AGENCE
DU NUMÉRIQUE
EN SANTÉ

Présentation exigences SSI et test d'intrusion

Médecine de ville, Officine, Paramed et Sage-femmes
Ségur numérique Vague 2

19 septembre 2025

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Exigences SSI

Médecine de ville, Officine, Paramed et Sage-femmes
Ségur numérique Vague 2

/ 01 Périmètre d’applicabilité des exigences SSI

Un programme autour des éditeurs en santé et de la SSI

Le dispositif SONS est un financement incitatif proposé par l'Etat pour soutenir la modernisation et la sécurisation des logiciels métiers en santé. Dans ce cadre, la conformité des solutions candidates au référencement est évaluée afin de s'assurer de l'atteinte d'un niveau de maturité et de la conformité avec les **réglementations et initiatives** en cours dans l'écosystème santé

Contexte

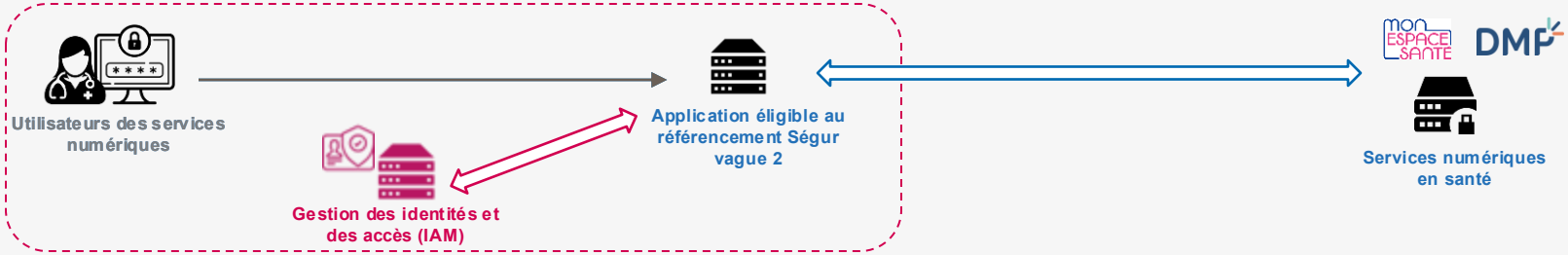
- L'actualité fait régulièrement état de cyberattaques **touchant des structures de santé**
- Le fonctionnement de ces structures peut être impacté de **façon grave voire même irréversible** dans certains cas
- Les structures de santé manipulent au sein de leurs systèmes d'information des données de santé à **caractère personnel**, données particulièrement **sensibles** et qui doivent être protégées en conséquence.

Enjeux de sécurité

- Les applications utilisées sont progressivement amenées à s'interconnecter avec **Mon Espace Santé et notamment le DMP**
- L'application des bonnes pratiques de sécurité est plus que jamais **indispensable** sur les SI des structures de santé et doit être prise en compte dans **les solutions numériques qu'elles utilisent au quotidien**
- Les solutions logicielles font partie des **vecteurs d'attaque** qui peuvent être utilisés pour **accéder au SI d'une structure de santé**

L'ambition du Ségur numérique est le partage fluide et **sécurisé** des données de santé. Il est donc essentiel que la dimension cybersécurité soit abordée dans le cadre du Ségur numérique et que cela vise les logiciels métiers utilisés au sein des structures de santé

Vague 2 – Synthèse des exigences SSI



Socle commun d'exigences SSI

- **6 exigences critiques** permettant de garantir un **niveau de sécurité suffisant** de la solution
- Les exigences sont validées en se basant sur une **revue documentaire.**

Exigences sur l'Identification Electronique

- **3 exigences** en lien avec le référentiel IE portant sur la **gestion des comptes utilisateurs** et la **sécurité du système.**

Exigences sur la gestion des identités

- **1 à 2 exigences** liées à la gestion des identités et des accès, concernant la **gestion des traces** et la **politique de mots de passe pour les comptes d'administration**

/ 02 Synthèse des exigences SSI

Synthèse des exigences du socle commun SSI

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence
SC.SSI/GEN.1	Désignation des responsables du suivi et maintien des mesures de sécurité	Dans les équipes en charge de la solution, les responsables de la sécurité doivent être identifiés ainsi que leurs responsabilités (activités de conception, de développement, d'installation, d'exploitation, d'administration, de maintenance et de support)
SC.SSI/GEN.2.BIS	Sensibilisation des équipes en charge	Une sensibilisation à la SSI doit être menée pour l'ensemble des équipes du système en charge des activités de conception, de développement, d'installation, d'exploitation, d'administration, de maintenance et de support. Dans le cas où le système est destiné à traiter des données à caractère personnel, ALORS la sensibilisation DOIT intégrer les obligations légales.
SC.SSI/GEN.3.BIS	Plan d'Assurance Sécurité du produit	Si l'industriel ou un tiers sous sa responsabilité assure l'hébergement de tout ou partie des composants du système, ou fournit tout ou partie du système sous forme de service (SaaS) ALORS, il DOIT intégrer dans le PAS du système les mesures de sécurité et les engagements entre l'hébergeur et la structure utilisatrice, pour l'environnement de mise en œuvre.
SC.SSI/GEN.11	Développement sécurisé	Les bonnes pratiques pour le développement et la configuration sécurisés doivent être définies et suivies tant dans la création du système que dans l'implémentation de nouvelles fonctionnalités (vérification de qualité du code, gestion de l'obsolescence des bibliothèques, sécurisation de la plateforme système, etc.)
SC.SSI/GEN.20	Veille et patch management	Un processus de veille sur les vulnérabilités des composants doit être défini et appliqué. Un processus de patch management ou de distribution des patchs (dans le cas d'une solution hébergée par une structure utilisatrice) doit être déterminé et mis en œuvre (application / distribution des patchs, des mises à jour des composants, etc.)
SC.SSI/GEN.21.BIS	Réalisation des sauvegardes	Pour toutes les solutions, l'industriel DOIT proposer une procédure de sauvegarde et de restauration ainsi que la documentation associée.

Synthèse des exigences sur l'identification électronique (IE)

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence
SC.SSI/IE.33	Gestion des comptes des utilisateurs	Le système DOIT gérer a minima les identifiants et attributs suivants d'un PS : - Numéro RPPS (si existant) - Identifiant privé (si existant), dont l'unicité doit être assurée - Nom d'exercice ; - Prénom ; - Profession ou une mention appropriée à la situation de la personne.
SC.SSI/IE.38	Déconnexion du système	Le système DOIT permettre au professionnel de fermer sa session.
SC.SSI/IE.58 **SC.SSI/IE.59**	Gestion des comptes, des permissions et des sessions des administrateurs et des utilisateurs	Le système DOIT se verrouiller après une durée d'inactivité de 2 heures ou moins.* ** La durée d'inactivité est en cours de validation pour les LGO (avec l'utilisation potentielle de MIE de type clé FIDO2)*

Synthèse des exigences sur la gestion des mots de passe

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence
SC.SSI/IAM.91	Conservation des traces de modification de mot de passe	**Pour les Profils Structures d'exercice coordonné (LGC), Structures de ville (Paramed) et LGO uniquement* :** Le système doit conserver des traces de toutes les opérations réalisées en lien avec le cycle de vie des comptes (modification d'attributs d'identité, permissions, tentative de connexion et de modification de mot de passe)
SC.SSI/IAM.92	Politique de mot de passe pour les comptes d'administration	Le système doit permettre à la structure de santé de mettre en place une politique de mots de passe robuste sur les comptes d'administration sur la base de certains critères (caractères minimum, jeu de caractères, délais d'expiration, blocage du compte)

*Les autres profils, ne relevant pas d'une organisation structurée ou coordonnée impliquant une gestion mutualisée des accès ou des responsabilités, ne sont pas concernés par l'exigence SC.SSI/IAM.91. Dans ces contextes, le besoin de conservation des traces de modification de mot de passe est considéré comme moins critique.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Tests d’intrusion

Médecine de ville, Officine, Paramed et Sage-femmes Ségur numérique Vague 2

/ 01 Contexte de réalisation

Contexte de la réalisation des tests d'intrusion

L'un des principaux piliers du programme Ségur Numérique **est la sécurité**. Par conséquent, chaque solution **candidate fait l'objet d'une évaluation cyber** afin de s'assurer qu'elle ne présente pas de vulnérabilités potentiellement exploitables.

CADRE

- À ce titre, les éditeurs sont tenus de **réaliser un test d'intrusion LPS et un test d'intrusion proxy** en vue de se conformer à **l'exigence SC.PSC.14** du référentiel **Espace de Confiance ProSantéConnect.**
- Ces tests d'intrusion donnent lieu au **remplissage d'un formulaire** par l'auditeur, qui sera ensuite soumis par l'éditeur dans le cadre de la demande de référencement.

INTERVENANTS

- Les tests d'intrusion doivent être réalisés **par un prestataire qualifié PASSI.**
- Cependant, **il ne s'agit pas d'un audit PASSI** (la certification PASSI n'est pas requise pour l'auditeur et les conditions de réalisation du test d'intrusion ne sont pas celles d'un audit PASSI).

DOCUMENTS POUR LA RÉALISATION DU TEST D'INTRUSION

Guide d'utilisation : **Lecture préalable nécessaire** avant de commencer le test d'intrusion, détaillant ses spécificités

Formulaire Excel : Grille d'audit à télécharger par l'éditeur depuis la plateforme **Convergence, puis à transmettre à l'auditeur pour complétion.**

/ 02

Contenu et critères de validation des tests d’intrusions

Base de conception des tests d'intrusion

L'OWASP (Open Web Application Security Project) est une **organisation à but non lucratif mondialement reconnue** en matière de cybersécurité. Elle offre des ressources et des outils pour aider à construire et à maintenir la sécurité informatique des applications. Ainsi, l'OWASP publie et met à jour la liste du **top 10 de l'OWASP**, qui répertorie les **dix principales menaces et vulnérabilités cyber.** Ce classement est une référence mondiale qui permet de **cibler en priorité les vulnérabilités présentant les risques les plus critiques**.

Couverture SSI

Les points de contrôle du formulaire de test d'intrusion sont basés sur le **Top 10 de l'OWASP**, afin de se concentrer sur les vulnérabilités qui présentent le plus de risques

Clarté & légitimité

Les liens entre les points de contrôle des tests d'intrusion et les principales vulnérabilités de l'OWASP ont été établis et précisés dans le guide du test d'intrusion fourni à l'éditeur et à l'auditeur. Cela apporte clarté et crédibilité à la démarche (appui sur une référence internationalement reconnue).

Equité

La description des points de contrôle précis qui devront être audités lors des tests d'intrusion permet de garantir que le **périmètre de couverture sera identique** quel que soit l'auditeur intervenant (prestataire PASSI disposant de compétences suffisantes pour réaliser l'audit).

A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A010:2021	Server-Side Request Forgery

Contenu des tests d'intrusion à compléter par l'auditeur

Deux types de points de contrôle*

- **15 à 18 points de contrôle communs à toutes les solutions** (**obligatoirement analysés** par l'auditeur quelle que soit la solution concernée)
- **20 à 23 points de contrôle spécifiques au type de périmètre testé** (certaines mesures de sécurité devront être évaluées **selon l'architecture de la solution**)

**sauf pour le formulaire de TI proxy : 18 points de contrôle spécifiques au proxy PSC uniquement*

Deux niveaux de « gravité » définis

GRAVITÉ HAUTE

La non-conformité au point de contrôle attendu est **éliminatoire**. L'éditeur ne sera pas éligible au référencement dans ce cas.

GRAVITÉ MOYENNE

Jusqu'à **10 réponses négatives à des points de contrôles de gravité moyenne** peuvent être acceptées au maximum.

NA

Pour les architectures inférieures à 3-Tiers uniquement : Les points de contrôle notés « NA » **doivent être audités** pour valider le processus de référencement, mais **ne rentrent pas dans l'évaluation du score**.

Le formulaire de test d'intrusion intègre une **macro qui génère automatiquement le rapport d'audit** et confirme la validation de l'audit **sur la base des champs complétés par l'auditeur**.

/ 03 Planning et phases de l’audit

Description des phases du processus de test d'intrusion

Le test d'intrusion se déroule généralement sur **une période d'une semaine (5 jours/homme)** et s'organise en **quatre phases** définies ci-dessous :

Phase de cadrage

Contractualisation avec un PASSI

Signature du contrat (audit PASSI non requis), incluant une « clause de revoyure » pour les points de contrôles non-validés

Communication des entrants à l'auditeur

Dates de réalisation de l'audit, solution logicielle, prérequis, contacts ainsi que le formulaire du test d'intrusion et son guide d'utilisation

Phase de test

Réalisation des tests sur la brique logicielle

Réalisation des tests sur la brique logicielle, sur une période de 3 à 4 jours

Recensement des Non conformités

Identification des failles et des vulnérabilités de l'application pour une évaluation complète de sa sécurité

Remplissage du Formulaire du test d'intrusion

Complétion de l'onglet « Base commune » ainsi que de l'onglet correspondant au type de l'application et/ou de celui dédié au proxy

Génération du PDF

Génération automatique du PDF à partir de la macro du fichier Excel ou de façon manuelle

Phase de rapport

Signature électronique du PDF

Signature électronique du PDF avec un certificat de signature délivré par TSP

Transmission du formulaire à l'éditeur

Transmission par l'auditeur à l'éditeur du formulaire du test d'intrusion

[optionnel] Réévaluation

Réalisation des tests uniquement sur les points de contrôle non validés pour valider la correction des non-conformités

Soumission des formulaires

Envoi de formulaire dans le cadre de l'habilitation « Espace de confiance PSC »

Phase de communication des résultats

Habilitation EDC PSC

Validation des tests d'intrusion dans l'absence de toute gravité haute et si moins de 10 gravité moyennes ont été identifiées.

Éléments attendus lors de la phase de cadrage

Pour assurer le bon déroulement des tests d'intrusion, l'éditeur doit respecter quelques prérequis et s'assurer que certains éléments ont été transmis à l'auditeur

01 Prérequis

- Veiller à ce que l'environnement proposé à l'auditeur soit un **environnement iso-prod**
- S'assurer que l'application fournie soit **dans la version majeure** pour laquelle l'éditeur candidate
- Vérifier que tous les **dispositifs de sécurité** (WAF, sondes, passerelles, etc.) sont désactivés
- **Renseigner le type d'application** dans le formulaire

02 Entrants

Pour toutes les applications

- Plusieurs **comptes avec différents niveaux de privilèges**
- Liste des **comptes génériques**
- **Matrice des flux**
- Extraction des **logs techniques** sur les tests réalisés lors du premier jour opérationnel
- Information sur **les vulnérabilités connues** et les **mesures de sécurité mises en œuvre** pour les contourner
- LGO uniquement :
  - **MIE clé ou carte FIDO2 NFC** préalablement enrôlé
  - **Proxy PSC** utilisé par la solution

Selon le type d'application

- **App Web** : URL ou adresse IP
- **App mobile** : APK sans pinning de certificat et sans vérification du débridage du téléphone et, si possible, terminaux débridés
- **Client lourd** : client et accès aux configurations

Règles de remplissage du formulaire

L'auditeur doit tester tous les points de contrôle énumérés dans le formulaire de test d'intrusion et évaluer la conformité de l'application à ces points. Ensuite, il peut remplir le formulaire en respectant les instructions suivantes :

Remplissage de 2 onglets

Seuls deux onglets doivent être remplis par l'auditeur : l'onglet « Base Commune » ainsi que l'onglet correspondant au type d'application audité.

Notation des règles

Seule la notation "Oui, Non ou N/A" est autorisée. Pour chacune des règles de sécurité, une notation doit être attribuée.

N.B.

La notation "N/A" ou "NON" **doit être limitée** et nécessite une **justification en commentaire**.

La notation N/A est utilisée lorsque la règle de sécurité ne dépend pas de l'éditeur mais de la structure utilisatrice ou n'est pas applicable au système.

Cas des architectures multiples

Si l'application possède plusieurs types d'architectures (ex : app Web et app mobile) ou d'infrastructures (SaaS, on-premise, etc.), **un formulaire doit être réalisé pour chaque partie**.

Exception : Si un type d'architecture est dédié à une partie de l'application ne traitant aucune donnée personnelle ou de santé (ex : commande en rayon pour les LGO), il n'est pas nécessaire de remplir un formulaire.

AGENCE DU NUMÉRIQUE EN SANTÉ

Présentation du formulaire de test d'intrusion

Nouvelle version du formulaire pour les LGC
(actualisé en septembre 2025)

Pour les autres dispositifs, le TI LGC
est présenté à titre indicatif

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?