Pré-requis pour une installation de i-Parapheur

Version 4.7.x

Libriciel SCOP

Libriciel SCOP

Document

Auteur	Stéphane VAST	***Date de diffusion***	13/09/2021
Chef de projet	Lukas HAMEURY	***N° de version***	4.7.x

Évolution du document

Version	Auteur	Nature des changements	Date
1.0	Stéphane VAST	Création du document selon la version 4.7.0	27/03/2020
1.1	Stéphane VAST	Ajout précisions sur flux réseaux (nexus, sentry)	16/04/2020
1.2	Stéphane VAST	Réévaluation des pré-requis RAM serveur à la hausse	6/05/2020
1.3	Stéphane VAST	Précisions sur accès Internet en exploitation, et sécurité TLS	9/09/2020
1.4	Stéphane VAST	Précisions sur RAM à 16Go, ajout de Ubuntu20.04, abandon de CentOS 8	25/01/2021
1.5	Stéphane VAST	Précisions poste de travail, environnements de bureau à distance	24/05/2021
1.6	Stéphane VAST	les applications tablette réclament Android 6 minimum	15/06/2021
1.7	Stéphane VAST	Ajout précision pour pré-requis télémaintenance update.libriciel.fr	13/09/2021
1.8	Stéphane VAST	Ajout précision pour pré-requis navigateurs compatibles	15/03/2022
1.9	Stéphane VAST	Ajout précision pour pré-requis serveur 'non graphique'	05/04/2022
1.10	Stéphane VAST	Docker est requis à compter de v4.7.8	14/04/2022
1.11	Stéphane VAST	Précision sur fins de vie RedHat 7, et Debian	27/07/2022
1.12	Mathias Martin	Ajout précision pour pré-requis OS et autres	27/09/2024
1.13	Mathias Martin	Clarification du dimensionnement disque — utiliser /opt au lieu de /data	30/10/2025
1.14	Mathias Martin	Ajout d'une note pré-requis rappelant l'obligation d'une BDD locale	07/01/2026

Licence

Libriciel SCOP

Table des matières

1. PRÉSENTATION

1.1. Objectifs

Ce manuel décrit succinctement les pré-requis à l'installation d'un serveur iparapheur version 4.7 sur un système d'exploitation GNU/Linux. Il s'adresse aux administrateurs techniques et systèmes de celui-ci.

1.2. Étendue

Outre les composants et ressources de base, on y parle également certificats électroniques pour connexions HTTPS serveur.

> Attention toutefois, l'installation est une opération relativement complexe; ce n'est pas un "setup.exe" en mode graphique. Elle réclame de nombreuses dépendances logicielles, et des compétences confirmées en administration système GNU/Linux.

2. LISTE DES SYSTÈMES D'EXPLOITATION SUPPORTÉS

Seuls les systèmes d'exploitation 64 bits suivants sont supportés :

OS serveur 64 bits	Statut
Ubuntu 22.04 LTS Server	**Supporté**
RedHat 8 (RHEL 8)	**Supporté**
Autres versions	`Non supporté`

> **Remarque :** L'installation sur un serveur 32 bits n'est pas supportée.

2.1. Migration vers la version 5

Nous recommandons vivement la migration vers la **version 5** pour bénéficier d'un socle plus récent. Les systèmes Ubuntu 22.04 et RedHat 8 sont les plateformes validées pour cette version.

3. DIMENSIONNEMENT ET RESSOURCES

Le dimensionnement disque peut être effectué tout en une même partition, ou plusieurs selon le choix assumé de l'exploitant technique.
Le formatage des partitions en **LVM** est fortement conseillé afin de pouvoir augmenter à chaud l'espace disque.

Le tableau suivant donne des valeurs indicatives :

Ressource	Quantité	Commentaires
Disque système (racine)	~20 Go	L'espace disque non-swap peut être réuni en une seule partition de 80 Go minimum
Disque " `/opt` "	Tests: >40 Go Prod: > 100 Go	**Répertoire de stockage principal des données de l'application iparapheur.** Il est recommandé de monter une partition dédiée sur /opt et de dimensionner cet espace selon la volumétrie cible de l'application.
Espace "swap"	> 3 Go	Il y a toujours besoin d'un peu de `swap`.
CPU 64 bits	4 à 32	**Indicateur minimum**, 6 recommandé
Quantité RAM	16 Go	> 10 Go de toute façon en test. Production: 16 Go minimum Indicateur minimum, augmenter selon le besoin

Explications détaillées :

- **CPU 64 bit** : 4 cœurs minimum: naturellement, plus de ressources il y a, mieux c'est. Avec 6,8, 12 coeurs ou davantage, l'application sera plus réactive et fluide.
- **Mémoire** : 16 Go (20 Go fortement recommandé) de **RAM minimum** pour le serveur. En effet il faut considérer en production les ordres de grandeur suivants
  - 3,5 Go de RAM minimum (5 à 6 Go recommandé) disponibles pour le cœur d'application (iparapheur)
  - 1 Go pour les composants back-office: MySQL
  - 1 Go pour NginX (4 workers d'environ 250Mo chacun)
  - 1 Go pour LibreOffice
  - 6-8 Go pour les conteneurs Docker (pastell-connector, pes-viewer, crypto, pdf-stamp, redis, libriciel-pdf)

Et tout cela, hors la consommation de ressources du système d'exploitation en lui-même.
Davantage de RAM aidera également l'application, pour absorber les pics de charge (sur les services "crypto" et "pes-viewer" en particulier).
Provisionner au moins 1Go de RAM supplémentaire en cas d'installation d'automates Pushdoc/Getdoc.

Si 30 utilisateurs simultanés ou 300 utilisateurs occasionnels (ce sont des MINIMA !) :

- Minimum RAM : 4 Go pour l'application, soit 16 Go pour la machine virtuelle
- Minimum CPU : 4 cœurs (soit 2x server-class CPU, ou 2xDual-core)

Si 100 utilisateurs simultanés ou 1000 utilisateurs occasionnels :

- Minimum RAM : 6 Go pour l'application, soit 20 Go pour la machine virtuelle
- Minimum CPU : 8-10 cœurs (soit 4x server-class CPU, ou 6xDual-core)

Selon la charge et/ou la qualité de service attendues, il est possible de répartir les composants sur différentes machines. (NB : la mise en cluster n'est pas supportée par les équipes techniques Libriciel SCOP).

> *NB :*
> • Prévoir un minimum de 40Go d'espace disque libre 'data' en mode "expérimentation".
> Pour une utilisation en **production, prévoir un minimum de 200Go** de disque pour les données, et 40Go pour la base de données.
> • Les valeurs de consommation mémoire sont des minima absolus de démarrage, et ne constituent pas des valeurs de confort ni de production. En effet, iparapheur s'appuie sur un moteur de GED Alfresco Community (et ses nombreuses dépendances) qui est un gros consommateur de ressources à lui tout seul.
> Ne pas hésiter à gonfler ces valeurs tant au niveau RAM que CPU.

> **Remarque importante :** iparapheur stocke toutes ses données dans le répertoire `/opt/iParapheur`. Il est donc essentiel de monter une partition dédiée et dimensionnée pour `/opt`, plutôt que d'utiliser `/data`.

Il est important de noter que certains éléments de iparapheur sont maintenant livrés sous forme de conteneurs Docker. La configuration des conteneurs est définie dans le répertoire `/opt/iParapheur`. Sur une installation fonctionnelle iparapheur, les services suivants sont hébergés dans des conteneurs :

- pastell-connector
- pes-viewer
- crypto
- pdf-stamp
- redis
- libriciel-pdf

Cette architecture en conteneurs permet une meilleure isolation des services et une gestion plus flexible des ressources. Cependant, elle nécessite une attention particulière lors du dimensionnement des ressources, notamment en termes de mémoire et d'espace disque.

4. COMMUNICATION RÉSEAU / INTERNET

4.1. Tableau de flux réseau

Voici la liste des ports utilisés en entrée et sortie.

Certains applicatifs doivent etres visibles depuis internet.

Protocole	Entrée	Sortie	Commentaires
HTTP (80 TCP)	Non	Oui	**http://validca.libriciel.fr** : récupération des AC et CRL RGS (politique de sécurité applicative)
HTTPS (443 TCP)	Non	Oui	**https://validca.libriciel.fr** : récupération des AC et CRL RGS (politique de sécurité applicative)
HTTPS (443 TCP)	Non	Oui	**https://libersign.libriciel.fr** : Entretien de LiberSign2
HTTPS (443 TCP)	Non	Oui	**https://update.libriciel.fr** : télémaintenance
HTTPS (443 TCP)	Non	Oui	**https://nexus.libriciel.fr** : Mise-à-jour de services Libriciel Concerne "crypto", "pes-viewer",...
HTTPS (443 TCP)	Non	Oui	**https://registry.libriciel.fr** : Mise-à-jour de "libriciel-pdf"
HTTPS (443 TCP)	Non	Oui	**https://hubdocker.libriciel.fr**
HTTPS (443 TCP)	Non	Oui	**https://sentry.libriciel.fr** : Remontée d'anomalies de services Libriciel Concerne "crypto", "pes-viewer", "pdf-stamp",...
HTTPS (443 TCP)	Non	Oui	**https://pypi.org** : Mise-à-jour de "iparapheur-utils"
HTTPS (443 TCP)	Non	Oui	**Serveur pastell** : En cas de mise en place du connecteur Pastell mail-sécurisé
HTTPS (443 TCP)	Oui	Oui	En entrée: si usage extranet En sortie: **www.s2low.org** ou **s2low.formations.libriciel.fr** Pour envoi des flux vers le TDT mail-sécurisé
SMTP (25 TCP)	Non	Oui	Généralement paramétré vers le relais SMTP local
LDAP (389 TCP)	Non	Option	si couplage annuaire pour synchronisation de comptes utilisateurs

> **NB** : Pendant l'installation, le serveur doit être connecté à internet (flux sortants full HTTP + HTTPS, sans proxy) afin de récupérer et installer les dernières mises-à-jour des composants logiciels nécessaires.

4.2. Accès nécessaires à ouvrir pour iparapheur

Reprenant les éléments du tableau précédent, les accès suivants sont nécessaires à l'exploitation :

- https://validca.libriciel.fr
- https://libersign.libriciel.fr
- https://nexus.libriciel.fr
- https://sentry.libriciel.fr
- https://update.libriciel.fr
- https://registry.libriciel.fr
- https://hubdocker.libriciel.fr

En outre, pour l'installation, ou une mise à jour de iparapheur:

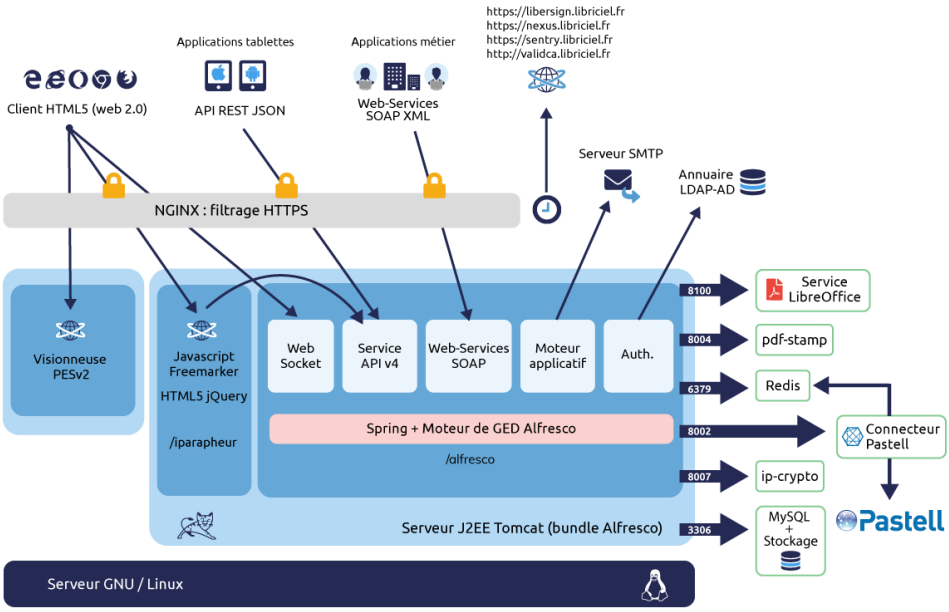
- Les ressources natives du système d'exploitation doivent être accessibles, et le gestionnaire de paquets `apt` ou `yum`) doit être opérationnel.
- https://ressources.libriciel.fr: téléchargement de ressources et utilitaires,
- https://omnitruck.chef.io: pour installer l'outil "Chef".
- https://omnitruck.chef.io: pour déployer via l'outil "Chef".
- https://mattermost.libriciel.fr : pour accéder à Mattermost.
- https://deploiement.libriciel.fr : pour le déploiement.
- https://download.docker.com : pour installer l'outil "Docker".

- https://github.com : pour installer la version temurin 8 de la JDK à l'URL complète https://github.com/adoptium/temurin8-binaries/releases/download/jdk8u352-b08/OpenJDK8U-jdk_x64_linux_hotspot_8u352b08.tar.gz
- https://rubygems.org : pour installer les libraiaires ruby.

5. SCHÉMA D'ARCHITECTURE

Le schéma d'architecture montre en substance les briques logicielles utilisées.

Ces briques peuvent être réparties sur différentes machines, nous conseillons de regrouper toutes ces briques dans un même serveur.



L'application iparapheur peut être exploitée en réseau local, ou être utilisée pour la réception de flux provenant d'Internet.

L'accès utilisateur à iparapheur s'effectue principalement par navigateur, une URL en domaine ou sous-domaine dédié sera nécessaire, par exemple : **iparapheur.mondomaine.fr**.

Dans le cas d'un accès nécessaire depuis l'extérieur, seront nécessaires :

- Une URL en domaine ou sous-domaine public
- L'accès au port 443 HTTPS devra être ouvert depuis l'extérieur du réseau et routé correctement vers le serveur (ex : NAT, reverse proxy).

> *Remarque* : À chaque instance de iparapheur (ex: test, qualification, production) doit être provisionnée sa propre machine.

6. BRIQUES TECHNIQUES

Voici la liste des briques techniques qui supportent l'application.

Ces briques sont des pré-requis, et seront déployées à l'installation (voir manuel d'installation); inutile de procéder à leur mise en place préalablement à l'intervention planifiée d'un technicien Libriciel SCOP.

Composant	Version	Commentaires
MariaDB ou MySQL	10 (MariaDB) 5.7 à 8.0 (MySQL)	par défaut sur le même hôte que l'application
NginX	> 1.8	points d'entrée HTTP/HTTPS. Prévoir certificats TLS serveur
LibreOffice	4.2.8 à 7.x	Génération de fichiers PDF, PDF d'impression
Alfresco Community	3.4.c	socle technique à usage dédié et exclusif
JAVA JDK	1.8_u171	En support du serveur d'application web
Python	3.x	pour procédures d'exploitation
Redis	> 3.0	Pour fonctionnement avec le connecteur Pastell
Docker	Dernière version stable	socle de "libriciel-pdf", à partir de v4.7.8

> **Note impérative :** la base de données doit résider localement sur le même serveur que l'application iparapheur (pas d'hébergement externe, de cluster, ni d'architecture N-tiers). Toute désynchronisation entre BDD et données disque rend l'instance irrécupérable et n'est pas couverte par le support.

> Autres moteurs de base de donnée : iparapheur v4.xx n'est pas conçu ni qualifié pour tourner sur les moteurs PostgreSQL, MS SQL-server ni Oracle.
> Seuls MariaDB et MySQL sont supportés, dans les versions précisées ci-dessus.

6.1. Points du serveur impactés

Installer iparapheur nécessite d'intervenir sur l'arborescence GNU/Linux:

- `/opt/` pour y déposer l'application iparapheur. Sinon, possibilité d'installer un lien symbolique de /opt/iParapheur -> [dir]/iParapheur
- `/etc/profile` pour configurer les variables d'environnement `JAVA_HOME`, et `LC_ALL`
- `/etc/nginx/` pour configurer les hôtes virtuels (modes HTTP, HTTPS et autorités de certification de confiance pour les certificats)
- `/tmp/` de taille respectable (5 Go minimum), pour effectuer les opérations courantes d'installation et d'usage.
- `/var/log/` pour y déposer les logs applicatives de Tomcat et Alfresco
- `/var/lib/` (alfresco/tmp/) pour y déposer des fichiers temporaires d'Alfresco
- `/etc/init.d/` pour y installer le script de démarrage de iparapheur, en qualité de service autonome.
- `/etc/systemd/system` pour y installer le script de démarrage des modules Connecteur Pastell et Pes-viewer

6.2. Autres points notables

Cette opération d'installation nécessite également des droits d'administrateur (root) afin de:

- installer les packages de distribution GNU/Linux correspondant aux pré-requis, ainsi que l'application
- configurer et relancer les services HTTP-HTTPS, MySQL, Postfix, CRON
- mettre à jour périodiquement la politique de sécurité HTTPS
- lancer/arrêter l'application iparapheur, effectuer les backups

> Notes : L'installation sur plate-forme serveur Microsoft Windows est théoriquement possible, mais cela reste non supporté à ce jour par l'équipe technique Libriciel SCOP: en particulier, le paramétrage HTTPS/TLS avec authentification forte par certificat y est délicat, en outre l'exécution de GhostScript n'y est pas thread-safe (donc dangereux et inexploitable en production).
> L'utilisation d'autres systèmes de base de données libres ou propriétaires (PostgreSQL, Oracle,...) n'est pas qualifiée ni supportée par Libriciel SCOP.

7. POSTE CLIENT

L'application iparapheur est développée dans le respect des standards du web (standard W3C), et nécessite les particularités suivantes :

- Activation de JavaScript,
- Acceptation des cookies de session,

> *NB* : Le port HTTPS (TCP 443) doit être ouvert entre les postes clients et le serveur d'application.

7.1. Navigateurs compatibles

Les logiciels produits par Libriciel SCOP sont développés principalement pourGoogle Chrome et Mozilla Firefox.

Libriciel SCOP assure la compatibilité de tous ses logiciels avec :

- la dernière version stable de Google Chrome;
- la dernière version de Mozilla Firefox;
- les versions ESR de Mozilla Firefox maintenues par Mozilla.

Bien que développés pour les standards du web, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont pas garantis :

- sur d'autres versions de Google Chrome (beta, canary) ou Mozilla Firefox (ESR non maintenues, anciennes versions) ;
- sur d'autres navigateurs (Microsoft Internet Explorer, Microsoft Edge, Apple Safari, Opera, ...) ;
- sur les technologies de bureau à distance (Citrix XenApp, Citrix XenDesktop, Microsoft RDS, Microsoft Terminal Server, ...), en particulier pour les fonctionnalités de signature électronique.

Remarques :

- Une expérience de bon fonctionnement avec Microsoft IE-11 ou Edge(Chromium) ne constitue pas motif d'éligibilité au support technique.
- À propos de Mozilla Firefox : Firefox ESR 102 est paru le 28 juin 2022
  Voir l' article WIKIPEDIA : https://en.wikipedia.org/wiki/Firefox_version_history
  La version "ESR 102" a pris fin le 12 septembre 2023.

7.2. Systèmes d'exploitation compatibles

D'une manière générale, Libriciel assure la compatibilité côté client avec la plupart des systèmes d'exploitations grand public maintenus par leurs distributeurs et permettant de faire fonctionner les navigateurs compatibles.

Néanmoins, le fonctionnement et l'affichage des logiciels produits par Libriciel SCOP ne sont garantis que sur les versions du système Microsoft Windows maintenues par Microsoft à destination des postes clients.

En particulier, les outils de signature (Libersign) ne sont développés que pour Microsoft Windows sur les architectures Intel-x86 et AMD-64, et ne fonctionnent pas avec d'autres systèmes d'exploitations.

Les systèmes d'exploitation suivants sont non supportés, car hors du support de Microsoft : Windows XP, Vista, Windows 7, 8 et 8.1.

7.3. Signature électronique sur poste PC Windows

L'outil de signature (LiberSign) s'adapte selon le navigateur utilisé:

- Pour Mozilla Firefox , Google Chrome , Microsoft Edge, ou Opera: pas "d'applet JAVA", car une extension de navigateur est utilisée, en liaison avec un "logiciel compagnon".
- Le logiciel compagnon est installé dans le répertoire utilisateur, normalement accessible sans droit administrateur.
- Remarque pour les postes sous contrainte (avec GPO ou restriction de droit de type Citrix): le poste utilisateur doit avoir accès au répertoire `%LOCALAPPDATA%`, directement utilisé par l'extension LiberSign
- Pour Microsoft Internet Explorer 11 : déploiement du plugin JAVA à jour, pour permettre la signature électronique. En l'absence de "magasin d'extensions", le recours au système d'applets JAVA reste obligatoire.

L'usage de certains serveurs mandataires (proxy HTTP et HTTPS) peut gêner le bon fonctionnement des applets Java de signature électronique.

Cas particulier : avec le navigateur Edge , sur Windows 10, le plugin "Sun/Oracle JAVA" n'est pas disponible.
La version sortie en Jan.2020 dénommée "Edge(Chromium)" permet l'installation des extensions du Chrome-web-store. Avec l'extension Libersign du Chrome-web-store, il devient possible de signer électroniquement avec ce navigateur.

7.4. Signature électronique sur poste Apple macbook (macOS), ou Linux

La signature électronique sur les ordinateurs Apple macOS n'est pas supportée.

Seule la plateforme Microsoft est supportée pour les opérations de signature électronique.
Sur les matériels Apple, seule la virtualisation Windows permet de signer électroniquement: par exemple, avec "VMware Fusion" ou "Parallels".

NB : Le support des certificats matériels (par exemple "RGS deux étoiles") sur Apple macOS nécessite un perpétuel re-développement, grâce aux changements incessants opérés par Apple dans la gestion des tokens USB.
Les experts de l'écosystème Apple sont bienvenus: vous pouvez contacter Libriciel SCOP, et contribuer à écrire du code libre compatible avec les nouvelles couches de sécurité cryptographiques pour chaque nouvelle version de macOS.

7.5. Cas des tablettes numériques (Android, iOS)

L'application iparapheur mettant en œuvre des fonctions de signature électronique, certains détails sont à noter sur tablette numérique:

- Apple i-Pad :
  - une application native est publiée et maintenue par Libriciel SCOP sur l'App Store (tm).
  - Elle permet toutes les opérations de consultation courante, annotations, visa/rejet.
  - Attention: En l'absence de support (USB, carte à puce) et de pilote pour certificat matériel (par exemple de type RGS deux étoiles), il n'est réglementairement pas possible d'y signer électroniquement les flux Actes.
- Android tablette (à partir de Google Android version 6) :
  - une application native est publiée par Libriciel SCOP sur Google Play (tm).
  - Elle permet toutes les opérations de consultation courante, annotations, visa/rejet, ainsi que signature avec certificat logiciel.
  - Attention: En l'absence de support et de pilote pour certificat matériel (par exemple de type RGS deux étoiles), il n'est réglementairement pas possible d'y signer électroniquement les flux Actes.
- Windows tablette tactile de type "Surface Pro" (processeur Intel x86) :
  - En réalité c'est un PC déguisé en tablette numérique ; iparapheur y fonctionne comme sur un PC classique depuis un navigateur.
  - Se référer aux pré-requis classiques pour poste de travail client.
  - Il n'existe pas d'application "client lourd" pour Windows tablettes ni sur le "Windows Store".

8. ANNEXE - POUR L'ENVIRONNEMENT D'EXPLOITATION

8.1. Nombre d'adresses IP à réserver

Configuration HTTPS: la multiplicité des connexions entrantes et sortantes nécessite une (voire deux) adresses IPv4 dédiées à iparapheur. Pour éviter la multiplicité des adresses IP à réserver, la configuration serveur se repose sur le système SNI (ServerName Indication) dans les connexions HTTPS.
Il faut DEUX adresses IP si l'environnement métier (se connectant avec iparapheur) ne supporte pas les connexions de type SNI, par exemple:

- si mise en SSO CAS, avec CAS ne supportant pas le SNI (si opéré avec tomcat6),
- si application tierce (par exemple opérée par tomcat6,...) ne supportant pas non plus le SNI

8.2. Certificats SSL pour service HTTPS

Les connexions iparapheur entrantes sont sécurisées par certificat électronique.
Pour chaque FQDN=*iparapheur.dom.local* (adapter naturellement le nom au besoin, il s'agit ici d'un exemple illustratif), il faut prévoir:

- 2 enregistrements dans le service DNS :
  - accès web sur `iparapheur.dom.local` ,
  - et web-services sur `secure-iparapheur.dom.local` (pour les applications métiers)
- Acquérir le ou les certificat(s) électronique(s) protégeant les noms FQDN*iparapheur.dom.local* + *secure-iparapheur.dom.local*
- Si usage de l'application tablette : prévoir 1 enregistrement supplémentaire dans le service DNS pour `m.iparapheur.dom.local`, et commander le certificat adéquat auprès de Libriciel SCOP.

8.3. Chiffrement HTTPS et sécurité TLS

Le protocole de sécurisation TLS a évolué dans sa version 1.3, voir la RFC8446. Cela donne les possibilités de sécurisation suivantes:

- SSLv2, SSLv3 : pas suffisamment robuste, abandonné pour iparapheur
- TLS 1.0, TLS 1.1 : actifs par défaut, modifiable dans la configuration
- TLS 1.2 : actif par défaut, modifiable dans la configuration
- TLS 1.3 : inactif par défaut.

L'ANSSI recommande de prendre en charge la version "`TLS 1.3`".
En particulier, dans son document de "Recommandations de sécurité relatives à TLS" :

- [R3] : Privilégier TLS 1.3 et accepter TLS 1.2
- [R4] : Ne pas utiliser SSLv2, SSLv3, TLS 1.0 et TLS 1.1

Cependant, ces recommandations ANSSI ne sont pas toujours adaptées à l'environnement d'exploitation, et aux clients (navigateurs, applications métier) qui se connectent à iparapheur.

Client navigateur	**TLS 1**	**TLS 1.1**	**TLS 1.2**	**TLS 1.3**
InternetExplorer 11	oui	oui	oui	NON
Edge 12-18	oui	oui	oui	NON
Edge Chromium 79+	oui	oui	oui	oui
Chrome 70+	oui	oui	oui	oui
Firefox 63+	oui	oui	oui	oui

Technologie d'Application métier	**TLS 1.2**	**TLS 1.3**
.NET sur Windows Server	depuis 2008r2	non
OpenSSL stack	v1.0.1a et +	v1.1.1 et +
Java stack	1.7.0_u131 et +	Java 11

De nombreuses applications métier actuellement en production s'appuient sur des composants dans des versions antérieures à celles indiquées dans le tableau ci-dessus, donc inaptes aux recommandations concernant TLSv1.3 et/ou TLSv1.2:

- Les applications basées sur "Axis 1.4" pour leurs web-services ne sont pas capables de tenir une négociation TLSv1.2, revenant en TLSv1. Exemple parmi d'autres, certaines versions de GFI-GECCO dialoguent avec iparapheur en "TLSv1", comme l'application KOLOK d'Arawak.

De même tous les systèmes serveur hébergeant iparapheur ne sont pas égaux sur la capacité à opérer avec un niveau de sécurité élevé, par exemple :

- CentOS 7 : incompatible TLS 1.3 avec les dépendances standards
- Ubuntu 16.04 : incompatible TLS 1.3 avec les dépendances standards

Ressources :

- TLS 1.2
- Can I use
- Site Microsoft
- La Chine bloque le HTTPS utilisant TLS 1.3 et ESNI

8.4. Couplages annuaires, SSO

8.4.1. Capacités LDAP / ActiveDirectory

Il est possible de synchroniser l'application iparapheur avec les comptes utilisateurs gérés sur un annuaire de LDAP (OpenLDAP), ainsi que Microsoft ActiveDirectory.
Si un tel annuaire est déjà en place, son organisation doit être connue de l'exploitant et avoir été communiquée au préalable, afin de créer le lien avec le parapheur. Ceci afin que les comptes d'utilisateurs inscrits dans l'annuaire soient importés et connus de iparapheur.

8.4.2. Capacités SSO

L'application iparapheur peut être connecté avec certains systèmes de web-SSO:

- "Apereo CAS" (ex- Jasig CAS): protocole v2 ou v3, avec usage nécessaire de PGT (proxy granting ticket). A noter que le protocole CASv1 n'est pas supporté. Peu importe la version du serveur CAS, du moment que la version de protocole est respectée.
- "Keycloak" : testé avec succès sur le protocole OpenID Connect.
- "LemonLDAP::NG".

Se rapprocher de Libriciel SCOP pour les modalités techniques et commerciales d'accompagnement à la mise en place.