



Spécifications Informatiques

Objet : Analyse CCTP Trieur-Spécifications informatiques

Direction émettrice : DSICI
Nom du rédacteur : R. BOISSEL

Date : 30-01-2026

Participants :
DSICI : L.MINIER - R.BOISSEL

Diffusion : C.GAMONET - S.DUVIVIER - L.SANSEIGNE - M.ADAMCZEWSKI

Table des matières

1	Spécifications	2
1.1	Spécifications fonctionnelles.....	2
1.1.1	Gestion des utilisateurs	2
1.1.2	Gestion des données.....	2
1.2	Spécifications non fonctionnelles	3
1.2.1	Performance	3
1.2.2	Sécurité.....	4
1.2.3	Compatibilité	4
1.2.4	Maintenance et évolution.....	5
1.2.5	Conformité	5
1.2.6	Archivage	6
1.2.7	Responsabilité fournisseur	6

1 SPECIFICATIONS

1.1 Spécifications fonctionnelles

1.1.1 Gestion des utilisateurs

Spécification ID	Spécification fonctionnelle	Détail
SF-001	Authentification utilisateur à l'application	La solution doit permettre aux utilisateurs de se connecter avec un identifiant et un mot de passe conforme à la PNSSI et aux recommandations de l'ANSSI. Le mot de passe doit être robuste (suffisamment long, complexe et aléatoire) de 12 caractères minimums pour les utilisateurs et de 16 pour les administrateurs. Il doit être composé avec des minuscules, des majuscules, des chiffres et des caractères spéciaux. L'application doit gérer la vérification de la robustesse du mot de passe.
SF-002	Gestion des rôles et permissions	La solution doit permettre de définir, attribuer, et modifier des rôles basés sur des permissions préconfigurées, incluant une gestion granulaire des autorisations basée sur le principe du moindre privilège, auditable et révisé périodiquement.
SF-003	Cycle de vie des comptes	La création, modification, désactivation et suppression des comptes doit être effectuée par des profils habilités.
SF-004	Réinitialisation de mot de passe	Les utilisateurs doivent pouvoir réinitialiser leur mot de passe. L'application doit en proposer le renouvellement au-delà de 90 jours et doit empêcher la réutilisation d'un mot de passe parmi les 5 derniers déjà utilisés. Les mots de passe ne doivent pas être stockés en clair par l'application.
SF-005	Déconnexion automatique	La solution doit automatiquement déconnecter les utilisateurs après une période d'inactivité de 30 minutes. Dans la mesure du possible ce délai doit pouvoir être configurable.
SF-018	Fonctionnement	L'application doit fonctionner en mode utilisateur et non administrateur

1.1.2 Gestion des données

Spécification ID	Spécification fonctionnelle	Détail
SF-011	Extraction de données	Les utilisateurs doivent pouvoir extraire des données en formats normalisés (Excel, PDF, XML, CSV) tout en respectant les permissions d'accès
SF-012	Gestion des données archivées	La solution doit permettre de rechercher, consulter et restaurer des données archivées de manière pérenne dans la durée en s'appuyant sur

		des formats de données standards [non propriétaire] (TXT, XML, PDF)
SF-013	Historique et audit	La solution doit conserver un historique des modifications effectuées sur les données et le paramétrage, incluant les informations sur l'auteur, l'horodatage, et les modifications précises.
SF-014	Impression	La solution doit permettre d'imprimer les résultats
SF-015	Recherche avancée	La solution doit permettre de filtrer, trier et paginer les données. Les données ainsi sélectionnées doivent pouvoir être exportées
SF-016	Mapping des données	Si présence d'un module de mapping (transcodage) celui-ci doit permettre une mécanisme de traçabilité des versions
SF-017	Export des données autre que vers SIL	Les utilisateurs doivent pouvoir de préférence exporter des données en formats normalisés standards

1.2 Spécifications non fonctionnelles

1.2.1 Performance

Spécification ID	Spécification non fonctionnelle	Détail
SNF-001	Temps de réponse	Les temps de réponse pour toutes les actions critiques (connexion, échange de données, recherche, sauvegarde) ne devront pas dépasser le délai acceptable défini en fonction de l'activité, même sous une charge moyenne. A préciser par le candidat.
SNF-002	Capacité de traitement	En fonction de la nature de l'activité le système devra pouvoir supporter plusieurs utilisateurs actifs simultanément sans dégradation notable des performances.
SNF-003	Sauvegarde \ restauration	Le fournisseur doit s'assurer de pouvoir réinstaller et reconfigurer l'automate dans le délai indiqué dans le marché. Il doit fournir les moyens nécessaires. L'EFS ne sauvegarde pas les données ni la configuration de l'automate. Seules les données transférées sur le serveur d'échange ou le serveur de rebond facultatif sont sauvegardés.
SNF-005	PRA - PCA	Les différents Mode opératoires, procédures et Mode dégradés doivent être présents, identifiés et testés
SNF-006	Sauvegarde / Archivage Des données	Les sauvegardes et archivages des données brutes et/ou interprétées devront être conforme à la réglementation de l'activité
SNF-007	Volumétrie	La solution doit répondre à la volumétrie de données à traiter et à stocker
SNF-008	Emplacement des données	Les données persistantes de l'application doivent être centralisées sur un serveur de données unique et identifié.

1.2.2 Sécurité

Spécification ID	Spécification non fonctionnelle	Détail
SNF-009	Chiffrement des données	Description : Toutes les données doivent être chiffrées au repos et en transit en utilisant à minima de l'AES-256 et TLS 1.2.
SNF-010	Gestion des permissions	Le système doit appliquer des modèles de permissions basés sur le principe du moindre privilège, avec des journaux pour surveiller les accès autorisés et non autorisés
SNF-011	Surveillance des intrusions	Une détection automatique des intrusions et des tentatives suspectes d'accès doit être présente, avec alertes configurables
SNF-012	Port USB	Les ports USB doivent être désactivés par défaut
SNF-013	Version OS	La version de l'OS doit être supportée par l'éditeur et à jour.
SNF-014	Echange de fichiers	Les échanges de fichiers doivent passer en utilisant le protocoles SFTP / SSH à défaut SMB V3 (dans les zones de confiance). L'usage de SMBv3 doit être endurci conformément aux bonnes pratiques de sécurité et configuré de façon à imposer le chiffrement, désactiver les protocoles/algorithmes obsolètes.
SNF-015	Sécurisation du réseau	L'équipement doit être placé dans un sous-réseau cloisonné et filtré sur la base des protocoles au juste nécessaire (1 automate par VLAN). Le système doit être placé hors domaine EFS hormis le cas où l'EFS fournit le PC automate (notamment pour les mises à jour OS /GPO)
SNF-016	Adressage IP	Le système doit permettre une configuration réseau complète avec adresse IP fixe, masque (CIDR), passerelle et paramètres associés
SNF-017	Internet	Le système ne devra pas accéder à Internet
SNF-018	Antivirus	L'antivirus fournisseur ne sera pas mis à jour et l'EFS n'installera pas d'antivirus hormis le cas où l'EFS fournit le PC automate.
SNF-020	Sécurité	Les flux réseaux doivent être ouverts des postes ou des serveurs EFS vers les automates et pas dans l'autre sens

1.2.3 Compatibilité

Spécification ID	Spécification non fonctionnelle	Détail
SNF-020	Navigateurs pris en charge	L'application doit être compatible avec les navigateurs Web standards (Chrome, Firefox, Edge) dans leurs versions N et N-1.

SNF-022 Imprimantes

Dans la mesure où les systèmes d'impressions sont compatibles avec la solution ils seront à utiliser en priorité pour des raisons de consommables

1.2.4 Maintenance et évolution

Spécification ID	Spécification non fonctionnelle	Détail
SNF-022	Version	Les mises à jour de versions doivent pouvoir être appliquées avec un temps d'arrêt minimal et compatible avec l'activité, tout préservant les données.
SNF-024	Extensibilité	Le système doit permettre l'intégration de nouveaux modules ou extensions sans régression sur les fonctionnalités existantes.
SNF-028	Supervision système	Une supervision système doit être mise en place pour les automates, environnement applicatif et réseau.
SNF-029	Maintenance base de données	Un plan de maintenance de la base données devra être intégré à la solution
SNF-030	Télémaintenance	Accès par bastion sécurisé <ul style="list-style-type: none">- VNC / RDP- Harmonisation complétude de la matrice du bastion
SNF-031	Télémaintenance	Echanges de fichiers SFTP par bastion avec fournisseur L'accès aux bases de données doit être segmenté pour ne pas interférer avec d'autres bases
SNF-032	Maintenance prédictive	La maintenance prédictive ne devra pas avoir d'impact sur le processus analytique et sera soumise à une validation par le service Cybersécurité qui autorisera son déploiement et les modalités

1.2.5 Conformité

Spécification ID	Spécification non fonctionnelle	Détail
SNF-033	Conformité RGPD	Le système doit respecter les Spécifications du Règlement Général sur la Protection des Données (RGPD), incluant les droits d'accès, de rectification, et de suppression des données.
SNF-035	Conformité réglementaire	Spécifications réglementaires de l'activité. Cf Annexe 21 CFR part 11 et l'annexe 11 des BPF
SNF-036	Bonnes pratiques	Bonnes pratiques liées à l'activité (Chapitre 7 Annexe11 - SI du document BPF)
SNF-038	Mise au rebut	La mise au rebut de l'équipement et tout changement de support de données doit entraîner la destruction des données avant sortie de l'EFS.

1.2.6 Archivage

Spécification ID	Spécification non fonctionnelle	Détail
SNF-040	Génération du fichier d'archivage	Le fournisseur aura en charge si possible la création du fichier d'archivage et définir le lieu de stockage
SNF-041	Transfert de l'archivage	Le SI de l'EFS viendra récupérer le fichier d'archivage via un flux SFTP sur le lieu de stockage prévu par le fournisseur

1.2.7 Responsabilité fournisseur

Spécification ID	Spécification non fonctionnelle	Détail
SNF-043	Responsabilité	Le fournisseur aura la responsabilité de la MCO de l'automate, l'installation et la réinstallation en cas de sinistre