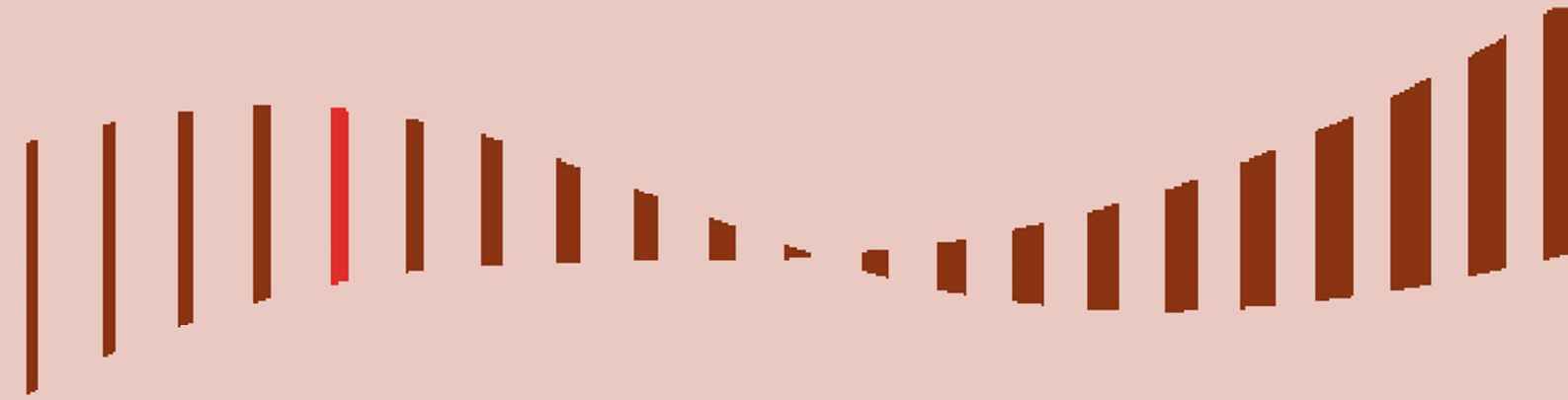
Guide gestion des habilitations d'accès au SI

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) - Janvier 2017 - V1.0



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

asipsanté
L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Sommaire

1 Introduction

1.1 Objet du document

La gestion des habilitations a pour finalités de protéger l'accès aux ressources du système d'information (SI) et de permettre de retrouver a posteriori qui était habilité à quoi.

Ce guide présente les concepts, principes et modalités de gestion des habilitations qui conditionnent les accès au SI afin de répondre aux exigences de maîtrise des accès aux informations et aux traitements fixées par la Politique de Sécurité du Système d'Information (PSSI) de la structure.

Ce document fait partie des guides pratiques spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

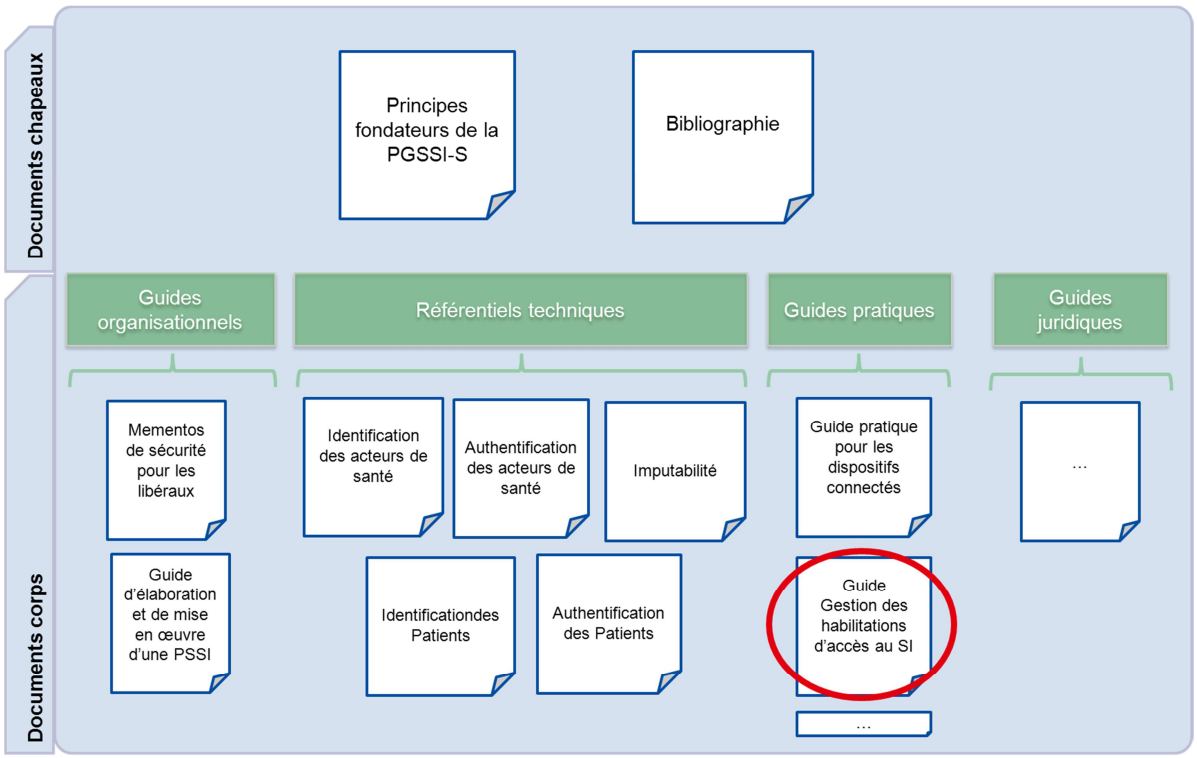


Figure 1 : Organisation du Corpus documentaire de la PGSSI-S

Ce document s'adresse :

- aux responsables de structure utilisatrice de SI ;
- aux responsables de traitements informatiques assurés par le SI ;
- aux personnes agissant sous leur responsabilité, et en particulier celles impliquées dans :
  - la définition de la politique de sécurité des SI et sa mise en œuvre au sein de la structure,
  - la définition des politiques d'habilitation et de contrôle d'accès au SI,
  - la définition des exigences et des mécanismes de sécurité dans les cahiers des charges de produits à acquérir ou de développements à réaliser par la structure,
  - la mise en œuvre et le suivi opérationnel des contrôles d'accès au SI ;

- aux fournisseurs de produits ou de services utilisés dans le cadre de systèmes d'information de santé. En effet, il est recommandé que les solutions proposées par ces fournisseurs soient cohérentes avec les principes exposés dans le présent guide.

1.2 Champ d'application du guide

Dans le cadre de ce guide, tous les contextes de systèmes d'information de santé (SIS) au sens des « Principes fondateurs de la PGSSI-S » sont concernés quelles que soient les finalités du SIS (production de soin, recherche …), le mode d'exercice (professionnel de santé en exercice libéral, établissement de santé…) et les étapes du cycle de vie de la donnée (conservation, échange/partage, …).

Le cartouche ci-après présente de manière synthétique le champ d'application du document.

Santé						**Médico Social**
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Applicabilité du guide aux différentes composantes techniques du SI

Le guide s'applique à la gestion des habilitations pour l'accès aux informations et fonctions informatiques ainsi que pour l'accès physique aux locaux et aux équipements.

Applicabilité du guide à différents types d'acteurs

Le guide s'applique à la gestion des habilitations pour les accès réalisées aussi bien par des personnes physiques que par des composants de SI (logiciels, dispositifs biomédicaux connectés…) agissant pour le compte de personnes physiques ou morales.

1.3 Définitions

Les encadrés illustrés par le pictogramme  *proposent des informations complémentaires sur le sujet traité. Ceux illustrés par le pictogramme* ☞ *constituent des notes ou remarques.*

Les documents sur lesquels se base ce guide ou qui sont cités en référence sont listés en Annexe 7 « Documents de référence ».

Les définitions ci-dessous sont données dans le contexte de la Politique Générale de Sécurité des Systèmes d'Information de Santé *(Référentiels et guides pratique du corpus documentaire PGSSI-S [Réf. n°1])*.

Ces différents termes sont utilisés dans la suite du document.

Système d'information (SI)

Au-delà des systèmes informatiques, le terme « Systèmes d'Information » correspond à l'ensemble des ressources (les hommes, le matériel, les logiciels) organisées pour collecter, stocker, traiter et communiquer de l'information au sein même d'une organisation et dans ses relations avec l'extérieur.

(Source : PSSI-MCAS - Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales [Réf. n°6])

Ressources du SI

Le terme « ressource du SI » utilisé dans ce guide se limite aux aspects non humains du SI par rapport à la définition de ressource incluse dans la définition du SI ci-dessus.

Ainsi, dans ce guide, les ressources du SI peuvent être, par exemple :

- les moyens techniques d'infrastructure nécessaires à la mise en œuvre et au fonctionnement du SI : *locaux, alimentation électrique, câblage réseau, climatisation,…*
- les moyens de télécommunication : *liaisons de télécommunication, centraux téléphoniques, téléphones, antennes…*
- les moyens informatiques matériels : *serveurs, postes de travail, équipements réseau, équipements de sécurité, lecteurs de badge…*
- les équipements métiers connectés au SI : *équipements biomédicaux…*
- les moyens informatiques logiciels : *systèmes d'exploitation, applications métier, applications d'administrations et de gestion de la sécurité du SI…*
- les informations traitées par le SI.

Identification et identifiant

L'identification a pour but de déterminer l'identité d'un acteur (personne physique, composant technique agissant pour le compte d'une personne morale…) via un identifiant qui lui a été attribué préalablement lors de la vérification et de l'enregistrement de ses traits d'identité.

Un identifiant est un attribut donné à un acteur, en lien avec son identité, permettant de différencier deux acteurs même dans le cas où leurs traits d'identité sont similaires ou très proches.

(Source : Référentiel d'identification des acteurs sanitaires et médico-sociaux [Réf. n°1.1])

Par exemple :

- *identifiant constitué de lettres du prénom et du nom de l'utilisateur et complété par un numéro pour distinguer les homonymes « jfdupont02 » pour un usage interne à la structure (identifiant de portée locale ou « identifiant privé ») ;*
- *identifiant numérique attribué lors de l'enregistrement d'un médecin dans référentiel d'identité national (répertoire partagé des professionnels de santé RPPS), et stocké dans sa carte de professionnel de santé (CPS) (identifiant de portée nationale ou « identifiant public ») ;*
- *identifiant, constitué d'une chaine unique de caractères, enregistré dans le certificat électronique présenté par un serveur web lors de l'établissement de la connexion sécurisée (« https »).*

Authentification

L'authentification a pour but de vérifier l'identité dont se réclame une personne ou une machine. (S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification).

(Source : RGS - Référentiel Général de Sécurité [Réf. n°2] §3.2.a.1)

Par exemple :

- authentification de l'utilisateur à l'aide d'un mot de passe connu de lui seul ;
- authentification de l'utilisateur à l'aide de sa carte CPx[1] et du code PIN associé connu de lui seul, permettant une authentification réalisée au niveau technique à l'aide de secrets cryptographiques et d'un certificat électronique stockés dans la carte.

Le cas échéant, il peut être prévu que l'authentification (et l'identification préalable) de tout ou partie des acteurs soit réalisée par une personne morale externe à la structure. Il s'agit du cas de l'authentification indirecte et de l'authentification par délégation, décrites au chapitre 4.7 du *Référentiel d'authentification des acteurs de santé [Réf. n°1.2]*.

Habilitation

Dans le cadre de la PGSSI-S, l'habilitation est la décision fonctionnelle explicite, délivrée sous l'autorité du responsable du traitement informatique concerné, de permettre à un acteur (personne physique, composant technique agissant pour le compte d'une personne morale…), qu'il soit interne ou externe, d'accéder à certaines informations ou fonctions de ce SI qui sont nécessaires à la réalisation des activités dont il a la charge.

(Définition établie dans le cadre de la PGSSI-S sur la base des définitions données par l'Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD [Réf. n°4] et la RFC 4949 [Réf. n°3] « authorization »).

La gestion des habilitations recouvre les processus qui permettent :

- de définir le périmètre couvert par les différentes habilitations possibles et d'organiser ces habilitations ;
- de gérer le cycle de vie complet (attribution, évolution et retrait) des habilitations aux acteurs qui le nécessitent, selon des conditions fixées. Une habilitation peut être :

[1] CPx : Terme générique désignant une carte appartenant à la famille des cartes à puce qui portent des certificats issus de l'IGC CPS ou de l'IGC Santé c'est-à-dire les cartes CPS, CPE, CPA, CDE et CDA (http://esante.gouv.fr/services/espace-cps/les-cartes-de-la-famille-cps).

- soit délivrée à un acteur explicitement identifié : cas d'une habilitation attribuée nominativement à une personne. Ce mode d'attribution est appelé « attribution discrétionnaire » dans la suite du guide (voir 2.1.2.1) ;

  Par exemple, dans une structure, quatre personnes nominativement désignées sont habilitées par le responsable du SI à réaliser les sauvegardes informatiques : deux titulaires et deux suppléants.

- soit établie de manière générique, sous forme de règles indiquant les conditions requises pour les acteurs et les permissions d'accès aux informations ou fonctions du SI associées. Le mode d'attribution « par profil utilisateur » détaillé au 2.1.2.2 entre dans ce cadre.

  Par exemple, dans un établissement de santé, les médecins sont habilités par le responsable du traitement, qui applique la loi en vigueur, à consulter et à mettre à jour le dossier médical informatisé des patients qu'ils prennent en charge.

Voir chapitre 2.1 pour plus de détail sur la manière de gérer les habilitations.

Imputabilité et traces

La norme ISO/CEI 27000:2014, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire *[Réf. n°8],* définit l'imputabilité comme la « responsabilité d'une entité par rapport à ses actions et ses décisions ».

Au sein d'un système d'information, l'imputabilité vise :

- à attribuer à chaque utilisateur ou à chaque machine l'intégralité des actions qu'il a effectuées sur le système d'information ;
- à s'assurer que chaque action est attribuée de façon univoque à l'utilisateur ou la machine l'ayant effectuée.

Dans le cadre des systèmes d'information, une trace correspond à un ensemble de données générées pour refléter une action sur le système ainsi que son contexte d'occurrence (ex. : type d'action, auteur de l'action, date et heure de l'action, données concernées...). Les traces contribuent à gérer l'imputabilité dans un SI en permettant la conservation du lien entre les actions réalisées sur le système d'information et leurs auteurs.

(Source : Référentiel d'imputabilité [Réf. n°1.3])

La gestion des habilitations a pour finalité de limiter les actions des acteurs du SI à ce qui est souhaité par les responsables des traitements, alors que l'imputabilité des actions dans le SI a pour finalité de permettre de vérifier a posteriori que les habilitations sont respectées, et notamment qu'elles sont correctement mises en application par les moyens assurant le contrôle d'accès aux données et fonctions.

Pour que les traces soient effectivement exploitées, il est nécessaire que des outils d'utilisation aisée soient disponibles, comme le requiert le *Référentiel d'imputabilité* dès le palier 1 d'imputabilité *[Réf. n°1.3, chap. 7.1.2.2] :*

« Les traces sont restituées à des non spécialistes de la sécurité au sein d'un outil de gestion de la preuve ergonomique et qui ne nécessite pas une formation importante des utilisateurs pour son usage. »

Autorisation d'accès ou droit d'accès

Dans le cadre de la PGSSI-S, l'autorisation d'accès ou droit d'accès est la permission, positionnée au niveau des composants techniques du SI, donnée à un acteur (personne physique, composant technique) authentifié vis-à-vis du SI, d'accéder à une ressource (information ou fonction) du SI. Les droits d'accès sont la traduction technique de l'habilitation dans le SI.

(Définition établie dans le cadre de la PGSSI-S sur la base des définitions données par la PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat [Réf. n°5] et la RFC 4949 [Réf. n°3] « permission »).

Pour le second exemple cité ci-dessus pour « Habilitation », les autorisations d'accès des médecins sont positionnées dans l'application de gestion des dossiers patient informatisés.

Un autre exemple est celui des droits de lecture et/ou d'écriture de fichier dont dispose chaque utilisateur du SI bureautique en fonction des répertoires où se situe le fichier concerné.

Pour les SI complexes ou hétérogènes au niveau technique, certains outils de gestion des habilitations permettent également de transposer ces habilitations en droits d'accès de manière automatisée sur différents composants du SI. Ce type d'outil est très utile sur la durée, mais requiert un important travail initial de modélisation du SI et de paramétrage de l'outil comme des différents composants du SI pris en compte.

Contrôle d'accès

Dans le cadre de la PGSSI-S, le contrôle d'accès est la vérification, au moment où un acteur demande à accéder à une ressource du SI, que cet acteur dispose bien de l'autorisation d'accès requise pour la ressource demandée.

(Définition établie dans le cadre de la PGSSI-S sur la base des définitions données par la PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat [Réf. n°5] et la RFC 4949 [Réf. n°3] « access control »).

Par exemple, quand un utilisateur ou un programme informatique tente de mettre à jour un fichier bureautique, cette action est soumise à un contrôle d'accès au cours duquel le système de fichiers vérifie que les droits d'accès associés à l'identifiant de l'acteur l'autorisent bien à modifier le fichier concerné.

Bien que sortant du strict cadre du présent guide, un rappel sur le déroulement technique générique d'un accès au SI est proposé en Annexe 3.

1.4 Enjeux relatifs à la gestion des habilitations

1.4.1 Obligations et contraintes

De manière générale, les structures des secteurs sanitaire et médico-social sont soumises à des obligations légales et règlementaires de contrôles d'accès aux données, comme par exemple pour :

- les données de santé à caractère personnel ;
- les autres données à caractère personnel.

En outre, d'autres contraintes ou bonnes pratiques imposent à la structure d'assurer la gestion des accès aux ressources fournies ou requises par le SI, comme par exemple :

- l'accès aux fonctions d'installation ou de mise à jour de logiciels sur les équipements informatiques ou informatisés, quels qu'ils soient (postes de travail, équipements biomédicaux, imprimantes, serveurs informatiques, équipements réseau…)
- l'accès aux fonctions d'administration et de paramétrage de ces mêmes équipements, dont le paramétrage des équipements biomédicaux ;
- l'accès aux diverses fonctionnalités utilisateurs offertes par les applications métier du SI ;
- l'accès aux locaux informatiques aux seules personnes en charge de l'installation et de la maintenance du matériel informatique.

La gestion de ces différents types d'accès s'appuie sur la traduction, au niveau des ressources techniques du SI, des habilitations délivrées par les responsables des traitements informatiques concernés.

1.4.2 Vulnérabilités potentielles du SI liées à la gestion des habilitations

Diverses défaillances dans la gestion des habilitations peuvent conduire la sécurité du SI à ne plus être conforme aux objectifs fixés par la structure, comme dans les exemples suivants :

- habilitation attribuée à la mauvaise personne, suite à une mauvaise identification des acteurs (erreur de traitement dans le processus de gestion des identités ou dans celui de gestion des habilitations) ;
- habilitation attribuée à une personne sur la base d'une qualité fausse et non vérifiée (erreur ou fraude) *(exemple : attribution d'habilitation à une personne par le gestionnaire des habilitations sur la base de fausses qualifications revendiquées par cette personne et qui n'ont pas été correctement vérifiées par le service du personnel lors de son embauche)* ;
- maintien d'habilitation précédemment attribuée à un acteur alors que celui-ci n'assure plus la fonction qui justifie cette habilitation (suite à un changement de poste, voire à un départ), cette défaillance pouvant également conduire à une accumulation dans le temps d'habilitations indues, voire incompatibles (voir dernier point ci-dessous) ;
- méconnaissance, par le responsable de traitement, du périmètre effectif des habilitations qu'il approuve, pouvant conduire à des attributions d'habilitation dépassant ce que le responsable souhaite, notamment dans le cas d'utilisation de profils d'habilitation (voir au 2.1.1.2) ;
- attribution à un même acteur, généralement par des personnes différentes et à des moments différents, d'habilitations identifiées comme incompatibles et interdites par les règles métier *(exemples : habilitation, dans des applications métier ou support, à des fonctions de validation d'opérations sensibles, en même temps que l'habilitation à réaliser ces mêmes opérations ; habilitation à ordonner des paiements en même temps que celle de valider ces mêmes paiements)*.

1.4.3 Impacts d'une défaillance dans la gestion des habilitations

Les vulnérabilités liées à la gestion des habilitations peuvent conduire à des incidents de sécurité aux conséquences parfois graves, comme par exemple :

- Modification ou suppression, par une personne qui ne devrait pas y être autorisée, de données traitées ou stockées par le SI ou déclenchement de processus qui modifient ou suppriment ces données : enjeu d'intégrité et de disponibilité des données pouvant induire des risques pour la santé de patients ;
- Déclenchement de processus contrôlés par le SI par une personne qui ne devrait pas y être autorisée (*ex : radiologie, traitement, acquittement indu d'une alarme…*) pouvant induire des risques pour la santé de patients ou du personnel ;
- Consultation de données traitées ou stockées par le SI ou déclenchement de processus qui permet cette consultation (*impression, transfert de données sur support amovible…*) par une personne qui ne devrait pas y être autorisée : enjeu de confidentialité des données ;
- Déclenchement de processus de contrôle du SI par une personne qui ne devrait pas y être autorisée : installation de logiciels malveillants ou non, arrêt de composants du SI : enjeux de disponibilité et d'intégrité du SI.

La gestion des habilitations est l'un des éléments indispensables de la chaîne qui protège le SI contre les dysfonctionnements d'origine humaine, les utilisations illégitimes, les détournements d'usages, la corruption et la perte de donnée. Il apparaît clairement qu'une défaillance dans la gestion des habilitations peut avoir des conséquences graves.

1.4.4 Objectifs pour une gestion maîtrisée des habilitations

Pour que le contrôle d'accès aux ressources du SI soit effectif, les processus de gestion des habilitations doivent :

- appliquer le principe du moindre privilège, c'est-à-dire attribuer à chaque acteur du SI (utilisateur ou composant technique du SI) les habilitations nécessaires à la réalisation des tâches qui lui sont confiées et uniquement celles-ci ;
- intégrer des étapes permettant de vérifier l'attribution des bonnes habilitations au bon acteur et de détecter les anomalies ;
- prendre en compte les arrivées, départs et changements de fonction des personnels et intervenants, permanents ou temporaires, amenés à accéder au SI ou à certains de ses composants ;
- être gérés et pilotés de manière consolidée, notamment quand des moyens de gestion des habilitations différents sont utilisés pour les habilitations à différentes ressources du SI, voire de la structure en général *(par exemple pour les accès physiques aux locaux, au SI, aux systèmes d'infrastructure divers)* ;
- mettre à la disposition des responsables de traitement les moyens de vérifier à tout moment qui possède quelles habilitations pour les traitements et données dont ils ont la charge.

2 Principes

2.1 Les différentes manières de gérer les habilitations

La détermination des habilitations peut être faite de différentes façons, mais dans tous les cas :

- le principe du moindre privilège doit être appliqué : il faut donner à chaque acteur du SI (utilisateur ou composant technique du SI) les habilitations nécessaires à la réalisation des tâches qui lui sont confiées et uniquement celles-ci ;
- l'attribution des habilitations doit toujours être réalisée sous la responsabilité des responsables de traitement qui sont garants des habilitations pour leurs traitements. Les tâches de définition des règles d'attribution des habilitations et d'attribution des habilitations en elles-mêmes peuvent bien sûr être confiées à d'autres personnes par les responsables, par exemple afin de centraliser la gestion des habilitations

2.1.1 Organisation des habilitations

La gestion des différentes habilitations possibles peut être organisée :

- soit par une définition unitaire des habilitations
- soit par une définition de profils d'habilitations

Ces deux modes d'organisation, détaillés ci-dessous, peuvent être utilisés conjointement dans une même structure si nécessaire.

2.1.1.1 Habilitations unitaires

Dans ce mode d'organisation des habilitations, chaque habilitation possible est définie et attribuée (ou non) de façon unitaire aux acteurs du SI (cette attribution étant réalisée selon les principes d'attribution exposés au 2.1.2)

> *Par exemple, dans le cadre de la dispensation des médicaments dans un ES, on pourrait avoir les habilitations unitaires suivantes :*
>
> - *(A) Consultation de la prescription établie par un médecin, qui intègre également les données concernant les allergies et autres contre-indications à prendre en compte pour le patient ;*
> - *(B) Mise à jour de l'état journalier de préparation du traitement ;*
> - *(C) Mise à jour de l'état journalier de distribution du traitement au patient ;*
> - *(D) Consultation du dossier médical du patient.*
>
> *Les préparateurs en pharmacie pourraient se voir attribuer les habilitations unitaires (A) et (B), le personnel infirmier les habilitations unitaires (A) et (C), et un médecin qui a en charge le patient les habilitations unitaires (A), (C) et (D).*

Ce mode d'organisation est essentiellement adapté quand le nombre de fonctions ou de périmètres de données (et donc d'habilitations associées) est faible.

2.1.1.2 Profil d'habilitation

Dans ce mode d'organisation, les habilitations unitaires sont regroupées en différents profils.

Un profil d'habilitation est un ensemble d'habilitation unitaires regroupées afin d'en simplifier la gestion et l'attribution. On peut noter que :

- un profil d'habilitation peut ne couvrir qu'une partie seulement des habilitations nécessaires dans le cadre d'une activité métier ou d'un poste donné, et c'est d'ailleurs souvent le cas en pratique ;

  Par exemple, dans le cadre des processus d'achats, un profil d'habilitation « demandeur d'achat » peut être défini, et un autre « suivi des achats ». Un chef de service peut se voir

attribuer les profils « demandeur d'achat » et « suivi des achats » en plus des autres profils d'habilitations spécifiques à l'activité de son service. Le même profil « suivi des achats » peut être attribué dans le même temps à un contrôleur de gestion.

- une même habilitation unitaire peut faire partie de plusieurs profils différents.

  Par exemple, si, à partir de l'exemple proposé ci-dessus au 2.1.1.1 on définit le profil d'habilitation « Préparateur en pharmacie » qui comporte les habilitations unitaires (A) et (B) et le profil d'habilitation « Infirmier » qui comporte les habilitations unitaires (A) et (C), on peut constater que la même habilitation unitaire (A) se retrouve dans les deux profils ;

- il peut arriver que des profils d'habilitation soient prévus pour être potentiellement utilisés par un même utilisateur mais à des moments différents et non pas simultanément. Les éventuelles incompatibilités entre ces profils d'habilitation doivent être identifiées, et l'activation de ces profils doit généralement faire l'objet de traçabilité.

Ce mode d'organisation est adapté aux SI complexes et aux structures dans lequel les activités et périmètres d'activité des différents acteurs utilisateurs du SI sont variés.

2.1.1.3 Combinaison des habilitations unitaires et des profils habilitations

Il arrive que des habilitations doivent être gérées par un profil d'habilitation combiné à une ou plusieurs habilitations unitaires, notamment quand ces dernières permettent de définir les périmètres auxquels le profil peut s'appliquer.

Par exemple, le profil d'habilitation « consultation des données de santé patient » peut être attribué au personnel de santé, mais doit être combiné à chaque fois avec une habilitation unitaire aux données de santé de chaque patient, délivrée à l'issue de la procédure prévue par la structure au regard du cadre légal et réglementaire.

La combinaison d'habilitation unitaire et de profils d'habilitation est aussi parfois mise en œuvre pour que l'habilitation à utiliser une application (*i.e. permettant à l'utilisateur de lancer l'application ou de s'y connecter*) soit discrétionnaire mais que les différentes fonctions accessibles dans le cadre de cette application puissent être gérées plus finement par profil utilisateur.

Par exemple, s'il ne doit y avoir qu'une assistante par service qui dispose de l'habilitation d'accéder à la gestion des approvisionnements, cette habilitation peut être attribuée de façon discrétionnaire. Néanmoins, toutes les assistantes de tous les services se voient attribuer, via leur profil utilisateur, un profil d'habilitation d'assistante dans l'application de gestion des approvisionnements.

Dans les deux cas présentés ci-dessus, la combinaison de différentes habilitations, ici une habilitation unitaire et une habilitation par profil, est nécessaire pour que l'accès à la ressource soit autorisé.

De manière générale, différentes habilitations peuvent correspondre à différents périmètres d'accès successifs, selon le principe illustré par le schéma ci-dessous : *accès global au SI (droit d'ouverture de session sur poste de travail, de connexion au réseau local…), lancement d'une application en particulier, utilisation de fonctions spécifiques ou d'accès à certaines données seulement dans cette application…*

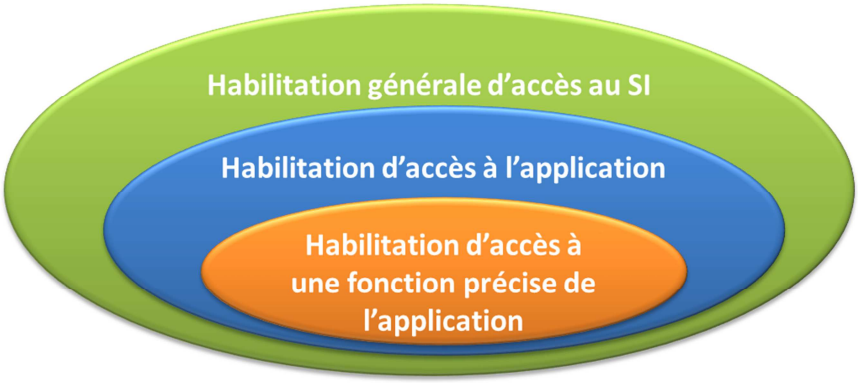


Figure 2 : Tableau récapitulatif des recommandations en fonction du contexte

2.1.2 Attribution des habilitations

Plusieurs modes d'attributions des habilitations sont possibles, que celles-ci soient organisées en habilitations unitaires ou en profils d'habilitations. On peut notamment distinguer :

- l'attribution discrétionnaire ;
- l'attribution par profil utilisateur.

2.1.2.1 Attribution discrétionnaire

Dans ce mode d'attribution, la personne en charge des habilitations les attribue nominativement en fonction des tâches confiées à chaque acteur.

Ce mode d'attribution nécessite que chaque acteur soit identifié, et que ses activités et périmètres d'activité soient établis de manière exhaustive : un enregistrement préalable de l'acteur est nécessaire et les informations requises doivent être disponibles pour la personne en charge des habilitations.

Ce mode d'attribution est adapté pour un petit nombre d'acteurs ou pour une répartition des tâches dont le périmètre est susceptible de varier fréquemment dans le temps *(par exemple en fonction de la charge de travail à traiter, du personnel disponible avec la compétence requise à un instant donné…)*.

Un exemple d'attribution discrétionnaire d'habilitation pourrait concerner l'activité « machine à machine » de sauvegarde des données : attribution discrétionnaire d'un profil d'habilitation autorisant la lecture des données de l'ensemble des serveurs informatiques à l'acteur « application de sauvegarde centralisée du SI ».

2.1.2.2 Attribution par profil utilisateur

Dans ce mode d'attribution, la personne en charge des habilitations définit des profils utilisateurs basés sur les caractéristiques des acteurs (ex. : appartenance à un service, profession, type de poste, implantation géographique, positionnement hiérarchique).

Pour chaque profil utilisateur, elle définit les habilitations (habilitations unitaires ou profils d'habilitation) qui doivent être attribuées à tout acteur correspondant à ce profil.

2.1.2.2.1 Attribution préalable

En général, un utilisateur est enregistré et se voit attribuer un ou plusieurs profils utilisateur qui pointent chacun sur des habilitations (ou des profils d'habilitation).

2.1.2.2.2 Attribution à la connexion

De manière plus exceptionnelle, lorsque les utilisateurs ne sont pas connus à l'avance et lorsque les habilitations peuvent être automatisées en fonction de traits d'identité diffusés lors de l'authentification, il est possible d'attribuer un profil utilisateur sans enregistrement préalable, de manière dynamique au moment de la connexion de l'utilisateur.

Ce type d'attribution des habilitations est le seul possible en situation d'authentification publique, par exemple dans le cadre d'accès à un service en ligne sans enregistrement préalable ou pour lequel les utilisateurs ne sont pas connus avant leur première connexion.

2.1.2.3 Délégation d'habilitation

Dans certains cas, il peut être utile que certains utilisateurs puissent déléguer, temporairement et sous leur responsabilité, une partie de leurs habilitations à un autre utilisateur.

Ce principe peut permettre d'éviter certaines dérives qui doivent être strictement interdites comme le partage de compte, où un utilisateur confie à un autre ses moyens d'identification et d'authentification afin qu'il puisse accéder au SI à sa place.

Si le principe de délégation d'habilitation est mis en œuvre dans la structure, les règles associées à ce principe doivent être clairement fixées. La capacité à déléguer ses habilitations doit constituer elle-même une habilitation attribuée à l'utilisateur pour un périmètre d'habilitations « délégables » défini.

Il est alors souhaitable que la délégation effective d'habilitations puisse être réalisée par l'utilisateur lui-même à l'aide d'une application simple d'emploi.

2.1.2.4 Attribution dynamique d'habilitation

Dans les cas où la liste des personnes nécessitant une habilitation particulière ne peut être complétement déterminée par avance, la structure doit prévoir des moyens spécifiques de gestion des habilitations qui permettent à la fois la maîtrise de l'accès aux ressources du SI et la souplesse pour la réalisation de l'activité métier. *Par exemple, les personnes qui interviennent dans les soins à un patient ne sont pas toujours identifiées a priori, et les personnels de santé utilisateurs du SI qui ont légitiment besoin d'accéder aux données de santé du patient peuvent varier dans le temps.*

Le principe d'attribution « à la demande », ou « dynamique », d'habilitations répondant à un besoin particulier, dans des limites de bénéficiaires, de périmètre d'habilitations et de durée, fixées par le gestionnaire des habilitations, peut constituer une solution à ce type de situation.

Par exemple, une règle de gestion peut être que tout médecin dispose d'une habilitation d'accès en lecture et en mise à jour des dossiers de l'ensemble des patients de la structure, mais uniquement pour les patients pour lesquels il dispose également d'une habilitation d'accès unitaire spécifique (cas des patients admis dans son service). Les habilitations d'accès peuvent alors être attribuées par une personne en charge de cette tâche au sein de chaque service en situation normale, mais également par chaque médecin pour lui-même afin d'être en mesure, si besoin, d'accéder aux informations nécessaires au suivi ou aux soins du patient, notamment en situation d'urgence ou de garde. Cette habilitation ne peut avoir qu'une durée temporaire, dans l'attente d'une régularisation selon la procédure standard si elle doit perdurer. Ce mode d'attribution dynamique, et qui plus est « d'auto-attribution », doit bien entendu faire l'objet de traçabilité.

2.1.2.5 Comptes génériques

Dans les systèmes informatiques, le « compte utilisateur » constitue généralement le moyen d'associer à un acteur les droits d'accès qui découlent de ses habilitations.

Des bonnes pratiques relatives à l'attribution et à l'utilisation de ces comptes sont énoncées dans la thématique T5-2.1 du « *Canevas de PSSI* » proposé avec le « *Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée » [Réf. n°1.4]*.

Ces bonnes pratiques ne s'opposent pas à l'utilisation de comptes génériques si les règles générales de gestion des comptes sont respectées :

- à tout instant, le compte doit être affecté à un utilisateur au maximum. Les périodes pendant lesquelles il n'est affecté à aucun utilisateur doivent être tracées ;
- l'identité de l'utilisateur auquel le compte est attribué doit être connue à tout instant et doit être tracée ;
- les moyens d'authentification (*mot de passe, code pin de carte à puce voire carte à puce elle-même…*) nécessaires pour l'utilisation du compte doivent être personnalisés pour l'utilisateur en cours, et doivent être invalidés dès que le compte n'est plus affecté à l'utilisateur ;
- les autorisations associées au compte doivent être positionnées en accord avec les habilitations de l'utilisateur, et doivent être supprimées dès que le compte n'est plus affecté à l'utilisateur ;
- le compte doit être attribué pour répondre à une situation temporaire dans laquelle la création immédiate d'un compte nominatif n'est pas possible ou n'est pas pertinente : visiteurs, stagiaires…

Ce type d'usage est à distinguer de celui du partage d'un même compte par plusieurs utilisateurs, pratique qui doit être strictement interdite (*sauf cas très spécifiques et encadrés pour l'administration technique du SI, voir T5-2.4 du « Canevas de PSSI » [Réf. n°1.4].*).

2.1.3 Recommandations pour le choix de l'organisation des habilitations et de l'attribution des habilitations

Le choix de l'organisation des habilitations et de leur mode d'attribution doit se faire en fonction du contexte. En règle générale, on utilise :

- pour la gestion des habilitations :
  - un profil d'habilitation lorsqu'il y a un nombre important de ressources auxquelles il faut donner accès et que les accès peuvent être liés (ex. : accès au catalogue fournisseur et accès au module de commande de fourniture),
  - des habilitations unitaires lorsqu'il y a un petit nombre de ressources qui permet la gestion unitaire et/ou pour les ressources sensibles qui ne sont liées à aucune autre ressource ;
- pour l'attribution des habilitations :
  - une attribution discrétionnaire lorsqu'il y a un petit nombre d'utilisateurs ou pour des habilitations sur des ressources sensibles,
  - une attribution par profil utilisateur lorsqu'il y a un nombre important d'utilisateurs et/ou que l'organisation interne permet aisément de déterminer des rôles formalisés,
  - une attribution à la connexion si les éléments nécessaires à la détermination du profil utilisateur et des habilitations associées sont déductibles des informations d'identité validées lors de l'authentification.

D'une manière générale, la logique est de passer autant que possible par des profils (profils d'habilitation et profils utilisateur), l'utilisation de profils faisant le plus souvent gagner du temps tout en apportant une meilleure lisibilité des habilitations par rapport à une gestion discrétionnaire.

L'utilisation de profils utilisateurs est également recommandée afin de répondre à la nécessité d'assurer une permanence des fonctions au sein de la structure, pour que les personnes en charge du remplacement de titulaires principaux de fonctions puissent se voir attribuer de manière simple les habilitations nécessaires.

Il est rappelé que la notion d'équipe de soin doit être prise en compte dans la gestion des habilitations dans le respect de la loi et en fonction de l'organisation propre à la structure.

Cette prise en compte peut constituer l'une des clés de définition des règles d'organisation et d'attribution des habilitations pour les personnels de santé.

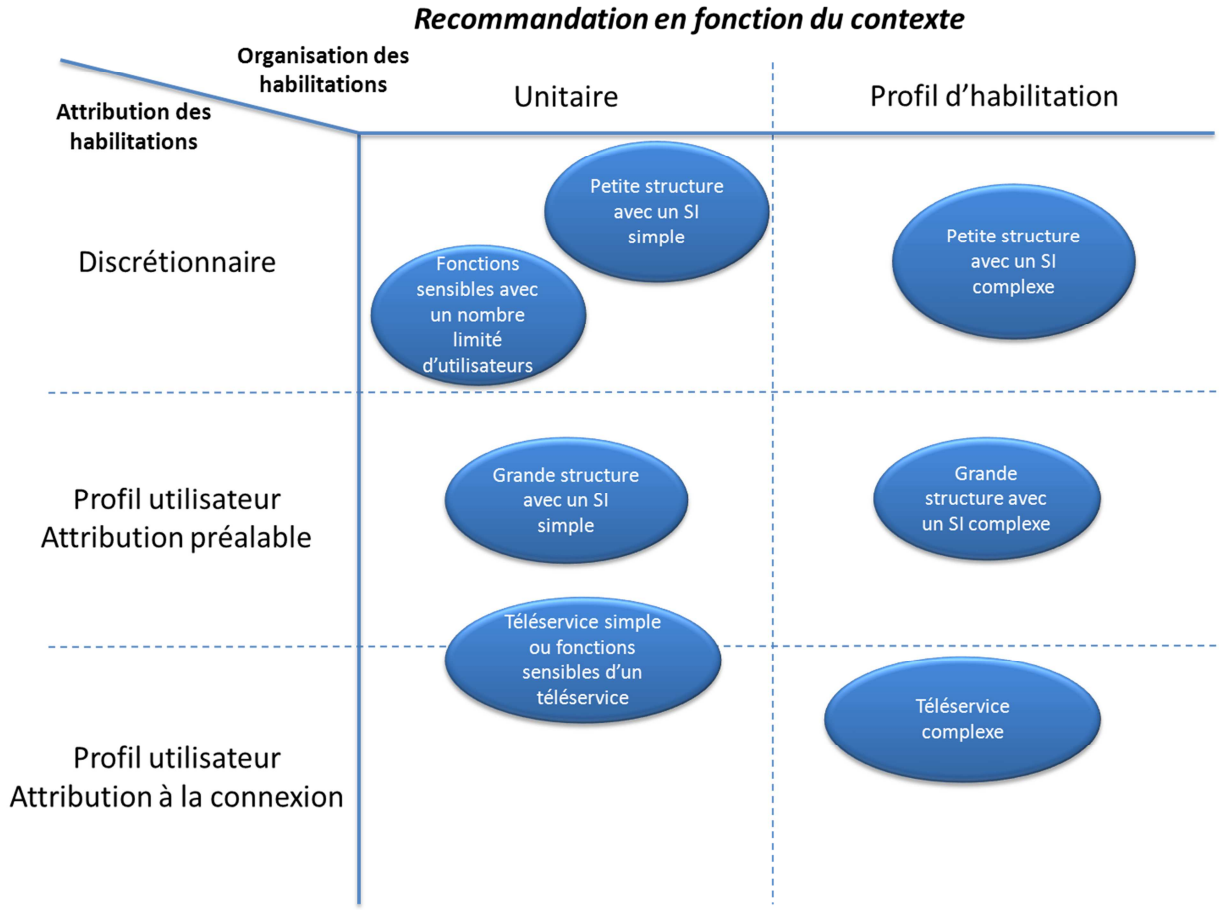


Figure 3 : Tableau récapitulatif des recommandations en fonction du contexte

La définition et l'attribution des habilitations peuvent également être exprimées sous forme de règles, plus souples mais aussi plus complexes car plus abstraites.

Par exemple, on pourrait exprimer l'habilitation donnée au personnel de santé de consulter les données de santé de patient par la règle : « pour tout utilisateur ayant le profil utilisateur <personnel de santé>, attribuer le profil d'habilitation **<***lecture des données de santé de patient> pour tout <patient> pour lequel l'utilisateur fait partie du personnel médical autorisé par <patient> ».*

Certains des modèles de gestion des habilitations présentées au chapitre suivant s'appuient sur ce type de représentation.

2.1.4 Modèles de gestion des habilitations

De nombreux modèles de gestion des habilitations sont décrits dans la littérature informatique. Ils diffèrent par les éléments qui sont utilisés pour organiser les habilitations et surtout pour les attribuer aux utilisateurs.

Dans la mesure où les logiciels de gestion des habilitations et des autorisations d'accès sont généralement basés sur l'un de ces modèles, les principaux d'entre eux sont présentés en

Annexe 4 pour aider le responsable à choisir les modèles les plus adaptés à son contexte d'usage.

En outre, il arrive que certains termes soient présentés à tort comme correspondant à des modèles particuliers de gestion des habilitations. Certains de ces termes sont présentés en Annexe 5.

2.2 Gestion des habilitations dans le temps

Afin d'éviter l'accumulation d'habilitations qui ne seraient pas strictement nécessaires aux utilisateurs, il est important que le principe de moindre privilège soit toujours respecté, tout en laissant le possibilité d'attribution d'accès exceptionnels et encadrés, pour une durée limitée.

Des revues régulières des habilitations doivent être menées afin de vérifier que les habilitations attribuées sont toujours justifiées, que les fins d'accès exceptionnels et les retraits d'habilitation liés aux départs ou aux changements de fonction du personnel ont bien été pris en compte, et d'activer le cas échéant les mesures correctives nécessaires.

3 Utilisation du guide

Le guide propose un ensemble de règles et de préconisations pour la définition des politiques et de procédures d'habilitations pour l'accès aux données, traitements informatiques et composants techniques du SI (également désignés sous le terme des « ressources du SI » par la suite).

Les responsables identifiés au chapitre 1.1 sont en charge :

- de mettre en œuvre les règles prescrites ou de les faire appliquer par leurs sous-traitants ;
- d'estimer et de traiter les risques induits par les règles non appliquées.

L'utilisation du guide s'effectue à partir de la liste des règles énoncées au chapitre 4, éclairées par l'exposé de différentes définitions, principes de base, recommandations et principaux modèles de gestion des habilitations aux chapitres 1.3 et 2.

En outre, deux modèles de fiches de définition des habilitations et autorisations sont proposés en Annexe 1 afin de faciliter la formalisation de la politique d'habilitation et des modalités de gestion des habilitations.

4 Règles de sécurité

4.1 Prérequis

N°	Règle
R01	Pour que les habilitations puissent être définies et traduites en autorisations d'accès pour chaque acteur (personne physique, composant technique agissant pour le compte d'une personne morale…) du SI, il faut au préalable que soient mises en œuvre dans le SI (ou dans le SI de tiers auxquels la structure fait confiance si ce sont ces tiers qui réalisent ces fonctions pour tout ou partie des utilisateurs) des fonctions : • d'enregistrement et d'identification des acteurs ; • d'authentification des acteurs. *Exemple : identification et authentification à l'aide d'une CPx[2], s'appuyant donc sur un référentiel d'identification national.* Ces fonctions doivent se conformer au *Référentiel d'identification des acteurs sanitaires et médico-sociaux [Réf. n°1.1]* et au *Référentiel d'authentification des acteurs de santé [Réf. n°1.2]* en appliquant les paliers définis par ces référentiels qui correspondent aux besoins de sécurité et au contexte du SI.
R02	Pour que les habilitations puissent être définies et traduites en autorisations d'accès aux différentes ressources du SI, il faut au préalable que ces ressources soient identifiées : un inventaire doit être établi pour les ressources (données, traitements informatiques ou applications, moyens support…) qui doivent faire l'objet d'un contrôle d'accès. ☞ Le « *Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée » [Réf. n°1.4] propose dans ses annexes un modèle d'inventaire qui peut être utilisé pour réaliser l'inventaire des ressources informatiques.*
R03	Le modèle retenu pour l'organisation et l'attribution des habilitations (voir 2.1.4) doit être déterminé et les principales orientations pour cette gestion doivent être explicitées. *Par exemple : application du modèle général de gestion par profils d'habilitation et profils utilisateurs, sur la base de profils utilisateurs correspondant aux fonctions mais également aux différents services de la structure, complétés par des habilitations (unitaires ou par profils d'habilitations) attribuées temporairement et tracées afin de répondre aux situations d'urgence où un personnel doit intervenir en dehors de son périmètre d'activité habituel.* Le modèle peut être défini de manière globale pour la structure, mais prévoir l'utilisation de modèles différents pour certains périmètres spécifiques du SI qui le requièrent.

[2] CPx : Terme générique désignant une carte appartenant à la famille des cartes à puce qui portent des certificats issus de l'IGC CPS ou de l'IGC Santé c'est-à-dire les cartes CPS, CPE, CPA, CDE et CDA (http://esante.gouv.fr/services/espace-cps/les-cartes-de-la-famille-cps).

4.2 Formalisation du processus de gestion et d'attribution des habilitations

N°	Règle
P01	La procédure de gestion des habilitations requises pour chaque ensemble cohérent de ressources doit être formalisée et appliquée lors de la mise en place initiale du système de gestion des habilitations ainsi qu'à chaque ajout ou retrait de ressources dans le SI.
P02	La procédure de gestion des habilitations requises doit permettre de définir, pour chaque ensemble cohérent de ressources : 1. le(s) responsable(s) de traitement auxquels sont rattachées ces ressources ; 2. les habilitations unitaires requises ; *Exemple pour des documents : création, consultation, impression, modification, sauvegarde, restauration…* *Exemple pour une base de données : création d'un nouvel enregistrement, consultation d'un ensemble défini de champs, modification d'un ensemble défini de champs, recherche multicritères, extraction en masse, sauvegarde, restauration…* 3. les profils d'habilitations pertinents (s'il y a lieu), qui regroupent les habilitations unitaires en fonction des pratiques souhaitées au sein de la structure ; *Exemple pour des documents : profil « lecteur » : consultation, profil « éditeur » : création + consultation + modification, profil « administrateur » sauvegarde + restauration…* 4. les habilitations (et profils d'habilitation) incompatibles entre elles, c'est-à-dire qui ne doivent jamais être détenues par un même acteur, qu'elles concernent cet ensemble de ressources uniquement ou qu'elles référencent des habilitations à des ressources définies par ailleurs. Il convient de noter que des habilitations incompatibles peuvent parfois porter sur des ressources différentes (*par exemple pour l'accès à une ressource logique d'une part, et pour l'accès à la ressource physique qui supporte cette ressource logique d'autre part*) ; 5. l'origine de l'identification utilisée, dont il convient de s'assurer que les informations collectées à l'enregistrement de l'utilisateur ou établies par la suite, couvrent tous les éléments nécessaire à la décision d'attribution des habilitations ; *Exemple pour des documents bureautique : l'annuaire système (Active Directory, autre LDAP…)* *Exemple pour un service en ligne : le certificat stocké dans la carte CPx de l'acteur de santé, utilisé pour l'identification et l'authentification de l'utilisateur.* 6. le périmètre des utilisateurs susceptibles de se voir attribuer des habilitations pour cet ensemble de ressources ; *Exemple : tout le personnel interne ou externe, le personnel médical uniquement, accès public…* 7. les profils utilisateurs (s'il y a lieu), qui doivent être établis dans le but de regrouper les différents utilisateurs de ces ressources en fonction des habilitations qui leur sont nécessaires et suffisantes, généralement en lien avec les activités métier ; 8. les spécificités des règles d'attribution des habilitations pour ces ressources, si elles dérogent aux règles et procédures générales (voir point suivant), avec le logigramme spécifique associé le cas échant ; *Exemple : délégation ou non de la gestion à une fonction mutualisée, voire*

externalisée, de gestionnaire des habilitations, nécessité de validation de l'attribution de certaines habilitations sensibles par le responsable du traitement lui-même,…

9. les habilitations à titre exceptionnel qu'il est prévu de pouvoir octroyer (s'il y a lieu), avec le contexte d'usage, les conditions, les limites, la durée et les contrôles à postériori qui doivent alors être appliqués.

   Exemple : accès de type « bris de glace » qui sont des accès permettant d'attribuer à la connexion des droits que l'utilisateur n'a pas en fonctionnement nominal, comme par exemple l'accès par un médecin, en situation d'urgence, aux données de santé d'un patient duquel il n'a pas reçu d'autorisation explicite (patient inconscient…). Ce type d'accès doit donner lieu à des traces et à un suivi spécifiques.

10. Si la délégation d'habilitation peut être utilisée : les conditions et modalités de cette délégation, les habilitations pouvant être déléguées, les règles définissant les personnes pouvant être habilitées à déléguer ces habilitations et les personnes pouvant bénéficier de ces délégations, la durée maximale de délégation, les modalités de vérification d'absence d'incompatibilité d'habilitation compte tenu des délégations, les modalités de traçabilité de ces délégations et les outils mis à disposition des utilisateurs pour gérer les délégations.
11. Si l'attribution dynamique d'habilitation peut être utilisée : les conditions et modalités de cette attribution, les habilitations pouvant être attribuées dans ce cadre, les règles définissant les personnes pouvant être habilitées à attribuer dynamiquement des habilitations et les personnes pouvant bénéficier de ces attributions, la durée maximale de ces habilitations, les modalités de vérification d'absence d'incompatibilité d'habilitation compte tenu des attributions dynamiques, les modalités de traçabilité de ces attributions et les outils mis à disposition des utilisateurs pour gérer les attributions dynamiques.

La procédure doit préciser les parties prenantes à cette procédure et les modalités de communication entre ces participants.

> ☞ *L'énoncé de cette règle correspond à un modèle de gestion des habilitations par profils d'habilitation et profils utilisateurs. Si un autre modèle de gestion est employé, la procédure de gestion des habilitations requises doit être adaptée en conséquence.*

P03 La procédure générale d'attribution des habilitations doit être formalisée et appliquée lors de la mise en place initiale du système d'attribution des habilitations comme à chaque demande d'habilitation à une ressource du SI, que ce soit dans le cadre d'un mouvement de personnel ou de l'évolution des ressources du SI.

P04 La procédure d'attribution des habilitations doit permettre de définir :

1. la logique d'attribution des habilitations (unitairement ou profil d'habilitation) aux acteurs (de façon discrétionnaire ou par profil utilisateur) ;
2. le logigramme correspondant (même si certaines parties du logigramme peuvent n'être que des étapes de décision humaine dans le cas d'habilitation unitaire et/ou d'attribution discrétionnaire) ;
3. les modalités d'échange sécurisé entre les parties prenantes à l'attribution des habilitations :
   - demandeur de l'habilitation (RH, responsable hiérarchique…),
   - gestionnaires des habilitations,
   - bénéficiaire de l'habilitation demandée,
   - gestionnaire technique des droits d'accès correspondant aux habilitations,

- responsable du traitement concerné (le cas échéant)

afin de préciser les moyens de communications utilisables, formulaires de demande, de notification d'attribution ou de refus, etc. en tenant compte de l'exigence de protection de ces échanges contre la falsification ;

4. la procédure générale d'attribution d'habilitations à titre exceptionnel, s'il y a lieu.

☞ *Les modèles de fiche n° 1 « Cadre général de gestion des habilitations » et de fiche n°2 « Gestion des habilitations par ensembles des ressources » proposés en Annexe 1 peuvent être utilisés pour collecter et formaliser les différentes informations requises par les règles de ce chapitre 4.2.*

4.3 Mise en œuvre des droits d'accès au sein du SI

La décision d'habiliter un acteur (ou un profil d'utilisateur) à accéder à une ressource est un acte fonctionnel, qui doit être transposé au niveau opérationnel du SI sous forme d'autorisation(s) technique(s) d'accès à certaines données ou fonctions informatiques.

> *Bien que sortant du strict cadre du présent guide, un rappel sur le déroulement technique générique d'un accès au SI est présenté en Annexe 3.*

N°	Règle
A01	Pour chaque ressource ou ensemble cohérent de ressources du SI, le gestionnaire technique des droits d'accès à ces ressources doit être identifié et approuvé par le(s) responsable(s) du traitement (ou par une personne à laquelle ces responsable ont délégué cette activité, comme par exemple le Responsable de la Sécurité du SI). *Il est fréquent que la gestion technique des droits d'accès soit réalisée par une même équipe mutualisée pour l'ensemble des ressources du SI. On peut cependant noter des situations où la gestion des droits d'accès à certaines ressources est réalisée par d'autres types d'acteurs, comme par exemple :* • *les cas où les droits d'accès peuvent être gérés directement dans une application par un utilisateur métier disposant d'un rôle d'administrateur fonctionnel de l'application ou de certains périmètres fonctionnels de l'application ;* • *le cas de certaines ressources particulièrement sensibles, comme par exemple les composants assurant la sécurité du SI, qui sont de préférence gérées par une équipe dédiée ;* • *le cas des droits d'accès physiques à des locaux ou à des équipements qui sont souvent gérés par les personnes en charge de la sécurité des locaux (non restreinte aux locaux liés au SI).*
A02	Si la gestion technique des droits d'accès à certaines ressources est déléguée à un organisme tiers, cette délégation doit être formalisée contractuellement afin de répondre aux exigences de sécurité applicables à la structure (voir la thématique T6-6 du « Canevas de PSSI » proposé avec le « *Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée* » [Réf. n°1.4])
A03	Les personnes en charge de la gestion technique des droits d'accès et celles en charge de la gestion et de l'attribution des habilitations doivent être distinctes quand la taille ou l'organisation de la structure le permettent.
A04	Les personnes en charge de la gestion technique des droits d'accès et celles en charge de l'administration technique du SI doivent être distinctes quand la taille ou l'organisation de la structure le permettent.
A05	Pour chaque ressource ou ensemble cohérent de ressources du SI, la traduction des habilitations fonctionnelles prévues en autorisations techniques à des données ou fonctions informatiques doit être documentée au niveau de chaque habilitation unitaire ou de chaque profil d'habilitation. Note : si les habilitations sont traduites de manière triviale en autorisation technique,

la documentation peut le préciser de manière tout aussi simple.

Par exemple : « Les droits d'accès aux répertoires et fichiers découlent directement des habilitations qui utilisent les mêmes termes (lecture, écriture, gestion des droits d'accès…) ».

☞ *Les modalités de paramétrage technique des droits d'accès varient fortement selon la ressource concernée d'une part, et selon les outils utilisés pour la gestion de ces droits d'autre part, comme par exemple :*

- *une gestion au niveau du système de fichier ou de l'annuaire de sécurité du système d'exploitation pour les fichiers bureautiques, en s'appuyant généralement sur des droits attribués individuellement aux utilisateurs, ou à des rôles ou à des groupes d'utilisateurs ;*
- *une gestion au niveau de la base de sécurité spécifique de certains composants d'infrastructure : systèmes de gestion de base de données… ;*
- *une gestion centralisée des droits pour tout ou partie des composants du SI (applications métier, messagerie, passerelle Internet…) dans un annuaire de sécurité de référence unique, que ce soit celui du système d'exploitation principalement utilisé dans la structure, ou que ce soit un composant dédié.*
- *une gestion centralisée à l'aide d'une application spécialisée pouvant prendre en charge l'ensemble du périmètre de gestion des identifiants, des habilitations, des autorisations qui en découlent, de leur déploiement effectif sur les composants du SI (création/suppression des comptes, positionnement des droits d'accès…) et du « workflow » correspondant, généralement désignée sous le terme de « solution IAM » pour « Identity Access Management » ou « Gestion des identités et des accès » au SI.*

☞ *Le modèle de fiche n°2 « Gestion des habilitations par ensembles des ressources » proposé en Annexe 1 peut être utilisé pour collecter et formaliser les différentes informations requises par les règles de ce chapitre 4.3.*

4.4 Lien avec les autres fonctions de sécurité

N°	Règle
S01	Dans les cas où l'attribution de certaines habilitations est liée à une qualité, propriété ou attribut de l'acteur certifiée par un tiers : • l'identification et l'authentification de l'acteur concerné doit être conforme aux exigences applicables à la structure pour la ressource concernée (voir 4.1) ; • la validité de cette qualité, propriété ou attribut et de son association à l'acteur concerné doit être vérifiée lors de leur premier usage au sein du SI, et à chaque fois que leur possible péremption le justifie. Ce principe d'adossement d'une habilitation à une qualité d'origine externe à la structure doit être validé par le responsable du traitement concerné. *Exemple : dans le cadre d'un accès à un service en ligne réservé aux professionnels de santé, l'habilitation des utilisateurs à accéder au service peut se baser sur une identification et authentification de l'utilisateur à l'aide de sa CPS ou d'un moyen d'authentification complémentaire à la CPS[3], et sur la qualité de professionnel de santé qui découle de cette authentification, sous réserve de la vérification que le moyen d'identification et d'authentification utilisé n'est pas révoqué (ex : liste de révocation des CPS).*
S02	Toute demande ou opération de modification, de définition ou d'attribution d'habilitations ou d'autorisation doit faire l'objet de traces établies et gérées en respectant au minimum le palier 1 du « Référentiel d'imputabilité » [Réf. n°1.3]. Un palier supérieur peut être sélectionné si les exigences de sécurité liées certaines ressources du SI le requièrent.

4.5 Gestion dans le temps

N°	Règle
G01	Afin de prendre au plus vite en compte les arrivées, départs et changements de fonction des personnels et intervenants, permanents ou temporaires, amenés à accéder au SI ou à certains de ses composants, une procédure doit être mise en place : • avec la direction en charge de la gestion du personnel d'une part ; • avec la direction en charge des achats de prestation d'autre part ; afin que les gestionnaires d'habilitation soient systématiquement : • informés de toute arrivée de personnel ou intervenant externe ; • notifiés de tout départ de personnel ou de fin de prestation d'intervenant ; • de tout changement de poste ou de fonction au sein du personnel ; et puissent ainsi valider les demandes qui leurs sont adressées par les responsables métier, s'informer auprès d'un responsable métier au sujet d'un départ ou changement qu'il ne leur aurait pas notifié, ou prendre tout mesure conservatoire nécessaire au respect des exigences de sécurité du SI.
G02	Pour chaque ressource ou ensemble cohérent de ressources du SI, les gestionnaires des habilitations pour ces ressources doivent être en mesure, à tout moment, de produire : • la liste des acteurs et profils utilisateurs auxquels des habilitations ou profils d'habilitation ont été attribués ;

[3] Voir « Référentiel d'authentification des acteurs de santé » [Réf. n°1.2]

	• les demandes d'habilitation qui justifient ces attributions.
G03	Pour chaque ressource ou ensemble cohérent de ressources du SI, les gestionnaires des autorisations de ces ressources doivent être en mesure, à tout moment, de produire : • la liste des acteurs autorisés, sous la forme de leur identifiant technique utilisé par la ressource (identifiant utilisateur, UID, …), • avec les autorisations techniques associées, • et les habilitations qui justifient ces autorisations, afin de permettre au gestionnaire des habilitations, aux responsables des traitements concernés ou à tout auditeur légitimement mandaté par ces responsables, de vérifier : • la conformité des autorisations effectivement positionnées sur les composants du SI avec les autorisations prévues ; l'adéquation des autorisations prévues avec les habilitations délivrées.
G04	Un processus de revue régulière et, si nécessaire, de correction des habilitations d'une part et des autorisations techniques effectives d'autre part, doit être défini et mis en œuvre, conformément aux exigences de sécurité applicables au SI de la structure. ☞ *Ce processus est généralement déroulé conjointement au processus de revue des comptes utilisateurs et des comptes techniques du SI.*
G05	Quand le nombre d'acteurs et de ressources à gérer est important, un outillage doit être mis en place afin de pouvoir établir facilement une vision consolidée de l'ensemble des habilitations attribuées à un acteur d'une part (profils d'habilitation attribués à un premier niveau, et habilitations unitaires induites à un second niveau), et de l'ensemble des autorisations techniques d'accès qui en découlent d'autre part.

Annexe 1 : Modèles de fiches de définition des habilitations et autorisations

☞ *Les fiches ci-dessous sont des modèles qui peuvent être utiles à la définition générale de modalités de gestion des habilitations, et à la définition des habilitations et des autorisations elles-mêmes.*

Les encadrés similaires au présent encadré contiennent des indications pour le remplissage des fiches et sont destinés à être supprimés des documents remplis.

Fiche n°1 : « Cadre général de gestion des habilitations »

☞ *Cette fiche est prévue pour couvrir le SI de la structure dans son ensemble, et devrait a priori constituer une fiche unique et globale.*

Cadre général de gestion des habilitations

Acteurs participant aux processus de gestion des habilitations

Fonction	Activités dans le processus

☞ *Le tableau ci-dessus permet de recenser les acteurs qui participent aux processus de gestion des habilitations (hors utilisateurs uniquement bénéficiaires des habilitations). Cf. règle P02*

Responsabilités relatives à la définition et à l'attribution des habilitations

Périmètre fonctionnel	Autorité	Responsable opérationnel

☞ *Le tableau ci-dessus permet d'identifier, pour chaque périmètre fonctionnel du SI, les responsables de traitement (« Autorité ») et les responsables de la gestion opérationnelle des habilitations. Cf. règle P02*

Règles pour la gestion des habilitations concernant les ressources mutualisées

☞ *Dans cette section doivent être formulées les règles générales pour la gestion des habilitations concernant les ressources qui participent à plusieurs périmètres fonctionnels ou traitements, pour la définition des habilitations d'une part et pour l'attribution des habilitations d'autre part (ex : délégation des différents responsables de traitement à un responsable unique, comité de décision…). Cf. règle P02 point 8*

Familles d'acteurs auxquels des habilitations pourraient être attribuées

Famille d'acteurs	Exemples et notes

☞ *Ce tableau correspond à la règle P02 point 6*

Familles des ressources du SI pour l'accès auxquelles les habilitations sont gérées

Famille de ressources	Exemples et notes

☞ *Ce tableau permet d'identifier les grands ensembles de ressources du SI pour lesquels la gestion des habilitations doit être mise en œuvre. Ces familles de ressources peuvent être établies, par exemple, sur la base de l'inventaire requis par la règle R02.*

Modèle général de gestion des habilitations

☞ *Dans cette section doivent être décrits les éléments requis par la règle R03.*

Processus général de définition des habilitations

Processus normal

> ☞ *Dans cette section doit être décrit le processus de définition des habilitations qui s'applique « par défaut » quand aucun processus spécifique n'est requis pour la ressource concernée. Cette description peut être utilement illustrée par un schéma (type logigramme ou autre). Cf. règle P01.*

Dérogations possibles et situations exceptionnelles

> ☞ *Dans cette section doit être décrit, s'il y lieu, le processus dérogatoire et exceptionnel de définition d'habilitation et les conditions et mesures de sécurité associées, qui s'appliquent « par défaut » quand aucun processus spécifique n'est précisé pour la ressource concernée. Cette description peut être utilement illustrée par un schéma (type logigramme ou autre).*

Processus général d'attribution des habilitations

Processus normal

> ☞ *Dans cette section doit être décrit le ou les processus d'attribution des habilitations qui s'applique(nt) « par défaut » quand aucun processus spécifique n'est requis pour la ressource concernée.*
>
> *Ces processus doivent prendre en compte les différents évènements susceptibles d'influer sur les habilitations attribuées aux utilisateurs du SI :*
>
> - *Arrivée de personnel (interne ou externe)*
> - *Changement ponctuel de fonction, absence temporaire de personnel*
> - *Départ de personnel*
> - *Mouvement interne de personnel : potentiellement similaire à un départ et à une arrivée du point de vue de la gestion des habilitations*
>
> *Elle peut être utilement illustrée par des schémas (type logigramme ou autre).*
>
> *Cf. règles P03 et P04.*

Dérogations possibles et situations exceptionnelles

> ☞ *Dans cette section doit être décrit le processus d'attribution dérogatoire et exceptionnelle d'habilitation et les conditions et mesures de sécurité associées, qui s'appliquent « par défaut » quand aucun processus spécifique n'est précisé pour la ressource concernée. Cette description peut être utilement illustrée par un schéma (type logigramme ou autre). Cf. règle P04.*

Politique générale de contrôle régulier des habilitations et des autorisations

☞ *Dans cette section doit être décrite la politique générale de suivi et de contrôle des habilitations et des autorisations. Les différents aspects qui peuvent être formalisés sont par exemple :*

- *l'objectif d'amélioration continue ;*
- *la fonction en charge du contrôle ;*
- *le découpage éventuel des périmètres fonctionnels et techniques pour segmenter les contrôles ;*
- *la fréquence des contrôles ;*
- *la description du processus de contrôle (par exemple, vérification des comptes utilisateurs et systèmes, puis des habilitations, puis des autorisations, puis rapport, revue avec les parties prenantes et corrections des anomalies, puis amélioration des processus et des outils).*

Cf. règles G03, G04 et G05.

Fiche n°2 : « Gestion des habilitations par ensembles des ressources »

> ☞ *Typiquement, une fiche n°2 « Gestion des habilitations par ensembles des ressources » doit être établie pour chacun des ensembles de ressources cohérentes en termes de nature (cf. les familles de ressource identifiées dans la fiche n°1), de contraintes de sécurité et de modalités d'accès. Le titre de la fiche doit être adapté en conséquence.*

Gestion des habilitations pour …(désignation de l'ensemble de ressources)

Ressources concernées

> ☞ *Cette section doit caractériser les ressources concernées par cette exemplaire de fiche, par exemple en précisant la famille de ressources, leur nature, les domaines métiers dans lesquels elles sont utilisées, ou des propriétés particulières qui les distinguent.*

Responsabilités

Traitements auxquels sont rattachées les ressources	Responsable de traitement

> ☞ *Le tableau ci-dessus permet de recenser les traitements informatiques auxquels participent les ressources, et les responsables de ces traitements. Cf. règle P02 point 1*

Modèle spécifique de gestion des habilitations

> ☞ *Si le modèle de gestion des habilitations pour cet ensemble de ressources diffère du modèle général de gestion des habilitations spécifié dans la fiche n°1, il doit être décrit ici selon les mêmes modalités que le modèle général. Cf. règle R03*
>
> *S'il n'y a pas de modèle spécifique pour ces ressources, indiquer simplement « Sans objet ».*

Processus spécifique de définition des habilitations

☞ *Si le processus normal et/ou dérogatoire de définition des habilitations pour cet ensemble de ressources diffère du processus général de définition des habilitations spécifié dans la fiche n°1, il doit être décrit ici selon les mêmes modalités que le processus général. Cf. règle P01*

S'il n'y a pas de processus normal ni dérogatoire spécifique pour ces ressources, indiquer simplement « Sans objet ».

Habilitations unitaires

Désignation	Définition et notes

☞ *Ce tableau recense les différentes habilitations unitaires prévues pour l'ensemble de ressources considéré. Cf. règle P02 point 2*

Combinaisons d'habilitations unitaires interdites

☞ *Cette section doit lister les combinaisons d'habilitations unitaires interdites. Cf. règle P02 point 4*

Si aucune combinaison ne doit être interdite, indiquer « Sans objet ».

Profils d'habilitation

Désignation	Habilitations unitaires	Notes

☞ *Ce tableau recense les différents profils d'habilitations prévus pour l'ensemble de ressources considéré. Cf. règle P02 point 3*

S'il n'est pas défini de profils d'habilitation pour ces ressources, cette section peut être supprimée.

Combinaisons de profils d'habilitations interdites

> ☞ *Cette section doit lister les combinaisons de profils d'habilitations interdites, qui découlent notamment des combinaisons d'habilitations unitaires interdites. Cf. règle P02 point 4*
>
> *Si aucune combinaison ne doit être interdite, indiquer « Sans objet ».*

Périmètre des acteurs auxquels des habilitations pourraient être attribuées

Famille d'acteurs	Sous-groupes d'acteurs concernés	Origine de l'identification utilisée

> ☞ *Ce tableau recense les familles d'acteurs, en les affinant si nécessaire en sous-groupes, auxquels des habilitations aux ressources considérées sont susceptibles d'être attribuées. Les familles d'acteurs font partie de celles recensées dans le fiche n°1. Cf. règle P02 point 6*
>
> *Pour chaque famille et sous-groupe doit également être indiquée l'origine de l'identification utilisée pour identifier les acteurs. Cf. règle P02 point 5*

Profils utilisateurs

Désignation	Définition, restrictions éventuelles et notes

> ☞ *Ce tableau recense les différents profils utilisateurs prévus pour l'attribution des habilitations aux ressources considérées. Cf. règle P02 point 7*
>
> *S'il n'est pas prévu d'utiliser de profils utilisateurs pour ces ressources, cette section peut être supprimée.*

Processus spécifique d'attribution des habilitations

☞ *Si le processus normal et/ou dérogatoire d'attribution des habilitations pour cet ensemble de ressources diffère du processus général d'attribution des habilitations spécifié dans la fiche n°1, il doit être décrit ici selon les mêmes modalités que le processus général. Cf. règle P02 points 8 et 9*

S'il n'y a pas de processus normal ni dérogatoire spécifique pour ces ressources, indiquer simplement « Sans objet ».

Habilitations attribuées par profil utilisateur

Profil utilisateur	Profils d'habilitation	Habilitations unitaires	Restrictions éventuelles et notes

☞ Quand des profils utilisateur sont utilisés, ce *tableau recense les différents profils d'habilitation et habilitations unitaires aux ressources considérées qu'il est prévu d'attribuer à chaque profil utilisateur. Cf. règle P02 point 7*

S'il n'est pas prévu d'utiliser de profils utilisateurs pour ces ressources, cette section peut être supprimée.

Politique spécifique de contrôle régulier des habilitations et des autorisations

☞ *Si le processus de contrôle régulier des habilitations et des autorisations pour cet ensemble de ressources diffère du processus général de contrôle régulier des habilitations et des autorisations spécifié dans la fiche n°1, il doit être décrit ici selon les mêmes modalités que le processus général. Cf. règles G03, G04 et G05.*

S'il n'y a pas de processus spécifique pour ces ressources, indiquer simplement « Sans objet ».

Annexe 2 : Exemples de fiches de définition des habilitations et autorisations

> ☞ *Les exemples de fiches de définition des habilitations et autorisations présentées ci-dessous sont destinées à illustrer l'usage des modèles de fiches proposés en Annexe 1.*
>
> Les encadrés similaires au présent encadré contiennent des remarques qui ne seraient pas présentes dans des fiches réelles.

Exemple de fiche n°1 : « Cadre général de gestion des habilitations »

> ☞ *Cet exemple illustre l'usage du modèle de fiche n°1 « Cadre général de gestion des habilitations » proposé en Annexe 1, décliné de manière simplifiée pour un des services uniquement d'un établissement de santé imaginaire (la fiche doit normalement porter sur l'établissement dans son ensemble). Il présente, pour chaque partie de la fiche, des exemples partiels de contenu afin d'illustrer le type d'information qui doit y être collectée. Cet exemple n'est pas destiné à être réutilisé tel quel, mais uniquement à présenter un cas de contenu possible.*

Cadre général de gestion des habilitations pour le Service de Soins de l'Etablissement

Acteurs participant aux processus de gestion des habilitations

Fonction	Activités dans le processus
Directeur de l'établissement	Valide les modalités, le déroulement, les acteurs et les rôles du processus de gestion des habilitations.
Responsables de périmètre fonctionnel *(médecins chefs de service, responsable du service administratif, responsable du service achats, responsable des services généraux, responsable du personnel, responsable du service informatique…)*	Responsable des traitements informatiques relevant de son périmètre fonctionnel, valide les habilitations unitaires, les profils d'habilitations et les profils utilisateurs pour ces traitements, et les règles d'attributions d'habilitations à ces traitements.
Gestionnaire des habilitations	Assure la gestion quotidienne des habilitations par délégation de chaque responsable de périmètre fonctionnel.
Responsable du personnel	S'assure que le service du personnel notifie le gestionnaire des habilitations des départs, arrivées et absences du personnel ou des intervenants extérieurs.
Administrateur sécurité informatique	Assure la gestion technique des droits d'accès qui découlent des habilitations.
Chefs d'équipes	Effectuent les demandes d'habilitation pour le personnel de leur équipe, notifient le gestionnaire des habilitations des départs,

	arrivées et absences au sein de leur équipe.
Responsable de la sécurité du SI	Contrôle le respect du processus de gestion des habilitations et vérifie la conformité des habilitations et autorisations aux règles validées par le directeur de l'établissement et les responsables de périmètres fonctionnels.

Responsabilités relatives à la définition et à l'attribution des habilitations

Périmètre fonctionnel	Autorité	Responsable opérationnel
Services de Soins	Médecin chef du service de soins	Gestionnaire des habilitations
Pharmacie	Pharmacien responsable de la pharmacie	Gestionnaire des habilitations
Gestion administrative et comptable, gestion des séjours des patients	Responsable du service administratif	Gestionnaire des habilitations
Achats	Responsable du service achats	Gestionnaire des habilitations
[…]	[…]	[…]
Sécurité du système d'information	Responsable de la sécurité du SI	Responsable de la sécurité du SI
Infrastructure informatique	Responsable du service informatique	Gestionnaire des habilitations

Règles pour la gestion des habilitations concernant les ressources mutualisées

Au sein de l'Etablissement, l'ensemble des responsables de périmètres fonctionnels délègue la gestion quotidienne des habilitations à la fonction « Gestionnaire des habilitations » afin d'assurer l'homogénéité » et la cohérence de cette gestion de manière transverse aux différents services de l'établissement, et d'en faciliter le suivi.

La seule exception à ce principe porte sur la gestion des habilitations liées à la gestion des dispositifs d'infrastructure réseau et de sécurité du SI, qui sont gérées directement par le Responsable de la Sécurité du Système d'Information.

En outre, l'ensemble des responsables de périmètres fonctionnels mandate le Responsable du Service Informatique pour réaliser l'exploitation et la maintenance des équipements informatiques et biomédicaux de leur périmètre.

Familles d'acteurs auxquels des habilitations pourraient être attribuées

Famille d'acteurs	Exemples et notes
Acteurs de santé	Médecins, pharmaciens, infirmiers, aides-soignants…
Personnel administratif	Hôtes et hôtesse d'accueil, comptables, contrôleurs de gestion, directeur de l'établissement, secrétaires administratives
Personnel de maintenance technique	Électriciens internes et externes, Plombiers internes et externes, chauffagistes internes et externes
Personnel de maintenance	Techniciens postes de travail informatiques, techniciens

informatique	équipements biomédicaux connectés
Personnel des services généraux	Personnel de la lingerie, de la cantine, d'entretien des locaux
Patients	
Autres personnes externes	Visiteurs de patients, autres visiteurs, prestataires non couverts par d'autres catégories
[…]	[…]

Familles des ressources du SI pour l'accès auxquelles les habilitations sont gérées

Famille de ressources	Exemples et notes
Informatique médicale	Applications médicales, équipements biomédicaux, terminaux et équipements informatiques en zone de soins, informations de santé
Application de gestion de la pharmacie	Application de gestion des stocks de la pharmacie
Informatique de gestion	Applications de gestion administrative et comptable, de gestion du personnel, de gestion des achats, de gestion des services généraux, de gestion de la cantine, de gestion des chambres
[…]	[…]
Autres équipements informatiques terminaux	Postes de travail fixes, terminaux mobiles, imprimantes, imprimantes multifonctions, lecteurs de carte de cantine, « imprimante » de cartes de cantine, autres équipements « connectés »
Infrastructure serveurs	Serveurs applicatifs, serveurs de base de données, serveurs et systèmes de stockage, frontaux web
Infrastructure réseau	Routeurs, commutateurs, hubs, points d'accès Wifi, serveurs DHCP, serveurs DNS, serveurs NTP
Infrastructure téléphonique	PABX, téléphones, téléphones IP, passerelles VoIP, serveur de taxation, enregistreurs, liaisons téléphoniques
Infrastructure sécurité du SI	Pare-feux, antivirus et console de gestion associée, serveur de mises à jour des logiciels, serveur d'authentification, passerelles Internet, serveur d'horodatage, serveur de centralisation des traces, serveur d'analyse des traces
Locaux d'hébergement du SI	Salles informatiques, locaux techniques d'étage
Locaux donnant accès au SI	Bâtiment d'accueil, Chambres, Chambres maternité, Bloc chirurgie, Locaux de radiologie, secteur administration
GTC-GTB (Gestion Technique Centralisée – Gestion Technique du Bâtiment)	Système GTC (Chauffage, climatisation, incendie), système d'alarme intrusion, serveur de contrôle d'accès (portes à ouverture par badge ou par code), lecteurs de badges, systèmes de personnalisation des badges d'accès, serveur de vidéo-protection, caméras de vidéo-protection

Modèle général de gestion des habilitations

L'organisation des habilitations se base prioritairement sur une gestion par profil d'habilitations. Les habilitations unitaires peuvent être utilisées s'il est certain qu'elles ne devront pas un jour évoluer en profil d'habilitation.

Les habilitations gérées sont de deux types destinés à être combinés au moment de leur attribution :

- Habilitations « de fonction » à un ensemble de fonctions et de type d'informations (l'habilitation détermine l'action concernée, par exemple : établir une prescription, consulter un dossier médical…)
- Habilitations « de périmètre » à un ou plusieurs périmètres organisationnel (l'habilitation définit l'objet concerné, par exemple : un service, un patient en particulier, l'ensemble de la structure…)

Des habilitations combinant « fonction » et « périmètre » (.i.e. action et objet) peuvent également être définies si c'est pertinent (pas de variabilité possible du périmètre par exemple).

Des profils utilisateurs sont définis afin de faciliter l'attribution des habilitations. Ces profils sont destinés à se voir attribuer des habilitations communes à plusieurs utilisateurs.

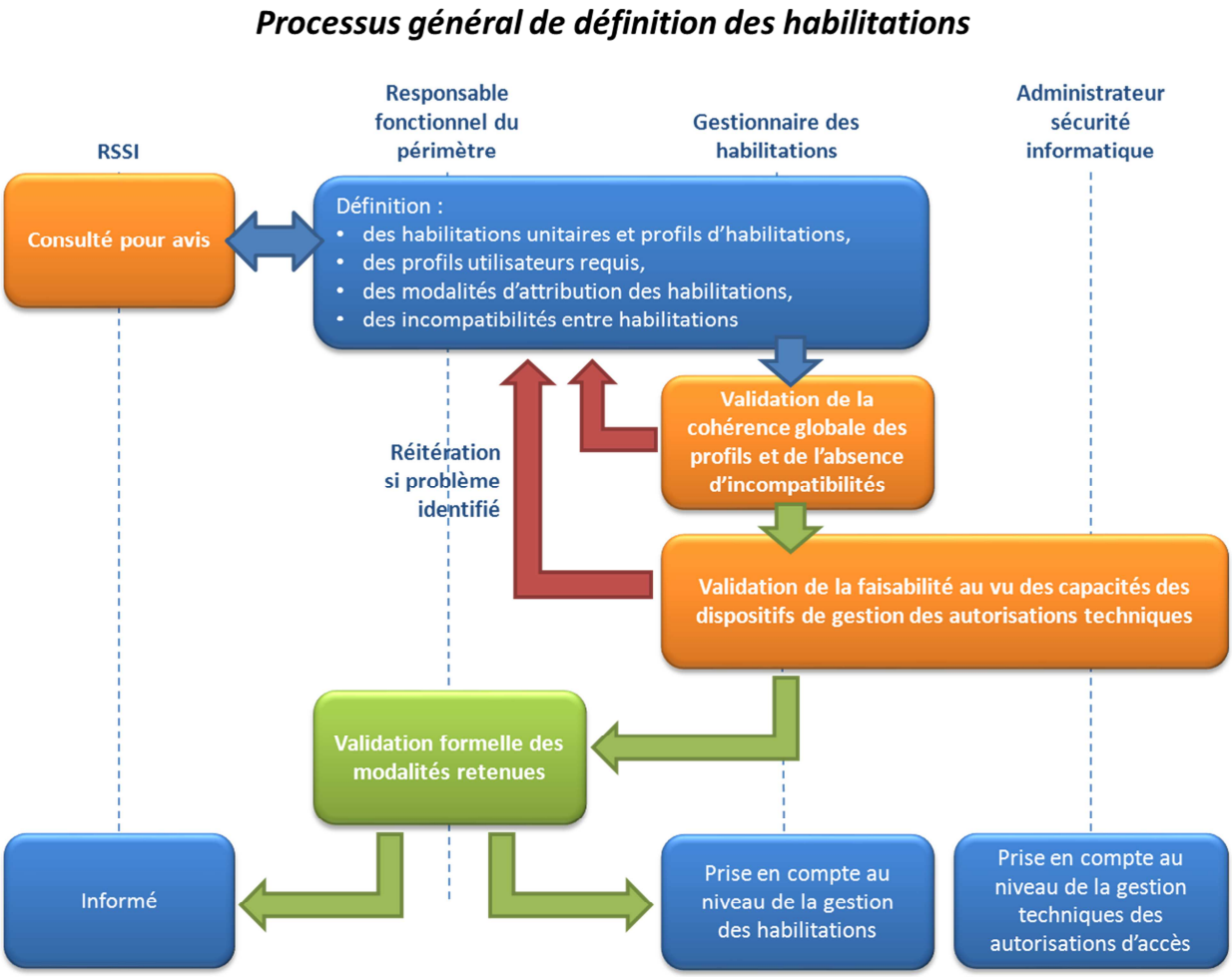
Un utilisateur peut être affecté à un ou plusieurs profils.

Des attributions discrétionnaires d'habilitation, c'est-à-dire directement à un utilisateur sans passer par l'intermédiaire d'un profil, peuvent être effectuées, mais doivent être évitées autant que possible au profit de l'usage de profils utilisateurs.

Les profils utilisateurs « de fonctions » sont définis, et destinés à se voir attribuer un ensemble de profils d'habilitations de fonction. Ces profils utilisateurs « de fonctions » doivent être affectés aux utilisateurs concernés conjointement à l'attribution d'habilitation « de périmètre ». Ce principe permet, par exemple, de définir un profil utilisateur de fonctions « infirmier », de l'attribuer à l'ensemble du personnel infirmier de l'établissement, et habiliter chaque personnel à ces fonctions sur les ressources de son service uniquement en lui attribuant une habilitation de périmètre pour son service.

Processus général de définition des habilitations

Processus normal



Les habilitations unitaires, profils d'habilitations, profils utilisateurs requis et modalités d'attribution des habilitations sont définis et mis à jour par le responsable fonctionnel de la ressource concernée avec l'assistance du gestionnaire des habilitations. Le RSSI (responsable de la sécurité du système d'information) est consulté afin qu'il communique ses commentaires et, le cas échéant, ses mises en garde.

Les incompatibilités éventuelles entre certaines habilitations unitaires doivent être identifiées, soulignée et expliquées.

Le gestionnaire des habilitations vérifie la cohérence des profils utilisateurs, s'assure de l'absence d'introduction de combinaisons d'habilitations incompatibles, vérifie avec le responsable avec l'administrateur sécurité informatique en charge du paramétrage des droits d'accès pour la ressource concernée, que le habilitations unitaires et profils d'habilitation concernés peuvent être paramétrés, revient vers le responsable fonctionnel de la ressource en cas de problème bloquant.

Quand ces différents aspects sont stabilisés, le responsable fonctionnel de la ressource concernée valide formellement la définition des habilitations et leurs modalités d'attribution, et le gestionnaire des habilitations prend en compte ces nouvelles règles.

Dérogations possibles et situations exceptionnelles

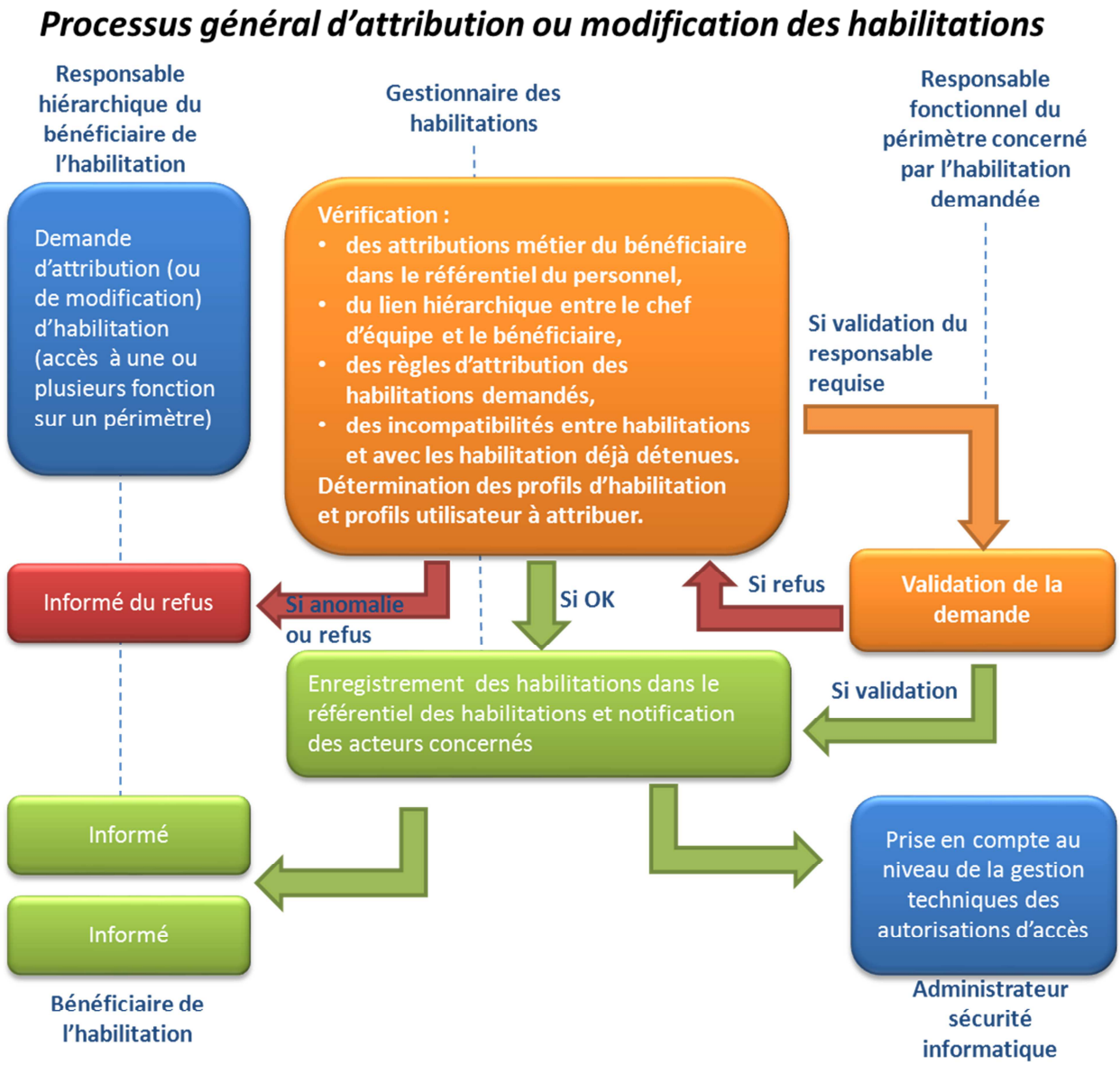
Pas de situation dérogatoire identifiée.

Processus général d'attribution des habilitations

Processus normal

Les processus d'attribution, de modification et de retrait des habilitations décrits ci-dessous s'appliquent « par défaut » quand aucun processus spécifique n'est requis pour la ressource concernée.

Attribution ou modification d'habilitation



Cas des départs ou de mobilité interne de personnel ou d'intervenants externe

En cas de départ ou de mobilité interne, qu'il s'agisse de personnel interne ou d'intervenants externe, le responsable hiérarchique doit informer le gestionnaire des habilitations de la date du changement, afin que l'ensemble des habilitations de la personne concernées soient retirées. En cas de mobilité interne, l'ensemble des habilitations requises par la personne dans sa nouvelle fonction devra être demandé par son nouveau responsable hiérarchique.

Afin de parer à toute défaillance dans l'information du gestionnaire des habilitations, le service du personnel doit également le notifier du changement le jour précédent sa date d'effet.

Dérogations possibles et situations exceptionnelles

Habilitation par le directeur de l'établissement

Pour toute ressource qui ne participe pas au traitement d'information de santé à caractère personnel, le directeur de l'établissement (ou une personne à qui il aura délégué cette tâche) peut se substituer au responsable fonctionnel de la ressource et décider de l'attribution d'habilitations données à la personne qu'il désigne. Le reste du processus normal d'attribution d'habilitation est déroulé, et le responsable de la ressource concernées et le RSSI sont informés de cette attribution exceptionnelle.

« Auto-habilitations » temporaires

Un responsable fonctionnel de ressources a la possibilité d'habiliter les personnes de son choix à s'auto-habiliter temporairement à certaines fonctions sur certains périmètres dont il est responsable. Il communique formellement au gestionnaire des habilitations les paramètres de ces auto-habilitations : utilisateurs ou (de préférence) profils d'utilisateurs concernés, profils d'habilitations de fonctions autorisés dans ce cadre, profils d'habilitations de périmètre autorisés dans ce cadre, durée maximale de validité de l'auto-habilitation, restriction éventuelles (plages horaires…).

Les bénéficiaires de cette habilitation à « s'auto-habiliter » doivent en être informés. Ils doivent également être informés du cadre d'activation de cette auto-habilitation.

Toute activation d'une auto-habilitation par un utilisateur doit faire l'objet d'une trace.

Le gestionnaire des habilitations et le responsable hiérarchique du bénéficiaire de l'habilitation sont informés au plus tôt de l'activation de l'auto-habilitation. Ils procèdent le cas échéant à la régularisation des habilitations en attribuant les habilitations nécessaires par le processus normal si ce besoin n'est pas temporaire. Le gestionnaire des habilitations notifie le responsable de la ressource concernée si l'activation de l'auto-habilitation lui semble non pertinente ou suspecte.

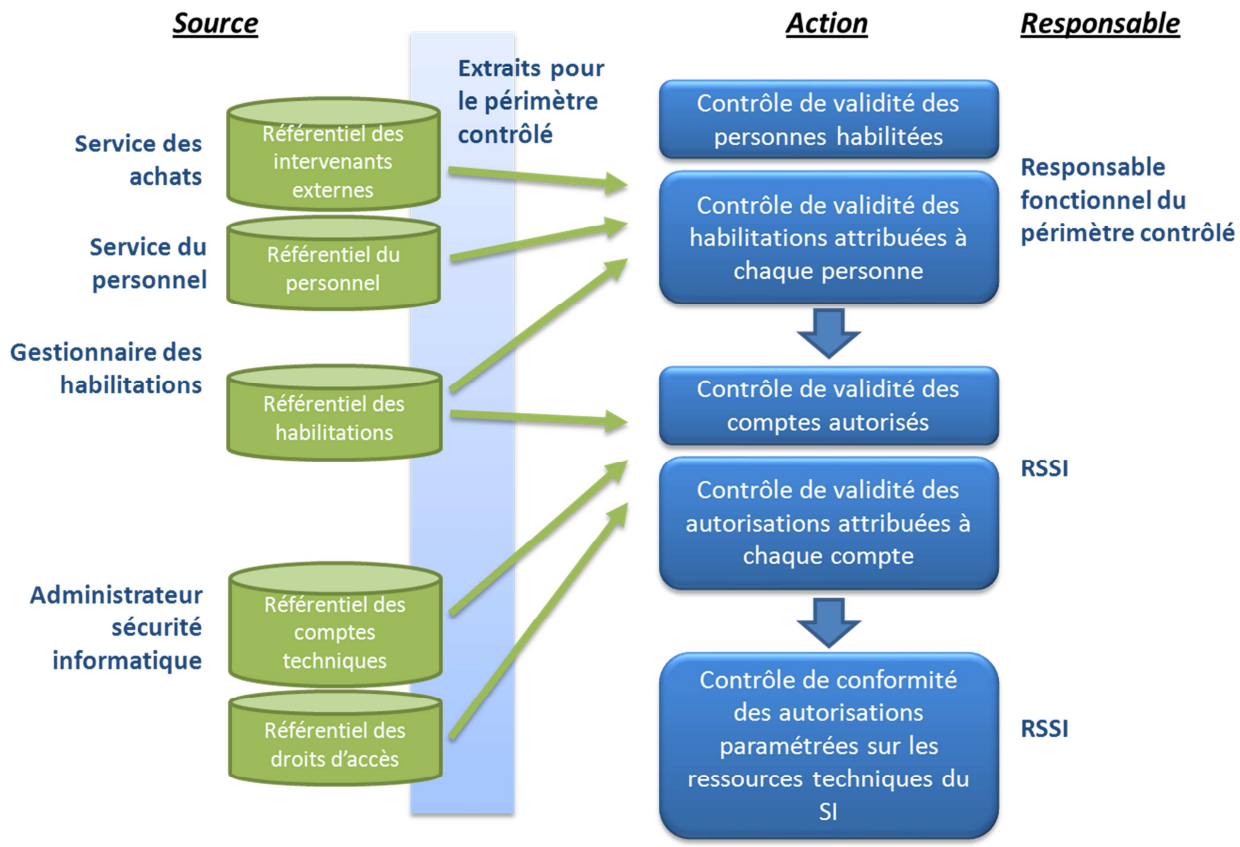
Le gestionnaire des habilitations fournit au responsable de la ressource un rapport quotidien des états d'activation de l'auto-habilitation et des actions réalisés par leur bénéficiaire dans ce cadre.

Politique générale de contrôle régulier des habilitations et des autorisations

Afin de permettre, au minimum, un maintien du niveau de sécurisation du SI sur la durée et, si possible, une amélioration continue de ce niveau, un contrôle régulier des habilitations et des autorisations doit être effectué.

Ce contrôle est piloté par le RSSI et doit être réalisé une fois par an pour chaque périmètre fonctionnel.

Processus de contrôle des habilitations et des autorisations



Exemple de fiche n°2 : « Gestion des habilitations par ensembles des ressources »

> ☞ *Cet exemple illustre l'usage du modèle de fiche n°2 «Gestion des habilitations par ensembles des ressources » proposé en Annexe 1, décliné de manière simplifiée pour le système de gestion des prescriptions d'un établissement de santé imaginaire. Il présente, pour chaque partie de la fiche, des exemples partiels de contenu afin d'illustrer le type d'information qui doit y être collectée. Cet exemple n'est pas destiné à être réutilisé tel quel, mais uniquement à présenter un cas de contenu possible.*

Gestion des habilitations pour le système de gestion des prescriptions

Ressources concernées

Les ressources sur lesquelles porte cette fiche sont les ressources informatiques utilisées par les activités de gestion des prescriptions médicales et de suivi de leur réalisation :

- Application centrale de gestion des prescriptions médicales et de suivi de leur réalisation ;
- Logiciel client de gestion des prescriptions médicales et de suivi de leur réalisation ;
- Informations des prescriptions médicales et de suivi de leur réalisation pour chaque patient ;
- Serveurs hébergeant l'application centrale et le stockage des données associées ;
- Postes de travail du personnel de santé, hébergeant le logiciel client ;
- Imprimantes.

Responsabilités

Traitements auxquels sont rattachées les ressources	Responsable de traitement
Saisie des prescriptions médicales et de suivi de leur réalisation	Médecin chef du service de soins
Préparation des traitements médicamenteux	Responsable pharmacie

Modèle spécifique de gestion des habilitations

Sans objet

Processus spécifique de définition des habilitations

Sans objet

Habilitations unitaires

Désignation	Définition et notes
PRESC-MAJ	Saisie et mise à jour de la prescription, intégrant également les données concernant les allergies et autres contre-indications à prendre en compte pour le patient.
PRESC-LECT	Consultation des prescriptions et des informations associées pour un patient.
PRESC-PREP	Mise à jour de l'état de suivi de la préparation des traitements médicamenteux prévus par les prescriptions pour un patient.
PRESC-REAL	Mise à jour de l'état de suivi de la réalisation des prescriptions prévues pour un patient.
HAB-<patient>	*Habilitation de périmètre transverse autorisant l'accès au DPI de <patient> dans la limite des autres habilitations attribuées.*

Pas d'attribution directe d'habilitation unitaire prévue.

Combinaisons d'habilitations unitaires interdites

Sans objet.

Profils d'habilitation

Désignation	Habilitations unitaires	Notes
PRESC-Médecin	PRESC-MAJ, PRESC-LECT, PRESC-REAL	
PRESC-Pharmacien	PRESC-LECT, PRESC-PREP	
PRESC-Infirmier	PRESC-LECT, PRESC-REAL	

Combinaisons de profils d'habilitations interdites

Sans objet

Périmètre des acteurs auxquels des habilitations pourraient être attribuées

Famille d'acteurs	Sous-groupes d'acteurs concernés	Origine de l'identification utilisée
Professionnels de santé	Médecins	Carte CPS
Professionnels de santé	Infirmiers	Carte CPS
Professionnels de santé	Pharmaciens	Carte CPS

Profils utilisateurs

Désignation	Définition, restrictions éventuelles et notes
PROF-Médecin	*Profil transverse, attribués aux médecins participant aux équipes de soin au sein du service de soins*
PROF-Infirmier	*Profil transverse, attribués aux infirmiers participant aux équipes de soin au sein du service de soins*

PROF-Pharmacien	*Profil transverse, attribués aux pharmaciens assurant la préparation des traitements médicamenteux et la gestion du stock de pharmacie*

Ces profils transverses sont attribués et gérés par le Responsable du Service de soins, hors du cadre spécifique de la gestion et du suivi des prescriptions.

Processus spécifique d'attribution des habilitations

Sans objet

Habilitations attribuées par profil utilisateur

Profil utilisateur	Profils d'habilitation	Habilitations unitaires	Restrictions éventuelles et notes
PROF-Médecin	PRESC-Médecin	Néant	
PROF-Infirmier	PRESC-Pharmacien	Néant	
PROF-Pharmacien	PRESC-Infirmier	Néant	

Politique spécifique de contrôle régulier des habilitations et des autorisations

Sans objet

Annexe 3 : Rappel sur le déroulement technique d'un accès au SI

Cette annexe propose une présentation synthétique du déroulement d'un accès technique à une ressource du SI du point de vue du contrôle d'accès quand un acteur demande l'accès à une ressource (données, fonction informatique, composant technique du SI…).

Le schéma ci-dessous présente une vue générique globale d'un tel accès (étapes sur la gauche du schéma), et positionne les processus amonts de gestion des habilitations et des droits d'accès (à droite du schéma) par rapport à l'accès effectif.

Les étapes de l'accès au SI sont détaillées dans les chapitres qui suivent.

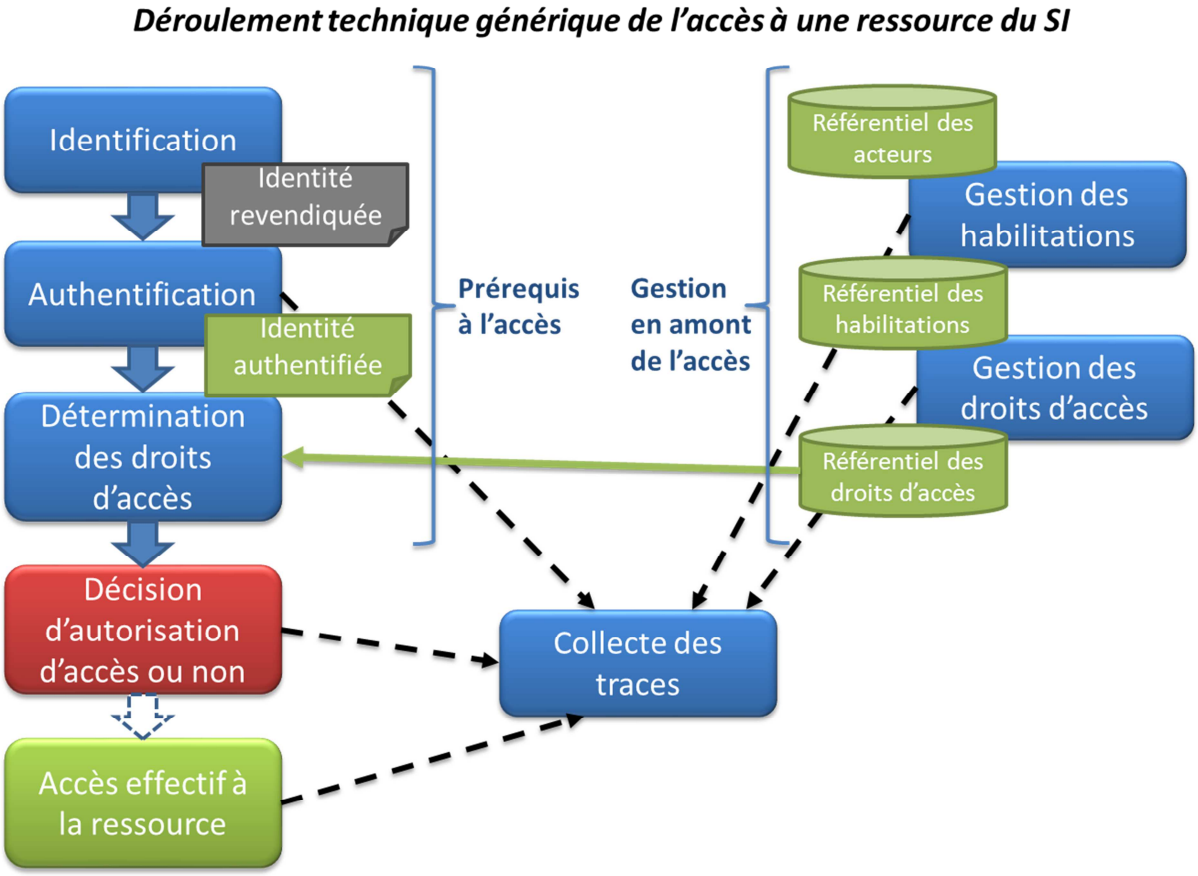


Figure 4 : Etapes du déroulement technique générique de l'accès à une ressource du SI

Premiers préalables : identification et authentification

Pour qu'il puisse être décidé si un accès demandé doit être autorisé ou non, il est nécessaire de connaître l'identité du demandeur. Une étape d'identification est requise à cette fin, qui permet de recueillir l'identité communiquée par l'utilisateur, parfois appelée « identité revendiquée », et de vérifier qu'elle est recevable par le SI (*par exemple : elle correspond bien à un utilisateur enregistré, ou elle est de la forme attendue si l'accès au SI est potentiellement possible pour des utilisateurs qui n'ont pas été préenregistrés, comme dans le cas de services en ligne ouverts au public*).

Il convient alors de s'assurer que cette identité est revendiquée par l'utilisateur auquel elle a été attribuée, et lui seul (i.e. qu'elle n'a pas été usurpée), au cours de l'étape d'authentification.

Si l'authentification est positive, le SI dispose de l'identité authentifiée de l'utilisateur pour baser ses décisions d'accès.

Dans certains cas, des informations sur l'utilisateur qui peuvent être utiles à la détermination des droits d'accès sont fournies conjointement aux informations d'identification. Il est important que l'authenticité de ces informations et de leur association avec l'acteur identifié soient garantis avec la même force que l'identité de l'utilisateur.

Par exemple, le certificat électronique qui est stocké dans la carte CPS et qui peut être transmis au SI auquel l'utilisateur veut accéder porte non seulement l'identifiant de l'utilisateur, mais également sa profession. L'étape d'authentification de l'utilisateur à l'aide de sa CPS permet d'authentifier à la fois son identité et sa profession, et d'utiliser ces deux informations par la suite pour baser les décisions de contrôle d'accès aux ressources du SI.

Il peut également être prévu, selon les choix d'architecture du SI, que dans le cas d'accès ne nécessitant pas d'enregistrement préalable (exemple : service en ligne avec authentification « publique »), un compte utilisateur local soit créé et associé à l'utilisateur authentifié afin de servir de base à ses interactions avec le SI. Il est important dans ce cas de figure de veiller à la bonne synchronisation entre ce compte local et le moyen d'identification et d'authentification de référence, notamment afin de valider que ce moyen reste valide dans le temps, et ce d'autant plus que des informations qui participent à la détermination des droits d'accès sont obtenues par ce moyen.

L'identification et l'authentification sont généralement réalisées de manière conjointe. Ces étapes peuvent cependant être réalisées :

- avant mais séparément de la tentative d'accès à la ressource : c'est le cas quand un utilisateur se « connecte » d'abord au SI, puis accès successivement à plusieurs ressource dans le cadre de cette « session » ;
- au moment de la tentative d'accès à la ressource, voire à chaque tentative d'accès : ça peut être le mode de fonctionnement retenu pour des échanges inter-applicatifs (« de machine à machine ») ponctuels pour lesquels l'établissement et le maintien d'une session n'est pas judicieux.

Sur ce sujet, la Politique générale de sécurité des systèmes d'information de santé établit les référentiels suivant :

- *Référentiel d'identification des acteurs sanitaires et médico-sociaux [Réf. n°1.1]*
- *Référentiel d'authentification des acteurs de santé [Réf. n°1.2]*

Second préalable : Détermination des droits d'accès

Cette étape consiste à rassembler les différents éléments nécessaires à déterminer les droits d'accès de l'utilisateur vis-à-vis de la ressource considérée.

Elle requiert que l'identité authentifiée de l'utilisateur soit connue.

Elle peut, comme l'identification et l'authentification, être réalisée lors de la connexion initiale de l'utilisateur, ou au moment de chaque demande d'accès à la ressource. Il convient de s'assurer, si la première option est prise, qu'il n'est pas nécessaire de prendre en compte une éventuelle modification des droits d'accès de l'utilisateur pendant la durée de sa session, ou de prévoir une mécanisme garantissant que l'utilisateur devra réinitialiser sa connexion dans cette situation.

Au niveau technique, cette étape est réalisée de manière très variable selon les systèmes, les architectures et les ressources concernées.

Par exemple :

- *Dans un système de fichier Unix « classique », la détermination des droits d'accès se base sur un ensemble d'information directement associées au ficher dans le système de fichier lui-même : identifiant de l'utilisateur « propriétaire » du fichier, identifiant d'un groupe d'utilisateur particulier, droit de lecture et d'écriture (entre autres) pour l'utilisateur « propriétaire » d'une part, pour un groupe d'utilisateurs déterminé d'autre part, et enfin pour tout autre utilisateur ne faisant pas partie e de ce groupe d'utilisateurs ;*
- *Dans une base de données relationnelle, la détermination des droits d'accès peut se baser sur une table contenant les groupes d'appartenance de l'utilisateur, et sur une table détaillant pour chaque utilisateur ou groupe d'utilisateur, les tables, champs de données ou requêtes auxquels ils sont autorisés, avec le type d'autorisation dont ils disposent (lecture, création, modification, suppression, gestion des droits d'accès…) ;*
- *Dans un service en ligne qui s'appuie sur une authentification publique et où les utilisateurs ne sont pas enregistrés préalablement à leur accès, les éléments nécessaires à la détermination des habilitations de chaque utilisateur peuvent être fournis lors de l'authentification. Par exemple, le volet transport synchrone pour client lourd du cadre d'interopérabilité des systèmes d'information de santé[4] spécifie le Vecteur d'Identification et d'Habilitation Formelles (VIHF) qui est une assertion SAML permettant de fournir au service les éléments nécessaires à la détermination des habilitations de l'utilisateur. Les éléments fournis dans le VIHF peuvent être vérifiées dans le référentiel d'identité utilisé comme base de la diffusion du moyen d'authentification utilisé.*
- *Une application qui permettrait des accès exceptionnels de type « bris de glace », délivrés selon des critères et une procédure vérifiés par l'application elle-même (sur la base des rôles attribués à l'utilisateur, de ses services d'appartenance et d'autres informations obtenues de l'annuaire de sécurité du SI), pourrait établir une attestation d'autorisation temporaire d'accès, par exemple sous forme de certificat électronique de courte durée de validité, collecté dans le cadre de cette seconde étape.*

Le processus technique de détermination des droits d'accès doit être conçu pour que les informations participant aux droits d'accès qu'il collecte ne puissent être falsifiées :

- ni au cours de leur communication depuis leurs sources ;
- ni pendant leur conservation ;
- ni au cours de la communication des informations résultantes au processus de décision effective d'autorisation d'accès.

[4] [Réf n°7] http://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport

Décision d'autorisation ou non de l'accès demandé

Cette étape consiste, pour le mécanisme de contrôle d'accès à la ressource concerné, à déterminer si l'accès doit être autorisé ou non à l'utilisateur authentifié.

Cette décision se base sur les différentes informations liées à l'utilisateur relatives à ses droits d'accès, déterminées au cours de l'étape précédente, et éventuellement sur des informations liés au contexte de l'accès : jour de la semaine, heure, origine géographique de la connexion, nature du terminal utilisé par l'utilisateur, …

Ces différentes informations sont généralement soumises à un ensemble de règles techniques, souvent paramétrables et parfois nommées « politique », qui s'appliquent à l'ensemble des accès aux ressources gérées par ces mécanismes. C'est de la confrontation de ces informations à cet ensemble de règles que découle la décision binaire : « accès autorisé » ou « accès refusé »

Accès effectif à la ressource

Dès lors que l'étape de décision d'autorisation d'accès conclut au résultat « accès autorisé », l'accès à la ressource peut effectivement être donné à l'utilisateur, pour cet accès unique.

Si une seconde demande d'accès identique à la même ressource est émise par le même utilisateur, la décision d'autorisation d'accès (étape précédent) devra de nouveau être établie.

Traces

Avoir la possibilité d'analyser *a posteriori* « qui a fait quoi » est une capacité essentielle pour tout SI qui traite d'information sensible ou qui présente des exigences de continuité de fonctionnement élevées, ce qui est dans un cas comme dans l'autre une situation habituelle pour les SI de santé.

Cette capacité, nommée « Imputabilité » (voir définition en 1.3) est décrite et formalisée dans le *Référentiel d'imputabilité* [Réf. n°1.3] de la PGSSI-S, et s'appuie généralement sur des traces générées par certains composants du SI.

Au cours du déroulement technique d'un accès à une ressource du SI, si des traces peuvent être générées à chaque étape selon les besoins spécifiques au SI, il est important que ces traces soient systématiquement produites au moins :

- à l'étape d'authentification de l'utilisateur, pour conserver les éléments d'identité de l'utilisateur, les références des éléments qui ont permis d'établir (ou non) l'authentification de l'utilisateur, la référence de la session d'authentification éventuellement établie et les informations associées ;
- à l'étape de décision d'autorisation d'accès, pour conserver le résultat de la décision d'accès associé à l'identification de l'utilisateur et de l'éventuelle session associée, de la ressource concernée, de l'accès demandé, et le cas échéant de la règle ayant abouti à l'autorisation ou au refus de l'accès ;
- à l'étape d'accès effectif, pour conserver trace de la réalisation effective de l'accès par l'utilisateur, et le cas échéant de son résultat, notamment en cas d'erreur ou de dysfonctionnement détecté dans le cas de cet accès (qui pourrait révéler un défaut technique aussi bien qu'un tentative réussie ou non de piratage informatique).

Ces traces doivent être horodatées, collectées et conservées, si possible de façon centralisées afin de faciliter le rapprochement et l'analyse de ces traces issues de différents composants du SI.

Annexe 4 : Modèles de gestion des habilitations

De nombreux modèles de gestion des habilitations sont décrits dans la littérature informatique. Ils diffèrent par les éléments qui sont utilisés pour organiser les habilitations et surtout pour les attribuer aux utilisateurs.

Dans la mesure où les logiciels de gestion des habilitations et des autorisations d'accès sont généralement basés sur l'un de ces modèles, les principaux d'entre eux sont présentés ici pour aider le responsable à choisir le/les modèles le/les plus adapté(s) à son contexte.

Après un schéma qui récapitule le positionnement de différents modèles par rapport aux modes d'organisation et d'attribution des habilitations exposés plus haut, une présentation synthétique de chaque modèle est proposée.

Liste des modèles présentés :

- DAC « Discretionary Access Control » ou « Contrôle d'accès discrétionnaire »
- MAC « Mandatory Access Control » ou « Contrôle d'accès obligatoire »
- RBAC « Role Based Access Control » ou « Contrôle d'accès à base de rôles »
- TMAC « Team Based Access Control » ou « Contrôle d'accès basé sur les équipes »
- TBAC « Task Based Authorization Controls » ou « Habilitation basée sur les tâches »
- OrBAC « Organization Based Access Control » ou « Contrôle d'accès basé sur l'organisation »
- ABAC « Attribute Based Access Control » ou « Contrôle d'accès basé sur les attributs »

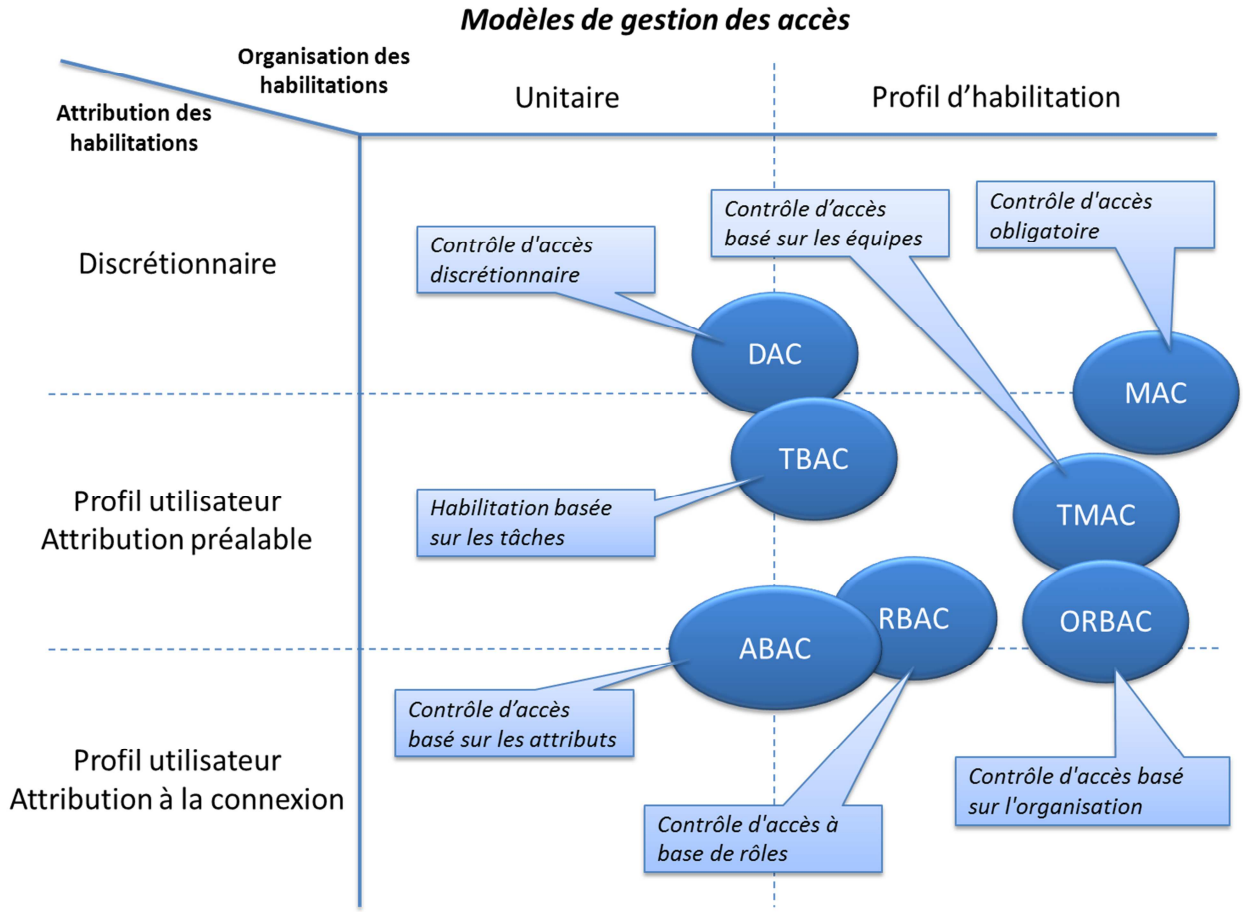


Figure 5 : Positionnement des différents modèles de gestion et d'attribution des habilitations

☞ *<u>Note:</u> dans les documents en anglais pointés ci-dessous :*

- *le terme « subject » (sujet) désigne généralement les acteurs (utilisateurs, composants ou mécanismes internes du SI) qui utilisent des ressources du SI ;*
- *le terme « object » (objet) désigne généralement les ressources du SI (fonction de traitement informatique, données ou autres ressources support) ;*
- *le terme « authorization » correspond généralement au terme « habilitation » tel que défini au 1.3. ;*
- *le terme « permission » correspond généralement au terme « autorisation d'accès » tel que défini au 1.3.*

DAC « Discretionary Access Control » ou « Contrôle d'accès discrétionnaire »

Le Contrôle d'accès discrétionnaire est un modèle de contrôle d'accès, défini par le Trusted Computer System Evaluation Criteria (TCSEC) comme moyen de limiter l'accès aux objets sur la base de l'identité des acteurs ou des groupes auxquels ils appartiennent. Le contrôle est discrétionnaire car il permet aux acteurs de gérer eux-mêmes le contrôle d'accès aux objets dont ils sont responsables et ainsi d'autoriser tout autre acteur à y accéder, dans les limites fixées par le contrôle d'accès obligatoire (voir ci-dessous) éventuellement en place dans le SI. »

(Basé sur http://csrc.nist.gov/publications/history/dod85.pdf)

Voir également https://fr.wikipedia.org/wiki/Contrôle_d'accès_discrétionnaire

MAC « Mandatory Access Control » ou « Contrôle d'accès obligatoire »

Le contrôle d'accès obligatoire est utilisé lorsque la politique de sécurité des systèmes d'information impose que les décisions de protection ne doivent pas être prises par le propriétaire des objets concernés, et lorsque ces décisions de protection doivent lui être imposées par le dit système.

(Source : https://fr.wikipedia.org/wiki/Contrôle_d'accès_obligatoire)

Ce modèle de contrôle d'accès définit plusieurs niveaux de sensibilité des ressources du SI et des règles strictes et incontournables pour les interactions entre ces niveaux. Il est essentiellement utilisé dans les SI militaires.

Par exemple, en France, dans le domaine étatique, quatre niveaux de sensibilité croissante peuvent être identifiés : la mention « Diffusion Restreinte » et les classifications de protection du secret de la défense Nationale « Confidentiel Défense », « Secret Défense », « Très Secret Défense ». Les règles du Contrôle d'accès obligatoire doivent (entre autres) empêcher toute transmission d'information de niveau « Secret défense » à un acteur ou un objet habilité à un niveau inférieur.

Voir également https://en.wikipedia.org/wiki/Mandatory_access_control

RBAC « Role Based Access Control » ou « Contrôle d'accès à base de rôles »

RBAC ou, en français, contrôle d'accès à base de rôles est un modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché. Un rôle découle généralement de la structure d'une entreprise. Les utilisateurs exerçant des fonctions similaires peuvent être regroupés sous le même rôle. Un rôle, déterminé par une autorité centrale, associe à un sujet des autorisations d'accès sur un ensemble objets.

Ce modèle est également référencé sous le nom de nondiscretionary access control et constitue une nouvelle alternative, entre les systèmes Mandatory Access Control (MAC) et Discretionary Access Control (DAC).

(Source : https://fr.wikipedia.org/wiki/Contrôle_d'accès_à_base_de_rôles)

Voir également http://csrc.nist.gov/groups/SNS/rbac/documents/Role_Based_Access_Control-1992.html

Ce modèle est celui qui est majoritairement utilisé dans les SI actuels, notamment parce qu'il permet une gestion plus simple des habilitations en affectant les acteurs à des rôles ou en leur retirant ces rôles. Ce concept de rôle y est généralement mis en œuvre au niveau technique en utilisant des groupes auxquels sont affectés les utilisateurs. Certains systèmes « annuaires » (ou bases utilisateurs) proposent

néanmoins la notion de « rôle » de façon native et distincte de celles de « groupe » (annuaires « LDAP », X500…).

Voir également :

http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf

http://csrc.nist.gov/rbac/sandhu96.pdf

TMAC « Team Based Access Control » ou « Contrôle d'accès basé sur les équipes »

TMAC est une évolution du modèle RBAC (voir ci-dessus) destinée à faciliter la gestion de l'accès à l'information dans le contexte de travail en équipe et de workflow.

Voir http://dx.doi.org/10.1016/j.jbi.2012.06.001

TBAC « Task Based Authorization Controls » ou « Habilitation basée sur les tâches »

Ce modèle vise à permettre l'automatisation de l'attribution des habilitations et des autorisations d'accès associées, en fonction des besoins strictement nécessaires et pour des durées limitées, à des acteurs qui sont essentiellement des composants techniques du SI qui font appel aux fonctionnalités qu'ils offrent les uns aux autres.

Voir http://profsandhu.com/confrnc/ifip/i97tbac.pdf

OrBAC « Organization Based Access Control » ou « Contrôle d'accès basé sur l'organisation »

OrBAC ou, en français, le contrôle d'accès fondé sur l'organisation est un modèle de contrôle d'accès présenté pour la première fois en 2003. Dans OrBAC, l'expression d'une politique d'autorisation est centrée sur le concept d'organisation.

Le modèle OrBAC (Organization Based Access Control) s'appuie sur des concepts de rôle, d'activité, de vue et d'organisation qui sont des concepts organisationnels. Chaque organisation définit ainsi les rôles, les activités et les vues dont elle souhaite réglementer l'accès en appliquant une politique d'autorisation.

Le but principal d'OrBAC est de permettre de définir une politique de sécurité indépendamment de sa mise en œuvre opérationnelle. Un niveau abstrait est introduit à cette fin par rapport aux entités « sujet », « action » et « objet » généralement utilisés dans les modèles de contrôle d'accès :

- les sujets sont abstraits en rôle, ensemble de sujets sur lequel les mêmes règles de sécurité sont appliquées ;
- les actions sont abstraites en activité, un ensemble d'actions sur lequel les mêmes règles de sécurité sont appliquées ;
- les objets sont abstraits en vue, ensemble d'objets sur lequel les mêmes règles de sécurité sont appliquées.

Le modèle de contrôle d'accès OrBAC n'est pas restreint aux permissions. Il inclut aussi la possibilité de spécifier des interdictions et des obligations.

(Basé sur https://fr.wikipedia.org/wiki/Contrôle_d'accès_basé_sur_l'organisation)

Voir également http://orbac.org/?page_id=21

ABAC « Attribute Based Access Control » ou « Contrôle d'accès basé sur les attributs »

ABAC définit un modèle de contrôle d'accès où les droits d'accès sont donnés aux utilisateurs sur la base de politiques d'accès qui s'appuient sur les attributs des utilisateurs, des ressources, du contexte, de l'environnement… Un exemple d'attribut d'utilisateur peut être sa participation à un projet, son appartenance à un service, un rôle. Un exemple d'attribut d'une ressource peut être son responsable, sa sensibilité. Un exemple d'attribut de l'environnement peut être le jour de la semaine et l'heure. Les différents attributs sont mis en relation dans les politiques d'accès pour déterminer si un accès est autorisé ou non.

Ce modèle est mis en œuvre dans XACML « eXtensible Access Control Markup Language »

Voir :

https://en.wikipedia.org/wiki/Attribute-based_access_control

http://www.axiomatics.com/attribute-based-access-control.html

Pour XACML : http://www.oasis-open.org/committees/xacml/

Annexe 5 : Quelques acronymes qui ne correspondent pas à des modèles de gestion des habilitations

Il arrive que certains termes soient présentés à tort comme correspondant à des modèles particuliers de gestion des habilitations :

IBAC « Identity-based Access Control » ou « Contrôle d'accès basé sur l'identité »

IBAC n'est pas un modèle de gestion des habilitations, mais un principe de filtrage des flux réseau basé sur l'identité de l'utilisateur plutôt que sur les adresses IP. La mise en œuvre de ce principe est aujourd'hui disponible sur la plupart des produits « pare-feu » à usage professionnel du marché.

Voir :

http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=8,984,620.PN.&OS=PN/8,984,620&RS=PN/8,984,620

R-RBAC « Responsibility Role Based Access Control »

R-RBAC correspond au modèle RBAC auquel est ajouté un « modèle de gestion de la responsabilité » qui traite de la responsabilité de l'utilisateur vis-à-vis de ses obligations, des autorisations requises pour réaliser ces obligations, et des engagements pris par l'utilisateur à réaliser certaines actions.

Ce modèle de responsabilité associée aux habilitations part de l'hypothèse qu'habiliter un utilisateur à quelque chose est implicitement attendre de lui qu'il fasse cette chose, mais que RBAC ne permet pas de gérer cet aspect et n'est utilisable que dans des organisations très spécifiques.

Il semble que cette hypothèse ne corresponde ni aux pratiques ni aux lois en vigueurs en France quant à l'organisation du travail et aux responsabilités du personnel, où les missions confiées au personnel sont fixées dans un processus amont, et non pas conjoint, au processus d'attribution des habilitations au SI.

Voir http://ceur-ws.org/Vol-599/BUISTAL2010_Paper5.pdf

RSBAC « Rule Set Based Access Control » ou « Contrôle d'accès à base de règles »

RSBAC (Rule Set Based Access Control) est un ensemble [de mécanismes] de sécurité pour Linux dont la fonction est d'offrir un contrôle supplémentaire d'accès aux ressources. Il peut utiliser plusieurs modèles de sécurité différents.

Il est utilisé par exemple dans le cas où il est utile de restreindre l'accès à certaines ressources au seul utilisateur root (qui a normalement accès à toutes les ressources).

(Source : https://fr.wikipedia.org/wiki/Contrôle_d'accès_à_base_de_règles)

RSBAC n'est pas un modèle de gestion des habilitations ni des accès, mais un dispositif technique. En outre, ce n'est pas le mécanisme de sécurité système renforcée qui a été retenue comme solution principale pour Linux par la communauté.

Rule-Based Access Control ou « Contrôle d'accès à base de règles »

Ce terme n'est pas clairement défini et peut correspondre à l'un ou l'autre des acronymes RSBAC ou ABAC présenté ci-dessus.

Annexe 6 : Glossaire

Sigle / Acronyme	Signification
ABAC	Attribute Based Access Control
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CI-SIS	Cadre d'Interopérabilité des Systèmes d'Information de Santé
DAC	Discretionary Access Control
ES	Etablissement de Santé
GT	Groupe de Travail
IAM	Identity Access Management
IBAC	Identity Based Access Control
MAC	Mandatory Access Control
ORBAC	ORganization Based Access Control
PGSSI-S	Politique générale de sécurité des systèmes d'information de santé
PS	Professionnel de Santé
PSSI	Politique de Sécurité des Systèmes d'Information
PUSC	Pôle Urbanisation et Service de Confiance (ASIP Santé)
RBAC	Role-Based Access Control
R-RBAC	Responsibility - RBAC
SAML	Security Assertion Markup Language
SIS	Systèmes d'Information de Santé
TBAC	Task Based Access Control
TMAC	Team Based Access Control
VIHF	Vecteur d'Identification et d'Habilitation Formelles

Annexe 7 : Documents de référence

Référence n°1 : Référentiels et guides pratique du corpus documentaire PGSSI-S
http://esante.gouv.fr/pgssi-s/espace-publication

Référence n°1.1 : Référentiel d'identification des acteurs sanitaires et médico-sociaux

Référence n°1.2 : Référentiel d'authentification des acteurs de santé

Référence n°1.3 : Référentiel d'imputabilité

Référence n°1.4 : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Structure sans approche SSI formalisée

Référence n°2 : RGS - Référentiel Général de Sécurité - Version 2.0
http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/

Référence n°3 : RFC 4949 - Internet Security Glossary, Version 2
https://tools.ietf.org/html/rfc4949

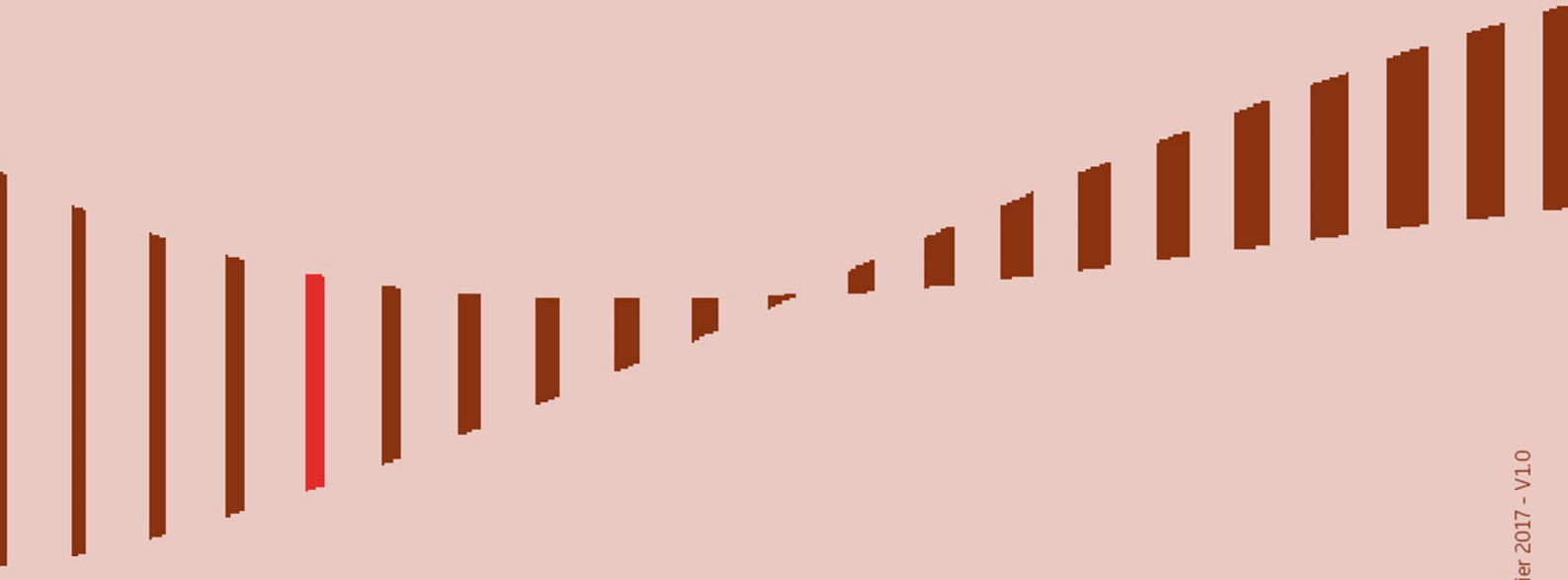
Référence n°4 : Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale (2011).

Référence n°5 : PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat (2014).
http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/

Référence n°6 : PSSI-MCAS - Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (2015).
http://www.legifrance.gouv.fr/jo_pdf.do?cidTexte=JORFTEXT000031386468

Référence n°7 : Volet Transport synchrone pour client lourd du Cadre d'Interopérabilité des Systèmes d'Information de Santé
http://esante.gouv.fr/services/referentiels/ci-sis/espace-publication/couche-transport

Référence n°8 : ISO/CEI 27000:2014, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.



L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

esante.gouv.fr

ASIP Santé
9, rue Georges Pitard - 75015 Paris
T. +33 (0)1 58 45 32 50
Du lundi au vendredi de 8h30 à 18h30 *(hors jours fériés)*