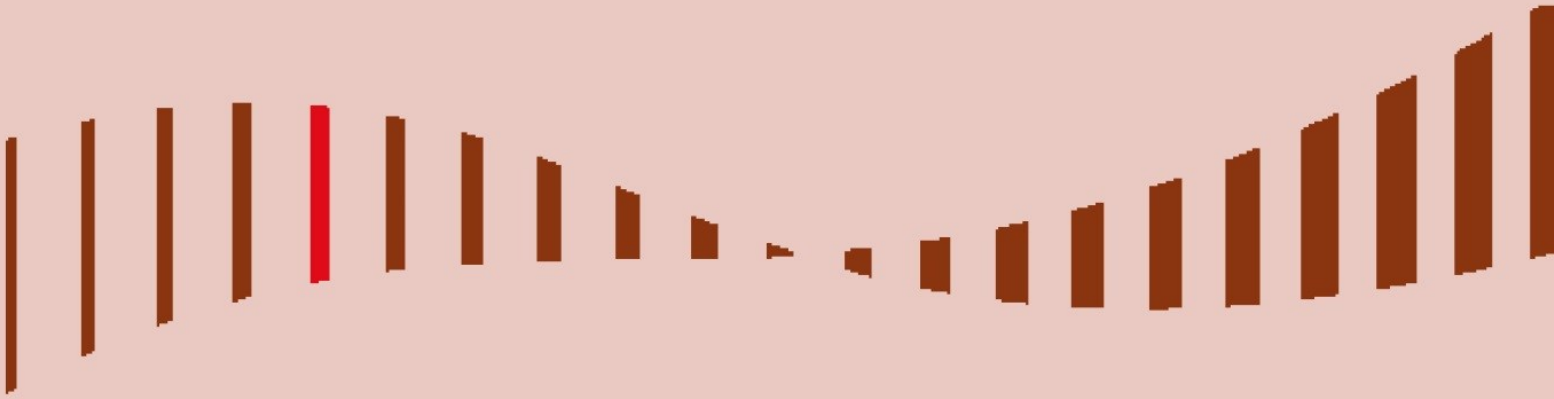
Guide pratique
Règles pour la mise en place d'un accès web au SIS pour des tiers

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) - Janvier 2016 - 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 Introduction

1.1 Objet du document

Le présent document définit les règles et les recommandations de sécurité relatives à la mise en place d'accès web au profit de tiers au sein d'un Système d'Information de Santé (SIS).

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

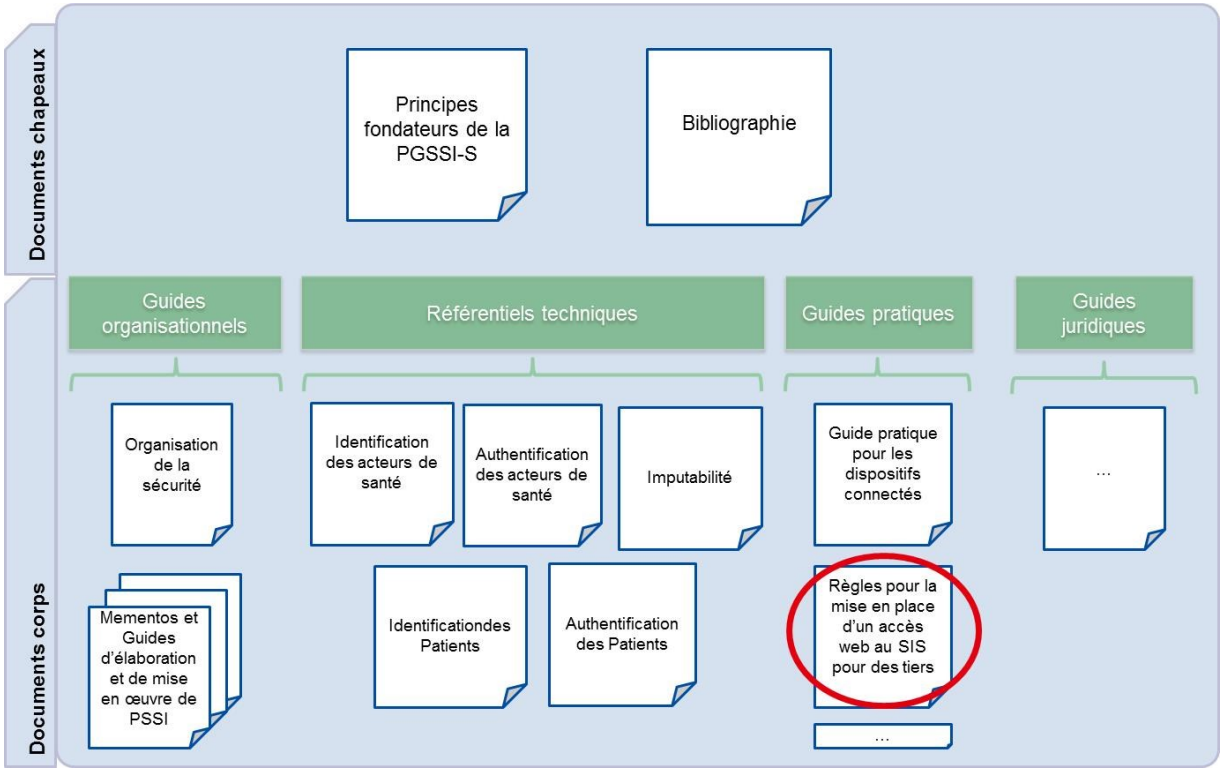


Figure 1 : Place du guide dans le Corpus documentaire de la PGSSI-S

Ce guide présente un ensemble de règles permettant de mettre en place, un niveau de protection minimum des données traitées par le SIS lorsque celui-ci fait l'objet d'accès Web par des tiers.

Les préconisations sont issues des bonnes pratiques en matière de Sécurité des Systèmes d'Information (SSI) et visent à traiter les principales vulnérabilités identifiées dans les documents de référence[1] par des experts du domaine de la sécurisation web tels que l'Agence Nationale de la Sécurité des systèmes d'Information (ANSSI) et la communauté Open Web Application Security Project (OWASP). Elles concernent les phases de construction et de fonctionnement des services exposés.

Il est rappelé que les structures publiques qui mettent en œuvre des services en ligne tels que des accès web doivent se conformer dans tous les cas au Référentiel Général de Sécurité [Réf. n°6].

[1] Ces documents de référence sont présentés plus loin.

Le guide s'adresse :

- aux responsables de structure qui, en tant que responsables de traitement, décident de la mise en œuvre des accès tiers à leur SIS dans le respect des finalités de l'application ;
- aux personnes qui agissent sous leur responsabilité, et en particulier celles impliquées dans :
    - la conception et la réalisation de l'application,
    - l'hébergement et l'exploitation de l'application,
    - la mise en œuvre de la sécurité des SIS.

Dans la suite du document, le terme générique « Responsable » est utilisé pour identifier toute personne en charge de la mise en œuvre de règles présentées dans le document, qu'elle soit la personne responsable de la structure ou une personne agissant sous sa responsabilité. Le rôle de Responsable est à distinguer de celui de responsable de traitement tel que défini dans la Loi Informatique et Libertés n°78-17 du 6 janvier 1978 modifiée bien que ces rôles puissent être tenus par une même personne.

Un glossaire en fin de document donne la signification des acronymes et de certains termes techniques utilisés.

1.2 Définitions

1.2.1 Service en ligne

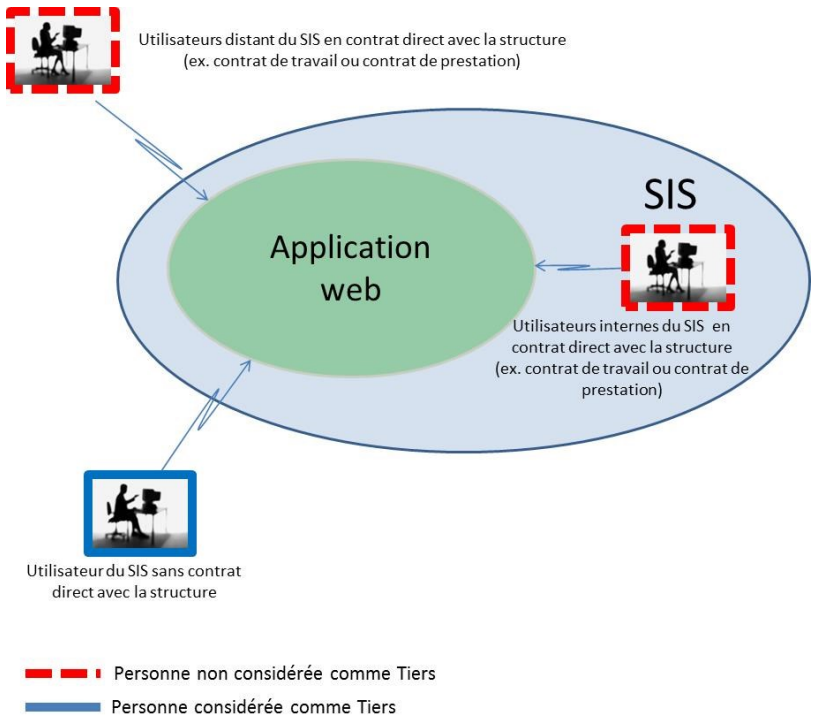
Dans le cadre de la PGSSI-S, le terme « service en ligne » désigne un service d'accès via Internet à des données et traitements mis à disposition par le SIS.

1.2.2 Application web

Dans le cadre de la PGSSI-S, un ou plusieurs services en ligne offerts à des tiers par le SIS constituent une application web.

1.2.3 Tiers

Le terme « tiers » désigne les patients et, de manière générale, toute personne que le Responsable autorise à accéder à des services en ligne fournis par le SIS, sans que ce Responsable n'ait de maîtrise sur l'environnement, le contexte d'utilisation ou les moyens mis en œuvre du côté de l'utilisateur.



1.3 Champ d'application du guide

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

Le cartouche ci-après présente de manière synthétique le périmètre 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						

Pour l'ensemble de ces périmètres, le présent guide décrit les règles applicables à l'accès de tiers aux SIS via application web.

Périmètre de système concerné : l'application web

Ce guide ne concerne que les accès web à des services offert par le SIS : les applications web considérées sont celles qui permettent à des tiers d'accéder (au sens large : lire, modifier, déposer, extraire, etc.) à des données de santé à caractère personnel (par exemple relatives au parcours de soins : prise de rendez-vous dans un cabinet ou un établissement de santé, consultation de résultats d'examens de biologie médicale, etc.), médico-économiques (par exemple relatives à de la facturation de soins ou de services complémentaires), ou de façon plus générale à des données à caractère personnel ou à des données sensibles, quelle que soit la finalité de cette application.

Dans la mesure où ces applications web traitent de telles données, elles sont considérées comme faisant partie d'un SIS.

La sécurité des applications web doit être prise en compte dans les phases de construction (conception et réalisation), de fonctionnement (hébergement et exploitation) et de fin de vie (migration ou arrêt définitif) des services en ligne.

Périmètre des utilisateurs concerné :

Ce guide ne concerne que les accès à des applications par des tiers[2].

Dans la pratique, et selon les cas, ces tiers peuvent être :

- des usagers des services proposés par l'établissement de santé (ex. : patients, proches de patient, fournisseurs…) ;
- des PS extérieurs à l'établissement de santé, qui n'ont pas de lien juridique direct (contrat ou autre) avec la structure et qui concourent à la prise en charge de patients.

Les accès en mobilité par des personnes disposant d'un lien juridique direct avec la structure sont, de fait, exclus du périmètre du document.

Limites du champ d'application du guide :

[2] Voir définition plus haut, au 1.2.3

Les autres modalités d'accès à des services ou données du SIS n'entrent pas dans le périmètre du guide (ex. : demande de dossier médical émanant de patient, représentant légal, ayant-droit, réquisition et plus généralement toute demande faite par écrit faisant l'objet d'une extraction réalisée par le Responsable et transmise au demandeur quel que soit le média utilisé pour cette transmission).

Les sites web proposant des services de télémédecine, de téléconseil ou de commerce en ligne sont également exclus du présent guide. Ils présentent en effet certains enjeux et risques spécifiques du fait de leurs fonctions et des technologies mises en œuvre, et requièrent des mesures de sécurité complémentaires qui ne sont pas présentées ici. Les règles proposées dans le présent guide restent néanmoins applicables et peuvent servir de base de travail pour la sécurisation de ce type de sites.

Le cas des interventions réalisées à distance sur le SIS n'entre pas dans le champ de ce guide. Il est traité dans le guide pratique spécifique « Règles pour les interventions à distance sur les Systèmes d'Information de Santé (SIS) » [Réf. n°5.5].

1.4 Enjeux relatifs aux accès au SIS par des tiers via une application web

1.4.1 Cadre de l'accès au SIS par des tiers

L'article L. 1111-7 du code de la santé publique dispose que « *Toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels et établissements de santé, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment des résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé* […] ». L'accès des titulaires de l'autorité parentale et des ayants droit est réglementé.

Il appartient au Responsable de mettre en place des procédures respectant la réglementation en vigueur dans le cas où l'accès à son dossier médical par le patient ou les personnes autorisées de son entourage se fait au moyen d'un accès tiers au SIS.

1.4.2 Multiplication des applications web liées aux données de santé à caractère personnel

Les services en ligne se développent de plus en plus dans le secteur de la santé.

L'ouverture d'un accès tiers à un SIS peut avoir plusieurs finalités :

- La communication d'informations à l'usager du système de santé, et en particulier données de santé lorsque celui-ci est patient de la structure ou personne autorisée (ex. : tuteur légal). Ce type d'accès autorise par exemple la dématérialisation qui permet une transmission rapide et évite l'envoi d'un courrier postal ou le déplacement de l'usager. Cette catégorie inclut notamment les serveurs de résultats pour les examens de biologie médicale.
- L'ouverture de services à destination des patients ou de personnes autorisées. Ce type d'accès permet par exemple d'améliorer l'efficacité de certains processus de prise en charge. Cette catégorie regroupe des services tels que la prise de rendez-vous en ligne, le rappel de certaines actions que le patient doit effectuer, les conseils personnalisés, la saisie d'informations en vue d'une hospitalisation.
- L'ouverture de services à destination de PS extérieurs à l'établissement de santé concourant à la prise en charge du patient. Ce type d'accès permet par exemple au PS d'accéder à un espace collaboratif de prise en charge du patient ou de visualiser des informations de soin concernant son patient. Cette catégorie inclut des services tels que l'imagerie médicale utile à la production de soins et n'ayant pas vocation à être intégré dans un outil de coordination des soins tel que le DMP.

1.4.3 Cadre juridique relatif au traitement des données de santé à caractère personnel

Le cadre législatif et réglementaire impose le respect de règles précises dès lors que sont traitées des données à caractère personnel, et en particulier quand elles sont traitées informatiquement. Ces règles sont d'autant plus contraignantes que ces données ont trait à la santé d'un patient et sont ainsi soumises au secret professionnel.

Le présent guide est notamment établi pour aider les acteurs concernés à respecter les obligations légales applicables au traitement informatisé des données de santé à caractère personnel, en particulier certaines exigences de la loi informatique et libertés et du code de la santé publique en matière de protection des données des patients en confidentialité et en intégrité.

Toutefois, le guide ne constitue qu'une aide et son application n'exonère pas des obligations en vigueur.

Il appartient à chaque responsable d'un traitement qui met en œuvre une application web d'identifier les lois et règlements applicables et de s'y conformer.[3]

Il est rappelé que la communication au patient de certaines informations doit parfois respecter un processus spécifique. En particulier, quand l'information communiquée entre dans le cadre du dispositif d'annonce, une consultation d'annonce doit impérativement précéder la mise à disposition des données de santé et du diagnostic.

1.4.4 Risques liés à la mise en œuvre d'accès de tiers aux données de santé du SIS

Les accès web constituent, par nature, des points d'entrée très exposés du système d'information. Leur sécurisation revêt une grande importance au regard des différents types d'atteintes au SIS induites par l'exploitation potentielle des vulnérabilités des services web par des personnes malintentionnées :

- atteinte à l'intégrité des informations (modifications illégitimes des données de santé à caractère personnel, des données de rendez-vous médical, …), en particulier lorsqu'elle a pour effet d'impacter les processus de prise en charge des patients ;
- atteinte à la confidentialité des données à caractère personnel du patient (divulgation au-delà de l'équipe de soins, voire divulgation publique) ;
- atteinte à la disponibilité des services proposés aux patients, en particulier lorsqu'elle est susceptible d'impacter les processus internes de la structure offrant le service (blocage du système de prise de rendez-vous du patient en ligne par exemple) ou de dégrader la prise en charge des patients ;
- atteinte à l'auditabilité des opérations réalisées sur les données de santé (absence de traces d'accès ou de modification des données, modification intempestive de ces traces...).

L'exploitation de vulnérabilités par des personnes malveillantes peut en outre conduire à l'intrusion dans le SIS ou dans les terminaux des tiers qui y accèdent, et à la propagation d'incidents de sécurité à ces systèmes.

La mise en œuvre de l'application web sur une plate-forme indépendante permet de limiter le risque de propagation au reste du SIS.

1.5 Remarque préalable

La conception, la réalisation et l'exploitation de services d'accès web au SIS ouvert aux tiers qui respectent les exigences de sécurité liées aux données de santé personnel nécessitent la mobilisation de moyens notables.

Aussi, dès lors qu'un tel projet est étudié, il est fortement recommandé de vérifier s'il existe déjà un service mutualisé en mesure de remplir les fonctions attendues.

Par exemple, s'il s'agit de conservation d'informations utiles à la coordination des soins, l'alimentation du Dossier Médical Personnel (DMP) du patient ou la transmission directe via une messagerie sécurisée telle que MSSanté devraient être privilégiées. Ces services bénéficient des moyens de protection appropriés pour ce type d'informations et ne nécessitent pas la mise en place d'application web au niveau des SIS.

[3] Les exigences applicables dépendent en particulier de la nature des données, de la finalité et de la nature du traitement, de l'organisation de mise en œuvre de l'application web.

2 Présentation des documents de référence

Les principaux documents de référence sur lesquels s'appuie le présent guide sont présentés dans ce chapitre. Bien entendu, le lecteur pourra, s'il le souhaite, consulter ces documents pour approfondir les thèmes traités.

Les références précises de ces documents sont fournies en Annexe 2.

2.1 Les vingt-neuf recommandations de l'ANSSI pour sécuriser votre site web[4]

L'ANSSI a publié en août 2013 un guide de recommandations pour la sécurisation des sites web en phase de construction et de fonctionnement. Il est destiné aux développeurs et aux administrateurs de sites web. Il propose de mettre en œuvre des mesures préventives et des mécanismes permettant de détecter des tentatives d'attaque.

2.2 Le " Guide de règles et de recommandations relatives au développement d'applications de sécurité en Java "[5]

Ce document produit par l'ANSSI constitue un ensemble de bonnes pratiques de développement en java (principal langage de développement d'applications web) concernant les aspects liés à la sécurité informatique. Elles ont été élaborées à partir de l'analyse du langage et de l'architecture de la plate-forme d'exécution Java.

Les vulnérabilités exposées dans le guide sont suffisamment génériques pour ne pas être limitées aux applications développées dans ce langage. Ainsi, ces vulnérabilités ont été retenues comme base pour le présent guide, bien que ce dernier s'étende à d'autres langages que Java.

2.3 Les dix vulnérabilités de sécurité applicatives web les plus critiques[6] selon l'OWASP

La communauté Open Web Application Security Project (OWASP) publie chaque année la liste des vulnérabilités les plus critiques des applications web et propose des mesures de protection à mettre en œuvre lors du développement (document de référence n°2).

Ce document est pris comme référence par plusieurs agences nationales et organismes de sécurité.

En outre, l'OWASP met en ligne d'autres documents et outils, notamment pour tester la sécurité des applications web. Ces éléments peuvent être utilisés en complément à certaines règles du guide.

[4] http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf

[5] http://www.ssi.gouv.fr/fr/anssi/publications/publications-scientifiques/autres-publications/securite-et-langage-java.html

[6] http://www.owasp.org - (OWASP_Top_10_2013_-_French.pdf)

3 Utilisation du guide

La sécurité d'une application web se met en place dans la phase de construction comme dans la phase de fonctionnement des services en ligne qu'elle propose. Les règles de sécurité du guide intéressent l'ensemble des acteurs de ces phases.

Le guide invite tout **Responsable** :

- à mettre en œuvre les règles générales ;
- à faire respecter toutes les règles par les services chargés de la mise en œuvre en interne et/ou par les prestataires externes et à en contrôler la bonne application.

Le guide invite les **acteurs en charge de la conception, de la réalisation ou de la maintenance** d'une application web :

- à mettre en œuvre les règles liées à la conception et à la réalisation de l'application ;
- à justifier de leur bonne application auprès du Responsable.

Le guide invite les **acteurs en charge de l'hébergement ou de l'exploitation** d'une application web :

- à mettre en œuvre les règles liées à l'hébergement et à l'exploitation de l'application ;
- à justifier de leur bonne application auprès du Responsable.

Les règles sont présentées au chapitre 4.

Afin que le guide soit directement utilisable, il ne se cantonne pas aux règles spécifiques à l'accès tiers, mais rappelle également les principales règles de bonne pratique applicables de manière plus générale. Pour en faciliter la lecture, les règles sont structurées en deux parties :

- la première spécifique à l'accès authentifié de tiers au SIS ;
- la seconde rappelant les principales bonnes pratiques pour la sécurisation de l'accès par le web à une application manipulant des données sensibles.

4 Règles de sécurité

4.1 Règles spécifiques à l'accès authentifié de tiers

N°	Règle
	Règles générales
[RA1]	Le Responsable doit s'appuyer sur un ensemble de procédures qui définissent les règles de gestion des comptes utilisateurs et qui couvrent notamment : • la phase d'enrôlement comprenant la création des comptes d'accès individuel des tiers et dans laquelle l'identité de chaque tiers est vérifiée lors de la remise des moyens d'identification et d'authentification à ce dernier (par exemple, l'utilisation de CPS pour l'authentification de tiers professionnels de santé) ; • la vérification régulière (au moins annuelle) de la légitimité du maintien de chaque compte ; • les situations dans lesquelles un compte doit être suspendu (par exemple : absence prolongée (ou non usage prolongé du service) du titulaire du compte, suspicion d'usurpation du compte…) ou bloqué (par exemple : départ du titulaire du compte, résiliation par le titulaire…). Ces différents aspects, comme ceux traités par les autres règles RA, doivent être modulés en fonction des enjeux spécifiques à l'application web considérée et de ses modalités d'utilisation.
[RA2]	L'identification des tiers acteurs sanitaires et médico-sociaux doit se conformer au Référentiel d'identification des acteurs sanitaires et médico-sociaux de la PGSSI-S [Réf. n°5.1].
[RA3]	L'authentification des tiers acteurs de santé doit se conformer au Référentiel d'authentification des acteurs de santé de la PGSSI-S [Réf. n°5.2].
[RA4]	Le choix des paliers pour l'identification des tiers acteurs sanitaires et médico-sociaux (cf. Réf. n°5.1) et pour l'authentification des tiers acteurs de santé (cf. Réf. n°5.2) doit être réalisé en cohérence avec les enjeux liés à l'application web concernée.
[RA5]	Pour les tiers qui n'entrent pas dans le cadre des règles [RA2] à [RA4], et qui ne bénéficient pas d'une identification nationale prévue pour être utilisée dans le cadre santé/médico-social, les éléments nécessaires à l'identification doivent être recueillis lors d'un processus d'enregistrement formalisé. L'identifiant attribué lors de cet enregistrement est alors un identifiant local délivré et géré sous la responsabilité de la structure. Ce processus doit être établi préalablement à l'ouverture de l'application web sur internet.
[RA6]	La délivrance du dispositif d'authentification à un tiers qui n'entre pas dans le cadre des règles [RA2] à [RA4] doit être intégrée dans le processus d'enregistrement identifié dans la règle [RA5].

N°	Règle
[RA7]	Le choix des dispositifs d'authentification utilisables par les tiers qui n'entrent pas dans le cadre des règles [RA2] à [RA4] pour se connecter à une application web doit être réalisé en cohérence avec les enjeux liés à cette application. Les paliers de l'authentification privée du Référentiel d'authentification des acteurs de santé de la PGSSI-S [Réf. n°5.2] peuvent servir de référence pour le choix des dispositifs d'authentification utilisables.
[RA8]	Dans le cas de tiers qui n'entrent pas dans le cadre des règles [RA2] à [RA4] et qui bénéficient de droits d'accès particuliers leur permettant d'accéder à des données de santé à caractère personnel relatives à une autre personne (ex. : titulaire de l'autorité parentale pour un mineur, tuteur ou curateur…), la procédure d'enregistrement doit prévoir la vérification des éléments qui justifient ces droits.
[RA9]	Afin de limiter le nombre d'identifiants et de dispositifs d'authentification attribués à un même tiers qui n'entre pas dans le cadre des règles [RA2] à [RA4], il est recommandé de favoriser la réutilisation de son compte utilisateur éventuellement existant lorsqu'un nouveau service est utilisé.
[RA10]	Le Responsable doit vérifier qu'il dispose des informations lui permettant d'informer chaque tiers, qu'il soit utilisateur ou bien qu'il soit la personne à laquelle se rapporte la donnée (ex. patient), en cas d'incident ou de suspicion d'incident pouvant affecter l'utilisation de l'application ou les données à caractère personnel le concernant.
[RA11]	Le Responsable doit sensibiliser les tiers à la sécurité des terminaux utilisés pour accéder à l'application.[7]
[RA12]	Le Responsable doit sensibiliser les tiers à la sécurité de leurs moyens d'identification et d'authentification.
[RA13]	Le Responsable doit donner aux tiers les coordonnées du support, leur permettant notamment de signaler des tentatives d'hameçonnage[8] ou d'autres courriels malveillants relatifs aux services offerts par l'application.
Règles liées à la conception et à la réalisation de l'application	
[DA1]	L'application doit permettre aux tiers de réaliser uniquement des actions qui relèvent de leur rôle (ex. pas de modification de documents médicaux par des non PS).
[DA2]	Dans le cas d'une authentification à un seul facteur[9], l'application doit identifier le tiers à l'aide d'un identifiant non signifiant, c'est-à-dire qui ne peut à lui seul indiquer le nom ou la localisation du tiers.[10]

[7] Pour cette règle comme pour les deux suivantes, il s'agit de mettre en place une sensibilisation adaptée à des tiers sans expertise spécifique.

[8] Egalement appelé « filoutage » ou « phishing » : technique d'obtention illicite d'identifiants et de mots de passe de victimes en usurpant l'identité d'une entreprise ou d'un organisme connu, généralement à l'aide de courriels imitant ceux de cet organisme.

[9] La notion de facteur d'authentification est explicitée dans le glossaire, en Annexe 1.

[10] Dans une version ultérieure de ce document, la règle DA2 pourra s'appuyer sur les référentiels d'identification et d'authentification de la PGSSI-S.

N°	Règle
[DA3]	Les mécanismes assurant le lien entre le tiers et les données auxquelles il accède doivent être robustes. En particulier, aucun tiers connecté ne doit pouvoir accéder à des données de santé à caractère personnel auxquelles il n'a pas droit (ex. : modification des paramètres de connexion, comme une modification de l'URL une fois la session ouverte, afin d'accéder à des données d'autres personnes).
[DA4]	L'application doit vérifier la validité (non-révocation et chaîne de certification) des certificats cryptographiques utilisés dans le cadre de ses échanges avec des équipements distants.
[DA5]	Si une authentification par identifiant et mot de passe a été choisie en accord avec l'analyse de risque, l'application doit imposer aux utilisateurs l'usage et le renouvellement de mots de passe complexes, respectant la note technique " Recommandations de sécurité relatives aux mots de passe " de l'ANSSI (document de référence n°4).
[DA6]	Si une authentification par identifiant et mot de passe a été choisie en accord avec l'analyse de risque, l'application doit de préférence mettre en œuvre un dispositif de saisie de mot de passe capable de mettre en échec des logiciels malveillants de type « keylogger » : saisie par clavier virtuel par exemple.
[DA7]	Quand l'analyse de risque fait apparaître qu'une authentification à deux facteurs (cf. Glossaire) est nécessaire (typiquement pour accéder aux données de santé), l'application peut mettre en œuvre des mots de passe à usage unique, de type One Time Password (OTP), reposant si possible sur un matériel distinct du terminal d'accès de l'utilisateur (par exemple, envoi de l'OTP par SMS au téléphone de l'utilisateur qui accède depuis son ordinateur).
[DA8]	Les mots de passe proposés par l'application aux utilisateurs (mot de passe initialement fourni à l'utilisateur pour son premier accès aux services ou OTP par exemple) ne doivent pas être prédictibles. L'algorithme de génération de ces mots de passe doit de préférence suivre les règles du RGS en matière de génération d'aléa[11].

[11] RGS v2 - Annexe B1 - Mécanismes cryptographiques [Réf. n°6.2]

N°	Règle
[DA9]	L'application doit comporter des mécanismes de détection et de protection contre les tentatives systématiques de connexion sous l'identifiant de tiers. En particulier, l'application doit limiter le nombre de tentatives de connexion infructueuses successives sous l'identité d'un même utilisateur. Après n tentatives infructueuses successives (n laissé à l'appréciation du Responsable), aucune tentative de connexion ne doit pouvoir s'effectuer avant une durée à déterminer par le Responsable. Cette durée ne doit pas être inférieure à une minute (ce laps de temps réduit les opportunités d'attaque par « force brute », c'est-à-dire le lancement de requêtes automatiques régulières cherchant le mot de passe d'un compte par essais successifs). Les mécanismes de limitation mis en œuvre doivent cependant éviter d'entrainer un blocage complet du compte utilisateur, qui requerrait une intervention manuelle de déblocage et ouvrirait la porte à un déni de service massif à l'encontre des utilisateurs. Par exemple, le système d'ouverture de session peut interdire toute nouvelle tentative de connexion avant un délai d'une seconde après le premier échec d'authentification, puis doubler ce délai entre les tentatives de connexion à chaque nouvel échec, jusqu'à un délai maximum de 5 minutes (soit à partir du 9^{e} échec) entre toutes les tentatives suivantes. Cette disposition ne remplace en rien la nécessité d'alerte automatique des administrateurs systèmes en cas d'échec d'authentification répété. En ralentissant l'attaque potentielle, elle laisse au contraire le temps au personnel compétent d'intervenir ou permet d'activer des dispositions automatiques (ex. blocage de l'adresse réseau source des tentatives de connexion).
[DA10]	L'application ne doit autoriser, à tout moment, qu'une seule session ouverte par utilisateur. L'application de cette règle peut se faire de deux manières, parmi lesquelles le Responsable doit choisir : • soit l'interdiction de nouvelles connexions de l'utilisateur tant qu'une session qui lui est associée est ouverte. Cette option nécessite que l'application vérifie fréquemment (par exemple toutes les minutes) que la partie « cliente » (navigateur web) est toujours active, à défaut de quoi une fermeture intempestive (ex : fermeture du navigateur sans action de déconnexion) du client pourrait laisser la session ouverte pendant une longue durée et interdire toute connexion légitime de l'utilisateur ; • soit la fermeture de toute session éventuellement en cours lorsque l'utilisateur associé se connecte. La tentative d'utilisation d'une session fermée automatiquement pour cette raison doit informer l'utilisateur de la raison de la fermeture et lui indiquer le moyen d'alerter la structure s'il soupçonne une usurpation de son compte.
[DA11]	A l'ouverture d'une session, l'application web doit indiquer à l'utilisateur la date et l'heure de la dernière connexion effectuée sous son identifiant.
[DA12]	Toute application web utilisant des jetons (cookies ou autres) de session doit effectuer un suivi des jetons pour chaque session ouverte. Elle doit vérifier l'authenticité de tout jeton qui lui est transmis par le navigateur de l'utilisateur avant de l'utiliser pour identifier la session utilisateur ou utiliser toute information qu'il transporte.

N°	Règle
[DA13]	Toute application web utilisant des jetons (cookies ou autres) de session doit limiter la durée de vie de ces jetons à chacune des sessions.
[DA14]	L'application doit permettre à l'utilisateur de se déconnecter à tout instant. Cette déconnexion doit entrainer la suppression des jetons de session.

4.2 Bonnes pratiques concernant l'accès à une application via le web

N°	Règle
	Règles générales
[RG1]	Le Responsable doit veiller au respect des obligations légales et qui relèvent de son périmètre de responsabilité pour l'application (finalité de l'application web, consentement du patient, agrément de l'hébergeur des données de santé, obligations relatives à la mise en ligne d'un site Internet : mentions légales, conditions générales d'utilisation, conservation des données de connexion, information des utilisateurs sur la collecte d'informations à caractère personnel, etc.).
[RG2]	Le Responsable doit veiller à ce que les données échangées entre l'application et le reste du SIS soient protégées en confidentialité et en intégrité et que leur origine soit garantie (authenticité des données).
[RG3]	Le Responsable doit veiller à ce que des dispositions de protection et de cloisonnement physique ou logique entre l'application (ou sa plateforme d'hébergement) et le reste du SIS empêchent la propagation d'incidents de sécurité ou de code malveillant entre ces deux sous-ensembles.
[RG4]	Le Responsable doit veiller à ce que des dispositions de protection et de cloisonnement physique ou logique entre l'application (ou sa plateforme d'hébergement) et des applications relevant d'autres Responsables empêchent la propagation d'incidents de sécurité ou de code malveillant entre ces applications.
[RG5]	Le Responsable doit veiller à interdire toute utilisation des données réelles de l'application à d'autres fins que celles prévues, notamment à l'exclure des activités de développement, de test ou de maintenance.
[RG6]	Le Responsable doit veiller à ce que chaque personne intervenant dans le maintien en condition opérationnelle de l'application (administrateur, exploitant, agent de maintenance, etc.) ait signé un engagement individuel de confidentialité.
[RG7]	L'exploitant et le Responsable doivent convenir de leurs engagements respectifs pour assurer le bon fonctionnement de l'application. A ce titre, ils doivent mettre en œuvre des procédures de surveillance de la sécurité, de gestion des incidents de sécurité et de gestion des vulnérabilités relatives à l'application web.

N°	Règle
[RG8]	Le Responsable doit suivre et faire contrôler au moins une fois tous les trois ans : • la sécurité de l'hébergement et de l'exploitation de l'application ; • la prise en compte du traitement des vulnérabilités dans l'application et dans sa plateforme d'hébergement. Il doit notamment s'assurer de la réalisation de tests de vulnérabilités et de tests d'intrusion sur l'application et sur la plateforme. Dans le cas d'un recours à une prestation d'hébergement externe par un hébergeur de données de santé agréé, le Responsable peut se baser sur l'attestation de renouvellement de l'agrément de l'hébergeur pour les aspects qui relèvent du périmètre de responsabilité de l'hébergeur en question et qui sont pris en compte dans l'agrément (exemple : le traitement des vulnérabilités applicatives peut relever de l'hébergeur ou de son client en fonction du contrat passé).
	Règles liées à la conception et à la réalisation de l'application
[DG1]	L'application web doit être de conception simple et son codage doit respecter des standards pérennes (issus du W3C[12] par exemple) afin de faciliter son contrôle, sa maintenance et sa réversibilité.
[DG2]	Le maître d'œuvre du développement de l'application doit garantir au Responsable que des mesures ont été prises afin d'éviter les différents types de vulnérabilités identifiées et publiées par l'OWASP et que l'absence de telles vulnérabilités a été vérifiée avant mise en production.
[DG3]	L'application doit intégrer des mécanismes de vérification des données qu'elle reçoit et de celles qu'elle transmet, associés à des mécanismes de traitement des erreurs. Les vérifications doivent porter sur le format et la vraisemblance des données et sur l'absence de code malveillant.
[DG4]	L'application web doit révéler le moins d'information possible à l'utilisateur sur sa réalisation ou son environnement d'exploitation (éviter par exemple de divulguer la configuration, la version, le langage utilisé, l'organisation des répertoires ; vulgariser les messages d'erreur visibles de l'utilisateur afin de limiter le contenu des messages d'erreur au strict minimum sur la raison de l'échec).
[DG5]	Le code de l'application doit au minimum être vérifié par un outil de détection automatique de vulnérabilités courantes dans les applications web (exemple : utilisation de fonction « dangereuses », absence de contrôle des entrées, absence de nettoyage des sorties…). Ces vérifications peuvent également être réalisées par une équipe interne si la structure dispose de ces compétences particulières, ou par un prestataire d'audit de code disposant si possible de la qualification PASSI[13] délivrée par l'ANSSI.
[DG6]	La phase de recette de l'application et de ses mises à jour majeures doit intégrer des tests de vulnérabilités et des tests d'intrusion.

[12] http://www.w3.org/

[13] Prestataire d'audit de la sécurité des systèmes d'information

N°	Règle
[DG7]	L'application ne doit pas permettre à l'utilisateur, par manipulation d'URL ou de paramètres de requête, d'explorer la structure applicative ou d'accéder à des données ou fonctions auxquelles il n'est pas autorisé.
[DG8]	Les données de santé à caractère personnel, conservées par l'application web[14] à titre permanent sur des supports de stockage, doivent l'être sous une forme protégée par chiffrement et par une fonction de contrôle d'intégrité (signature ou cachet électronique par exemple). Ces fonctions doivent être conformes aux règles techniques du RGS[15]. La mise en œuvre du chiffrement doit préserver la capacité de restituer en clair à chaque tiers les données auxquelles il a légitimement accès. Un soin particulier doit être apporté à la gestion des clés utilisées pour le chiffrement. On pourra se reporter au document du RGS qui traite de ce sujet[16]. Il est préconisé de favoriser, quand c'est possible, une architecture dans laquelle les données ne sont stockées ni sur les frontaux web, ni sur les serveurs d'applications.
[DG9]	Les données de santé à caractère personnel, conservées par l'application à titre temporaire sur des supports de stockage dans le cadre de leur traitement, doivent être effacées de ces supports à l'issue de leur traitement. Cet effacement doit être réalisé par écrasement, c'est-à-dire par réécriture des fichiers à l'aide d'un remplissage intégral par la valeur zéro, et non par une simple suppression des fichiers qui laisse généralement les données elles-mêmes inchangées sur le support physique (bien qu'elles n'apparaissent plus directement pour un utilisateur non expert). Pour plus d'information, se reporter au « Guide pratique spécifique à la destruction de données » du corpus documentaire PGSSI-S.
[DG10]	En vue du contrôle de la conformité des traitements et du traitement d'incidents de sécurité, l'application doit comporter une fonction d'enregistrement des événements relatifs à la sécurité des services offerts et de leur utilisation. Elle doit au minimum conserver les traces : • des ouvertures et des fermetures des services ; • des ouvertures et des fermetures des sessions ; • des refus d'accès et des anomalies ; • des dépôts et des accès en lecture aux données de santé à caractère personnel ; • des accès en modification ou en suppression à ces données.

[14] Au sens de la définition donnée au chapitre 1.2

[15] RGS v2 – Annexe A1 – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques [Réf. n°6.1]

[16] RGS v2 – Annexe B2 – Gestion des clés cryptographiques [Réf. n°6.3]

N°	Règle
[DG11]	Chaque trace doit comporter au minimum : • la date et l'heure précise de l'événement ; • le type de l'événement ; • les informations permettant de déterminer l'auteur de l'événement ; • l'adresse IP du terminal utilisé. Il convient de noter que l'adresse IP du terminal de l'utilisateur doit parfois être obtenue via les entêtes du protocole http plutôt qu'au niveau de la connexion IP à l'application. C'est par exemple le cas quand un « reverse-proxy » est utilisé en frontal de l'application web. Il convient alors d'utiliser la valeur de l'entête http « REMOTE_ADDR » ou « HTTP_X_FORWARDED_FOR » (ou autre selon la configuration du reverse proxy) ajoutée à la requête par le reverse proxy.
[DG12]	L'application doit permettre au personnel autorisé et à lui seul, placé sous l'autorité du Responsable, de paramétrer les types d'événements à enregistrer, les données constitutives des enregistrements (en respectant les données minimales identifiées dans la règle [DG11]) et la durée de rétention des enregistrements (et donc le délai d'effacement des traces) conformément à la politique de gestion des traces pour l'application concernée. Afin d'éviter un cumul de rôle préjudiciable à la qualité du système de traces, il est recommandé que ce personnel ne soit pas utilisateur de l'application concernée, ou au moins qu'il ne dispose d'aucun rôle privilégié ou sensible (administrateur de l'application, administrateur système, …). De manière plus générale, des dispositions doivent être prises pour garantir que les traces ne peuvent pas être modifiées de quelque manière que ce soit pendant toute leur durée de conservation, afin qu'elles puissent être utilisées en cas d'investigation, notamment judiciaire. Ces dispositions dépendent des enjeux spécifiques liées à l'application web considérée. Elles doivent également prendre en compte l'impact potentiel de la génération de traces sur les performances de l'application. Un compromis doit être recherché entre la réponse aux exigences de traces et la réponse aux exigences de performance. Pour plus d'information sur les traces, se reporter au « Référentiel d'imputabilité » du corpus documentaire PGSSI-S.
[DG13]	Dès lors que l'utilisateur s'authentifie, et pour toute la durée de sa session authentifiée, l'application web doit imposer la mise en œuvre d'un canal sécurisé HTTPS (à l'aide d'une version du protocole TLS à l'état de l'art et non-vulnérable) entre sa plateforme et le terminal de l'utilisateur et mettre en œuvre les fonctions d'authentification et de chiffrement que permet ce protocole, et le cas échéant de signature (ou cachet) électronique. Il est recommandé que la mise en œuvre de ces technologies se conforme aux règles et recommandations du RGS[17].
[DG14]	Toute session ayant provoqué une erreur de l'application web doit être automatiquement fermée.
[DG15]	L'application doit déconnecter automatiquement un utilisateur dont la session est inactive. La durée d'inactivité prise en compte doit être paramétrable par un administrateur de l'application placé sous l'autorité du Responsable.

[17] RGS v2 – Annexe A1 – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques [Réf. n°6.1]

N°	Règle
[DG16]	Lors de la déconnexion d'un utilisateur, l'application web doit, autant que possible (notamment si le côté « client » de l'application, sur le navigateur de l'utilisateur, est toujours actif) provoquer l'effacement des données résiduelles dans le terminal et le navigateur de l'utilisateur. De manière générale, l'application doit être conçue pour que les données liées à la session dans l'environnement utilisateur soient supprimées par le navigateur à la fermeture de la session, de la page web ou du navigateur.
[DG17]	L'application doit intégrer une aide destinée à faciliter son utilisation sûre, c'est-à-dire qui minimise les risques d'erreur ou d'incompréhension dans les actions effectuées par l'utilisateur. L'ergonomie de l'application doit viser le même objectif.
[DG18]	L'environnement de développement doit être distinct de l'environnement de production. Il doit disposer des protections mentionnées par la règle [EG2]. Les environnements de recette et de pré-production doivent être distincts de l'environnement de production. Ils doivent disposer de protections similaires à celles mises en œuvre pour la production (voir [DG20] et [EG2])
[DG19]	Pendant toute la durée de vie de l'application web, le maître d'œuvre de la réalisation de l'application doit : • signaler au Responsable les vulnérabilités publiées ou détectées relatives à l'application livrée ; • fournir les correctifs correspondants ou les consignes qui permettent d'empêcher l'exploitation des vulnérabilités dans l'attente de la fourniture du correctif.
[DG20]	Il est recommandé que l'architecture de la plate-forme applicative prévoie un dispositif de sécurité applicative, de type reverse-proxy ou pare-feu applicatif, en frontal de l'application, afin de ne pas laisser l'application en communication directe avec Internet, et d'être en mesure de bloquer en amont de multiples attaques génériques, et le cas échéant spécifiques, contre l'application.
[DG21]	L'application web doit être conçue pour fonctionner même si l'utilisateur y accède via un ou plusieurs proxy http.
Règles liées à l'hébergement et à l'exploitation de l'application	
[EG1]	L'hébergement de l'application web doit être réalisé conformément aux dispositions de l'article L. 1111-8 du code de la santé publique. Lorsque le Responsable fait appel à un tiers pour héberger les données de santé à caractère personnel ou l'application web, cet hébergeur doit être agréé par le ministre en charge de la santé (articles L. 1111-8 et R. 1111-9 et suivants du code de la santé publique)
[EG2]	L'application en production doit bénéficier d'un environnement de sécurité physique, technique et organisationnel conforme aux règles de l'art et capable de la protéger notamment contre : • les tentatives d'intrusion ou d'accès physique ou logique par des personnes non autorisées ; • les attaques logiques en provenance des réseaux ; • les codes malveillants.

N°	Règle
[EG3]	Les dispositions de sécurité de l'application et de sa plateforme d'hébergement doivent encadrer les accès des personnels chargés de son maintien en condition opérationnelle (exploitant, administrateur, agent de maintenance, etc…) afin de limiter l'accès aux données de santé de l'application à ce qui est strictement nécessaire pour l'exécution des missions des personnels précités. En outre, ces accès doivent être réalisés sous le contrôle et la responsabilité du Responsable et du médecin de l'hébergeur lorsque l'application est hébergée par un hébergeur agréé à cet effet.
[EG4]	Tous les accès d'exploitation à l'application doivent être répertoriés, contrôlés et limités au strict nécessaire. Les autres possibilités d'accès par le personnel chargé du maintien en condition opérationnelle doivent être neutralisées, et si nécessaire doivent pouvoir être ouvertes en cas de besoin pour une durée limitée dans le cadre d'un processus maîtrisé, sous le contrôle du Responsable.
[EG5]	Il est fortement recommandé que tous les accès logiques donnant aux exploitants ou aux administrateurs la possibilité de lire ou de modifier des données de santé, même de façon fortuite, soient soumis à une procédure d'identification individuelle et d'authentification forte (à deux facteurs). Les cas où ces principes ne peuvent pas être respectés doivent être identifiés, référencés et justifiés. Les accès doivent être tracés et ces traces ne doivent être exploitables que par le personnel en charge du contrôle de la conformité du traitement.
[EG6]	L'application doit faire l'objet d'une surveillance de la sécurité de son fonctionnement selon les règles de l'art, notamment par la mise en place de sondes de détection d'intrusion avec, quand l'analyse de risque permet de conclure que c'est pertinent, des règles de blocage selon les types d'attaques ou de comportements détectés. La mise en œuvre de blocage automatique doit être décidée en tenant compte du fait que cette disposition peut être exploitée par des personnes malveillantes afin de porter atteinte à la disponibilité du système. Elle résulte donc généralement du choix de privilégier la protection des données et traitements contre des accès illégitimes au dépend de la continuité des accès légitimes à ces données et traitement.

Annexe 1 : Glossaire

Sigle / Acronyme	Signification
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CPS	Carte de Professionnel de Santé
DMP	Dossier Médical Personnel
ES	Etablissements de santé
GT	Groupe de Travail
HTTPS	HyperText Transfer Protocol Secure : protocole de transfert hypertexte sécurisé
OWASP	Open Web Application Security Project
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PS	Professionnel de Santé
RGS	Référentiel Général de Sécurité
SIS	Système d'Information de Santé
URL	Uniform Resource Locator, (peut être traduit par adresse réticulaire ou adresse universelle, selon le JO du 16/03/1999)
W3C	World Wide Web Consortium

Facteur d'authentification

En pratique, la preuve de l'identité présentée lors d'une opération d'authentification peut être basée sur un ou plusieurs des facteurs d'authentification suivants :

- ce que la personne sait (ex. mot de passe) ;
- ce que la personne possède (ex. carte à puce, certificat électronique, token OTP, carte OTP, téléphone, tablette, boite aux lettres de messagerie, etc.) ;
- ce que la personne est (ex. caractéristique physique de type biométrie) ;
- ce que la personne sait faire (ex. biométrie comportementale telle que la signature manuscrite ou la manière de taper sur un clavier d'ordinateur aussi appelée « frappologie »).

Plus le nombre de facteurs utilisés lors d'une opération d'authentification est grand, plus l'authentification est considérée comme fiable.

Niveau d'authentification

On distingue deux niveaux d'authentification :

- l'authentification simple lorsque celle-ci ne repose que sur un seul facteur (exemple : l'utilisateur indique son mot de passe) ;
- l'authentification forte lorsque plusieurs facteurs différents sont combinés (par exemple, ce que je sais et ce que je possède : mot de passe saisi sur un terminal lui-même authentifié et enregistré comme appartenant à la personne authentifiée).

Les facteurs d'authentification sont associés à une personne physique ou morale. En cas d'authentification forte, les différents facteurs utilisés doivent être associés à la même personne (physique ou morale).

Annexe 2 : Documents de référence

Référence n°1 : Recommandations pour la sécurisation des sites web – Note Technique – Août 2013 - ANSSI

Référence n°2 : Les dix vulnérabilités de sécurité applicatives web les plus critiques (mise à jour annuelle) – OWASP

Référence n°3 : Guide de règles et de recommandations relatives au développement d'applications de sécurité en Java - V1.3 – Novembre 2009 – ANSSI

Référence n°4 : Recommandations de sécurité relatives aux mots de passe – Note technique – Juin 2012 – ANSSI

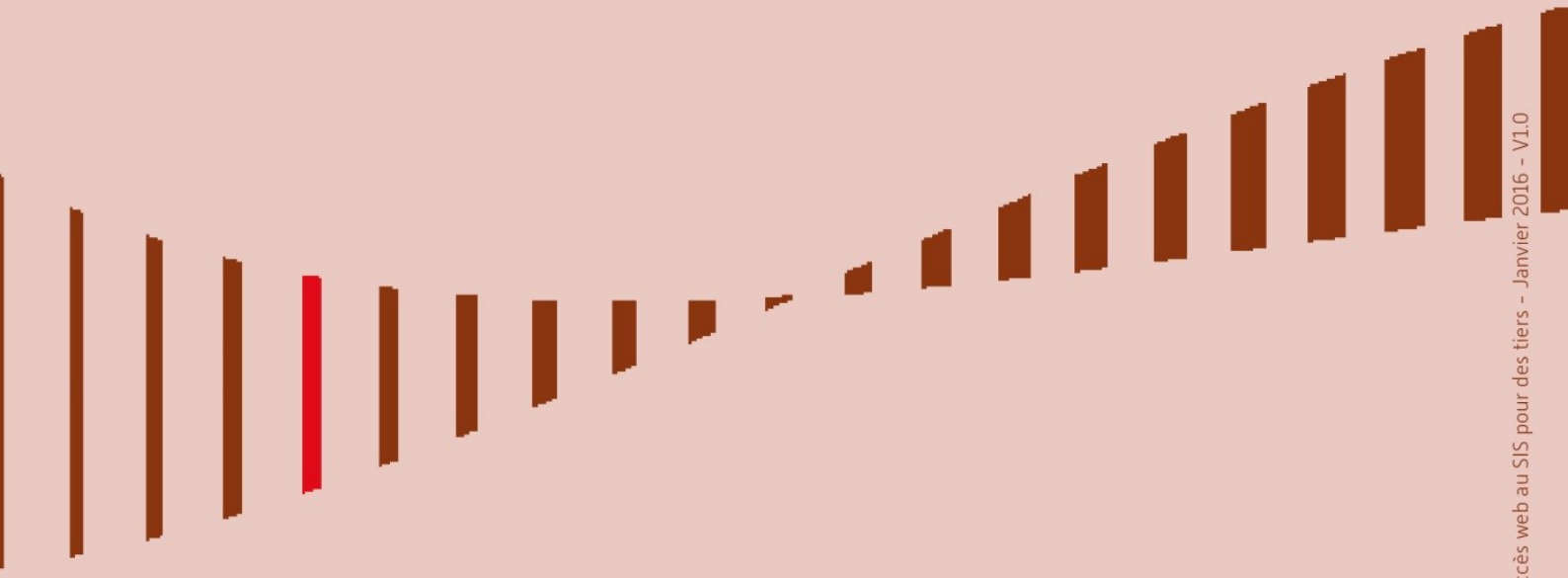
Référence n°5 : Corpus documentaire de la PGSSI-S (référentiels et guides pratiques)[18] http://esante.gouv.fr/pgssi-s/espace-publication

- Référence n°5.1 : Référentiel d'identification des acteurs sanitaires et médico-sociaux (voir Réf. n°5)
- Référence n°5.2 : Référentiel d'authentification des acteurs de santé (voir Réf. n°5)
- Référence n°5.3 : Référentiel des autorités de certification éligibles pour l'authentification publique dans le secteur de la santé (voir Réf. n°5)
- Référence n°5.4 : Référentiel d'imputabilité (voir Réf. n°5)
- Référence n°5.5 : Guide Pratique - Règles pour les interventions à distance sur les Systèmes d'Information de Santé (SIS)

Référence n°6 : Référentiel Général de Sécurité http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/

- Référence n°6.1 :RGS v2 - Annexe A1 - Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques
- Référence n°6.2 :RGS v2 - Annexe B1 - Mécanismes cryptographiques
- Référence n°6.3 :RGS v2 - Annexe B2 - Gestion des clés cryptographiques

[18] Le cas échéant, les évolutions du corpus documentaire de la PGSSI-S seront prises en compte dans des versions ultérieures de ce guide, notamment par référencement de certains guides pratiques sur des sujets spécifiques évoqués dans le chapitre 4 sur les règles.



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