ANSSI must be used in preference.

Password-based authentication services should be able to impose complexity rules. Otherwise, a formal procedure must be in place for periodic verification of password strength [69]. In general, password management rules must follow the recommendations of ANSSI [3] [70].

R40

Protecting authentication secrets

It is recommended that secondary authentication secrets should be protected using a single sign-on (SSO) system. It is further recommended that authentication secrets that cannot be handled by the single sign-on system should be protected by means of a password manager, if possible with a security visa issued by ANSSI.

Authorisations

To enforce compliance with the need to know, the entity responsible for a sensitive IS must implement a procedure whereby any assignment of logical access rights to a sensitive resource is conditional upon formal authorisation [71]. The roles of the people involved in the process of approving these requests for modification of logical access rights must be clearly defined. Requests to open, modify or delete authorisations should be archived for audit or investigation purposes following security incidents.

Access rights to resources must preferably be granted by assigning user accounts to user groups [72]

The logical access rights associated with a user account should reflect the position the user holds within the entity and be governed by the principle of least privilege. To this end, assignments, mod-

65. *Single Sign On*
66. Examples : Kerberos, CAS, identity federation protocols such as SAML or *WS-Federation*…
67. These solutions, which have the advantage of not requiring any adaptation of applications, automate the entry of ID codes and authentication secrets in the application authentication windows.
68. See security measures II 901 EXP-CONF-AUTH, EXP-GEST-PASS and EXP-INIT-PASS.
69. Refer to security measure II 901 EXP-QUAL-PASS.
70. Refer to security measure II 901 EXP-POL-PASS.
71. Refer to security measures 901 RH-MOUV, EXP-RIGHTS, EXP-PROFILS, EXP-PROC-AUTH.
72. It is not recommended to assign permissions directly to a user account as this complicates the procedures for granting and, more importantly, withdrawing logical rights.

ifications and deletions of rights must be made in accordance with changes in the user's position or function. At the end of its life cycle, the user account must be disabled[73] but not deleted.

The weaker the rights attached to a user account, the more the consequences of a user account being compromised are reduced. A review of the access rights assigned to user accounts (access privileges and authorisations) must be carried out annually at a minimum[74], in order to detect and correct any deviations. To be effective, these reviews should be conducted by those within the entity with a very good understanding of the nature of the information, as well as users with a legitimate need for access. These reviews are therefore carried out by business managers rather than infrastructure administrators.

All of the tasks listed above can be particularly burdensome and complex. For large entities, it is strongly recommended to equip these procedures with procedures through IAM[75] platforms.

R41

Rigorously manage the assignment of logical access rights to computer accounts

The management of rights on a sensitive IS must be controlled by a procedure allowing the attribution of the assignment, modification and deletion of rights throughout the life cycle of IT accounts. In addition, a periodic review of logical rights must be performed annually. For very extended sensitive ISs, the use of tools for identity management, single sign-on and authorisations is strongly recommended.

5.6 Protection against malware

II 901 requires a diversification of the antivirus technologies used to detect malware[76]. As such, it is recommended that anti-virus software be different on application servers, workstations and interconnection media.

However, this technological diversification must not be sought at all costs, in particular if the intrinsic security level of the products has not been assessed, or if technological diversification is achieved to the detriment of control over the various solutions by the staff in charge of their administration.

R42

Protecting the sensitive IS from malware

Antivirus software must be installed on all application servers, workstations and on the resources that interconnect the sensitive IS with other ISs. Wherever possible, it is recommended to diversify the anti-malware protection technologies on these different systems.

Furthermore, although not specific to sensitive ISs, certain points of attention are particularly important for sensitive ISs :

73. Disabling a user account depends on the capabilities of the operating system or application. It may consist, for example, of a particular configuration of the account settings or a removal of the privileges associated with the account.
74. Refer to security measure II 901 EXP-REVUE-AUTH.
75. *Identity and Access Management*
76. See security measure II 901 EXP-PROT-MALV.

- Removable media intended to be connected to a sensitive IS must be provided by the entity responsible for the IS and be analysed before being connected to the IS (see section 5.7 on devices and removable media).
- Dynamic content reputation evaluation features should be disabled when these evaluations are not performed locally (e. g. evaluation performed in the *cloud* or frameworks hosted in the *cloud*).
- In the particular case of highly critical systems where the attack surface has been strictly reduced, the installation of potentially vulnerable antivirus software may be counterproductive and is therefore not recommended (e. g. directory server).
- The service account privileges used by the antivirus software agents installed on systems are often high by default; it is necessary to review these rights and reduce them as much as possible (principle of least privilege)[77].
- Antivirus updates should be deployed promptly after they are made available by the protection software publishers. A maximum delay of 24 hours is recommended.

R43

Tailoring the malware protection policy

Malware protection solutions are essential, but they must be carefully deployed so that they do not weaken the security level (increase the attack surface, a source of data exfiltration, etc.)….

Depending on the results of the risk analysis and the monitoring strategy of the entity implementing a sensitive IS, it is recommended that solutions be deployed to reveal potentially suspicious behaviour (e.g. tools for checking the integrity of files in an operating system, HIDS[78], software restriction tools to limit program execution, etc.).

R44

Deploying tools to reveal suspicious activity

It is recommended that tools should be installed to detect suspicious behaviour and that the logs they generate be fed into the monitoring system implemented on the sensitive IS. This recommendation primarily concerns workstations.

5.7 Managing devices and removable media

Limiting the number of devices and removable media

Any device connected to a sensitive IS can be the vector of an electronic[79] attack. It is essential that the party responsible for a sensitive IS should approve the equipment to be used on the sensitive IS and manage its configuration and operation. The implementation of technical or organisational measures providing control over authorised devices on the sensitive IS is recommended (see recommendation R49).

77. Refer to security measure II 901 EXP-DOM-LIMITSERV.
78. *Host-based intrusion detection system*
79. For example, mice or keyboards can be booby-trapped for data collection purposes.

Of all devices, removable media for storing data [80] (USB sticks, external hard drives, cameras, memory cards, CD-ROMs, etc.) should be given special attention.

Exchanges via removable media can be seen as a particular form of IS interconnection, which can be described as "indirect interconnection", as opposed to the direct interconnections seen in chapter 4. Like direct interconnections, removable media are a potential vector for the propagation of malware or data exfiltration. The risk they pose stems from their ease of transportation and exchange.

Therefore, one risk reduction measure is to find alternatives to removable media. This means, for example, that data exchange should be carried out over the network wherever possible. In addition, data exchanges between the sensitive IS and the standard IS of the same entity should preferably be carried out by means of user exchange systems (see section 4.4).

R45

Removable media: limiting their use to operational needs only

It is strongly recommended that the entity implementing a sensitive IS reduce the number of removable media to strict operational needs and should opt in preference for exchange solutions via the network.

However, there may be cases of use where the use of removable media is unavoidable. This is, for example, the case when a sensitive IS is very small. It is therefore not appropriate to implement an exchange system for the users of this IS. Other examples concern the need for exchanges with isolated ISs (i.e. without direct interconnection), or with ISs of other entities for which it is not possible to achieve an interconnection.

Management and control of removable media

If an entity responsible for a sensitive IS authorises the use of removable media, it must have a policy defining the management rules and conditions of use. Such a removable media policy will incorporate at least the elements listed below.

Removable media:

- are provided by the entity responsible for a sensitive IS [81] ;
- are assigned to a single user, and their reassignment is governed by a procedure approved by the CISO [82];
- are ideally marked (see recommendation R37);
- are costed according to the R57 and R58 recommendations;
- If they contain sensitive data, they should be stored in locked cabinets outside their periods of use, in lockable cabinets [83] ;

80. In this guide, the term *removable media* is used to refer to *removable data storage media*.
81. Under no circumstances are personal removable media allowed to be connected to a sensitive IS (see security measure II 901 PDT-AMOV). Similarly, II 901 prohibits the connection to a sensitive IS of any removable media that is not under the direct control of the party responsible for the sensitive IS (see security measure II 901 EXP-MAIT-MAT). Data exchanges involving removable media provided by third parties must be carried out in accordance with the recommendation R48.
82. Refer to security measure II 901 EXP-REAFFECT.
83. Refer to security measure II 901 EXP-PROT-VOL.

- in the event of their loss or theft, this is to be declared to the CISO [84].

R46

Removable media: controlling their management and conditions of use

An entity that authorises the use of removable storage media on a sensitive IS must have a policy, in line with the security measures of II 901, specifying their management rules and conditions of use. In particular, this policy must prohibit the connection to the sensitive IS of any personal removable media and any removable media provided by a third party. Only removable media provided and administered by the party responsible for the sensitive IS, and explicitly authorised for use on the sensitive IS, may be connected to the sensitive IS.
It is recommended that technical resources be installed on users' workstations and on the workstations of administrators of the sensitive IS, ensuring that only explicitly authorised removable media can be connected.

The strict application of the recommendation R46 is all the more critical because removable media make it possible to export sensitive IS data. A measure to reduce the risk of uncontrolled data output from the sensitive IS is to opt in preference for the use of removable media which, when used on a sensitive workstation, restrict exchanges to only imports of data from the sensitive IS. In practice, this means using non-rewritable media (e.g. CD-ROMs) or devices that prohibit the writing of data when connected to the sensitive IS (e. g. USB blockers). Such media, in "read-only" form, only allow data to be imported to the sensitive IS but prohibit its export.

R47

Removable media: encouraging the use of read-only media

Wherever possible, the use of removable media or devices that ensure that only the import of data is possible on the sensitive IS is recommended.

Decontaminating removable media

Removable media must be decontaminated before any data is exchanged with a sensitive IS. The general rule is to carry out this clearance using dedicated resources: a *buffer device* or a *decontamination station*. This rule must be strictly adhered to in the case of removable media that are neither provided nor administered directly by the entity responsible for the sensitive IS [85] (e. g. media provided by a third party) or when the safety of the data stored on the removable medium is not guaranteed.

It is potentially possible to carry out the decontamination of a removable medium directly on the sensitive IS without the need to connect it first to a buffer device or a decontamination station. Any exemption from the general rule must be explicitly authorised by the party responsible for the sensitive IS and strictly monitored:

- the additional risk induced by an exemption must have been assessed in the risk analysis and be included in the residual risks when the sensitive IS is accredited;

84. . See security measure II 901 EXP-DECLAR-VOL.
85. II 901 prohibits the connection to a sensitive IS of any removable medium that is not under the direct control of the entity responsible for the sensitive IS. Refer to security measure II 901 EXP-MAIT-MAT.

- the removable medium used must be provided and administered by the entity responsible for the sensitive IS (see recommendation R46);
- the user's level of confidence in the safety of the medium must be high (e. g. the user knows the history of the medium's use).

In all other cases (use of a medium provided by a third party, use of a medium provided and administered by the party responsible for the sensitive IS but whose safety is not guaranteed, etc.), the use of resources dedicated to the decontamination of storage media is mandatory.

R48

Removable media : using storage media decontamination solutions

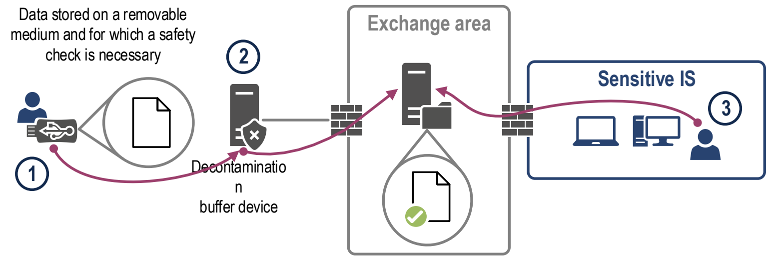
It is strongly recommended to use a dedicated decontamination solution (e.g. buffer device, decontamination station, etc.) for data exchanges with a sensitive IS carried out by means of removable media that are neither provided nor administered directly by the entity (media managed by a third party), or for which doubts exist as to the safety of their content. If this solution itself uses removable media, it is recommended that these be dedicated to this purpose and that technical or organisational measures are in place to ensure that they remain secure over time.

The following are examples of security functions that can be integrated into buffer device or decontamination station-type solutions:

- antivirus analysis from a knowledge base or heuristics;
- blocking of file formats that are not explicitly allowed;
- checking the conformity of the file structure against reference formats;
- behavioural analysis by opening the document or executable code to be analysed in a virtualised environment ("sandbox");
- conversion of documents from an editable office file format to an image format, in order to prevent any embedded code from being executed;
- protection of equipment against attacks aimed at the physical destruction of equipment (e. g. electrical overload);
- protection against malicious USB firmware.

Figures 18 and 19 show two examples of acceptable architecture for removable media decontamination solutions. In these two figures, only the case involving transfer of data stored on the removable medium to the sensitive IS is shown. For the export of data from the sensitive IS by means of removable media, the safety analysis with a buffer device or decontamination station is mandatory if the removable medium is provided by a third party, or if the medium used for this data export is provided and administered by the party responsible for the sensitive IS but its safety is not guaranteed.

For more information on buffer devices and decontamination stations, see the ANSSI document [30].

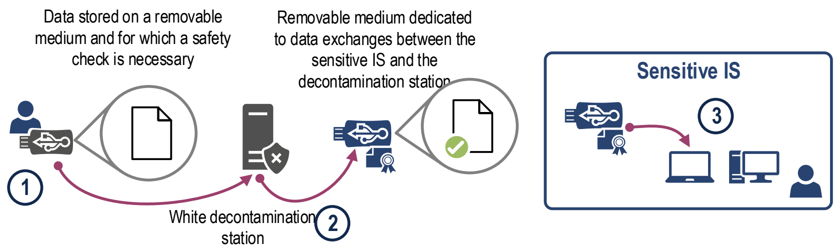


① The user connects the data medium to be analysed to the buffer device and selects the files he/she wants to transfer to the sensitive IS.

② The decontamination buffer device scans the files and copies the healthy files to the exchange zone, in a space accessible only to the only the user who initiated the transfer.

③ The user, having been authenticated with the sensitive IS, downloads the files from the exchange zone. This data import action is logged and attributed to the user. In order to minimise the impact in the event that the buffer device is compromised, an automatic mechanism removes the data from the exchange zone. This deletion is preferably done once the data has been imported to the sensitive IS or, failing that, periodically (e. g. daily).

Figure 18 – Illustration of the concept of a decontamination buffer device and explanation of its use in the case of importing data into the sensitive IS



① The user connects the removable medium to be scanned to the decontamination station and selects the files to be transferred to the sensitive IS.

② The decontamination station analyses the files and copies the healthy files onto a removable medium that is controlled and dedicated to the import and export of data between the sensitive IS and the decontamination station. In order to limit the impact in the event that the decontamination station is compromised, data transfers between the two data media are carried out while minimising temporary data as far as possible. If the use of such temporary data is unavoidable, an automatic mechanism deletes them periodically (e.g. daily).

③ The user, having been authenticated with the sensitive IS, connects the controlled removable medium to a data insertion point, which verifies that it is a controlled medium and that the security analysis has been performed by the decontamination station. This data import action is logged and attributed to the user.

Figure 19 – Illustration of the concept of a decontamination station and explanation of its use in the case of importing data into the sensitive IS

6
Securing sensitive workstations

Objective

Workstations are often favoured entry points for compromising an IS. Depending on the choice of architecture, they may be located at the confluence of the IS with different levels of exposure to threats and, as such, constitute bounce systems, which are particularly attractive from an attacker's point of view. But above all, workstations are the primary location of human-machine interactions between the IS and its users. And users can be tricked into becoming unwitting vehicles for malicious actions. User awareness plays a key role in preventing the compromise of workstations. This awareness must be complemented by technical and organisational security measures to reduce the likelihood of workstations being compromised. The purpose of this chapter is to set out such measures.

6.1 Controlling sensitive IS workstations

The entity implementing a sensitive IS must control the security of the workstations used to access sensitive information. In this respect, various measures must be taken:

- the software installed on the workstations, and its configuration, is under the exclusive control of the party responsible for the sensitive IS [86]. In particular, the use of type 2 hypervisors [87] is prohibited, except with the agreement of the party responsible for the sensitive IS, and then only for specific use cases;
- all equipment connected to a sensitive IS is administered and updated under the responsibility of the party responsible for the sensitive IS [88];
- lateral movements of an attacker who has compromised a workstation [89] are blocked by means of various complementary techniques: diversifying the means of authenticating local administrator accounts [90], prohibiting remote connection to these accounts, configuring a local firewall… [91] (see also recommendation R34);
- small fixed workstations are protected against theft by a secure attachment system [92];

86. Refer to security measure II 901 PDT-CONFIG and the recommendation R35 concerning the hardening of systems.
87. As opposed to a type 1 hypervisor, which runs directly on the hardware layer of a computer, a type 2 hypervisor runs on an operating system preinstalled on the computer. When used in an uncontrolled manner, a type 2 hypervisor represents a risk to the security of sensitive ISs because of its ability to bypass the security policy implemented on the computer where it is running.
88. Refer to security measure II 901 EXP-MAIT-MAT.
89. Refer to security measure II 901 EXP-DOM-ADMINLOC and recommendation R34.
90. If the operating system is Windows, the use of the *Local admin password solution* (LAPS) tool should be considered.
91. Note that this last technique can also satisfy the PDT-PART-FIC security measure of II 901, which aims to prohibit the sharing of locally hosted data on workstations.
92. See security measure II 901 PDT-VEROUIL-FIXED.

- the reallocation of a sensitive workstation to another user is subject to a specific procedure to ensure that the need-to-know is respected [93].

Warning

II 901 prohibits the connection of personal IT resources to sensitive ISs [94]. The use of personal resources for professional purposes [95] is therefore also prohibited.

R49

Controlling the IT resources allocated to users of a sensitive

IS Technical and organisational measures enable the entity responsible for a sensitive IS to control the IT resources made available to users, in order to reduce the risk of compromising the integrity of sensitive workstations. In particular, users do not have local administration rights, which are reserved for administrators in charge of operating and supporting workstations [96].
The computer resources entrusted to users are reserved for professional use.

Information

Personal electronic devices with a USB connection must be electrically recharged using dedicated chargers. Under no circumstances should they be connected to professional IT resources associated with a sensitive IS [97].

6.2 Connecting workstations to the network

With regard to the connection of distributed resources (workstations, printing resources, etc.. . .) to local networks, the best level of security is achieved by implementing a physical network dedicated to the sensitive IS.

R50

Connecting sensitive resources on a dedicated physical network

It is strongly recommended to deploy sensitive IS resources on a physical network dedicated for this purpose.

As the sensitive IS can potentially be very large, it will not always be possible to implement a dedicated physical network. In this case, the deployment of a dedicated logical network implementing network encryption and authentication mechanisms (IPsec protocol) is feasible.

R50 -

Connecting sensitive resources on a dedicated logical network

A degraded security measure of the R50 recommendation consists of deploying sensitive resources on a dedicated logical network protected using the IPsec protocol. In

93. Refer to security measures II 901 EXP-CI-EFFAC and PDT-REAFFECT.
94. See Article 17 of II 901 and safety measure II 901 PDT-GEST.
95. BYOD is the acronym for *Bring Your Own Device*.
96. See security measures II 901 EXP-RESTR-RIGHTS and PDT-ADM-LOCAL.
97. The application of this IT hygiene measure is recommended for all types of IS, and not only for sensitive ISs.

addition, logical segmentation (VLAN) and network filtering mechanisms are recommended to limit the exposure of the IPsec VPN concentrator to sensitive distributed assets.
For the implementation of the IPsec protocol, the recommendations of the ANSSI guide [17] must be applied.

Information

The R50- recommendation is not applicable to "physically isolated sensitive ISs" (see section 3.2.1) and "physically partitioned sensitive ISs" (see section 3.2.2) architectures, since in these cases the standard IS and the sensitive ISs are, by definition, completely separate.

In order to prevent non-explicitly authorised components from gaining network connectivity if they were to be connected to the LAN, accesses to a sensitive network must be controlled[98]. It is strongly recommended to implement a service for authenticating sensitive resources on the network. For example, this may involve establishing an IPsec VPN tunnel (see recommendation R50-) or implementing the 802.1X protocol, with authentication of the requesting equipment (*supplicants*) by electronic certificate.

Warning

Regarding the use of 802.1X protocol, the network authentication service must not weaken the security level of the sensitive IS. Particular attention must be paid to the partitioning of the authentication, authorisation and traceability server[99], especially if Wi-Fi access to the network is authorised by the party responsible for the sensitive IS (see also the recommendation R60 on wireless networks). The ANSSI guide to the deployment of the 802.1X protocol [8] explains in which cases the use of this technical solution is recommended.

R51

Authenticating sensitive resources to the network

It is strongly recommended that the resources of a sensitive IS, and distributed resources in particular, be authenticated, before being able to benefit from connectivity to the sensitive local network.

98. Refer to security measure II 901 EXP-CI-ACCRES.
99. This server is called the AAA server for *Authentication, Authorization and Accounting*. The most frequently used AAA server implements the RADIUS protocol. It is usually referred to as a "RADIUS server" by metonymy.

6.3 Workstation architecture

In order to allow users to access either a standard IS or a sensitive IS, three sensitive workstation architecture solutions are possible. They are presented below in descending order of security level in relation to the security objectives:

- a user workstation dedicated to the sensitive IS;
- a multi-level user workstation connected to the standard IS and the sensitive IS;
- a sensitive user workstation with remote access to the standard IS.

Dedicated sensitive user workstation

The solution that offers the best guarantee from a security point of view is to use two physically separate stations (see figure 20): one allows access to the standard IS and the second to the sensitive IS.

R52

Using a dedicated sensitive user workstation

It is recommended to implement sensitive workstations that are physically separate from any other IS.

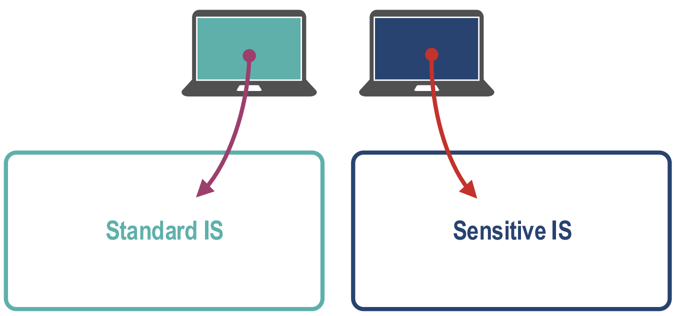


Figure 20 – Recommended architecture: dedicated sensitive user workstation

Information

In the case of sensitive IS architectures, where the sensitive user workstation is physically dedicated, the question of using KVMs [100] may arise. Ideally, if KVMs are implemented, they should be ANSSI-qualified. However, at the time of publication of this guide, no qualified KVM exists. KVMs that are Common Criteria certified, with the *Peripheral Sharing Switch* version 3.0 and earlier protection profile, do not guarantee the isolation of the various devices connected to them. The use of such a device between two workstations connected to different networks (e. g. a standard workstation and a sensitive workstation) must be subject to a risk analysis that has been tailored to the specific use case.

100. *Keyboard-Video-Mouse switch*. This is a hardware electronic device that allows a screen, a keyboard and mouse to be shared between two systems.

Multi-level user workstation

The principle of a multi-level workstation consists of having several software environments (usually two) on the same physical workstation, thanks to the use of virtualisation or containerisation technologies.

Core hardening and partitioning mechanisms can be used to isolate these environments to reduce the risk of compromise at the high-sensitivity level, or leakage of information from the high-sensitivity level (in this case, a sensitive IS), to the low-sensitivity level (in this case, a standard IS). An example of a practical implementation of a multi-level workstation is the *CLIP OS project* supported by ANSSI [101].

This solution (see figure 21) offers a lower level of security than physical separation. It is imperative that a trust evaluation of the isolation and partitioning mechanisms is carried out: the use of this solution, if not trusted, can give a false sense of security. It is also preferable that these mechanisms are managed at system level, and not by a user application (see figures 22 and 23).

R52 -

Using a multi-level user workstation

In the absence of a physically dedicated sensitive user workstation, the use of virtualisation or containerisation technologies to obtain a multi-level system is feasible, provided that the partitioning of environments is achieved by system-level mechanisms that have been assessed as being trustworthy.

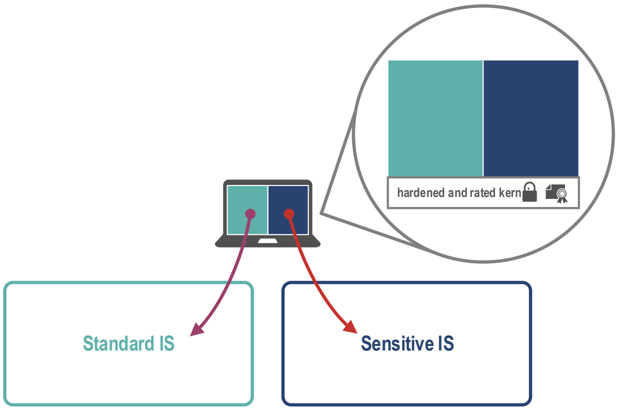


Figure 21 – Recommended architecture: multi-level user workstation

101. See the official project website for more website for more information: https://clip-os.org/.

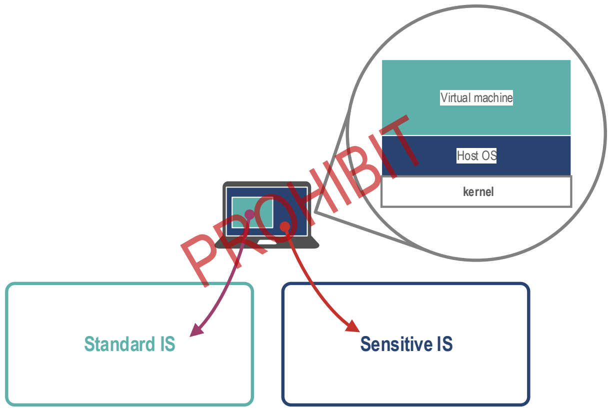


Figure 22 – Prohibited architecture: sensitive user workstation hosting a virtual machine

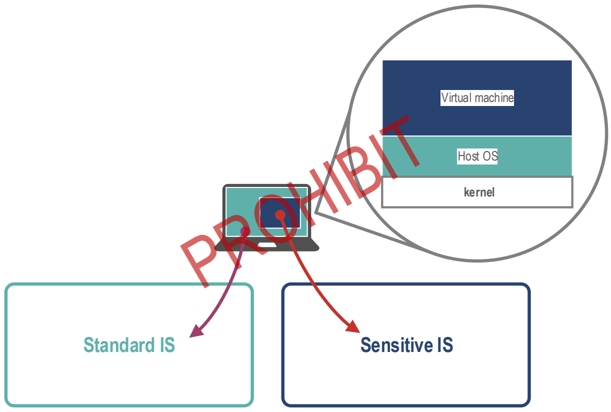


Figure 23 – Prohibited architecture: standard user workstation hosting a sensitive virtual machine

Sensitive user workstation with remote access to the standard IS

A last solution consists of using a physical user workstation connected to the sensitive network and allowing access to the standard IS by remote connection (see figure 24).

In this architecture, the level of security is even lower: the attack surface of the sensitive IS is increased by execution of code from a remote connection client on the sensitive workstation.

Warning

It should be noted that the opposite solution, which consists of accessing a sensitive workstation from a standard workstation via a remote connection, should be prohibited (see figure 25).
Because the level of protection of a standard workstation is lower than that of a sensitive workstation, its compromise could allow an attacker to spy on the actions carried out from this workstation (keystrokes, screen copies, etc.), including connections made to the sensitive workstation (e. g. IP address, password).
An attacker could then move on to illegitimately access the sensitive IS.

If this solution is implemented, the use of remote connection software requires configuration precautions to restrict the exchange functions between the local (sensitive) and the remote (standard) system: if the remote connection server is compromised, an attacker could then trace the established communication channel with the aim of compromising the sensitive workstation. In the absence of an evaluation at the time of production of this document, the exchange mechanisms used by remote connection software cannot, *a priori*, be considered as trustworthy.

A non-exhaustive list of information exchange functions to be disabled:

- advanced copy and paste functions;
- screen sharing;
- functions for supporting devices (USB, printers, etc.);
- network shares.

These functions are usually disabled at *Virtual Desktop Infrastructure* (VDI) server level. To improve the integrity of these servers and reduce their exposure to threats, it is recommended that they be hosted within a *gateway of class 1*.

Consequently, the establishment of a secure exchange system may be necessary. The concept of a secure exchange system is detailed in section 4.4.

R52 - -

Using a sensitive user workstation with remote access to the standard IS

In the absence of a sensitive workstation that is physically separate from the standard workstation or a multi-level trusted user workstation, a solution that offers a lower level of security may be to ensure that users of the sensitive IS:

- have a physical workstation to access the sensitive IS;
- have access, by remote connection only, to a standard workstation (e.g. physical or virtual: *Virtual Desktop Infrastructure*) from the sensitive workstation.

In all cases, functions that enable an exchange of information between the two IS must be deactivated.

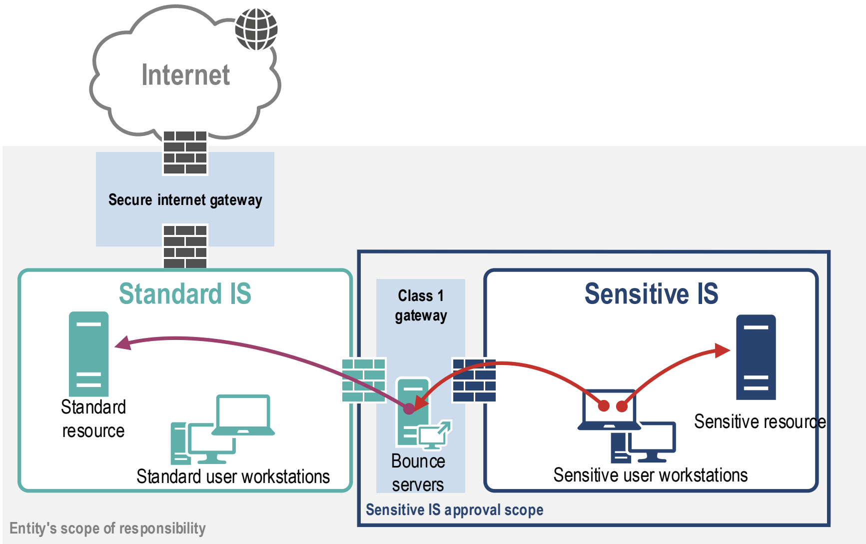


Figure 24 – Recommended architecture: physical workstation with remote access to a standard virtualised environment

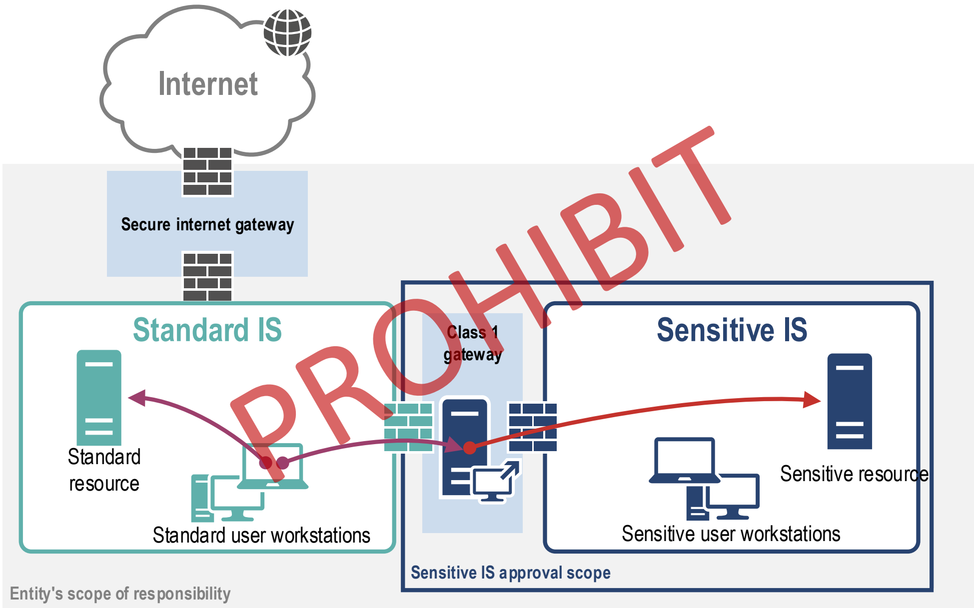


Figure 25 – Prohibited architecture: standard physical workstation with remote access to a virtual sensitive environment

In the case of the two downgraded recommendations R52- and R52--, the following requirements apply:

- filtering of remote connection flows to the standard IS must be carried out by means of a firewall;
- user authentication on the sensitive workstation must be carried out using the directory dedicated to the sensitive IS;

- user authentication on the standard workstation must be carried out using the directory dedicated to the standard IS (see recommendation R7).

6.4 Mobility

Information

This section deals with mobile user access to a sensitive IS. For administrators' mobile access to a sensitive IS, see section 7.3 of the chapter 7 on good practices in administering a sensitive IS.

It may be possible to implement a mobile service on a sensitive IS, whether it is of class 1 or of class 2.

A basic recommendation is to implement the good practices relating to digital mobility detailed in the ANSSI guide [22].

R53

Applying the ANSSI recommendations on digital mobility

The recommendations published by ANSSI in its guide on digital mobility [22] must be applied whenever a mobile service is put into production for remote access to a sensitive IS.

Information

The table in Annex D of this guide maps the security measures of II 901 relating to mobility and the recommendations of the ANSSI guide [22] in its version 1 of October 2018.

The following paragraphs are intended to draw the reader's attention to some recommendations of the [22] guide that are particularly important in a context of sensitive use.

Positioning of VPN concentrators

In the case of an IS of class 2 or an IS of class 1, it is necessary to set up a mobile access architecture in line with the recommendations of the guide [22].

In the case of a class 1 architecture, the VPN concentrator for sensitive IS users is hosted within a *gateway of class 1*. If the entity is also responsible for a standard IS, and a mobile service is implemented on this IS, the VPN termination equipment for users of the standard IS must be distinct from the equivalent equipment on the sensitive IS.

Physical protection of mobile access equipment

By definition, mobile access equipment in a mobile situation does not enjoy the same physical protection as fixed equipment. To reduce the risk of a data confidentiality breach, physical measures must be taken. For example, an anti-theft cable and a privacy filter should be provided with each piece of mobile access equipment and users should be made aware of their use [102].

R54

Physically protecting mobile access equipment

Sensitive mobile access equipment should be equipped with physical safeguards (e.g. anti-theft cable, privacy filter). They should not be left unattended when not in use.

Authentication of mobile users

In addition to strong user authentication (see recommendation R39), authentication of the access equipment is recommended. Annex D of the [22] guide in its version 1.0 provides additional information on possible authentication architectures.

Protection of the mobile interconnection channel

Depending on the use case – RD-level or sensitive-level IS – the encryption methods implemented in a mobile infrastructure (VPN clients and VPN concentrators) must be RD-approved (for RD ISs) or have a security visa (for sensitive ISs) [103].

R55

Securing the mobile interconnection channels of RD ISs

The interconnection channel between an RD mobile access device and an interconnection gateway providing access to the RD IS must be secured using RD-approved security products.

R56

Securing the mobile interconnection channels of sensitive ISs

Recommended practice is to secure the interconnection channel between sensitive mobile access equipment and an interconnection gateway allowing access to the sensitive IS, by means of security products with a security visa.

102. See security measures II 901 PDT-VEROUIL-PORT and PDT-NOMAD-FILT.
103. Refer to security measure II 901 PDT-NOMAD-ACCESS.

Encryption of sensitive mobile storage devices

All sensitive mobile data storage devices (hard drives, USB sticks, multifunction… phones) must be encrypted using approved encryption methods (in the case of RD data) or with a security visa (in the case of sensitive data) [104].

Information

Data stored on the hard disks of mobile access equipment can be encrypted in two ways, which are not mutually exclusive. This may involve (a) full encryption of the [105] and (b) selective encryption of certain files [106]. These two technical solutions are responses to different threats (protection in case of loss or theft in the first case ; protection of the need to know in the second). A risk analysis is used to determine which of these two techniques (potentially both) must be deployed.

R57

Encrypting RD data stored on removable media

RD data stored on removable media must be encrypted using RD-approved security products.

R58

Encrypting sensitive data stored on removable media

Sensitive data stored on removable media must be encrypted using security products with a security visa.

For more information on securing removable storage media, see section 5.7.

Local flow blocking and posture detection mechanisms

Sensitive mobile access equipment can only be attached to one sensitive IS, and can be seen as an extension of it. To avoid becoming an uncontrolled bridge between the sensitive IS and the uncontrolled ISs, it must be in one of two states at any given time: either disconnected from any network or connected to its associated sensitive IS. Access to services hosted by a third-party IS (typically web browsing) is possible only if the communication flows transit through the interconnection gateway between the sensitive IS and the third-party IS.

104. See Article 17 of II 901 and security measures II 901 PDT-NOMAD-STOCK and PDT-CHIFF-SENS.
105. In this case, the encryption granularity is at logical volume level. A secret must be entered to access the contents of the hard disk, but it is important to note that all data is decryptable once this secret has been provided to the operating system, making it possible for an attacker to access all the data on the hard disk.
106. In this case, the encryption granularity is at directory or file level for a file system. The encrypted data will only be accessible after the user has logged in and authenticated with third party data encryption software.

Mobile devices are sometimes configured to dynamically determine the nature of the networks to which they are connected, and then self-adapt their behaviour (establish/do not establish a VPN tunnel with their associated IS, benefit from more or less permissive local firewall flow rules, etc.). These so-called *posture detection mechanisms* cannot be considered reliable enough for use in a sensitive context. They are therefore strongly discouraged, and the recommendation is to set up two separate VPN concentrators: one for external access, the other for internal access.

R59

Encrypting network flows of sensitive mobile access equipment in all situations

It is strongly recommended that all mobile network flows of a sensitive IS should transit through dedicated VPN concentrators and be encapsulated in a VPN tunnel that is either RD-approved (for RD ISs) or has an ANSSI security visa (for sensitive ISs), whether the mobile access equipment is connected directly to the local network of the sensitive IS with which it is associated, or indirectly and remotely. The local firewall of the mobile access equipment must block all flows except for those necessary for the establishment of the tunnel [107], and the *split-tunnelling* function must be disabled by configuring the sensitive VPN concentrators.

For more information on posture detection mechanisms, see section 3.4.5 of the [22] guide in its version 1.

6.5 Wireless networks

In the case of wired sensitive networks, a user can generally only access the sensitive IS only after passing through physical protection barriers consisting of various devices (access control, video surveillance, intrusion detection, etc.). This principle of physical protection is not valid in the case of wireless networks, as radio waves can propagate beyond physical protection barriers.

This increases the risks involved in the implementation of wireless networks: breach of confidentiality of sensitive data transmitted by eavesdropping, denial of service, creation of pirate wireless access points, etc.

107. See security measure II 901 PDT-NOMAD-PAREFEU.

If the implementation of a wireless network is necessary to meet the operational requirements of a sensitive IS, the most secure approach is to consider the wireless network as an untrusted transport network [108]. Consequently, the sensitive access equipment using the wireless network is considered as a mobile workstation and complies with recommendation R59, which advises that flows should always transit through an RD-approved VPN tunnel (for RD ISs) or with an ANSSI security visa (for sensitive ISs).

R60

Implementing a wireless network architecture that is partitioned off from the sensitive IS

The implementation of wireless network technologies must be justified by operational imperatives. Wireless flows must be secured using a tunnel with an ANSSI security visa (in the case of sensitive ISs), or ANSSI approval (in the case of RD ISs), and must pass through a mobile gateway in accordance with the recommendations of the ANSSI recommendations on digital mobility [22].

The wireless access point can be of various kinds : an ADSL box, a public Wi-Fi access point or a Wi-Fi network deployed by the entity to provide Internet access to its visitors, with an SSID that may be reserved for its own mobile users. Regardless of the nature of the wireless access point, only flows necessary for the establishment of the tunnel should be allowed (see explanation of local flow blocking in the previous section). As a result of this restriction, the use of public captive portals is not possible [109] (e. g. wireless access offered to hotel residents). For more information on alternative secure solutions to public captive portals, please refer to Chapter 3.4.4 of version 1 of the ANSSI guide to digital mobility [22].

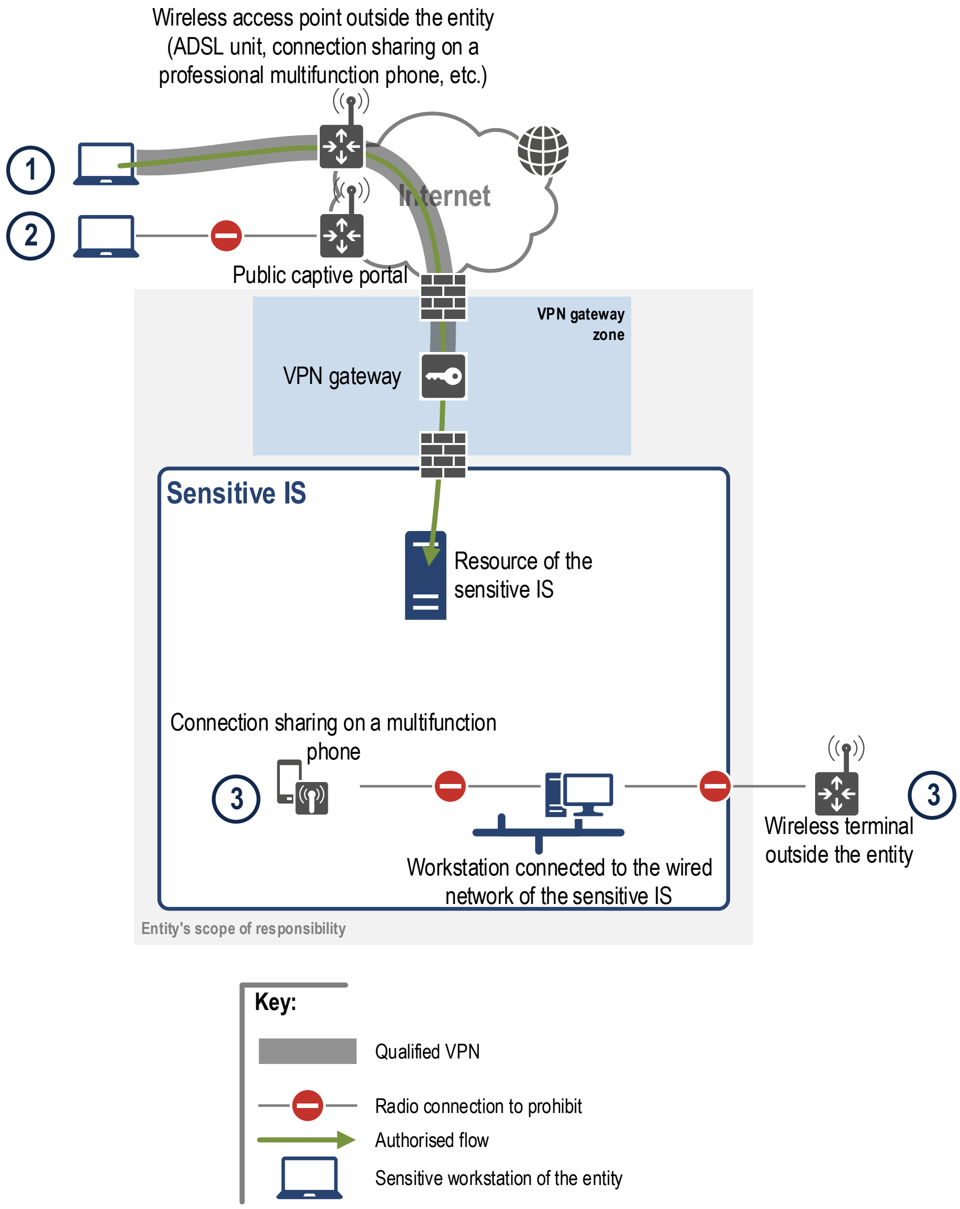
R61

Blocking access to captive portals from sensitive mobile access equipment

Access to public captive portals must be blocked on all mobile access equipment associated with a sensitive IS.

Figures 26 and 27 show use cases where the implementation of wireless networks is possible for sensitive flows, and use cases for which this implementation is prohibited.

108. Refer to security measure II 901 RES-SSFIL.
109. See security measure II 901 PDT-NOMAD-CONNEX.

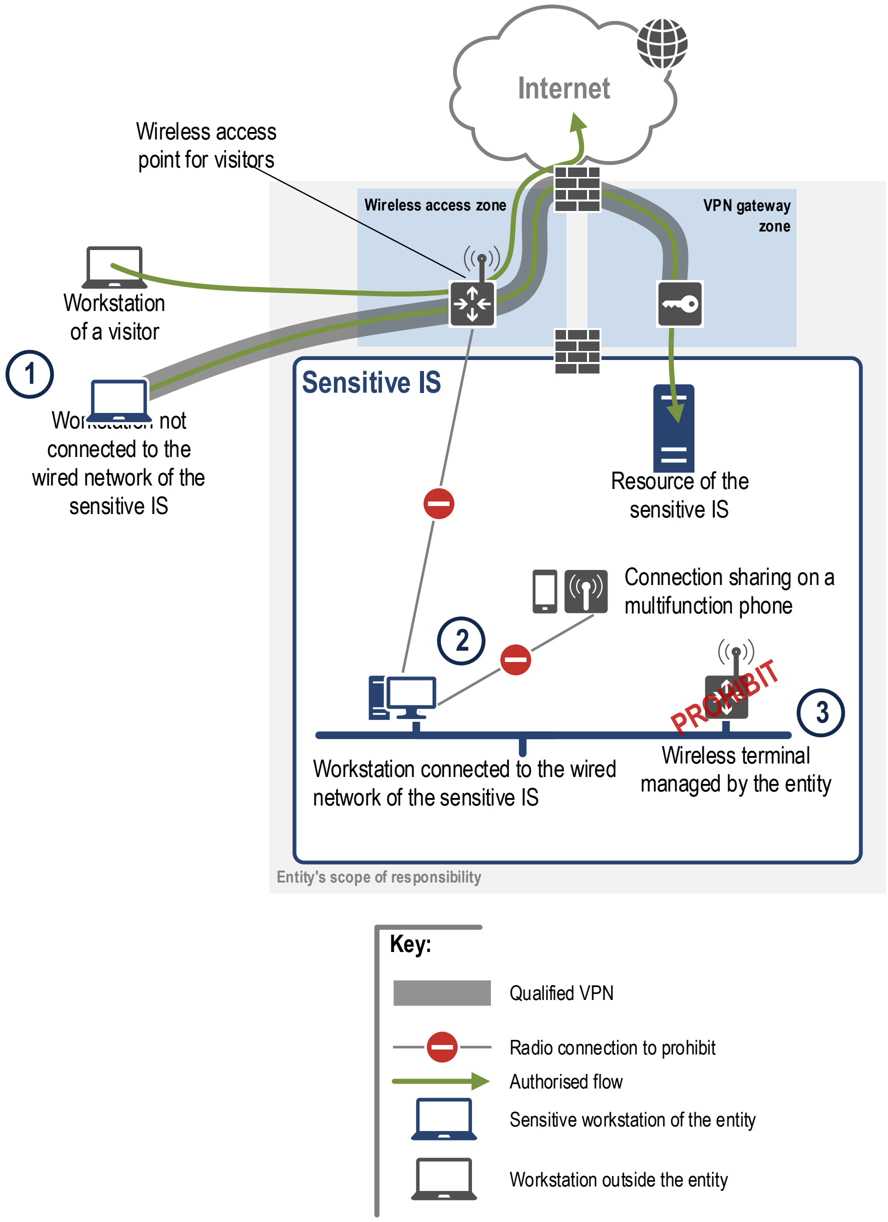


① Nominal case allowed in which the mobile workstation establishes a wireless connection with a wireless access point to the entity and then accesses sensitive IS resources exclusively through a VPN tunnel with an ANSSI security visa (in the case of sensitive ISs) or ANSSI approval (in the case of RD ISs).

② Flows required for establishing a wireless connection through a public captive portal are blocked, making this use case impossible.

③ Sensitive workstations (fixed or portable) connected by network cable to the sensitive IS must not be able to establish a wireless connection (either with a multifunction telephone or with a wireless box outside the entity, in the above example).

Figure 26 – Wireless network architecture: wireless access points are not controlled by the entity responsible for the sensitive IS



① If the entity implements a wireless access zone (typically to provide Internet access to its visitors), it is possible to provide a dedicated SSID for mobile users of the sensitive IS. This use case is comparable to case 1 in Figure 26, and the same technical security requirements apply.

② As in case 3 in 26, sensitive workstations connected to the wired network must not be able to establish a bi-connection with a wireless access point, even if it is implemented by the entity responsible for the sensitive IS (either with a multifunction phone or with the Internet access point for visitors, in the example above).

③ The entity responsible for a sensitive IS must not implement a wireless access point that is directly connected to the sensitive network, without filtering.

Figure 27 – Wireless network architecture: wireless access points are controlled by the entity responsible for the sensitive IS

7
Administration of sensitive ISs

Objective

This chapter presents good administration practices applicable to any sensitive IS. These good practices are not specific to sensitive ISs, but represent practices that are expected for the protection of any state-of-the-art managed IS.

7.1 General

Compliance with good administration practices is a very important issue for any IS, especially if it is a sensitive one [110]. The administration actions must be reserved for duly authorisedpersonnel, using dedicated resources. ANSSI has published a guide [25] providing good practices applicable to the secure administration of an IS.

R62

Applying the ANSSI recommendations on secure IS administration

The party responsible for a sensitive IS must comply with the recommendations of the guide relating to secure IS administration [25].

Information

The table in Annex E of this guide maps the security measures of II 901 relating to system administration to the recommendations of the good practice guide published by ANSSI [25] in its version 2 of April 2018.

Information

The IS for administering a sensitive IS is a subset of the sensitive IS. As a result, it must be accredited to the same level as the sensitive IS.

As administrators have extensive rights, they potentially have access to a significant amount of sensitive or RD data. Each of them may be required by the party responsible for the sensitive IS to obtain individual authorisation at a level that provides access to information covered by national defence secrets.

Administrator authorisation relates mainly to administrators of infrastructure components, not to functional or “business” administrators. In addition, among the infrastructure administrators, the requirement of authorisation for those with the highest levels of privileges is strongly recommended. This concerns two main groups of administrators :

110. See objective 22 of II 901.

- administrators with IS-wide privileges, with the ability to exceed their own rights and erase traces of their actions;
- administrators with privileges over many central resources (servers, storage facilities, etc.) or security resources.

R63

Managing the administrators of a sensitive IS

The list of administrators authorised to operate on a sensitive IS must be limited to specific need only, and must be known and approved by the accreditation authority[111]. It is further recommended that the administrators of an RD IS hold an individual clearance, at a level that allows access to information of national defence secrecy, especially if their privileges on the IS are extended.

7.2 Administration IS

This section presents the situation regarding administrative ISs for the three architectures shown in chapter 3 on the different types of sensitive IS.

111. Refer to security measure II 901 EXP-HABILIT-ADMIN.

7.2.1 Case of physically isolated sensitive ISs

In the case of "physically isolated sensitive IS architecture" (see section 3.2.1), two separate administration ISs are deployed to allow the administration of the sensitive IS on the one hand and the standard IS on the other. Administration workstations and administration tools servers [112] used for the administration of the sensitive IS are physically distinct from those used for the administration of the standard IS.

Figure 28 shows the situation of the administration IS in a "physically isolated sensitive IS" architecture.

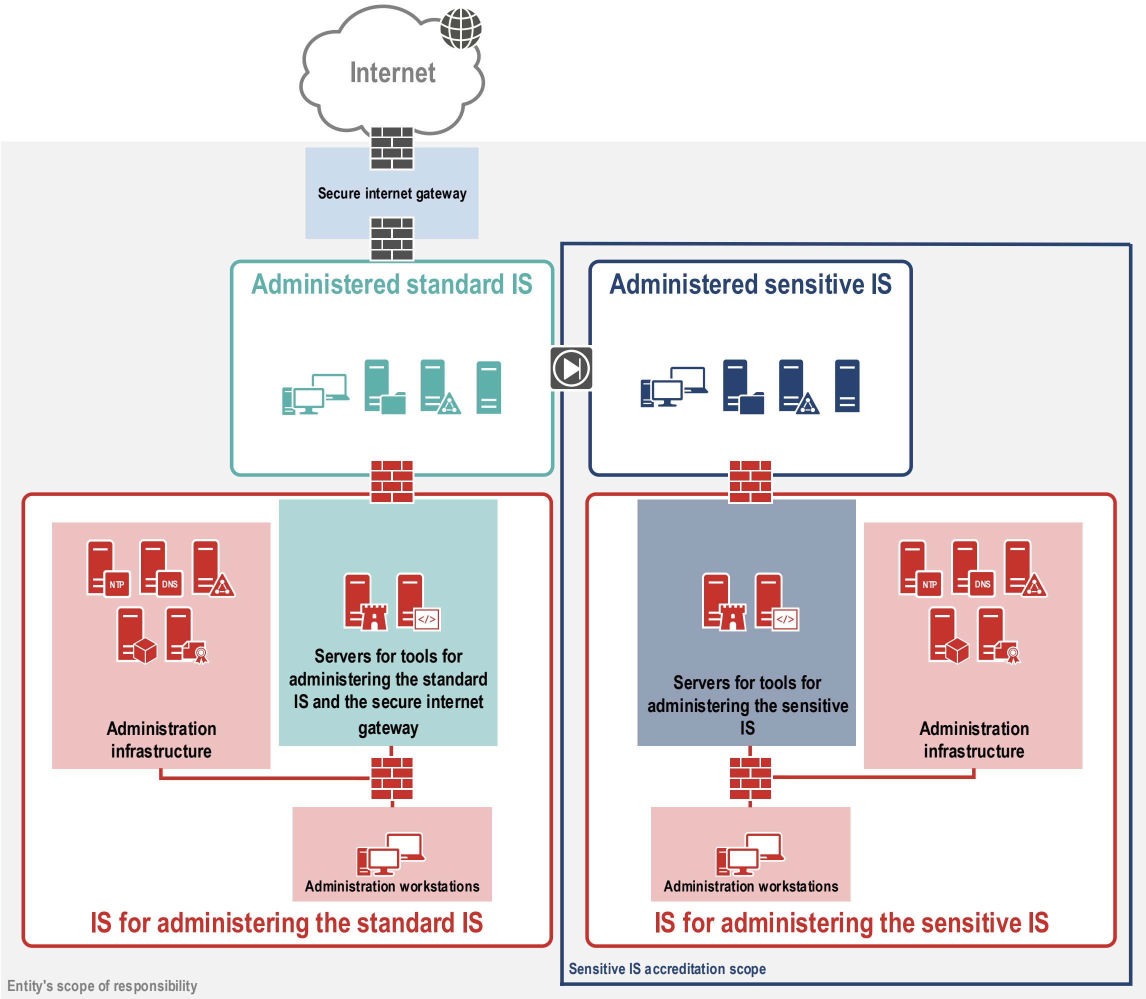


Figure 28 – Sensitive IS of class 2 - Situation of the administration IS in a "physically isolated sensitive IS"

112. *Administration tools servers* refer to servers dedicated to the execution of administration tools produced by publishers or equipment manufacturers (e.g. thick client or web service interacting with the administered resources). For more information on *administration tools servers*, see section 6.1 of the ANSSI guide to secure administration practices [25] in its version 2.

7.2.2 Case of physically partitioned sensitive ISs

In the case of "physically partitioned sensitive IS architecture" (see section 3.2.2), two separate administration ISs are deployed to enable the administration of the sensitive IS on the one hand and the standard IS on the other. The administration workstations and administration tools used for the administration of the sensitive IS are physically separate from those used for the administration of the standard IS.

Figure 29 shows the situation of the administration IS in the case of a "physically partitioned sensitive IS " architecture.

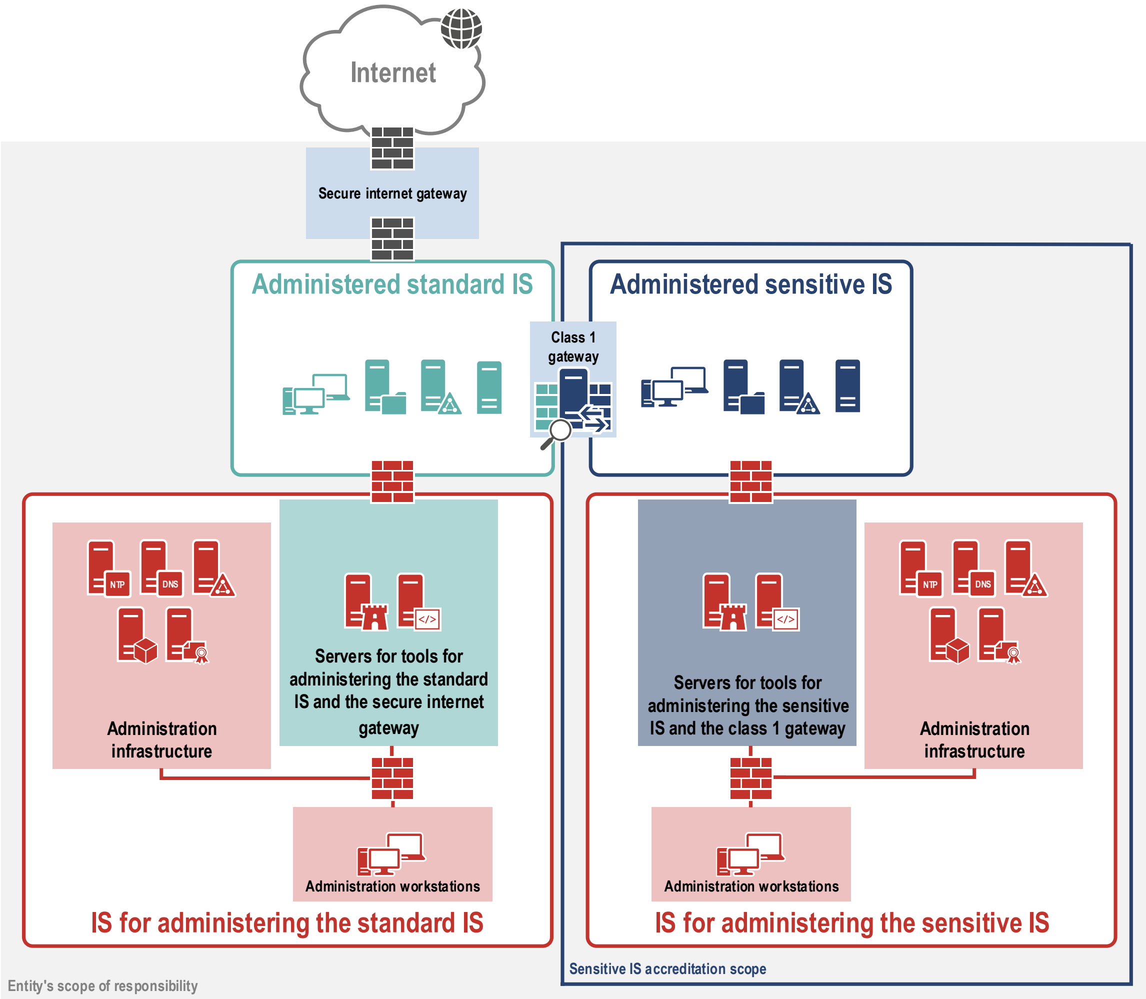


Figure 29 – Sensitive IS of class 1 - Positioning of the administration IS in the case of a "physically partitioned sensitive IS"

It is possible to use a single administration workstation to administer resources of a sensitive IS of Class 1 and resources of a standard IS (see Figure 30). The conditions for this mutualisation are explained in section 12.2 of the Guide [25] in its version 2. These conditions require in particular that the tool servers implemented for the administration of ISs with different levels of sensitivity (typically, sensitive level and standard level) must be dedicated by sensitivity level, with a partition between them.

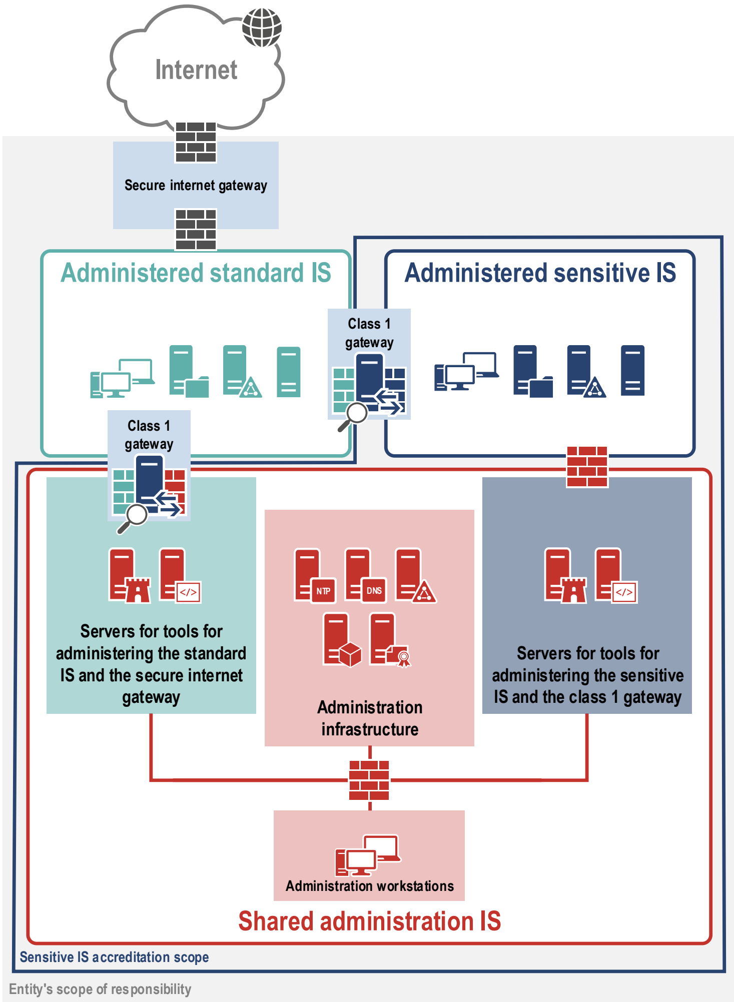


Figure 30 – Sensitive IS of class 1 - Example of mutualisation of the administration IS in the case of a “physically partitioned sensitive IS”

7.2.3 Case of sensitive ISs without standard IS

In the case of “sensitive IS architecture with no standard IS” (see section 3.2.3), the mutualisation of administration workstations is possible. However, administration tools must be dedicated to each IS : administration tools for the standard IS and other administration tools for the sensitive IS.

Figure 31 shows the situation of the administration IS in the case of a “Sensitive IS with no standard IS” architecture.

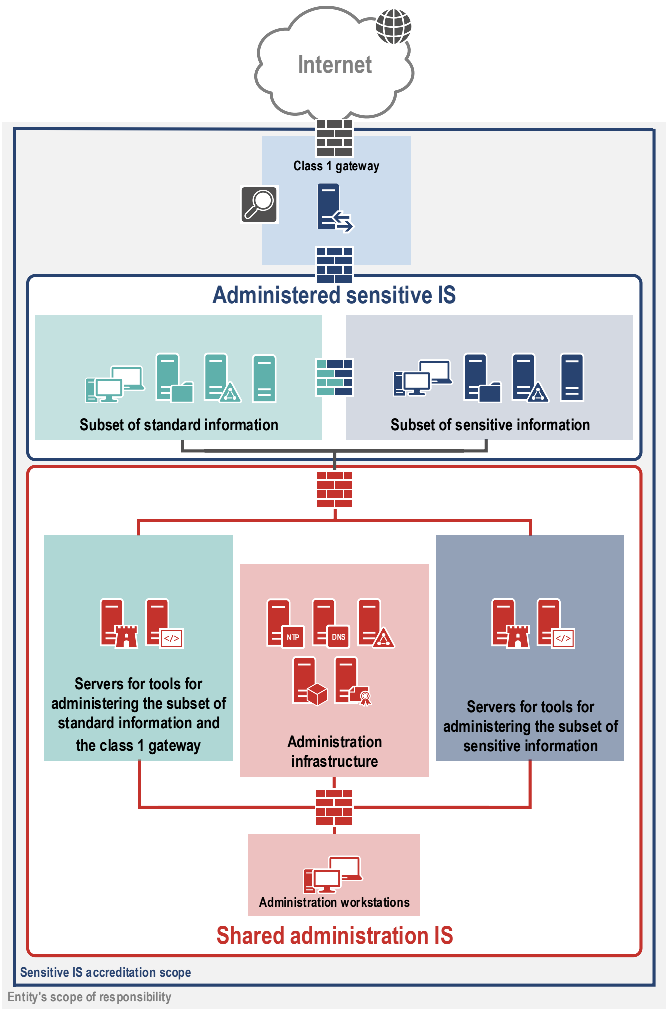


Figure 31 – Sensitive IS of class 1 - Positioning of the administration IS in the case of a “sensitive IS with no standard IS”

7.3 Remote administration

In accordance with the recommendations of the guide [25], the administration workstations used for these remote accesses must be managed and secured by the entity responsible for the sensitive IS. In addition, the IPsec VPN concentrator must be dedicated to remote administration and placed as close as possible to the administration IS. It is hosted in a *gateway of class 1* and the architecture ensures that the administration flows decrypted at this gateway remain partitioned off from the production flows of the sensitive IS [113].

R64

Securing the connection chain for remote administration

If a remote administration service is authorised for a sensitive IS, access must be from controlled administration workstations and the flows must be secured using an IPsec VPN tunnel. The VPN concentrator, dedicated to the remote administration service, must be approved (in the case of RD ISs) or have a security visa (in the case of sensitive ISs). The IPsec protocol must be configured according to the recommendations of the ANSSI guide [17]. The local firewall of an administration workstation must block all flows except those necessary to establish the tunnel, and the *split-tunnelling* function must be disabled in the VPN concentrator configuration settings.

A special case of remote administration is remote maintenance. Remote maintenance relates to a person's remote access to business assets, with an account that has special privileges for those assets (e. g. access to specific business software by experts from the publisher). In some cases of remote maintenance, it may be difficult for the entity responsible for a sensitive IS to control the administration workstation used for this remote access. Consequently, any access of this type must be subject to a specific risk analysis and technical or organisational measures must be implemented to reduce the risk of intrusion or exfiltration (e. g. no permanent connection but access is occasionally opened, the administrator is required to connect to a temporary intermediate machine that is reset after each use…).

Remote maintenance procedures must always be established under the control of the responsible entity (directly or indirectly through the implementation of contractual clauses). The ANSSI has published a guide [13] on the control of risks related to outsourcing.

R64 -

Controlling remote maintenance systems connected to sensitive IS

Remote maintenance interconnections are subject to a specific risk analysis and risk reduction measures are to be implemented.

7.4 Security maintenance (MCS)

The components of a sensitive IS must be regularly updated to correct the vulnerabilities that affect them. The entity implementing a sensitive IS must formalise a security maintenance policy which, for each component, specifies the methods for deploying security updates [114] (frequency, system

113. Refer to security measure II 901 EXP-SEC-FLUXADMIN.
114. See security measure II 901 EXP-POL-COR.

dependencies, non-regression tests…). These methods depend in particular on the exposure of the component, its business criticality and its operational availability constraints.

R65

Defining and implementing a security maintenance policy

The party responsible for a sensitive IS will establish a policy for the security maintenance of IS components and its administration IS. This policy will specify the deployment frequencies and testing procedures for security updates. It is recommended that critical security updates be deployed within one week and other security updates within four weeks.
To be effective, this policy requires that the entity responsible for the sensitive IS should keep its mapping up to date, including the inventory of the resources implemented [115].

It is recommended that a sensitive IS should be structured into trust zones with a homogeneous security level (see recommendation R32). One of the criteria for homogeneity is the ability of the entity to keep the components of this zone up to date. To achieve this, the use of centralised tools is recommended [116].

Any action that reduces the likelihood of having to manage obsolete systems must be examined. In particular, the entity responsible for a sensitive IS must be particularly vigilant in including clauses on security maintenance of the hardware or software solutions in the contracts between them and the publishers of the solutions [117].

Despite the entity's efforts, obsolete systems may remain. These systems, which are no longer maintained in secure condition, must be isolated from the sensitive IS and not share any resources with it [118].

It is not possible to give generic recommendations for the practical application of this isolation here: the technical response will vary depending on the scope of the obsolescence (does it relate only to server components or also to client components?), the level of integration of obsolete systems (strong or weak links to other components of the IS?), the number of users concerned, and their geographical distribution…

R66

Isolating obsolete systems

Obsolete systems that are kept in production to meet justified business needs must be isolated from the sensitive IS. The way in which this isolation is to be achieved must be the subject of a specific study.

7.5 Security logging and monitoring

The collection of logs, and the implementation of a qualified detection system (see section 4.3.1), is of little value if it is not accompanied by active and constant monitoring, carried out by secu-

115. Refer to Article 9 of II 901 and the security measures II 901 GDB-INVENT, GDB-CARTO and RES-CARTO.
116. Refer to security measure II 901 EXP-CENTRAL.
117. See security measure II 901 INT-REX-HS.
118. Refer to security measures II 901 EXP-OBSOLET and EXP-ISOL.

rity incident detection professionals. As a result, the logging policy must be closely linked to the monitoring strategy.

In addition to the guide on good administration practices [25], ANSSI has published a good practice guide concerning the logging of computerised systems[26]; its application is required when implementing a sensitive IS.

R67

Applying ANSSI recommendations on logging

Good architecture and configuration practices for the logging of security events formulated by the ANSSI [26] must be applied.

The system and security logs of a sensitive IS must be kept for a period of twelve rolling months [119]. The purpose of collecting and retaining them over this period is to increase the detection efficiency of the SOC [120] for:

- triggering security alerts when security events are matched with detection rules defined by the security monitoring function;
- improving the ability to qualify alerts raised (distinguish false positives from true positives) by analysing raw events (events that have not necessarily been correlated by detection rules);
- searching for suspicious events *after the fact* (e. g. search for new markers of compromise [121] in past data; applying new rules in archived logs, etc.).

R68

Keeping logs for a sensitive IS for 12 months

Security event logs must be kept for a period of twelve months, except in the case of specific legal and regulatory constraints imposing specific retention periods.

Once the logs have been collected, the purpose of security monitoring is to trigger alerts in response to the detection of pre-established threat scenarios, whether they are untargeted and opportunistic attacks or feared events in a specific business context.

As part of this process of developing the monitoring strategy, the IS manager ensures that the data needed for detection is generated, collected and centralised. If this is not the case, an improvement process must be implemented to address these shortcomings. Only an iterative approach of this kind can increase the detection coverage over time.

It is recommended that an entity implementing a sensitive IS uses the services of a security incident detection service provider (SIDS) qualified by ANSSI [122].

The detection service may be provided by the entity responsible for the sensitive IS to be monitored, or by an external company [123].

119. See security measure II 901 EXP-CONS-JOUR.
120. *Security operation center*
121. More information about indicators of compromise is available in section 4.3.1.
122. see article 16 of II 901.
123. Refer to chapter III.1 of the SIDS requirements [29] in its version 2.0 of December 2017. The list of SIDS who are qualified or in the process of qualification is available on the ANSSI website [33].

If a qualified service provider is not used, it is recommended that the party responsible for a sensitive IS should draw inspiration from the good practices described in the SIDS requirements framework [29] for designing, implementing and operating the monitoring system.

R69

Using a qualified provider for security

monitoring It is strongly recommended that the party responsible for a sensitive IS should use the services of a security incident detection service provider (SIDS) qualified by the ANSSI to set up a security monitoring system. If the services of an external provider are not used, an internal monitoring service must be set up by the entity and this service must be designed in accordance with the good practices described in the SIDS requirements framework.

i

Information

The requirements framework for the qualification of a SIDS requires that the data handled by the provider should be protected at Restricted Distribution level [124]. As a result, the detection architecture implemented by the service provider constitutes an accredited IS at RD level [125].

Whether the sensitive IS is subject to security monitoring by a qualified service provider or by the entity responsible for the sensitive IS, security incidents must be reported to the ANSSI as soon as they occur [126].

R70

Formalising a procedure for reporting security incidents to ANSSI

The party responsible for a sensitive IS must formalise a procedure for reporting incidents incidents to ANSSI. These declarations include incidents that exceed, or are likely to exceed, the scope of the sensitive IS and incidents relating to security alerts (including alerts issued by CERT-FR [127]).

124. This data includes, in particular, the documents supplied by the client, information collected, indicators of compromise, findings, logs, roadmap and analysis reports.

125. Refer to the SIDS requirements framework [29] in its version 2.0 of December 2017: *IV.3.2. c) The detection service's IS must be accredited at least to* Restricted Distribution *level for the monitoring of the sponsor's unclassified defence information systems.*

126. See security measure II 901 TI-INC-REM.

127. Governmental centre for monitoring, alert and response to computer attacks. Website: https://www.cert.ssi.gouv.fr/ .

Appendix A
Sensitive, RD and standard information - Detailed explanations

This annex is a complement to chapter 2 in which sensitive and standard IS are defined. It is divided into two parts. In the first section, the terms "sensitive information", "RD information" and "standard information" are defined. A second section then explains the legal differences between these types of information.

A.1 Definitions

Digital information assets

Any legal entity, public or private, is responsible for a body of digital information, which can be described as *digital information assets*. Theis information is processed on one or more information systems (IS). A subset of these assets comprises public information: this is information for which the need for security in terms of confidentiality is, by definition, zero [128].

Figure 32 gives a symbolic representation of information assets and public information.

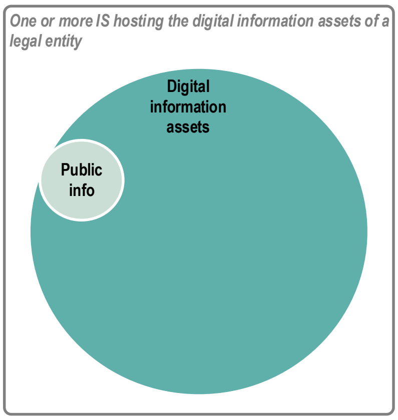


Figure 32 – Symbolic representation of the information assets of a legal entity

128. While the confidentiality security requirement for public information is zero, this is not the case for the need for integrity and availability of this data or of the IS hosting it.

This representation will be used in this annex as a guideline to explain the interlocking levels of information sensitivity.

Sensitive information

II 901, the reference legislation governing the protection of sensitive information systems in France, provides the following definition of sensitive information [129].

Sensitive information

Sensitive information is information whose disclosure to unauthorised persons, alteration or unavailability is likely to prejudice the achievement of the objectives of the entities that use it.

Information

Because its main objective is to define the rules for the management and *confidential* protection of certain *information*, II 901 differs from other regulations which aim primarily to ensure that the processing operations carried out on an IS are *complete* and *available*. Examples of such regulations are the French Military Planning Act 2014-2019 (which defines the concept of a critical information system (SIIV)) or the European directive on the security of networks and information systems, known as the "NIS directive" (which defines the concept of an essential information system (SIE)).

Sensitive information comprises a subset of digital information assets. Figure 33 illustrates this point.

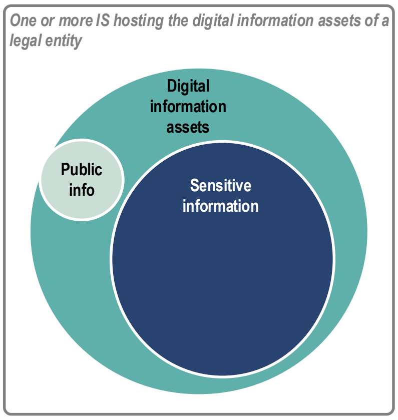


Figure 33 – Symbolic representation of sensitive information; a subset of the information assets of a legal entity

Restricted Distribution (RD) information

The concept of Restricted Distribution information is introduced in Annex 3 of the IGI 1300 [1]. This legislation specifies that the rules applicable to IS with this level of sensitivity are defined

129. See Article 1 of II 901.

in II 901 [28]. These protection rules are not limited to a specific community of interest, but are applicable to any French public or private entity [130].

Restricted Distribution information (defined in II 901)

Restricted Distribution (RD) information is sensitive information (as defined above) marked Restricted Distribution or its European or international [131] equivalents.

In II 901, the objective of protecting the confidentiality of information is enhanced in the case of information marked Restricted Distribution. The use of this qualifier makes the necessary restriction on the distribution of this information clear. RD information must not be made public. It may be communicated only to persons with a *need to know*, i.e. to persons who have a compelling need to access the information in order to carry out the tasks entrusted to them in the course of their duties.

In France, in contrast to some international regimes, the Restricted Distribution label is not a level of classification of national defence secrets, but a protection statement. It does not provide the information with the criminal law protection specific to information classified as national defence secrets. Nevertheless, a person who discloses Restricted Distribution information is potentially liable to disciplinary sanctions [132], or even to the engagement of its financial liability.

Restricted Distribution (RD) information is a subset of sensitive information. Figure 34 illustrates this point.

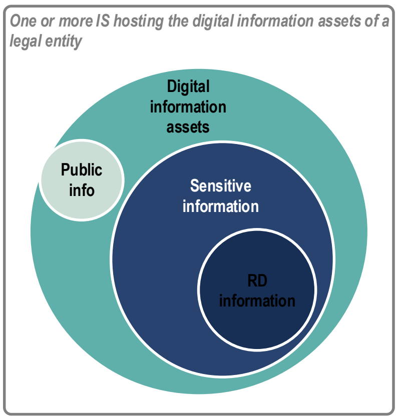


Figure 34 – Symbolic representation of RD information within the information assets of a legal entity

The information (and, more often than not, the physical medium containing this information) is explicitly marked RESTRICTED DISTRIBUTION. The point of this marking is to transfer the

130. Restriction of distribution notices equivalent to Restricted Distribution attributed to documents by foreign States or international organisations have the effect of subjecting these documents to the protection rules described in Article 5 and Annex 3 of the IGI 1300 and in the II 901. Note that the equivalent of the RD information in some regulations (e. g. *EU Restricted*, *NATO Restricted*) constitute classified information.

131. See Article 1 of II 901.

132. For example, see Article L. 4121-2 of the Defence Code for military personnel and Article 26 of Law No. 83-634 of 13 July 1983 on the rights and obligations of civil servants.

responsibility for the management and protection of this particular sensitive information to the legal entity receiving such information, subject to any applicable contractual arrangements between the issuing and receiving entities. For more information about marking information and data media, see section 5.4.

Users of a sensitive IS who have a justified need to process sensitive or even restricted information must be informed by the entity responsible for the IS of the need for confidentiality of this information. They must also be made aware of the obligations applicable to the processing of this information and the practical application of these obligations within the entity.

In case of transmission of Restricted Distribution data to a third party, the security rules to be applied by the third party to protect the data should be specified, especially within the framework of an agreement. Such an agreement may simply require compliance with II 901, or be more detailed and binding.

Finally, some RD information can also be marked Special France (SF). In this case, the entity responsible for an RD IS hosting SF RD data must implement the appropriate logical access control and organisational methods to ensure that the data is made accessible to French nationals only [133].

Standard information

One difficulty lies in what to name the subset of information that is neither sensitive information as defined in II 901, nor public information (freely accessible to all without prior authentication). It is tempting to refer to this subset using the expression "non-sensitive information". But this information nevertheless has a certain level of sensitivity, and therefore requires a level of protection: the entity responsible for it would not conceive of leaving it accessible without any protection.

Therefore, the term "non-sensitive information" is not used in this guide. Information that is neither sensitive under the meaning of II 901, nor public, is referred to as "standard information" and this subset of information is represented by the red coloured area in Figure 35.

133. Refer to article 65 of the IGI 1300.

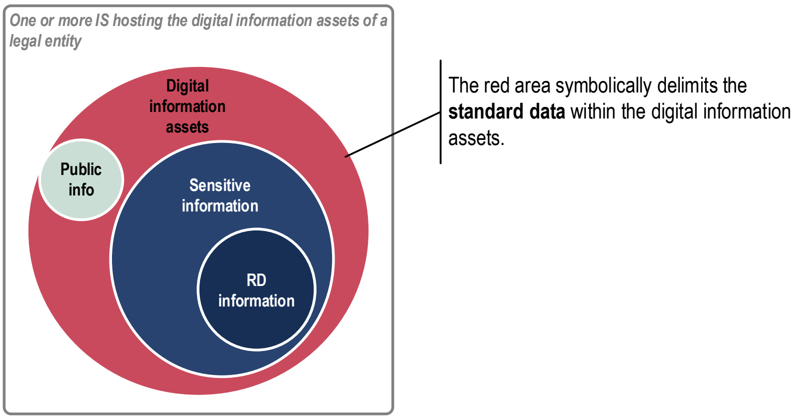


Figure 35 – Symbolic representation of standard information: neither sensitive nor public information

A.2 Legal differences between RD and non-RD information

The advantage, for the creator of an item of information, of qualifying it as Restricted Distribution is to subject all those who handle it to a restriction on distribution (see the definition of RD information at A.1). This qualification also makes it possible to pass on this distribution restriction when transferring the information to another legal entity. That entity must ensure the continuity of protection of the RD information by processing the decrypted RD information on an IS on which security measures specific to the protection of RD information are implemented.

Sensitive information that is not RD information is information protected by a regime specific to the entity that produces it. The choice of the terms used to designate such information is left to the entity implementing the protection regime. For illustration purposes, the following designations are examples of information protection statements that may be chosen by an entity to protect its sensitive non-RD data: LIMITED DISTRIBUTION, LIMITED COMPANY, RESTRICTED COMPANY, INDUSTRY CONFIDENTIAL.

This sensitive non-RD information can, however, benefit from legal protection through specific regulations (protection of business secrecy [134], information covered by professional secrecy [135], regulations specific to health data…).

134. Law no. 2018-670 of 30 July 2018 on the protection of business secrets. Under Article L. 151-1 of the Commercial Code, *any information meeting the following criteria is protected as a business secret: 1. It is not, in itself or in the exact configuration and assembly of its elements, generally known or readily available to those familiar with such information by virtue of their industry; 2. It has actual or potential commercial value because of its confidential nature; 3. It is subject to reasonable safeguards by its legitimate holder, having regard to the circumstances, for maintaining its secrecy.*

135. Law No. 78-754 of 17 July 1978 on various measures to improve various measures to improve relations between the administration and the public and various administrative provisions

The legal differences regarding transfers of sensitive information are illustrated in Figures 36 (transfers of sensitive non-RD information) and 37 (transfers of RD information).

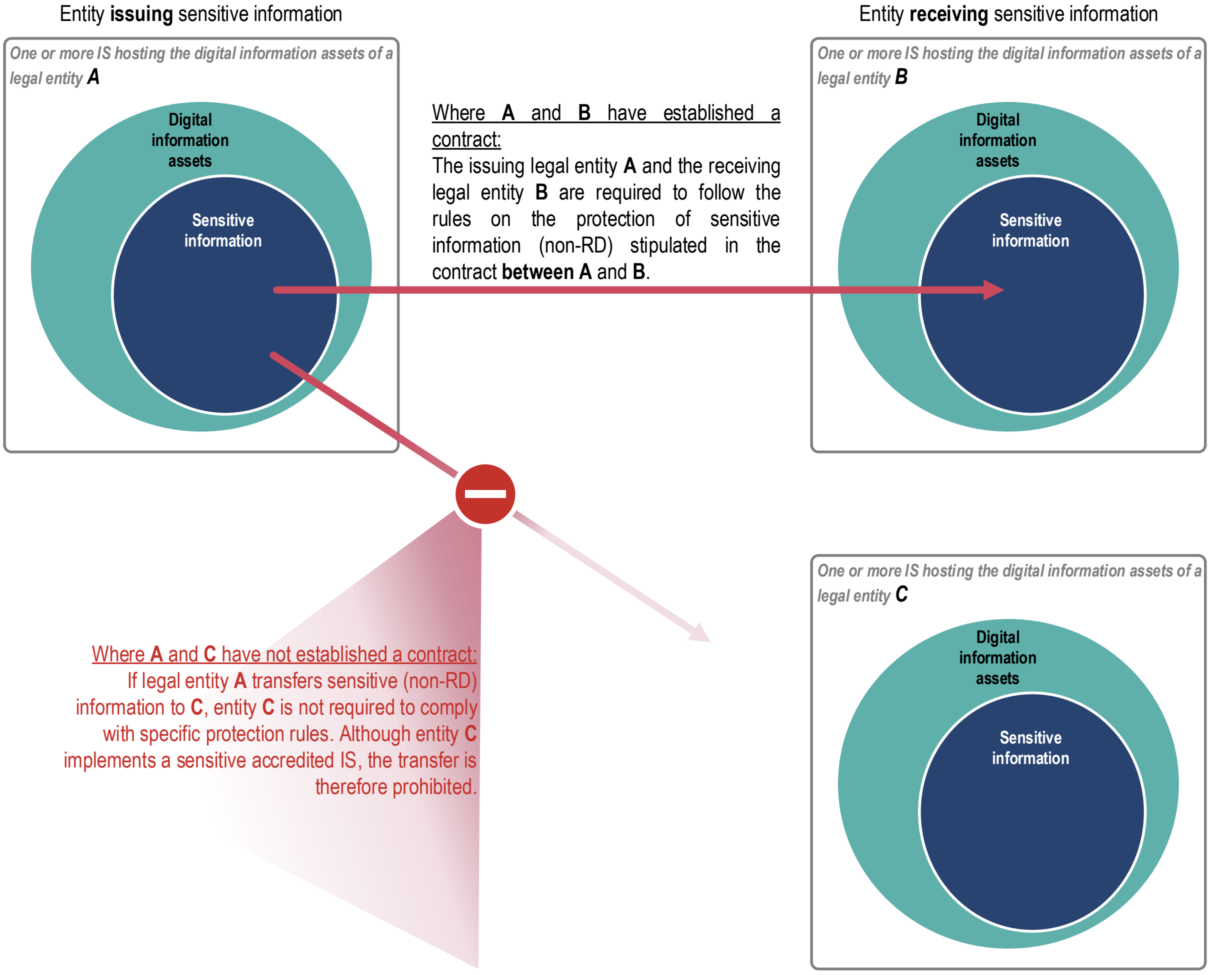


Figure 36 – Illustration of the transfer of sensitive (non RD) information from one legal entity to another legal entity

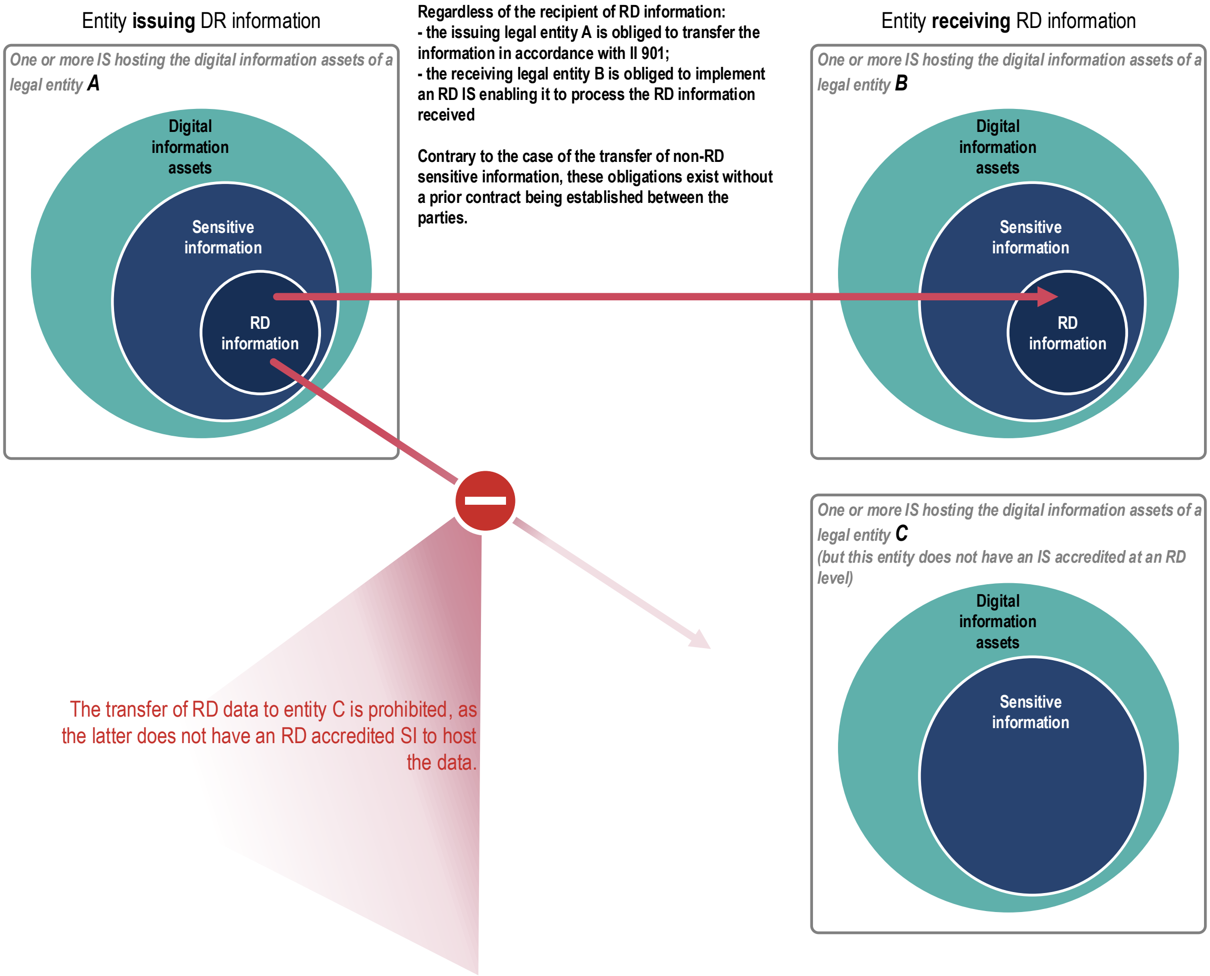


Figure 37 – Illustration of the transfer of RD information from one legal entity to another legal entity

Appendix B
Information sensitivity levels

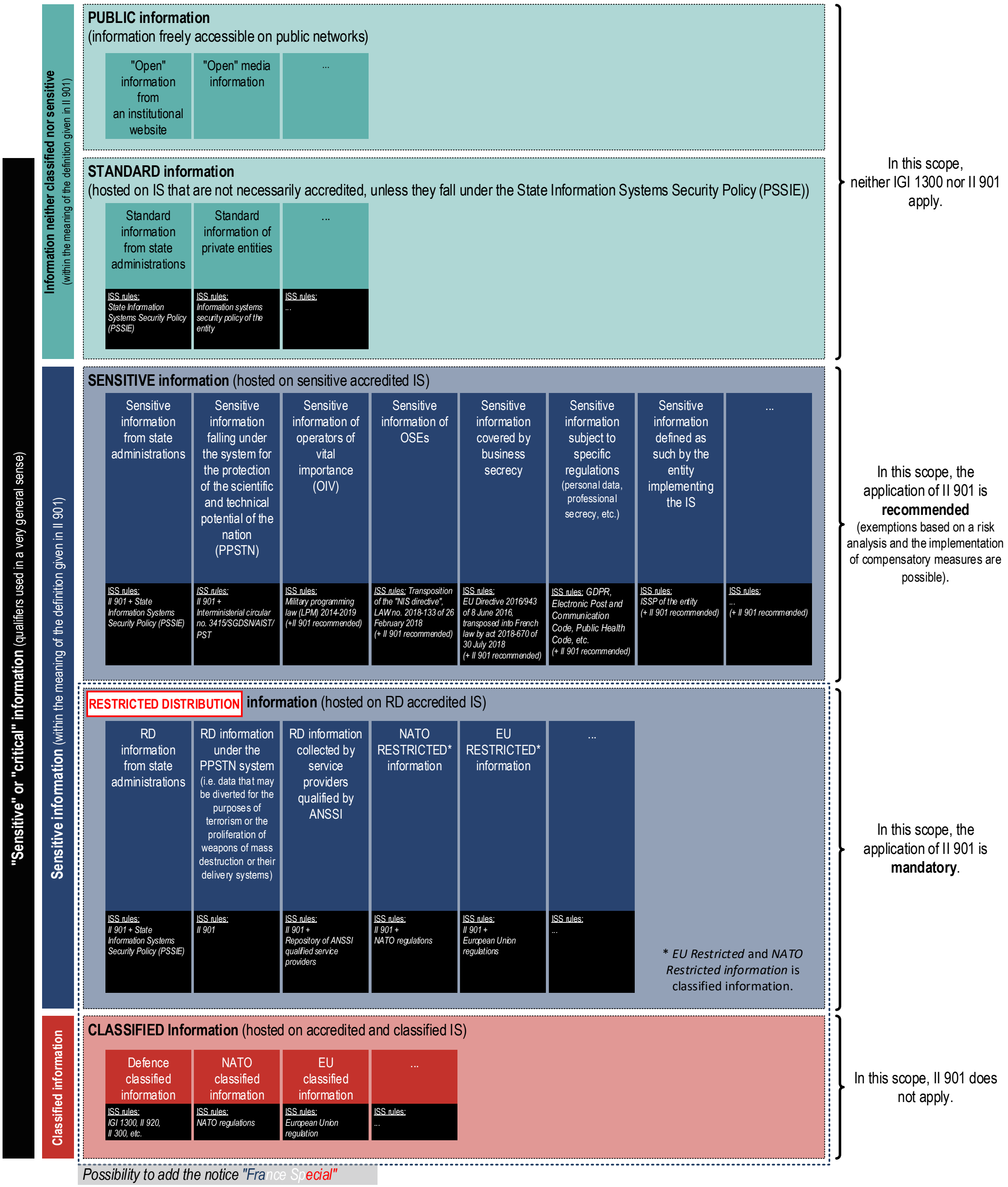


Figure 38 – Sensitivity levels of information in France and associated ISS standards

Appendix C
Security visas

A security visa is a certificate that a security level has been reached. It may relate to a security product or a security service provider.

Certification, qualification and accreditation are distinct concepts that should not be confused. All three terms are relevant to security products. For providers of trusted services, only the term "qualification" is used.

Product security certification

The security certification issued by ANSSI is a recognition of the robustness of a product, i.e. its ability to resist computer attacks. This robustness is tested through an evaluation by a third party, whose competence is guaranteed by ANSSI. These independent laboratories are called Information Technology Security Assessment Centres (CESTIs).

The certification also provides assurance of the conformity of the security functions with regard to expected behaviour, described in the security target, as well as the assurance of compliance with reference frameworks and evaluation criteria.

The security objectives and use cases for a certified solution are defined by the client, which may be the solution provider, the ANSSI, or a third party (typically interested in acquiring the solution). ANSSI is not involved in the definition of the security target [136] : security certification does not constitute a recommendation by the French government for use in a given framework.

The certifying evaluation can be conducted according to two types of methodologies:

- First Level Security Certification (CSPN), a national methodology focused on an analysis of vulnerability (robustness), which takes place under time and load constraints;
- the Common Criteria (CC), an international standardised methodology that allows the evaluation of the robustness of a product and attests to a level of assurance (several levels of assurance are defined, from EAL [137] 1 (lowest level) to EAL 7 (highest level).

136. In a certification procedure, ANSSI intervenes only to challenge security targets that are misleading.
137. *Evaluation Assurance Level*

Security qualification of a product or service

For products and services alike, trust is assessed as part of the qualification process and its follow-up. The trust evaluation consists of testing the supplier's ability to fulfil a set of commitments made to ANSSI over the long term:

- for products: confidentiality and protection of data entrusted by the user of the product, correction of flaws and vulnerabilities, etc.;
- for services: ability to identify and control threats and risks to meet the requirements set out in business standards, to maintain skills, etc.

The qualification procedure for a security product is based on one or more security certifications(CSPN or CC certification). However, unlike the certification procedure described in the previous paragraph, ANSSI can correct the definition of the security requirements specified in the security target. In addition, in its capacity as a national security authority, ANSSI analyses and guides the work carried out by the evaluation centres.

For any given use, qualification is the recommendation by the French State of a product or service. It attests simultaneously to the quality of the solution (robustness of a product or competence of a service provider), the confidence that the State has in the supplier, and the relevance of the solution to a need identified by the State, whether it is its own need, the need of operators of vital importance (OIVs) or that of any other actor identified in a regulatory framework.

The qualification of a product (or a service) may be accompanied by a level of recommendation for use, which evolves according to the monitoring of the qualification over time, and takes the practical form of a colour code:

- Green category: unreservedly recommended solution, including for new uses (new product deployment, new service contract);
- Orange category: solution recommended only for existing uses, not recommended for new uses (e. g. a product for which a new, more effective qualified version is available and should be preferred for new deployments);
- Red category: solution whose qualification will be revoked soon and whose replacement or withdrawal from service must be planned for (product no longer maintained by its developer, service soon to be discontinued).

The list of qualified products and services is regularly updated and available on the ANSSI website: https://www.ssi.gouv.fr/liste-produits-et-services-qualifies/ .

Product security approval

A security approval is associated with a level of sensitivity for the information to be protected. For example, security approval at RD level issued by ANSSI attests to the ability of a product to protect RD information.

In cases where a product is RD-approved, this is explicitly stated on the product's qualification certificate.

For more information

The list of qualified products is available on the ANSSI website:

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

For more information on security visas:

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

Appendix D

Mobility - II 901 security measures and ANSSI guide

Table 1 – Correspondence table between the II 901 security measures relating to mobility and the ANSSI "Recommendations on digital mobility" [22] (version 1, October 2018)

II 901 ref.	**Description of the security measure**	**Recommendation(s) of ANSSI guide on digital mobility (version 1, October 2018)**
EXP-NOMAD-SENS	Declaration of mobile equipment capable of handling sensitive information	R2, R3
EXP-ACC-DIST	Remote access to the organisation's information system	R21, R22
PDT-VEROUIL-PORT	Locking of mobile devices	A7 - The use of an anti-theft cable is strongly recommended for sensitive access equipment.
PDT-NOMAD-ACCESS	Remote access to the entity's IS	R16, R17, R18, R19, R20
PDT-NOMAD-PAREFEU	Local firewall	R11, R17
PDT-NOMAD-STOCK	Local storage of information on mobile workstations	A9 - An approved encryption solution is mandatory to protect RD data on the mobile access equipment.
PDT-NOMAD-FILT	Privacy filter	R7
PDT-NOMAD-CONNEX	Configuring wireless connection interfaces	R12, [14]
PDT-NOMAD-DESACTIV	Disabling wireless connection interfaces	R12

Appendix E
IS administration - II 901 security measures and ANSSI guide

Table 2 – Table of correspondence between the II 901 security measures relating to administration and the ANSSI "Recommendations for the secure administration of information systems V2" [25] (version 2, April 2018)

II 901 ref.	**Description of the security measure**	**Recommendation(s) of the ANSSI guide on secure administration (version 2, April 2018)**
EXP-RESTR-DROITS	Restricting rights	R27
EXP-PROT-ADMIN	Protecting access to administrative tools	R1, R2, R15/R15-, R16, R18/R18-, R22, R23, R32
EXP-HABILIT-ADMIN	Authorising administrators	R39, R40, R41
EXP-GEST-ADMIN	Managing administrative actions	R45, R46, R47
EXP-SEC-FLUXADMIN	Securing administration flows	R8, R9/R9-/R9- -, R10, R11, R12, R13, R15, R15-, R18, R18-, R19, R20, R21, R23, R24, R24-
EXP-CENTRAL	Managing administrative actions	R22
EXP-CI-MESSTECH	Technical messaging	R53
PDT-PRIV	Using administrator access privileges	R29
PDT-ADM-LOCAL	Managing the local administrator account	R1

Appendix F
II 901 security measures

Table 3 – Comprehensive list of II 901 security measures with cross-references to the sections of this guide where these measures are mentioned or, where appropriate, references to other ANSSI publications

II 901 ref.	**Description of the security measure**	**Ref. in this guide (or other ANSSI reference)**
Article 1	Definitions	2.1, A.1
Article 2	Scope of application	R3
Article 3	Strategic principles applied	R4 (continuous improvement) ; 5, R6 (defence in depth) ; R62 (secure administration) ; R29, R30 (qualified security products and services)
Article 4	Applying rules	
Article 5	Determining information sensitivity	R1, R36
Article 6	Governance of information systems protection	
Article 7	Risk management	2.1,
Article 8	Approving sensitive information systems	2.4
Article 9	Protecting information systems	R65 (mapping) ; [24] (physical protection) ; 5, 6 (logical protection)
Article 10	Managing information systems security incidents	7.5
Article 11	Evaluating security levels	R4
Article 12	Relationship with State authorities	
Article 13	Accreditation of *Restricted Distribution* information systems	2.4
Article 14	Processing of information marked *Restricted Distribution*	2.2 (IS classes) ; R19, R9, R55 (encryption of RD information)
Article 15	Physical protection of premises	[24]
Article 16	Outsourcing	5.1, 7.3, [10]
Article 17	Use in uncontrolled environments	R19 (encryption of RD information) ; 6.4 (special precautions in mobile situations)
Article 18	Audio-visual media	
Article 19	Authorisations of derogations	
Article 20	Transitional provisions	
Article 21	Repeal	
ORG-SSI	Organisation of the ISS	
ORG-ACT-SSI	Identifying ISS actors	
ORG-RSSI	Nominating the party responsible for the ISS	
ORG-RESP	Formalising responsibilities	
ORG-TIERS	Contractual management of third parties	5.1, 7.3, [10]
ORG-PIL-PSSI	Defining and managing the ISSP	[12]

Continued on next page...

Ref.	Description of the security measure	Ref. in this guide (or other ANSSI reference)
ORG-APP-INSTR	Applying the instruction within the entity	
ORG-APP-DOCS	Formalising application documents	
RH-SSI	ISS Implementation Charter	
RH-MOTIV	Selecting and raising awareness among people in key ISS positions	
RH-CONF	Trusted personnel	
RH-UTIL	Raising awareness of information system users	
RH-MOUV	Managing arrivals, transfers and departures	5.5
RH-NPERM	Managing non-permanent staff (trainees, temporary staff, contractors)	
GDB-INVENT	Inventory of IT resources	7.4
GDB-CARTO	Mapping	7.4
GDB-QUALIF-SENSI	Qualifying information	5.4, 2.1
GDB-PROT-IS	Protecting information	3.3
INT-HOMOLOG-SSI	Approving information systems security	2.4, 4.2, [16]
INT-SSI	Integrating security into projects	7.4
INT-QUOT-SSI	Implementing the ISS at a day-to-day level	7.4
INT-TDB	Creating an ISS dashboard	
INT-AQ-PSL	Acquiring security products and trust services	5.1
INT-PRES-CS	Security clauses	5.1, 7.3, [10]
INT-PRES-CNTRL	Monitoring and controlling supplied services	[10]
INT-REX-AR	Risk analysis	2.4, [16]
INT-REX-HB	Hosting	
INT-REX-HS	Hosting and security clauses	5.1, 7.4, [10]
PHY-ZONES	Dividing sites into security zones	
PHY-PUBL	Network access in public reception areas	5.3
PHY-SENS	Protecting sensitive information within reception areas	5.3
PHY-TECH	Physical security of technical premises	
PHY-TELECOM	Protecting electrical and telecommunications cables	
PHY-CTRL	Anti-tampering controls	
PHY-CI-LOC	Dividing premises into security zones	
PHY-CI-HEBERG	Service agreement for third-party hosting	[10]
PHY-CI-CTRLACC	Physical access control	5.1
PHY-CI-MOYENS	Issuing physical access media	
PHY-CI-TRACE	Traceability of access	
PHY-CI-ENERGIE	Energy facility	
PHY-CI-CLIM	Air conditioning	
PHY-CI-INC	Fire-fighting	
PHY-CI-EAU	Anti-flooding measures	
PHY-SI-SUR	Securing the security IS	[24]
RES-MAITRISE	Systems allowed on the network	6.1
RES-INTERCO	Interconnections with external networks	4.2, 4.3, [23]
RES-ENTSOR	Setting up network filtering for outgoing and incoming flows	4.2, 4.3, [21], [5], [15], [18], [23]
RES-PROT	Protecting information	4.2, 4.3, [23]
RES-CLOIS	Partitioning the IS into sub-networks with homogeneous security levels	5.3
RES-INTERCOGEO	Interconnecting local geographical sites of a body	4.2
RES-RESS	Partitioning resources in the case of shared premises	
RES-INTERNET-SPECIFIQUE	Special case of specific accesses in an entity	4.3.3
RES-SSFIL	Setting up wireless networks	6.5
RES-COUCHBAS	Implementing protection mechanisms against attacks on lower layers	[6]
RES-ROUTDYN	Monitoring routing announcements	
RES-ROUTDYN-IGP	Securely configuring the IGP protocol	
RES-ROUTDYN-EGP	Securing EGP sessions	
RES-SECRET	Systematically changing the default authentication elements of equipment and services	5.3
RES-DURCI	Hardening network equipment configurations	5.3, [6]
RES-CARTO	Developing technical and functional architecture documents	7.4
ARCHI-HEBERG	Architecture principles of the hosting zone	5.3
ARCHI-STOCKCI	Storage and backup architecture	
ARCHI-PASS	Internet Gateway	4.3, [23]
EXP-PROT-INF	Protecting the confidentiality and integrity of sensitive information	5.2
EXP-TRAC	Traceability of interventions on the system	
EXP-CONFIG	Configuring IT resources	5.3
EXP-DOC-CONFIG	Documenting configurations	
EXP-ID-AUTH	Identification, authentication and logical access control	5.5

Continued on next page...

Ref.	Description of the security measure	Ref. in this guide (or other ANSSI reference)
EXP-DROITS	Access rights to resources	5.5
EXP-PROFILS	Managing application access profiles	5.5
EXP-PROC-AUTH	User access permissions	5.5
EXP-REVUE-AUTH	Reviewing access permissions	5.5
EXP-CONF-AUTH	Confidentiality of authentication information	5.5
EXP-GEST-PASS	Managing passwords	5.5
EXP-INIT-PASS	Setting up passwords	5.5
EXP-POL-PASS	Password policies	5.5
EXP-CERTIFS	Utilisation de certificats électroniques	[27]
EXP-QUAL-PASS	Systematically controlling password quality	5.5
EXP-SEQ-ADMIN	Escrow of administrators' credentials	7, [25]
EXP-POL-ADMIN	Administrator password policy	7, [25]
EXP-DEP-ADMIN	Managing the departure of an IS administrator	7, [25]
EXP-RESTR-DROITS	Restricting rights	6.1
EXP-PROT-ADMIN	Protecting access to administrative tools	7, [25]
EXP-HABILIT-ADMIN	Authorising administrators	7, [25]
EXP-GEST-ADMIN	Managing administrative actions	7, [25]
EXP-SEC-FLUXADMIN	Securing administration flows	7, [25]
EXP-CENTRAL	Centralising the management of the information system	7.4
EXP-SECX-DIST	Securing remote control tools	[19]
EXP-DOM-POL	Defining a domain account management policy	
EXP-DOM-PASS	Configuring domain password policy	
EXP-DOM-NOMENCLAT	Defining and applying a nomenclature for domain accounts	[25]
EXP-DOM-RESTADMIN	Restricting membership of domain administration groups to a minimum	
EXP-DOM-SERV	Controlling the use of service accounts	
EXP-DOM-LIMITSERV	Limiting the rights of service accounts	
EXP-DOM-OBSOLET	Disabling obsolete domain accounts	
EXP-DOM-ADMINLOC	Improving the management of local administrator accounts	6.1, [25]
EXP-MAINT-EXT	External maintenance	5.4
EXP-MIS-REB	Disposal	5.4
EXP-PROT-MALV	Protection against malware	5.6
EXP-GES-ANTIVIR	Managing antivirus security events	5.6, 7.5
EXP-MAJ-ANTIVIR	Updating the signature database	5.6, 7.4
EXP-NAVIG	Configuring the Internet browser	5.3
EXP-POL-COR	Defining and implementing a policy for monitoring and applying security patches	7.4
EXP-COR-SEC	Deploying security patches	7.4
EXP-OBSOLET	Handling the migration of obsolete systems	7.4
EXP-ISOL	Isolating remaining obsolete systems	7.4
EXP-JOUR-SUR	"Logging" of alerts	7.5
EXP-POL-JOUR	Defining and implementing a trace log management and analysis policy	7.5
EXP-CONS-JOUR	Storing logs	7.5
EXP-GES-DYN	Dynamic security management	7.5
EXP-MAIT-MAT	Controlling materials	6
EXP-PROT-VOL	Reminder of protection measures against theft	6, 5.7
EXP-DECLAR-VOL	Reporting losses and thefts	5.7
EXP-REAFFECT	Reallocating computer equipment	5.7
EXP-NOMAD-SENS	Declaring mobile equipment with the ability to handle sensitive information	6.4
EXP-ACC-DIST	Remote access to the organisation's information system	6.4
EXP-IMP-SENS	Printing sensitive information	
EXP-IMP-2	Security of multi-function printers and copiers	4.1
EXP-CI-OS	Operating systems	5.3, 7.4, [2], [7]
EXP-CI-LTP	Software in presentation tier	
EXP-CI-LTA	Software in application tier	
EXP-CI-LTD	Software in data tier	
EXP-CI-PROTFIC	File exchange gateway	4.4
EXP-CI-MESSTECH	Technical messaging	[25]
EXP-CI-FILT	Filtering application flows	5.3
EXP-CI-ADMIN	Administration flows	
EXP-CI-DNS	Domain name service - Technical DNS	
EXP-CI-EFFAC	Deleting media	5.4, 6.1
EXP-CI-DESTR	Destroying media	5.7
EXP-CI-TRAC	Traceability and attributability	7.5
EXP-CI-SUPERVIS	Monitoring	7.5
EXP-CI-AMOV	Accessing removable devices	5.7

Continued on next page...

Ref.	Description of the security measure	Ref. in this guide (or other ANSSI reference)
EXP-CI-ACCRES	Accessing networks	6.2
EXP-CI-AUDIT	Audit and control	2.4
PDT-GEST	Providing and managing workstations	6
PDT-CONFIG	Formalising workstation configurations	6
PDT-VEROUIL-FIX	Locking the central unit of fixed workstations	6
PDT-VEROUIL-PORT	Locking of mobile devices	6.4
PDT-REAFFECT	Reassigning workstations	6.1
PDT-PRIVIL	User privileges on workstations	6
PDT-PRIV	Using administrator access privileges	7, [25]
PDT-ADM-LOCAL	Managing the local administrator account	7, [25]
PDT-STOCK	Storing information	6.4
PDT-SAUV-LOC	Backing up and synchronising local data	6
PDT-PART-FIC	File sharing	6
PDT-SUPPR-PART	Deleting data on shared workstations	6
PDT-CHIFF-SENS	Encrypting sensitive data	5.2, 6.4
PDT-AMOV	Supplying removable storage media	5.7
PDT-NOMAD-ACCESS	Remote access to the entity's IS	6.4
PDT-NOMAD-PAREFEU	Local firewall	6.4, 5.3
PDT-NOMAD-STOCK	Local storage of information on mobile workstations	5.2, 6.4
PDT-NOMAD-FILT	Privacy filter	6.4
PDT-NOMAD-CONNEX	Configuring wireless connection interfaces	6.5
PDT-NOMAD-DESACTIV	Disabling wireless connection interfaces	6.5
PDT-MUL-DURCISS	Hardening of printers and multi-function copiers	
PDT-MUL-SECNUM	Securing the scanning function	
PDT-TEL-MINIM	Securing the configuration of PBXs	
PDT-TEL-CODES	Telephone access codes	
PDT-TEL-DECT	Limiting the use of DECT	
PDT-CONF-VERIF	Using automatic compliance checking tools	7.4
DEV-INTEGR-SECLOC	Integrating security into local developments	
DEV-SOUS-TRAIT	Including ISS clauses in IT development subcontracts	[10]
DEV-FUITES	Limiting information leakage	
DEV-LOG-ADHER	Reducing applications' reliance on specific products or technologies	
DEV-LOG-CRIT	Establishing secure development criteria	
DEV-LOG-CYCLE	Integrating security into the software life cycle	
DEV-LOG-WEB	Improving security awareness in web development	
DEV-LOG-PASS	Securely calculating password fingerprints	
DEV-FILT-APPL	Implementing application filtering capabilities for high-risk applications	
TI-OPS-SSI	Operational chains of the ISS	7.5
TI-MOB	Mobilisation in the event of an alert	7.5
TI-QUAL-TRAIT	Qualifying and handling incidents	7.5
TI-INC-REM	Reporting incidents	7.5
PCA-MINIS	Defining the IS business continuity plan	
PCA-LOCAL	Defining the local business continuity plan for information systems	
PCA-SUIVILOCAL	Monitoring the implementation of the local IS business continuity plan	
PCA-PROC	Implementing technical devices and operational procedures	7.4
PCA-SAUVE	Protecting backup availability	
PCA-PROT	Protecting backup confidentiality	
PCA-EXERC	Regularly exercising the local business continuity plan for information systems	
PCA-MISAJOUR	Updating the local business continuity plan for information systems	
CONTR-SSI	Local controls	

Recommendation List

Bibliography

[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] *Inter-ministerial directive 901*.
Regulation 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.

[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] *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte*.
Guide ANSSI-PG-075 v1.1, ANSSI, décembre 2020.
https://www.ssi.gouv.fr/archi-sensible-DR.

[32] *Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte*.
Guide ANSSI-PG-075 v1.1, ANSSI, décembre 2020.
https://www.ssi.gouv.fr/archi-sensible-DR.

[33] *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.

[34] *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-EN

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN