



Gestion des habilitations au système d’informationRGPD : articles types à intégrer dans la charte informatique

Rédigé Par:

**Sébastien CLAUDE**

Délégué à la protection des données

***Date de publication: 05/09/2018***

|  |  |  |
| --- | --- | --- |
| **Historique** | | |
| Version | Date de modification | Champ des modifications |
| 01 | 05/09/2018 | Création |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Légitimité** | | | |
| **Rédigé par :**  Mr S. CLAUDE,  DPD GHT  Le | **Validé par :**  Le : | **Vérifié par :**  Mr S. CLAUDE,  DPD GHT  Le : | **Approuvé par :**  Le : |

Sommaire

[I . Description du document 4](#_Toc523929772)

[II . Introduction 4](#_Toc523929773)

[1 ) Vulnérabilités potentielles du SI liées à la gestion des habilitations 5](#_Toc523929774)

[2 ) Principes de gestion des habilitations 5](#_Toc523929775)

[III . Règles applicable au SI 6](#_Toc523929776)

[IV . Description du processus 7](#_Toc523929777)

[1 ) Processus général de définition des habilitations 7](#_Toc523929778)

[a / Processus normal 7](#_Toc523929779)

[b / Dérogations possibles et situations exceptionnelles 7](#_Toc523929780)

[2 ) Processus général d’attribution des habilitations 7](#_Toc523929781)

[a / Processus normal 7](#_Toc523929782)

[b / Dérogations possibles et situations exceptionnelles 7](#_Toc523929783)

[V . Logigramme décrivant le processus 8](#_Toc523929784)

[VI . Audit du système de gestion des habilitations 8](#_Toc523929785)

[VII . Lexique 8](#_Toc523929786)

[i - Habilitation 8](#_Toc523929787)

[VIII . Annexe 1 : Exemple de Matrice de rôle 9](#_Toc523929788)

[IX . Annexe 2 : exemple de processus de définition des habilitations 10](#_Toc523929789)

[X . Annexe 3 : exemple de processus d’attribution de habilitations 12](#_Toc523929790)

[1 ) Processus normal 12](#_Toc523929791)

[2 ) Dérogations possibles et situations exceptionnelles 13](#_Toc523929792)

[XI . Annexe 4 exemple de politique contrôle régulier des habilitations et des autorisations 15](#_Toc523929793)

# Description du document

Le présent document décrit les modalités d’accès au SI de l’[organisme] et la déclinaison opérationnelle nécessaire pour gérer les habilitations du SI. Il a été élaboré à partir des documents suivants :

• « Guide pratique de gestion des habilitations d’accès au SI » ; ASIP Santé, version 0.2 05/2016

# Introduction

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 document 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].

La sécurité du SI impose 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 des services techniques, imprimantes, serveurs informatiques, équipements réseau…)
* l’accès aux fonctions d’administration et de paramétrage de ces mêmes équipements, dont le paramétrage des équipements techniques (CTA,..) ;
* 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.

## 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 ;
* 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).

## Principes de gestion des 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

# Règles applicable au SI

Le tableau ci-dessous regroupe l’ensemble des mesures mise en place pour assurer l’opérationnalité du processus de gestion des habilitations au SI :

|  |  |  |
| --- | --- | --- |
| **Id** | **Définition** | **exemple** |
| R1 | L’identification des acteurs du SI est basé sur le Matricule des [agents/salariés] définit par le logiciel de gestion ressources humaines. |  |
| R2 | Modalité technique mis en œuvre pour l’authentification : utilisation de token physique, login/mdp |  |
| R3 | l’identification des ressources se fait grâce au référentiel de structure disponible [ICI] |  |
| R4 | L’attribution des habilitations se fait sur la base de profil définit dans des matrices de droits accessibles décliné par application et métier [ICI] |  |
| R5 | L’attribution des droits des utilisateurs est effectuée par des gestionnaires de droits dont la désignation a été décrite dans [ce document] en fonction des pôles d’organisation de l’organisme |  |
| R6 | La validation d’attribution de droits à un utilisateur doit systématique être validé par un gestionnaire lors : d’une arrivée, d’une mutation ou d’un départ de collaborateurs |  |

# Description du processus

## 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).*

### 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).*

### 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.*

# Logigramme décrivant le processus

# Audit du système de gestion des habilitations

*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. Il convient également de mettre en place des indicateurs de vérification (ex NB utilisateur/ NB salariés).*

Afin de contrôler les accès en place sur le SI des extractions régulières [préciser la fréquences] sont effectuées. Il est ainsi vérifier de façon discrétionnaire et aléatoire que les matrices sont respectés et opérationnelles.

# Lexique

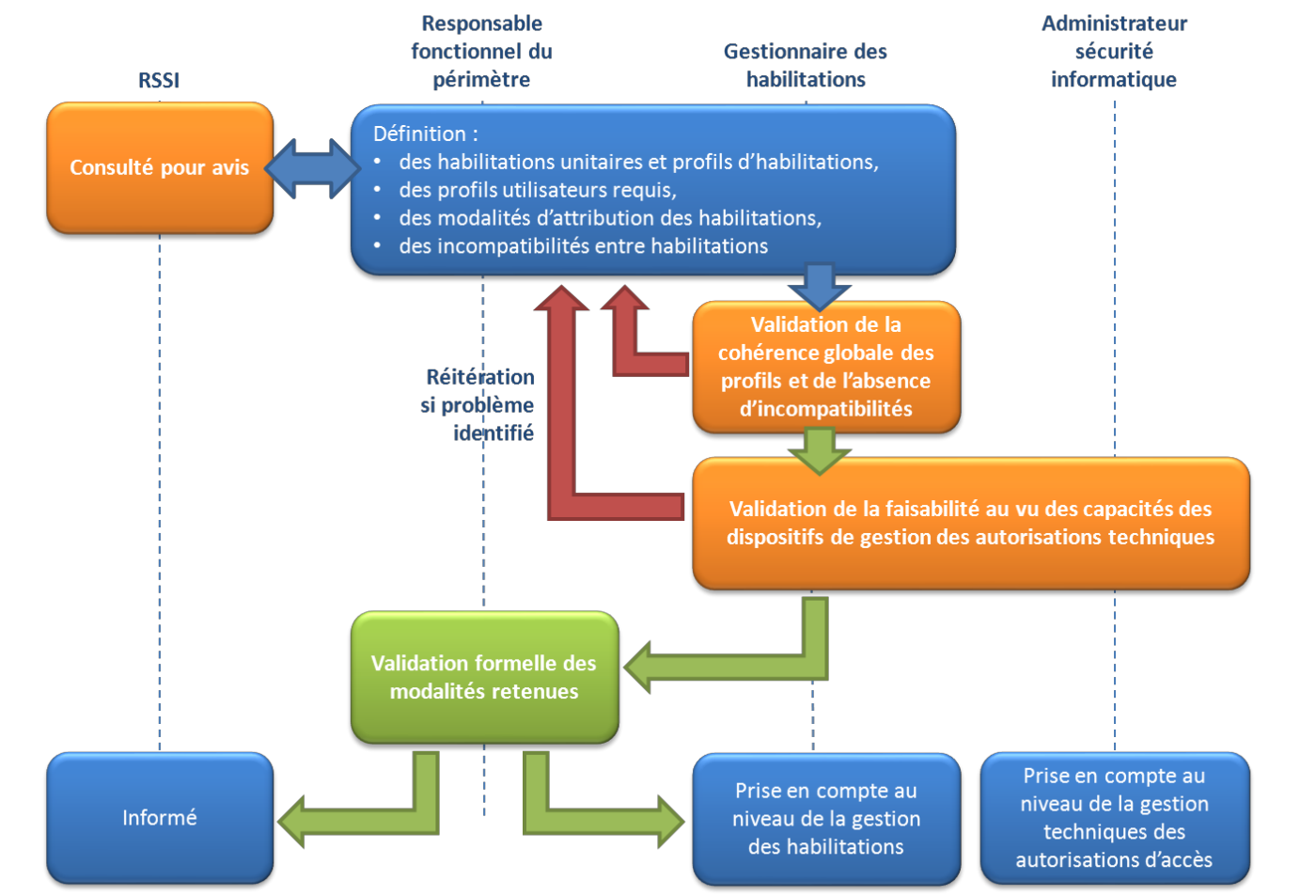
#### Habilitation

Dans le cadre de la PGSSI, 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.

# Annexe 1 : Exemple de Matrice de rôle

|  |  |
| --- | --- |
| **Fonction** | **Activités dans le processus** |
| **Directeur** | Valide les modalités, le déroulement, les acteurs et les rôles du processus de gestion des habilitations. |
| **Responsables de périmètre**  **fonctionnel (DRH,..)** | 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. |

# Annexe 2 : exemple de processus de définition des habilitations

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.

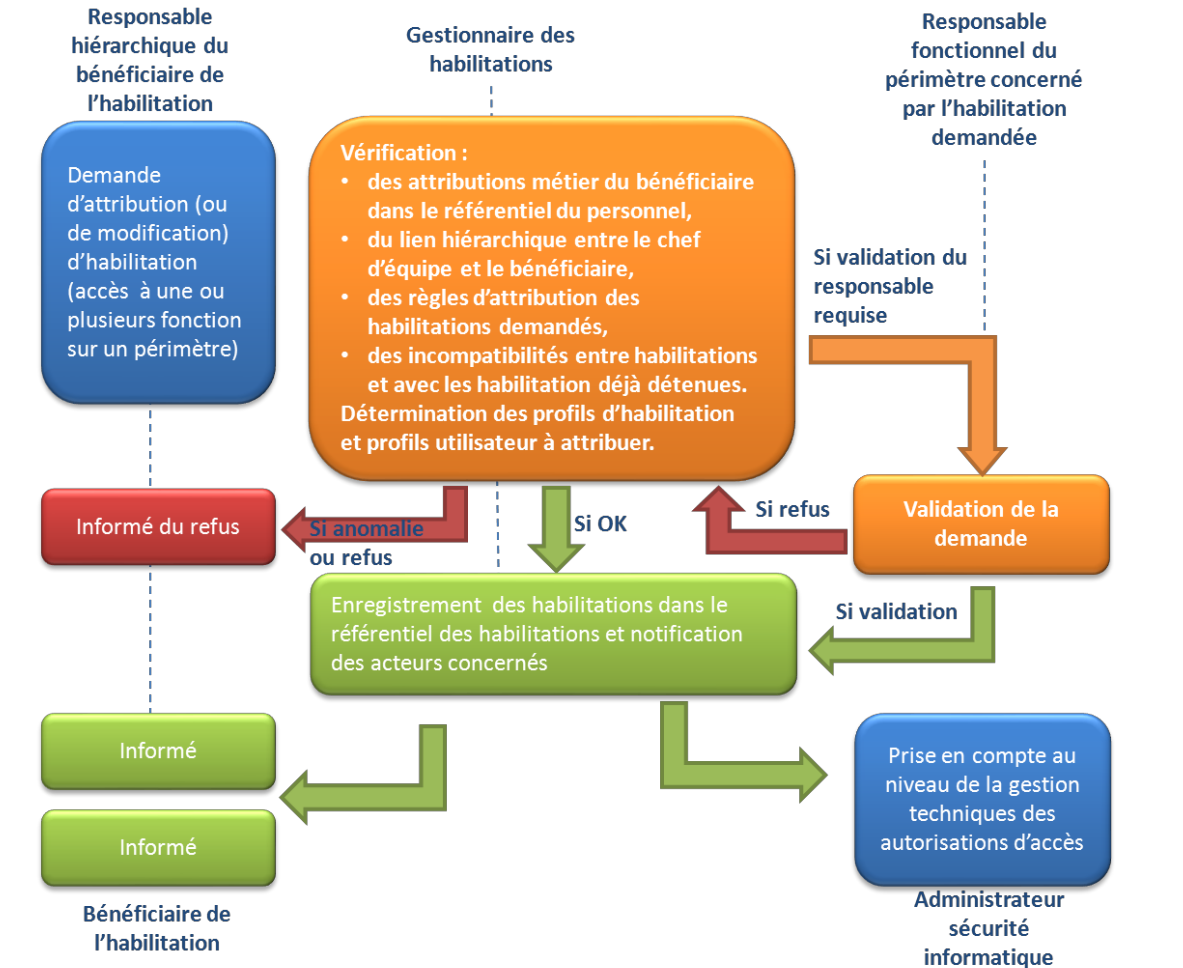
Le gestionnaire des habilitations vérifie la cohérence des profils utilisateurs, s’assure de l’absence d’introduction de combinaisons d’habilitations incompatibles, vérifie avec le responsable avec l’administrateur sécurité informatique en charge du paramétrage des droits d’accès pour la ressource concernée, 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.

# Annexe 3 : exemple de processus d’attribution de 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.

**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**

Pour toute ressource qui ne participe pas au traitement d’information de santé à caractère personnel, le directeur (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.

# Annexe 4 exemple de politique 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.

