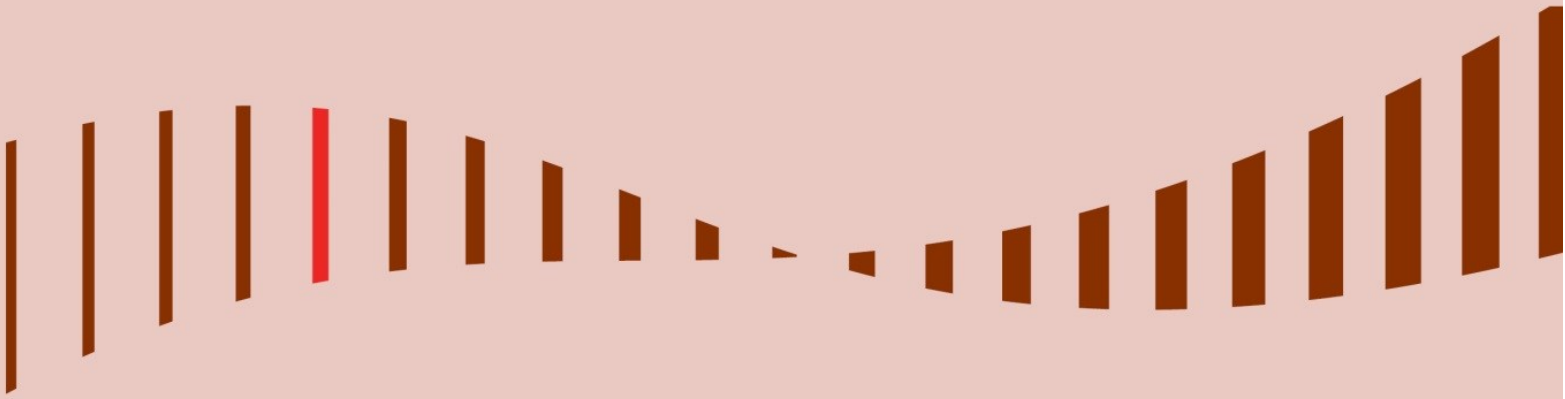
Grille d'applicabilité des référentiels de la PGSSI-S

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) - Mai 2015 - V1.0



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES,
DE LA SANTÉ
ET DES DROITS DES FEMMES

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Sommaire

1 Objet du document

Le présent document expose les logiques d'application des référentiels de la PGSSI-S suivants:

- le référentiel d'identification des acteurs sanitaires et médico-sociaux ;
- le référentiel d'authentification des acteurs de santé ;
- le référentiel d'imputabilité.

Ces logiques sont déclinées selon les contextes d'application de chaque référentiel. Elles constituent un retour du groupe de travail PGSSI-S sur l'application des référentiels et peuvent constituer une aide à la rédaction d'arrêtés rendant opposables ces référentiels.

2 Applicabilité des référentiels

2.1 Logique d'applicabilité

Bien que toutes les situations puissent être spécifiques, il est possible d'identifier de manière générale des paliers minimum à mettre en œuvre en fonction des caractéristiques des contextes d'application métier. Ces paliers sont bien des paliers minimum qui, pour chaque Système d'Information de Santé (SIS), pourront être réévalués à la hausse en fonction de spécificités liées au SIS (ex. contraintes règlementaires spécifiques, risques particuliers…). En tout état de cause, toute particularité doit faire l'objet d'une analyse de risques spécifique pour évaluer la nécessité de réévaluer le palier cible pour chacun des référentiels.

2.2 Les différents contextes considérés

Les contextes d'application pris en compte sont :

- Contexte 1 : exercice individuel pour lequel les accès au système d'information sont sous le contrôle du professionnel de santé (ex. cabinet libéral) ;
- Contexte 2 : exercice collectif pour lequel les accès au système d'information sont chacun sous le contrôle d'un utilisateur (ex. cabinet de groupe) ;
- Contexte 3 : exercice collectif pour lequel au moins une partie du système d'information est mutualisée entre plusieurs utilisateurs (ex. hôpital, pharmacie) ;
- Contexte 4 : téléservices avec enregistrement préalable des utilisateurs (ex. site marchand) ;
- Contexte 5 : téléservices sans enregistrement préalable des utilisateurs (ex. DMP, E-fit) ;
- Contexte 6 : documents de santé électroniques[1] quand ils sont amenés à sortir du SIS producteur pour échange ou mise en partage (ex. compte rendu d'examen de biologie médicale envoyé par messagerie sécurisée, partage de plan personnalisé de santé…).

Ces contextes sont basés sur des caractéristiques génériques discriminantes du point de vue de la sécurité. Ils ne correspondent pas directement à des systèmes d'information en particulier, Un système d'information peut notamment présenter des caractéristiques correspondant à plusieurs contextes. Le palier à mettre en œuvre est alors le palier le plus élevé parmi les paliers minimums correspondant aux contextes applicables Néanmoins, pour

[1] pris en tant qu'ensemble de données associées durablement les unes aux autres et qui sont stockées, échangées, diffusées ou partagées ensemble quel que soit le médium utilisé. Il est à noter que certaines données ne sont pas identifiées a priori comme ayant vocation à être sorties du système d'information lors de leur production mais peuvent être amenées à l'être ultérieurement (par exemple suite à une demande patient d'accès à ses données). Dans ce cas, c'est bien à l'opération de constitution du document que sont appliqués les référentiels et non à la production initiale des données qui elle est traité comme partie intégrante du contexte du SIS dans le cadre duquel elles sont produite.

des raisons de coût de mise en œuvre, il est possible de séparer le système d'information en sous-ensembles cohérents correspondant à un nombre réduit de contextes et d'appliquer des paliers différencié selon les sous-ensembles.

2.3 Applicabilité du référentiel d'identification des acteurs sanitaires et médico-sociaux

Pour des raisons de lisibilité, le périmètre des paliers identifiés n'est pas repris dans le tableau. Pour référence, une synthèse des différents paliers du référentiel est fournie dans la section 4.1 de l'annexe 1.

Contexte	Palier d'identification minimum
Contexte 1 : exercice individuel pour lequel les accès au système d'information sont sous le contrôle du professionnel de santé	Palier 1
Contexte 2 : exercice collectif pour lequel les accès au système d'information sont chacun sous le contrôle d'un utilisateur	Palier 1
Contexte 3 : exercice collectif pour lequel au moins une partie du système d'information est mutualisée entre plusieurs utilisateurs	Palier 1
Contexte 4 : téléservices avec enregistrement préalable des utilisateurs	Palier 1
Contexte 5 : téléservices sans enregistrement préalable des utilisateurs	Palier 2
Contexte 6 : documents de santé électroniques quand ils sont amenés à sortir du SIS producteur pour échange ou mise en partage	Palier 2 (notamment pour l'identification de l'auteur)

2.4 Applicabilité du référentiel d'authentification des acteurs de santé

Pour des raisons de lisibilité, le périmètre des paliers identifiés n'est pas repris dans le tableau. Pour référence, une synthèse des différents paliers du référentiel est fournie dans la section 4.2 de l'annexe 1.

Contexte	Type d'authentification	Palier d'authentification minimum	Dispositions complémentaires
Contexte 1 : exercice individuel pour lequel les accès au système d'information sont sous le contrôle du professionnel de santé	privée	Palier 1	
Contexte 2 : exercice collectif pour lequel les accès au système d'information sont chacun sous le contrôle d'un utilisateur	privée	Palier 1	
Contexte 3 : exercice collectif pour lequel au moins une partie du système d'information est mutualisée entre plusieurs utilisateurs	privée	Palier 2	Palier 1 possible associé avec des dispositions de protection d'accès physique et logique aux éléments du SI (postes, serveurs, réseau)
Contexte 4 : téléservices avec enregistrement préalable des utilisateurs	privée	Palier 1 à 2	En fonction de la sensibilité du service évaluée par le responsable de traitement (ex. palier 1 pour des données générales et palier 2 pour des données de santé à caractère personnel)
Contexte 5 : téléservices sans enregistrement préalable des utilisateurs	publique	Palier 2 à 3	En fonction de la sensibilité du service évaluée par le responsable de traitement (ex. palier 2 pour des données générales et palier 3 pour des données de santé à caractère personnel)
Contexte 6 : documents de santé électroniques quand ils sont amenés à sortir du SIS producteur pour échange ou mise en partage	privée	Palier 1	Pour les aspects imputabilité de l'élaboration. Sauf prérequis supérieur pour la traçabilité embarquée (cf. section 2.5), en l'occurrence, palier 3 de l'authentification publique pour une mise en œuvre du palier 4 de l'imputabilité.

2.5 Applicabilité du référentiel d'imputabilité

Pour des raisons de lisibilité, le périmètre des paliers identifiés n'est pas repris dans le tableau. Pour référence, une synthèse des différents paliers du référentiel est fournie dans la section 4.3 de l'annexe 1.

Contexte	Palier d'imputabilité minimum	Dispositions complémentaires
Contexte 1 : exercice individuel pour lequel les accès au système d'information sont sous le contrôle du professionnel de santé	Palier 1	
Contexte 2 : exercice collectif pour lequel les accès au système d'information sont chacun sous le contrôle d'un utilisateur	Palier 2	
Contexte 3 : exercice collectif pour lequel au moins une partie du système d'information est mutualisée entre plusieurs utilisateurs	Palier 2	
Contexte 4 : téléservices avec enregistrement préalable des utilisateurs	Palier 2 à 4	En fonction de la sensibilité du service évaluée par le responsable de traitement (ex. palier 2 pour la consultation de données générales et palier 4 pour la modification de données de santé à caractère personnel)
Contexte 5 : téléservices sans enregistrement préalable des utilisateurs	Palier 2 à 5	En fonction de la sensibilité du service évaluée par le responsable de traitement (ex. palier 2 pour la consultation de données générales et palier 5 pour la modification de données de santé à caractère personnel)
Contexte 6 : documents de santé électroniques quand ils sont amenés à sortir du SIS producteur pour échange ou mise en partage	Palier 2 à 5	Palier 2 pour les documents ne nécessitant pas de traçabilité embarquée. Traçabilité embarquée via signature électronique sous forme : • soit de scellement faisant référence au SI d'origine (auquel cas le palier minimum pour l'authentification est le palier 1 de l'authentification privée) – Palier 4 de l'imputabilité ; • soit de signature utilisateur faisant référence à un utilisateur du SI d'origine (auquel cas le palier minimum pour l'authentification est le palier 3 de l'authentification publique) – palier 5 de l'imputabilité. Charge au SI d'origine d'assurer en interne la piste d'audit des opérations qui ont menées à la création et à la sortie du document du SI.

Note : Pour les documents identifiés dans la loi comme devant être signés, la règlementation européenne implique que cela soit réalisé avec une signature électronique présumée fiable (i.e. à base de certificats qualifiés sur un dispositif de création de signature sécurisé…). En pratique, la combinaison des rares éléments actuellement disponibles sur le marché pour répondre à l'ensemble des conditions de génération de signature présumée fiable au regard des exigences fixées par la loi n°2000-230 du 13 mars 2000 et précisée par le décret n°2001-272 du 30 mars 2001 est trop complexe pour être opérationnelle dans le contexte des SIS.
Dans l'attente de cette capacité, il est proposé pour ces documents que l'application du référentiel d'imputabilité soit complétée d'un prérequis d'authentification publique au palier 3 (y compris pour un scellement) ainsi que d'une convention de preuve entre le SI d'origine et la personne physique ou morale accédant au document. Cette convention de preuve peut être contractée :

- soit antérieurement à l'accès au document (ex. convention de preuve signée entre deux institutions avant la mise en œuvre d'un système de gestion de documents partagé) ;
- soit concomitamment à l'accès au document (ex. intégration de la convention de preuve à la pièce jointe d'une diffusion par mail d'un document et référence à cette convention dans la signature électronique).

3 ANNEXE 1 – Tableaux de synthèse des paliers

Les paliers définis en l'état (avant concertation publique) pour chacun des référentiels sont rappelés dans les sections suivantes.

3.1 Référentiel d'identification des acteurs sanitaires et médico-sociaux

<table>
<tr><th colspan="2"></th><th>Palier 1</th><th>Palier 2</th><th>Palier 3</th></tr>
<tr><td rowspan="2">Personne physique</td><td>Enregistrée dans un référentiel d'identité national en lien avec le domaine sanitaire et médico-social</td><td><u>Identification locale :</u>
identifiant « privé » avec possibilité de plusieurs identifiants « privés » par personne
<u>Identification nationale :</u>
identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</td><td colspan="2"><u>Identification locale ou nationale :</u>
identifiant « public » (RPPS ou ADELI)</td></tr>
<tr><td>Non enregistrée dans un référentiel d'identité national en lien avec le domaine sanitaire et médico-social</td><td><u>Identification locale :</u>
identifiant « privé » avec possibilité de plusieurs identifiants « privés » par personne
<u>Identification nationale :</u>
identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</td><td colspan="2"><u>Identification locale :</u>
identifiant « privé » unique
<u>Identification nationale :</u>
identification indirecte (identifiant « public » de la personne morale + identifiant « privé » de la personne physique)</td></tr>
<tr><td colspan="2">Personne morale</td><td>Non applicable</td><td><u>Identification locale ou nationale :</u>
identifiant « public » (FINESS EJ, FINESS ET, SIREN ou SIRET) y compris identifiant opérationnel de portée national (RPPS-rang ou ADELI-rang)</td><td><u>Identification locale ou nationale :</u>
identifiant « public » (FINESS EJ, FINESS ET, SIREN ou SIRET)</td></tr>
</table>

3.2 Référentiel d'authentification des acteurs de santé

<table>
<tr><th colspan="2"></th><th>Palier 1</th><th>Palier 2</th><th>Palier 3</th></tr>
<tr><td rowspan="3">Authentification « publique » des personnes physiques</td><td>Directe</td><td></td><td>Certificat logiciel de personne physique</td><td>• Carte de la famille CPx 
ou
• Dispositifs alternatifs : Mot de passe à usage unique (OTP SMS / Mail / Push)</td></tr>
<tr><td rowspan="2">Architecture d'authentification</td><td rowspan="2"></td><td>Authentification indirecte :
• Authentification « publique » de la personne morale 
• Identification de portée nationale ou locale de la personne physique
• Authentification « privée » de la personne physique</td><td></td></tr>
<tr><td></td><td>Authentification par délégation :
• Authentification « publique » de la personne morale 
• Identification de l'acteur de santé de portée nationale
• Authentification « publique » de la personne physique
• Exigences de sécurité imposées par le système d'information cible</td></tr>
<tr><td>Authentification « privée » des personnes physiques</td><td>Directe</td><td>Authentification basée sur un couple [identifiant individuel / mot de passe]
Identification de l'acteur de santé de portée nationale ou locale.
Contraintes pour la construction des mots de passe (cf. Recommandations de sécurité relatives aux mots de passe – Réf 3).</td><td>Tout dispositif d'authentification forte, au choix et sous la responsabilité du directeur d'Etablissement.
Identification de l'acteur de santé de portée nationale ou locale.</td><td>Authentification selon les mêmes modalités que pour le palier 3 de l'authentification « publique » des personnes physiques.</td></tr>
<tr><td colspan="2">Authentification « publique » des personnes morales</td><td></td><td>Certificat serveur 
Référence à la personne morale responsable du serveur et identifiée dans le certificat. L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).</td><td>Certificat logiciel de personne morale 
L'identifiant de la personne morale utilisé est national (FINESS, SIRET / SIREN).</td></tr>
</table>

3.3 Référentiel d'imputabilité

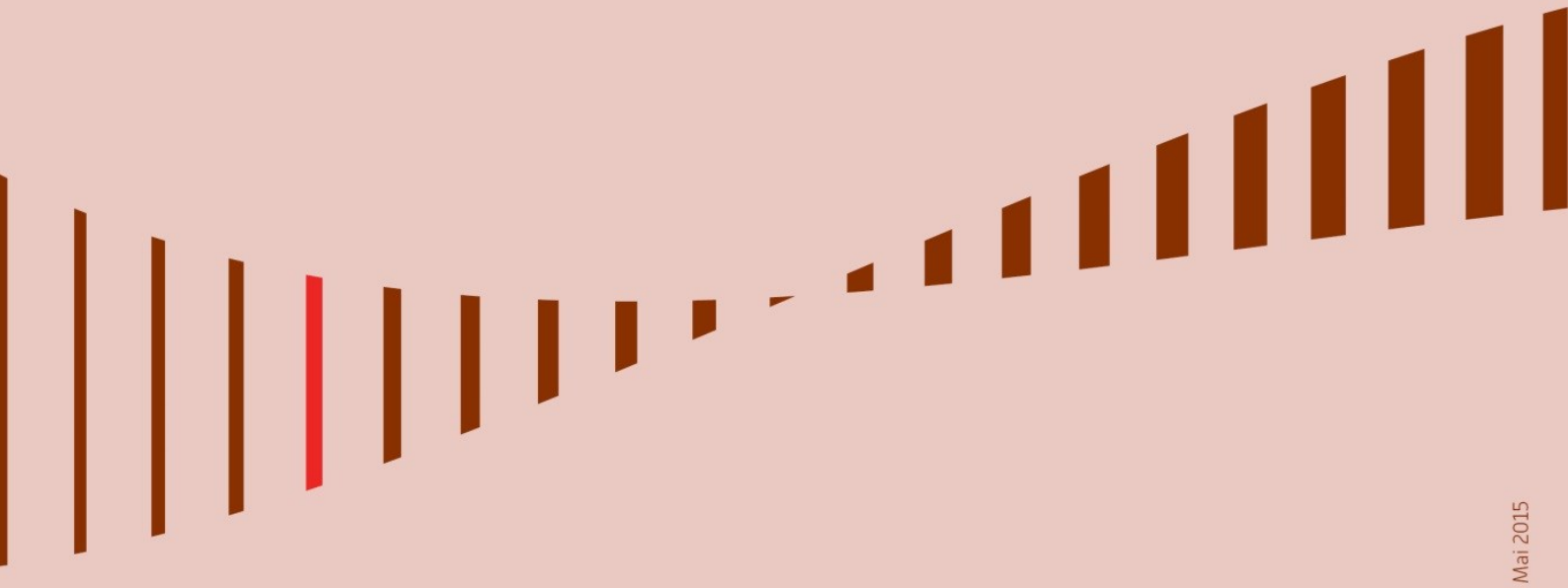
<table>
<tr><th>Paliers</th><th>Prérequis</th><th>Génération de la piste d'audit</th><th>Conservation des traces</th><th>Restitution de la piste d'audit</th><th>Documentation spécifique</th></tr>
<tr><td>1</td><td rowspan="3">• Palier 1 du référentiel d'identification et d'authentification
• Gestion dans le temps des identités, des rôles et des habilitations
• Heure partagée par l'ensemble des composants du SIS</td><td>• Traces fonctionnelles</td><td>• Possibilité d'extraction des traces pour conservation dans des endroits multiples pour réduire le risque de modifications systémiques</td><td rowspan="2">• Outil de gestion de la preuve permettant la restitution ergonomique des traces fonctionnelles utilisable par des non spécialistes de la sécurité</td><td>• Documentation des dispositifs d'authentification, de gestion des identités, des rôles, des habilitations et des traces</td></tr>
<tr><td>2</td><td rowspan="2">• Traces fonctionnelles
• Traces techniques provenant d'au moins un type de composant du SIS</td><td>• Archives journalières regroupant l'ensemble des traces</td><td>• Idem palier 1 +
• Description des sources des traces et des processus mis en œuvre de la génération à la constitution de l'archive journalière</td></tr>
<tr><td>3</td><td rowspan="2">• Scellement quotidien des traces</td><td rowspan="3">• Idem palier 1 +
• L'outil de gestion de la preuve permet de réconcilier les traces autant que de besoin
• L'outil de gestion de la preuve gère un format pivot ou gère de nombreux formats de traces
• Guide didactique d'utilisation de l'outil de gestion de la preuve</td><td>• Idem palier 2 +
• Description des processus mis en œuvre de la génération à la réconciliation</td></tr>
<tr><td>4</td><td>• Idem palier 2 +
• Au moins un élément de traçabilité discrète basé sur un scellement serveur</td><td rowspan="2">• Idem palier 3 +
• Documentation de la mise en œuvre de la signature électronique</td></tr>
<tr><td>5</td><td>• Idem palier 1 +
• Mise en œuvre d'un processus d'authentification générant une signature électronique</td><td>• Continuité totale de la piste d'audit par réconciliation de l'ensemble des traces fonctionnelles et techniques et au moins un élément de traçabilité discrète basé sur une signature utilisateur</td><td>• Mise en œuvre du scellement et de l'horodatage de ce scellement des traces</td></tr>
</table>

4 ANNEXE 2 - Glossaire

Sigle / Acronyme	Signification
DMP	Dossier Médical Personnel
EHPAD	Etablissement d'hébergement pour personnes âgées dépendantes
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
SCM	Société Civile de Moyen
SIS	Système d'Information de Santé

5 ANNEXE 3 – Documents de référence

Référence n°1 : PGSSI-S Référentiel d'identification des acteurs sanitaires et médico-sociaux.
Référence n°2 : PGSSI-S Référentiel d'authentification des acteurs de santé.
Référence n°3 : PGSSI-S Référentiel d'imputabilité.



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES,
DE LA SANTÉ
ET DES DROITS DES FEMMES

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr