sesam-vitale

Cahier des Charges SESAM-Vitale

Version 1.40 – Avril 2003

Annexe 7

Architecture et Sécurité

Intégrant l'Addendum n°8

CDC

GIE SESAM-Vitale
5, boulevard Marie et Alexandre Oyon – 72 019 LE MANS Cedex 2
www.sesam-vitale.fr

Ce document a été élaboré par le GIE SESAM-Vitale.

Sommaire

1 Introduction

La présente annexe a pour but de :

- Spécifier les exigences sécuritaires applicables aux solutions agréées.
- Décrire les différentes configurations et architectures techniques du Poste de Travail du Professionnel de Santé autorisées dans le cadre de l'agrément SESAM-Vitale.
- Définir parmi les configurations autorisées celles devant faire l'objet d'un dossier de sécurité soumis à l'agrément et celles devant faire l'objet d'une déclaration des fonctions de sécurités mises en œuvre sur la solution présentée :
  - Dans le premier cas (réalisation d'un dossier de sécurité), le dossier sera examiné lors de la phase d'agrément pour vérifier la conformité de la solution proposée aux présentes exigences de sécurité.
  - Dans le second cas (déclaration des fonctions de sécurités mises en œuvre), la déclaration est fournie à titre informatif et n'a pas d'incidence sur l'obtention de l'agrément de la solution.

2 Acronymes, définitions et références

Tableau 1 : acronymes

Terme	Définition
API	Application Programming Interface
CNIL	Commission Nationale de l'Informatique et des Libertés
CPS	Carte Professionnel de Santé
DAM	Domaine Assurance Maladie
DRE	Demande de Remboursement Electronique
FSE	Feuille de soins électronique
FSV	Fournitures SESAM-Vitale
GIE S/V	GIE SESAM-Vitale
HSM	Hardware Security Module
LAN	Local Area Network (Réseau local utilisant typiquement une connectivité Ethernet ou Wi-Fi)
LV	Lecture Vitale (services de pré-lecture des données Vitale)
NCC	Numéro de Certificat de Conformité
OCT	Organisme Concentrateur Technique
OS	Operating Systeme (Système d'exploitation)
OWASP	Open Web Application Security Project, https://www.owasp.org
PAN	Personal Area Network (Réseau « personnel », utilisant typiquement une connectivité de type Bluetooth)
PS	Professionnel de Santé
RAC	Référentiel Accès cartes
RGS	Référentiel Général de Sécurité
SV	SESAM-Vitale
TL	Terminal Lecteur
TLA	Terminal Lecteur Application (TL déporté)
TLS	Transport Layer Security
WAN	Wide Area Network (Réseau couvrant une région très étendue, typiquement de type réseau de téléphonie mobile ou internet)

Tableau 2 : définitions

Termes	Définition
Composant	Ensemble des éléments logiciels ou matériel nécessaires à l'exécution des fonctions SESAM-Vitale de l'équipement (facturation, certification des factures, lecture ou écriture d'une carte) et des fonctions de sécurité de la solution. Selon l'architecture de la solution, cela peut par exemple inclure des applications, l'OS et également l'espace mémoire des données applicatives liées à ces composants.
Environnement physique	Décrit l'ensemble des locaux et/ou bâtiments (distant et/ou local) hébergeant tout ou partie de la solution. L'environnement physique d'un Professionnel de Santé sera par exemple un cabinet ou une pharmacie. L'environnement physique d'un service distant sera par exemple un « data center ».
Équipement	L'équipement est le composant physique de la solution manipulé par l'utilisateur comprenant le matériel (dont le lecteur de carte) et le logiciel associé.
Lecteur	Le lecteur désigne le dispositif permettant d'accéder aux cartes Vitale et CPS. Celui-ci peut aussi comporter un clavier, un afficheur, une connectique,...
Opérateur de la solution	Ensemble des acteurs chargés de l'exploitation ou de la maintenance de tout ou partie de la solution et de son infrastructure, y compris les sous-traitants éventuels.
Editeur	Acteur faisant la demande d'agrément de la solution auprès du CNDA. L'éditeur n'est pas nécessairement l'opérateur de la solution.
Utilisateur de la solution	Acteur final « client » de la solution agréée à qui elle est destinée. Il s'agit en général d'un Professionnel de Santé.
Solution	La solution désigne le système informatique global répondant au présent cahier des charges. Il inclut typiquement : Un ou plusieurs *équipements* client, pouvant éventuellement être interconnectés sous forme d'un ou plusieurs *environnements locaux* ; Un ou plusieurs *environnements distants*
Environnement Distant	L'environnement distant désigne un système informatique situé hors de l'environnement physique de l'utilisateur, offrant un service au travers d'une connexion réseau.
Environnement local	L'environnement local désigne le système informatique situé dans l'environnement physique de l'utilisateur.

Tableau 3 : références externes

Référence	Titre
CNIL	Commission Informatique et Liberté : http://www.cnil.fr/
ANSSI-RGS	Référentiel Générale de sécurité (RGS) : http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/
ANSSI-NOTES	Bonnes pratiques à destinations des industriels : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
RFC-TLS	TLS désignera dans ce document la dernière version disponible du protocole Transport Layer Security. A date de rédaction de ce document, il s'agit de la version 1.2 (https://tools.ietf.org/html/rfc5246)
DECRET-2007-960	Ministère de la santé et de la solidarité : Décret n°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique
ASIP-PGSSIS	Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), http://esante.gouv.fr/services/referentiels/securite/pgssi
ANSSI-MDP	Recommandations de sécurité relatives aux mots de passe, http://www.ssi.gouv.fr/guide/mot-de-passe/
ANSSI-SYSTEME	Recommandations de configuration d'un système GNU/Linux, DAT-NT-28/ANSSI/SDE/NP, http://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/
ANSSI-PASSERELLE	Guide de définition d'une architecture de passerelle d'interconnexion sécurisée, 3248/ANSSI/ACE, http://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
HDS	Référentiel hébergeur de données de santé : http://esante.gouv.fr/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des

Tableau 4 : Documents de référence

Référence	Titre
GUIDE	Guide de rédaction du dossier de sécurité (PDT-GU-009)
FORMULAIRE	Déclaration des fonctions de sécurité mises en œuvre (PDT-GU-010)

3 Biens et fonctions sensibles à protéger

Le chapitre suivant décrit les biens sensibles à protéger par la solution soumise au présent référentiel d'exigences.

Ce référentiel d'exigence de sécurité ne traite pas de données de santé, il n'y a donc pas de données sensibles associées. En revanche, le référentiel identifie des biens à protéger parmi les données médico-administratives et les données sensibles de la solution elle-même (par exemple les éléments cryptographiques servant à protéger ces données sensibles).

Les biens sensibles identifiés ci-après sont classifiés en termes d'intégrité et de confidentialité de la façon suivante :

Classification	Intégrité	Confidentialité
Moyen	Simple contrôle d'intégrité et de syntaxe des données	Diffusion restreinte aux personnes ayant besoin d'en connaître le contenu
Fort	Authenticité et intégrité de la donnée garanties	Informations spécifiques (données médicales, fort impact sécurité)

3.1 Biens liés aux bénéficiaires de soins et aux PS

Dénomination	Biens sensibles
Données sensibles bénéficiaire	Données sensibles administratives et médico-administratives stockées dans le support Vitale du bénéficiaire ou tout autre support. • Sont considérées comme sensibles « Moyen » en confidentialité : ○ Le NIR, nom et prénom du bénéficiaire ○ Le code couverture du bénéficiaire de soins ○ Les périodes de droits AMO et AMC • Sont considérées comme sensibles « Moyen » en intégrité : ○ Toutes les données issues du support Vitale
Données sensibles PS	Données sensibles administratives et médicaux-administratives stockées dans la carte CPS ou tout autre support. • Sont considérées comme sensibles « Moyen » en confidentialité : ○ DAM – Informations nécessaires à la facturation ○ L'identifiant du PS • Sont considérées comme sensibles « Moyen » en intégrité : ○ Toutes les données issues de la carte CPS

Dénomination	Biens sensibles
Données cryptographiques CPS	Code porteur CPS (code authentifiant le PS sur la carte) : « Fort » en confidentialité et intégrité.

3.2 Biens liés à la création, certification et télétransmission des FSE/DRE

Dénomination	Biens sensibles
Données de facturation	Ces données incluent : • Les données sensibles du bénéficiaire et du PS issues du support Vitale et de la CPS • Les FSE et DRE dans leur ensemble Sont considérés comme sensibles « Moyen » en intégrité : ○ tous Sont considérés comme sensibles « Moyen » en confidentialité : ○ Les données des FSE/DRE faisant l'objet d'un chiffrement applicatif
Données d'authentification PS	Les données d'authentification PS incluent : • Les données d'authentification pour accéder à l'environnement distant, si la solution inclut un environnement distant : « Fort » en confidentialité et intégrité.
Applications et données hors SESAM Vitale	Cette catégorie recouvre les applications et données résidant dans la solution hors SESAM-Vitale, mais pouvant impacter les biens SESAM-Vitale, notamment : • Les clés propres à l'industriel, certificats, autorités de confiance. • Le système de mise à jour de la solution et les clés associées • Système de contrôle d'accès et clés associées

3.3 Fonctions liées à la création, certification et télétransmission des FSE/DRE

Dénomination	Biens sensibles
Acquisition des données bénéficiaires	Fonction permettant l'acquisition dans la solution des données bénéficiaires de soins en provenance du support Vitale ou tout autre support

Dénomination	Biens sensibles
Acquisition des données PS	Fonction permettant l'acquisition dans la solution des données d'identification du PS
Réalisation des factures	Fonction permettant l'acquisition des données constitutives des factures, leur formatage et leur sécurisation.
Transmission des factures	Fonction permettant la transmission des factures réalisées vers l'assurance maladie.

4 Objectifs de Sécurité

Le référentiel est structuré en fonction des besoins de sécurité principaux des solutions :

- La protection des biens liés aux bénéficiaires de soins et au PS
- La protection des biens et fonctions liés à la création, certification et télétransmission des FSE/DRE

De ces deux besoins principaux découlent les objectifs présentés dans le tableau suivant. Ces objectifs sont déclinés en exigences dans la suite du document.

Gestion de la sécurité

L'éditeur doit mettre en œuvre une organisation permettant la gestion de la sécurité de sa solution. Cette gestion doit être effective tout au long de la durée de vie du produit (phases de conception, développement, déploiement, fonctionnement, mise au rebut).

Protéger l'environnement local

- *Autoprotection logique des équipements de la solution*

L'éditeur doit s'assurer de la protection logique des équipements de la solution, principalement au travers de mesures permettant de :

- minimiser la surface d'attaque logicielle de sa plate-forme.
- assurer l'intégrité et l'authenticité de ses composants
- assurer un contrôle d'accès et une traçabilité des opérations sensibles

Protection des données et fonctions sensibles

Les données sensibles stockées et traitées par la solution doivent être protégées. La solution doit implémenter divers mécanismes afin que seules les personnes autorisées et les applications authentiques SESAM-Vitale puissent manipuler les informations et fonctions sensibles.

Les principaux biens et fonctions sensibles à protéger sont listés au chapitre 3.

Protéger les communications

La solution et ses composants ne doivent accepter que les flux nécessaires et autorisés. Les données transitant par ces flux doivent être protégées.

La solution ne doit utiliser que des protocoles de communication à l'état de l'art de la sécurité (conformes RGS) garantissant la confidentialité, l'intégrité et l'authenticité des données pendant leur transmission.

Toutes les communications entre composants passant par un réseau ou par une liaison sans fil sont concernées

Protéger l'environnement distant

L'éditeur doit s'assurer de la protection logique et physique de l'environnement distant.

- *Autoprotection physique de l'environnement distant*

Une gestion des accès à la ou aux salle(s) hébergeant l'environnement distant doit être réalisée.

- *Autoprotection logique de l'environnement distant*

Des mesures de sécurité logiques couvrant les architectures et composants doivent être mises en place.

- *Contrôle d'accès à l'environnement distant*

Un contrôle d'accès et une gestion des habilitations doivent être mis en place.

Tableau 5 : objectifs de sécurité

5 Exigences de sécurité

5.1 Introduction

Ce chapitre a pour objectif la définition des exigences de sécurité applicables à toute solution répondant au présent cahier des charges. Ces exigences de sécurité sont des exigences contractuelles demandées par le GIE SESAM-Vitale.

Certaines des exigences peuvent être issues des bonnes pratiques *ANSSI-NOTES* émises par l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI).

Ce référentiel ne reprend pas les exigences générales relatives au respect de la législation française et internationale en vigueur, qui doivent par ailleurs être respectées par les éditeurs.

On notera ainsi que les exigences de sécurité ne se substituent en aucun cas aux exigences d'autres référentiels tels que, par exemple :

- Décret N°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique,
- Décret n°2006-6 du 4 janvier 2006 pour l'agrément des hébergeurs de données de santé à caractère personnel.
- Décret n° 98275 du 9 avril 1998 relatif à la carte d'assurance maladie.
- Décret 98-271 du 9 avril 1998 relatif à la carte de professionnel de santé (CPS).
- La PGSSI-S de l'ASIP Santé

Les exigences de ce référentiel couvrent :

- la solution dans son ensemble couvrant l'environnement local et les environnements distants,
- des processus organisationnels mis en place par l'éditeur.

Toute solution élaborée par un éditeur doit être conforme à l'ensemble des exigences listées dans ce chapitre.

Enfin, il est rappelé que l'usage du support Vitale et de la CPx implique de respecter une colocalisation du support et de son porteur :

- La carte CPx doit rester sous le contrôle de son porteur tant au niveau physique que logique.
- Le support Vitale doit rester sous le contrôle de son porteur tant au niveau physique que logique.

5.2 Gestion de la Sécurité

L'éditeur doit mettre en œuvre une organisation permettant la gestion de la sécurité de sa solution. Cette gestion doit être effective tout au long de la durée de vie de la solution (phases de conception, développement, déploiement, fonctionnement, mise au rebut).

5.2.1 Règles de gestion de la sécurité

G1 : ANALYSE DE RISQUES

L'éditeur doit conduire une analyse des risques de sa solution. L'éditeur doit identifier les biens sensibles et les risques associés, permettant d'identifier les mesures de sécurité à mettre en œuvre dans la solution.

Le processus mis en place doit être décrit dans le dossier sécurité.

G2 : GESTION DES BIENS SENSIBLES

L'éditeur doit décrire la gestion des biens sensibles dans sa solution. Cette description comprend a minima :

- l'ensemble des biens sensibles de la solution,
- l'usage et l'utilisation de chacun de ces biens,
- les mécanismes de protection de ces biens.
- les évènements de sécurité donnant lieu à un effacement de certains biens sensibles.

Bien cryptographiques :

L'éditeur doit recenser les biens cryptographiques utilisés (clés, certificats - y compris les clés remises par le GIE SESAM-Vitale), ainsi que leurs usages (algorithmes, protocoles).

Protection des clés :

L'éditeur décrira les moyens mis en œuvre pour assurer la confidentialité, l'authenticité et l'intégrité des biens cryptographiques utilisées tout au long du cycle de vie de celles-ci. Cela comprend :

- La génération,
- Le transport,
- Le chargement dans l'équipement,
- Le stockage,
- Le traitement,
- L'effacement

En cas d'atteinte à la confidentialité de clé cryptographique secrète (perte ou vol), celle-ci doit faire l'objet d'une révocation.

La description des biens sensibles doit figurer dans le dossier de sécurité.

G3 : **AUDIT DE LA SOLUTION :**

Audit de l'équipement :

L'éditeur doit présenter son plan d'assurance visant à vérifier la bonne mise en œuvre et l'efficacité des mesures de sécurité mises en place dans l'équipement (audit de configuration, audit de code, etc.).

L'éditeur décrira le processus de vérification sécuritaire mis en œuvre et précisera les composants audités

Audits de l'environnement distant :

L'éditeur doit mener des audits techniques (y compris tests d'intrusion) et organisationnels afin d'identifier et corriger les éventuelles vulnérabilités et tester l'efficacité des mesures de sécurité mises en place.

Ces audits devront donner lieu à l'élaboration de plans d'actions devant être mis en œuvre par l'éditeur.

Le processus mis en place doit être décrit dans le dossier sécurité.

G4 : **FORMATION ET SENSIBILISATION DU PERSONNEL**

Le personnel intervenant dans les phases de conception, développement, déploiement, maintenance doit être formé et sensibilisé à la sécurité de l'information et aux bonnes pratiques de sécurité.

Le processus mis en place doit être décrit dans le dossier sécurité.

G5 : **CRYPTOGRAPHIE**

L'éditeur ne doit mettre en œuvre dans sa solution que des algorithmes et des protocoles conformes au RGS.

L'ensemble des algorithmes utilisés ainsi que leurs usages doivent être listés dans le dossier sécurité.

G6 : **GESTION DES CORRECTIFS DE SECURITE**

L'éditeur doit décrire son processus de gestion des correctifs de sécurité : il doit mettre en œuvre des mesures organisationnelles et techniques permettant de garantir le maintien de la sécurité de la solution, incluant à minima :

- Une veille relative aux vulnérabilités de l'ensemble des composants logiciels et matériels de la solution,
- La mise en œuvre des correctifs de sécurité (développement des correctifs, déploiement, assistance aux utilisateurs),
- La notification du GIE SESAM-Vitale en cas de faille identifiée.

Le processus mis en place doit être décrit dans le dossier sécurité.

G7 : **SUPERVISION ET GESTION DES INCIDENTS DE SECURITE**

L'éditeur met en place l'organisation et les outils lui permettant de réaliser une supervision des anomalies et événements de sécurité liés à la solution et à son système d'information.

Il s'appuie sur les journaux des systèmes d'infrastructure (pare-feu, outils de détection d'intrusions, contrôle d'intégrité, etc.) et des services liés à la solution.

L'éditeur dispose d'un processus de gestion des incidents. Il informe le GIE SESAM-Vitale de tous les incidents de sécurité dont il a eu connaissance portant atteinte aux données sensibles.

Le processus mis en place doit être décrit dans le dossier sécurité.

G8 : GUIDE D'INSTALLATION ET CONDITIONS D'UTILISATION

L'éditeur doit mettre à disposition des guides et conditions d'utilisation afin de permettre une bonne intégration et un usage dans de bonnes conditions de sécurité de sa solution au sein du système d'information du professionnel de santé.

Le guide doit rappeler les bonnes pratiques et besoins de sécurité ainsi que les conditions d'utilisation de la solution au niveau du SI PS (mises à jour de sécurité du système, présence d'un anti-virus, etc.). Il doit également indiquer la responsabilité de l'utilisateur vis-à-vis de la sécurisation de son système d'information et notamment de son réseau local (filaire, wifi…).

Ces éléments doivent figurer dans le contrat de mise à disposition de la solution aux clients / utilisateurs ou dans une de ces annexes (CGU…). Le guide doit être fourni en annexe du dossier sécurité.

5.3 Protéger l'environnement local

5.3.1 Règles d'autoprotection logique des équipements de l'environnement local

L'éditeur doit s'assurer de la protection logique des équipements de l'environnement local, principalement au travers de mesures permettant de :

- minimiser la surface d'attaque logicielle de sa plateforme.
- assurer un contrôle d'accès et une traçabilité des opérations sensibles
- assurer l'intégrité et l'authenticité de ses composants

EL1 : Traçabilité des événements de sécurité

La solution doit conserver une trace des opérations sensibles et des événements de sécurité.

La solution doit tracer au minimum les éléments suivants :

- Modification du firmware/système d'exploitation/noyau
- Chargement/suppression d'éléments cryptographiques
- Modification de certificat
- Modification de chaine de confiance
- Ajout/mise à jour/suppression d'application

Les traces ne doivent pas contenir de données sensibles.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

EL2 : Renforcement du Système d'Exploitation

La configuration des composants logiciels de la solution doit être sécurisée, notamment :

- désactivation des services réseaux inutiles,
- restriction du code présent dans la solution : présence uniquement des applications et bibliothèques nécessaires au fonctionnement de la solution,
- désactivation des fonctions de debug logicielles,
- désactivation des comptes inutiles,
- configuration des systèmes de fichier selon le principe de moindres privilèges,
- protection contre l'exploitation de vulnérabilité (ASLR, etc.)

Les mécanismes mis en place pour renforcer la sécurité de l'équipement doivent être décrits dans le dossier sécurité.

Recommandation : dans le cas de systèmes d'exploitation standards, l'industriel pourra s'appuyer sur des guides de bonnes pratiques de renforcement de la sécurité publiés par l'ANSSI tel que ANSSI-SYSTEME.

EL3 : Effacement sécurisé des données sensibles

La solution doit mettre en œuvre un mécanisme d'effacement sécurisé, couvrant notamment l'effacement après usage.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

5.4 Protéger les données et fonctions sensibles

5.4.1 Règles de protection des données

Les données sensibles stockées et traitées par la solution doivent être protégées en confidentialité et en intégrité selon leur classification. La solution doit protéger la confidentialité des biens sensibles en implémentant divers mécanismes et en assurant que seules les personnes autorisées et les applications SESAM-Vitale peuvent manipuler les informations sensibles.

Les principaux biens sensibles à protéger sont listés au chapitre 3.

SP1 : Intégrité des données

La solution doit garantir et contrôler l'intégrité des données sensibles classées « Fort » à l'aide de mécanismes cryptographiques conformes au RGS.

En cas d'altération, la solution doit être rendue inutilisable.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

SP2 : Confidentialité des données

La confidentialité des données sensibles classées « Fort » de la solution doit être assurée à l'aide de mécanismes cryptographiques conformes au RGS.

La confidentialité des éléments sensibles doit être garantie pendant les opérations d'administration (mise à jour des logiciels, clefs, etc.).

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

SP3 : Contrôle d'accès, habilitation

Les actions ayant un impact sur les données sensibles ou les mécanismes de sécurité de la solution doivent faire l'objet d'une authentification et d'une vérification des droits par la solution.

Un mécanisme d'habilitation doit être mis en œuvre selon le principe du moindre privilège.

Pour les utilisateurs de la solution : utilisation de la CPS ou d'une authentification double facteur.

Pour les opérations d'administrateurs ou de maintenance : carte à puce ou authentification double facteur.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

SP4 : Mémorisation du code porteur de la CPS

La mémorisation du code porteur de la Carte du Professionnel de Santé (CPS) est interdite sauf sur des équipements Lecteur autonomes, mobiles et alimentés par batterie. Dans ce cas, la donnée doit être protégée en confidentialité et en intégrité selon les exigences définies ci-dessus.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

5.4.2 Règles de protection des fonctions

Un contrôle d'accès et une gestion des habilitations sur les fonctions sensibles, qu'elles soient sur l'environnement local ou sur l'environnement distant, doivent être mis en place.

SA1 : Contrôle d'accès, habilitation

Des mécanismes de contrôle d'accès et de gestion d'habilitation des utilisateurs doit être mise en œuvre.

Les accès doivent être gérés à l'aide de comptes individuels, et se limiter aux opérations autorisées pour le rôle ou groupe auquel appartient l'utilisateur.

L'organisation et les mécanismes de contrôle d'accès mis en place doivent être décrits dans le dossier sécurité.

SA2 : Journalisation et traçabilité

Le système doit être en mesure de conserver :

- l'historique des accès à son système d'information,
- l'établissement de sessions avec les équipements afin de permettre de vérifier le non-détournement des connexions au sein de la solution,
- les actions d'exploitation (administration, configuration, etc.) des systèmes.

Ces traces doivent être horodatées et doivent contenir les informations d'identification du correspondant distant. Ces informations doivent être conservées pendant une période de 12 mois au minimum.

Ces traces ne doivent pas contenir d'informations sensibles.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

SA3 : Politique de mots de passe

Une politique de mots de passe doit être mise en œuvre pour permettre un contrôle d'accès robuste. Celle-ci doit prévoir de limiter le nombre de tentatives et identifier les cas provoquant le blocage des comptes.

Dans le cas d'un blocage de compte, un administrateur doit réinitialiser le mot de passe et le transmettre à l'utilisateur de manière sécurisée, c'est-à-dire après vérification de son identité.

La politique de mots de passe doit être décrite dans le dossier sécurité.

SA4 : Durée des sessions utilisateur

Les sessions doivent expirer après un temps d'inactivité. Passé ce délai, le système doit fermer ou verrouiller la session.

Pour reprendre alors la session, l'utilisateur doit s'authentifier à nouveau.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

5.5 Protéger les communications

5.5.1 Règles de protection des communications

La solution et ses composants ne doivent accepter que les flux nécessaires et autorisés. Les données transitant par ces flux doivent être protégées.

La solution ne doit utiliser que des protocoles de communication à l'état de l'art de la sécurité (conformes RGS) garantissant la confidentialité, l'intégrité et l'authenticité des données pendant leur transmission.

Toutes les communications entre composants passant par un réseau ou par une liaison sans fil sont concernées.

C1 : Contrôle des flux

La solution et ses composants ne doivent accepter que les flux nécessaires et autorisés.

- L'ensemble des flux autorisés et interdits doivent être identifiés,
- Un filtrage des flux doit être mis en œuvre.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

C2 : **Authentification mutuelle et chiffrement**

Pour toutes les communications entre deux composants de la solution, des algorithmes cryptographiques conformes au RGS doivent être utilisés.

- Un chiffrement de bout en bout est requis,
- Une authentification mutuelle des deux parties doit être mise en œuvre :
  - Entre l'utilisateur et les environnements distants : l'authentification de l'utilisateur doit se faire par carte CPS ou par une authentification forte double facteur.
  - Entre deux composants de la solution : l'authentification doit être effectuée à partir de certificats.

  Dans le cas où des certificats sont utilisés, la vérification de ces derniers doit porter sur :
  - la parenté (autorité de confiance)
  - la validité (date début et de fin)
  - l'usage (authentification ou authentification serveur)
  - La révocation éventuelle du certificat (CRL ou requête OCSP)
- Les suites de chiffrement activées doivent être listées

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

C3 : **Protocoles sans fil**

Les protocoles sans fil doivent être configurés de manière à fournir une couche d'authentification, d'intégrité et de chiffrement conforme au RGS.

Pour les solutions n'offrant pas en natif une implémentation conforme au RGS (solution Bluetooth par exemple), le GIE-SESAM-Vitale exige une protection applicative conforme au RGS (par exemple TLS).

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

C4 : **Validation par l'utilisateur des accès distants à l'équipement**

L'établissement d'une connexion entre un équipement et un service distant doit toujours être à l'initiative de l'utilisateur de l'équipement.

Toute connexion entrante doit être validée par l'utilisateur.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

5.6 Protéger l'environnement distant

5.6.1 Règles de protection physique de l'environnement distant

Remarque : Si la solution n'intègre pas d'environnement de ce type, cette section est non applicable.

Une gestion des accès à la ou aux salles hébergeant l'environnement distant doit être réalisé.

DO1 : **Accès à /aux salle(s) d'hébergement**

La ou les salles hébergeant l'environnement distant de la solution doit être équipée d'un système de contrôle d'accès. Seuls les personnels habilités doivent pouvoir y accéder.

Une revue des accès doit être effectuée périodiquement pour s'assurer que tout accès obsolète soit bien supprimé.

L'organisation et les moyens de contrôle d'accès mis en place doivent être décrits dans le dossier sécurité.

5.6.2 Règles d'autoprotection logique de l'environnement distant

Des mesures de sécurité logiques couvrant les architectures et composants doivent être mises en place.

DL1 : **Cloisonnement réseau**

L'isolation des composants de l'environnement distant doit être assurée vis-à-vis :

- Du réseau local
- D'internet
- Du réseau de communication entre environnement distant et équipement (si distinct d'internet)

Un incident en provenance d'un des réseaux utilisés par la solution ne doit pas pouvoir se propager à un autre réseau. Le serveur d'application et les serveurs de données associés doivent être protégés en recourant à une ou plusieurs zones réseau dédiées.

La cartographie de l'environnement distant doit être décrite dans le dossier sécurité.

DL2 : **Renforcement des configurations**

La configuration des composants de l'infrastructure (serveurs, routeurs, etc.) doit être sécurisée :

- Changement des mots de passe par défaut,
- Suppression des services/daemons inutiles,
- Fichiers de configuration,
- Durcissement des droits d'accès sur le système de fichiers,
- utilisation de protocoles sécurisés (SSH, SFTP, etc.)
- utilisation d'un anti-virus sur les systèmes,
- Etc.

La configuration des composants doit être décrite dans le dossier sécurité

DL3 : **Intégrité des composants logiciels de l'environnement distant**

L'intégrité des composants logiciels de l'environnement distant doit être régulièrement vérifiée et supervisé.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

DL4 : **Protection des sauvegardes et archives**

La confidentialité des données sensibles stockées dans les sauvegardes et archives doit être assurée.

Les mécanismes mis en place doivent être décrits dans le dossier sécurité.

DL5 : **Effacement sécurisé des données**

Les données sensibles doivent être effacées de façon sécurisée.

L'industriel décrira dans le dossier de sécurité les techniques employées.

6 Les architectures du Poste de Travail

6.1 L'analyse sécuritaire dans le cadre de la procédure d'agrément

Les configurations du poste de travail acceptées dans le cadre de l'agrément SESAM-Vitale se classe en deux catégories :

- Les configurations hébergées dans un unique environnement local constitué de l'environnement physique de l'utilisateur de la solution soumise à agrément.
- Les configurations hébergées sur de multiples environnements locaux ou distants ou les configurations comprenant des équipements utilisant spécifiquement des liaisons sans fil[1].

La procédure à suivre pour tout éditeur souhaitant présenter un produit à l'agrément SESAM-Vitale est la suivante :

- lors de la conception de sa solution, l'éditeur doit identifier sur quelle catégorie de configuration sa solution se base ;
- en fonction de la configuration adoptée, l'éditeur doit s'assurer que sa solution respecte bien les exigences de sécurité fournies dans le présent document ;
- lors de la signature du protocole d'agrément avec le CNDA, l'éditeur doit déclarer sur quelle configuration ou combinaison de configurations sa solution présentée se base.

Si l'architecture de la solution est conforme à une des configurations « environnement local », le questionnaire relatif à la déclaration des fonctions de sécurité mises en œuvre sur la solution présentée (cf. FORMULAIRE) doit être rempli et fourni au CNDA.

Pour tout autre type d'architecture, un dossier de sécurité doit être transmis au CNDA (cf. *GUIDE*) qui s'assurera de la validité des fonctions de sécurité proposées par l'éditeur en effectuant une analyse dudit dossier. Celui-ci doit impérativement répondre à chacune des exigences de sécurité présentes dans ce document.

Il est également à noter que le CNDA se réserve le droit de vérifier par toute méthode de son choix la conformité des solutions agréées par rapport aux exigences de sécurité par exemple via un audit de la solution.

[1] Les équipements sans fil servant à l'acquisition des données issues de l'ApCV n'entrent pas dans cette catégorie et peuvent être utilisés dans un environnement local.

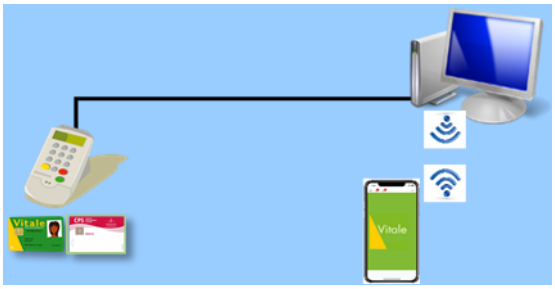
6.2 Les architectures « environnement local »

6.2.1 Généralités

Le présent chapitre décrit les différentes configurations acceptées dans le cadre de l'agrément se situant dans un unique environnement local constitué de l'environnement physique de l'utilisateur final de la solution présentée à l'agrément.

Pour ces configurations, il est demandé uniquement de remplir le questionnaire relatif aux fonctions de sécurité implémentée dans la solution (cf. FORMULAIRE)

6.2.2 Configuration 1 : Poste de Travail seul



Dans le cas d'un lecteur homologué, la liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

Dans le cas d'un lecteur PC/SC, seules les liaisons série et USB (filaire) sont autorisées.

Les équipements sans fil permettant l'acquisition des données de l'ApCV sont autorisés.

6.2.3 Configuration 2 : Réseau local

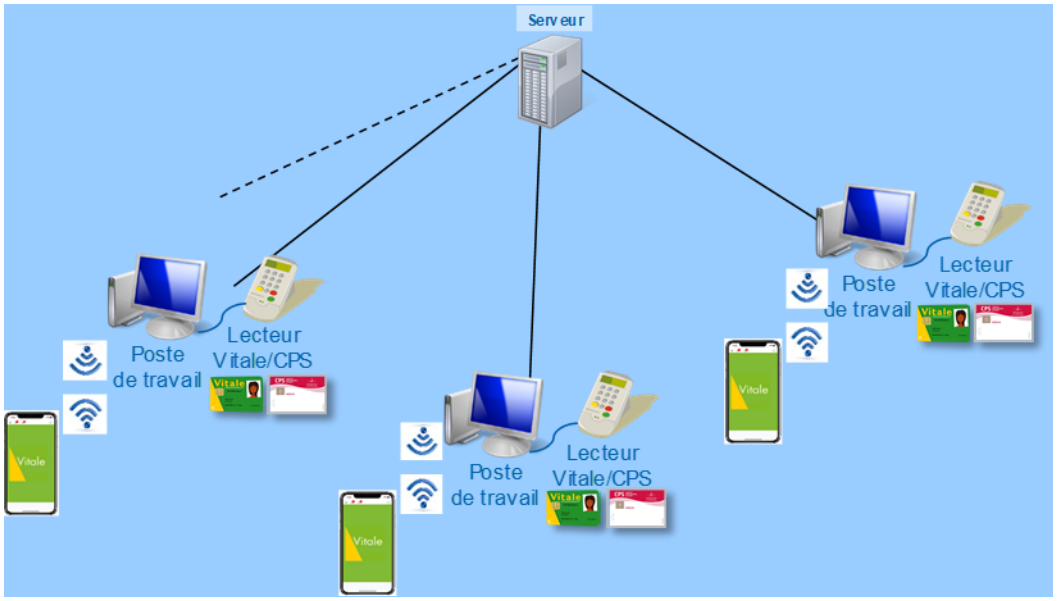
Les Postes de Travail sont connectés les uns aux autres mais restent dans un réseau local.

Dans le cas d'un lecteur homologué, la liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

Dans le cas d'un lecteur PC/SC, seules les liaisons série et USB (filaire) sont autorisées.

Les équipements sans fil permettant l'acquisition des données de l'ApCV sont autorisés.

6.2.4 Configuration 3 : Grappe de Postes de Travail en réseau local



Dans le cas d'un lecteur homologué, la liaison entre le poste de travail et le lecteur est obligatoirement une des liaisons pour laquelle le lecteur utilisé a été homologué.

Dans le cas d'un lecteur PC/SC, seules les liaisons série et USB (filaire) sont autorisées.

Les Postes de Travail sont connectés à un serveur mais l'ensemble des composants de la solution reste dans l'environnement local.

Les équipements sans fil permettant l'acquisition des données de l'ApCV sont autorisés.

6.2.5 Configuration : Configurations « réseau local » mixtes

Chaque Poste de Travail défini dans la configuration 3 peut être un des postes décrits dans la configuration 1, indépendamment des autres postes du réseau local.

Les configurations 2 et 3 peuvent être regroupées dans un même réseau local, le serveur de postes de la configuration 3 étant obligatoirement un serveur sur le réseau local. Le serveur de stockage est accessible par les Postes de Travail réalisant les factures et les lots.

6.3 Les architectures « environnements local et distant »

6.3.1 Généralités

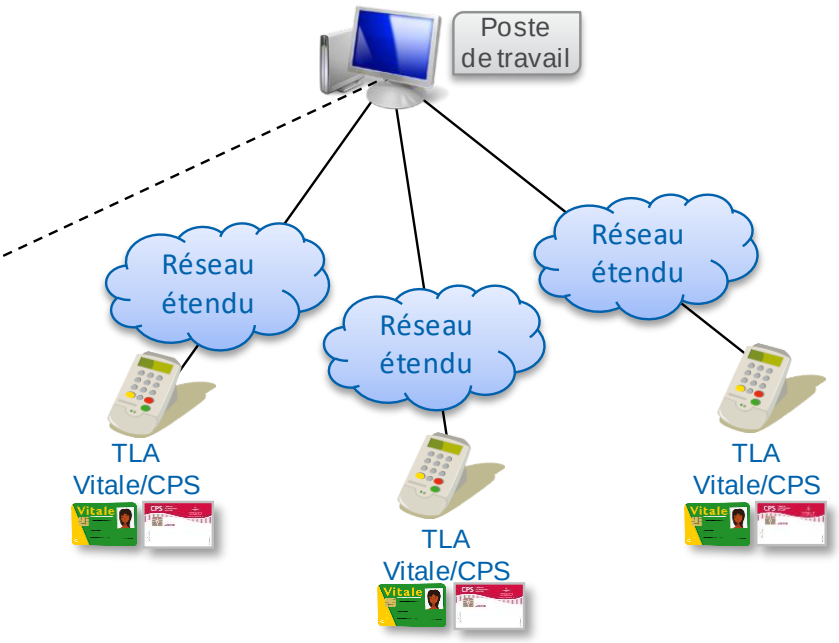
Le présent chapitre décrit les différentes configurations acceptées dans le cadre de l'agrément pour lesquelles il existe au moins un environnement distant ou au moins un équipement utilisant obligatoirement une liaison sans fil[2].

L'éditeur doit déposer au CNDA un dossier sécurité décrivant l'architecture technique et sécuritaire de sa solution. Ce dossier doit être rédigé sur la base des exigences fournies dans le présent document (cf. *GUIDE*).

6.3.2 Configuration 6 : TLA(s) distant(s)

Toute configuration proposant la connexion distante entre un TLA et un Poste de Travail entre dans cette catégorie. Dans cette configuration, le « Poste de Travail » peut être soit utilisé dans le cabinet du Professionnel de Santé soit géré par l'opérateur fournissant la solution de facturation.

NB : dans cette configuration, seules les fonctionnalités TLA peuvent être utilisées de manière distante.



Gestion de la sécurité, **Protéger les données et fonctions sensibles**	Ces exigences s'appliquent à l'ensemble de la configuration.
Protéger l'environnement local	Ces exigences s'appliquent à l'ensemble des lecteurs TLA
Protéger les communications	Ces exigences s'appliquent à l'ensemble des connexions entre le Poste de Travail et les lecteurs TLA
Protéger l'environnement distant	Ces exigences s'appliquent au Poste de Travail distant.

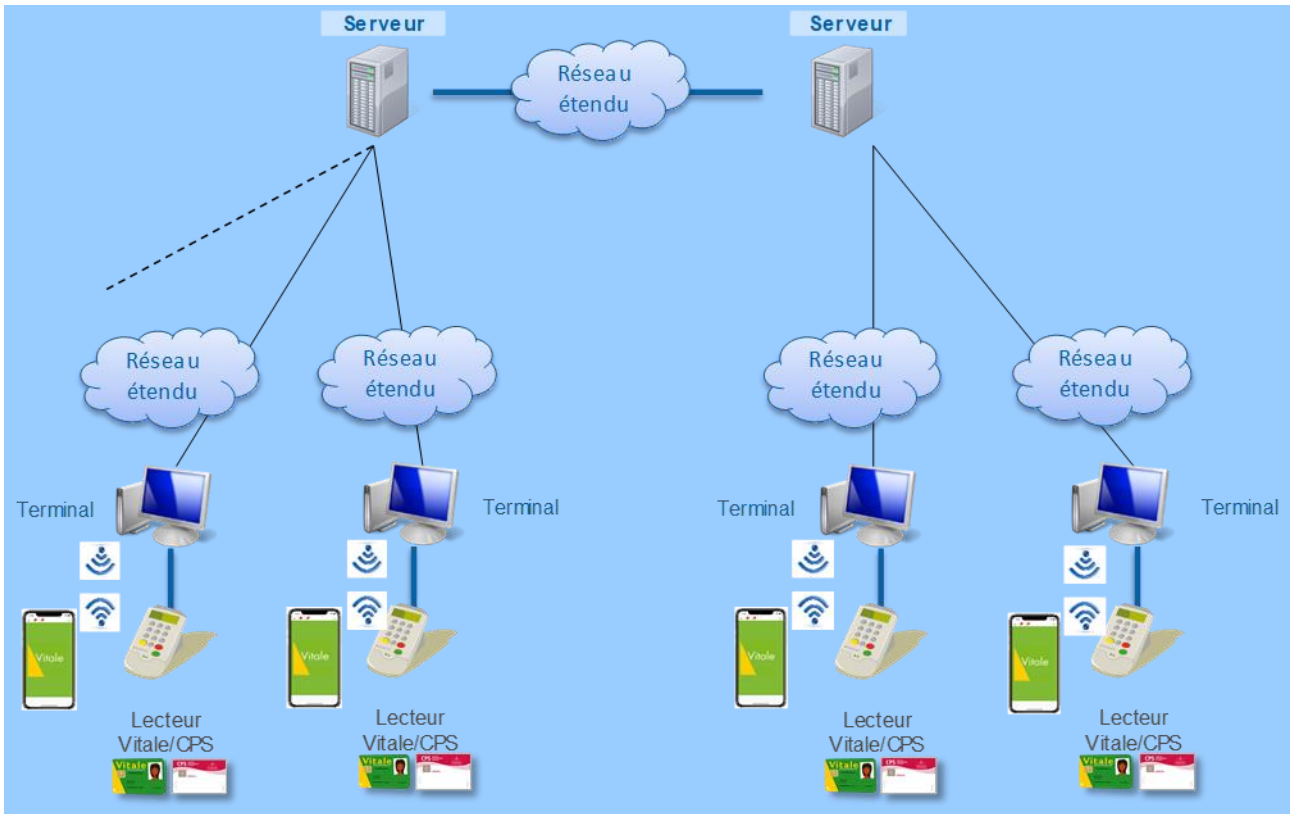
[2] Les équipements sans fil servant à l'acquisition des données issues de l'ApCV n'entrent pas dans cette catégorie et peuvent être utilisés dans un environnement local.

6.3.3 Configuration 7 : Gestion multiserveurs distants et multi Postes de Travail distants

Cette configuration décrit la connexion multipostes de travail à de multiples serveurs distants.

Pour cette configuration :

- le nombre de serveurs est supérieur ou égal à 1 ;
- des Postes de Travail peuvent être connectés à un serveur dans un même réseau local ;
- deux serveurs au moins peuvent être connectés dans un même réseau local ;
- au moins une des connexions « serveur – Poste de Travail » ou « inter serveurs » opère sur un réseau étendu.



Les exigences sécurité applicables sont les suivantes :

Gestion de la sécurité, **Protéger les données et fonctions sensibles**	Ces exigences s'appliquent à l'ensemble de la configuration.
Protéger l'environnement local	Ces exigences s'appliquent à l'ensemble des Postes de Travail
Protéger les communications	Ces exigences s'appliquent à : • l'ensemble des connexions distantes entre les Postes de Travail et les serveurs • l'ensemble des connections distantes entre les serveurs distants s'il y a plusieurs serveurs.
Protéger l'environnement distant	Ces exigences s'appliquent à l'ensemble des serveurs

NB : les progiciels opérant sous Citrix™ ou sous TSE™ entrent dans cette configuration.

6.3.4 Configurations 8 : Autres configurations

Cette configuration regroupe toutes les configurations qui ne rentrent dans aucune des configurations de 1 à 7 définies dans le présent document. L'éditeur doit malgré tout déposer au CNDA un dossier sécurité décrivant l'architecture technique et sécuritaire de sa solution. Ce dossier doit être rédigé sur la base des exigences fournies dans le présent document (cf. GUIDE).

Cette configuration comporte notamment les cas d'utilisation d'équipements spécifiques connectés au SI PS par une liaison sans fil (par exemple lecteur de carte embarquant une partie du logiciel soumis à l'agrément) ou des lecteurs de cartes non homologué RAC[3] connectés au SI PS avec une liaison autre qu'une liaison filaire USB ou série.

[3] L'utilisation d'un lecteur homologué RAC pour accéder aux cartes Vitale et CPS entre dans la configuration 1