

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

MARCHÉ PUBLIC DE TECHNIQUE DE L'INFORMATION ET DE LA COMMUNICATION

**Acquisition d'un Système d'Information de Gestion des
Identités et des Accès (IAM/IGA)**

M26.0038

TABLE DES MATIERES

ARTICLE 1 – PRÉSENTATION DU BESOIN	4
1.1 – Présentation de l'INSA Lyon	4
1.2 – Contexte et enjeux	4
1.3 – Volumétrie des identités.....	5
1.4 – Recommandations à suivre	5
ARTICLE 2 – OBJET DE LA CONSULTATION	6
ARTICLE 3 – SPÉCIFICATIONS TECHNIQUES DE LA SOLUTION	7
3.1 – Architecture et mode de déploiement	7
3.1.1 Mode on-premise	7
3.1.2 – Mode SaaS	7
3.1.3 – Livrables attendus dans l'offre technique	7
3.2 – Interopérabilité et protocoles	7
3.3 – Sécurité de la plateforme	8
3.4 – Performances et disponibilité	8
3.5 – Environnements et sauvegardes (mode on-premise).....	8
ARTICLE 4 – SPÉCIFICATIONS FONCTIONNELLES DE LA SOLUTION.....	9
4.1 – Gestion du cycle de vie des identités (Joiner / Mover / Leaver)	9
4.2 – Authentification et gestion des accès.....	9
4.3 – Gestion des droits, rôles et habilitations	9
4.4 – Gouvernance des accès	10
4.5 – Pilotage, reporting et tableaux de bord	10
4.6 – Administration de la solution	11
4.7 – Portail utilisateurs finaux.....	11
ARTICLE 5 – URBANISATION, RÉFÉRENTIELS ET INTERFACES SI	11
5.1 – Référentiels sources.....	11
5.1.1 – SIRH Mangue (Solution Cocktail)	11
5.1.2 – SI Scolarité (Pégase).....	12
5.1.3 – Identités externes (non référencées).....	12
5.1.4 – Annuaire (LDAP et Active Directory).....	12
5.2 – Systèmes cibles à connecter	12

5.3 – Exigences techniques des échanges inter-applicatifs	13
ARTICLE 6 – PRESTATIONS D'INSTALLATION ET DE CONFIGURATION INITIALE	13
6.1 – Périmètre	13
6.2 – Contenu de la configuration initiale	13
6.3 – Calendrier prévisionnel.....	14
ARTICLE 7 – FORMATION	14
7.1 – Objectifs généraux	14
7.1.2 – Formation des administrateurs techniques	14
7.1.3 – Formation des administrateurs fonctionnels RH	15
7.1.4 – Formation des référents sécurité.....	15
7.1.5 – Formation des utilisateurs finaux	15
7.1.6 – Modalités et livrables.....	15
ARTICLE 8 – MAINTENANCE DE LA SOLUTION	15
8.1 – Périmètre et durée	15
8.2 – Types de maintenance	15
8.2.1 – Maintenance corrective.....	15
8.2.2 – Maintenance préventive.....	16
8.2.3 – Maintenance curative.....	16
8.2.4 – Maintenance évolutive	16
8.3 – Support éditeur et accès.....	16
8.4 – Niveaux de sévérité et délais d'intervention.....	17
8.5 – Compte-rendu et pilotage	17
8.6 – Réversibilité	17
8.7 – Spécifications RGPD	18
ARTICLE - 9 PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES FACULTATIVES (PSE)	18
ARTICLE 10 – TRANCHE OPTIONNELLE	18
ARTICLE 11 – RÉCAPITULATIF DES FONCTIONNALITÉS ATTENDUES.....	19
ARTICLE 12 – GLOSSAIRE	20

ARTICLE 1 – PRÉSENTATION DU BESOIN

1.1 – Présentation de l'INSA Lyon

L'Institut National des Sciences Appliquées de Lyon (INSA Lyon) est un établissement public d'enseignement supérieur et de recherche, placé sous la tutelle du Ministère de l'Enseignement Supérieur, de la Recherche et de l'Espace. Fondé en 1957, il est le premier INSA créé en France et figure parmi les établissements d'ingénieurs les plus importants d'Europe.

L'INSA Lyon accueille chaque année environ 6 200 étudiants (cycle ingénieur, masters, doctorants), encadrés par près de 3 000 personnels permanents et contractuels (enseignants-chercheurs, personnels administratifs et techniques, vacataires, intervenants extérieurs et prestataires). L'établissement est réparti principalement sur le campus de La Doua à Villeurbanne.

Sa Direction des Systèmes d'Information (DSI) est chargée de la gestion et de l'évolution du Système d'Information (SI), incluant l'ensemble des infrastructures, des applications métier et des outils collaboratifs.

1.2 – Contexte et enjeux

Dans le cadre de la modernisation de son système d'information et du renforcement de ses exigences de sécurité, l'INSA Lyon souhaite se doter d'un Système d'Information de Gestion des Identités et des Accès (IAM/IGA). Le constat actuel fait état d'une gestion des identités partiellement manuelle, peu centralisée, avec des pratiques hétérogènes. Cette situation génère plusieurs risques :

- Des processus Joiner / Mover / Leaver largement manuels, sources d'erreurs et de délais,
- Une multiplication des comptes orphelins et des droits d'accès non révoqués après départ,
- Une absence de gouvernance unifiée des habilitations sur l'ensemble du SI,
- Une conformité réglementaire (RGPD, NIS2) difficile à démontrer en l'absence de traçabilité centralisée,
- Une gestion des comptes à privilèges (PAM) insuffisante et dispersée.
Les accès au PAM devront pouvoir être gérés par une dizaine de personnes. Les accès à privilèges concernent plusieurs dizaines de personnes selon les périmètres concernés.

Le projet vise à répondre à ces enjeux en mettant en place une solution IAM/IGA couvrant l'ensemble du cycle de vie des identités, le provisionnement automatisé des accès, la gouvernance des habilitations et la gestion des accès à privilèges.

1.3 – Volumétrie des identités

Catégorie d'identité	Volume estimé	Observations
Personnels permanents fonctionnaires ou contractuels (enseignants/chercheurs, BIATSS)	~1600	Référentiel SIRH Cocktail (Mangue)
Vacataires	~1000 / an	Saisie manuelle / référentiel partiel
Extérieurs / prestataires	~1200	Saisie manuelle / référentiel partiel
Étudiants (ingénieurs, masters, doctorants)	~6200 / an	Référentiel SI scolarité Pégase Sur certaines périodes, les étudiants sortants continuent de bénéficier d'une identité numérique active, notamment durant la phase de rentrée.
TOTAL	~10000	Volume maximum

⚠ Note : Contrainte forte : l'INSA Lyon présente de nombreuses identités à profils multiples (doctorant + vacataire, enseignant + étudiant en formation continue). La solution devra gérer cette multi-appartenance nativement. Une tarification allégée est attendue pour les comptes étudiants. Les environnements de recette (REC) et développement (DEV) ne doivent pas donner lieu à une facturation de licences supplémentaires.

1.4 – Recommandations à suivre

Le Titulaire doit se conformer à l'ensemble des réglementations et recommandations applicables, notamment :

- Référentiel Général de Sécurité (RGS) de l'ANSSI,
- Qualification SecNumCloud pour un l'hébergement cloud d'une offre saas,
- Guide de l'hygiène informatique ANSSI,
- Recommandations OWASP Top Ten pour les développements Web,
- Normes d'accessibilité RGAA,

Si la solution propose des fonctionnalités techniques d'intelligence artificielle, elles doivent être souveraines et les données de l'INSA Lyon ne doivent ni être réutilisées, ni transférées.

ARTICLE 2 – OBJET DE LA CONSULTATION

La présente consultation porte sur la fourniture de la solution logicielle IAM/IGA, avec deux environnements de tests et recette (dont un obligatoire) son installation et sa configuration initiale, la formation des équipes de l'INSA Lyon et la maintenance de la solution pendant 4 ans à compter de la mise en production. Il comprend :

La fourniture des licences logicielles pour l'ensemble des composants de la solution (moteur IGA, module PAM, module Access Management, module gouvernance), sans surcoût pour les environnements de tests (DEV et REC),

L'installation et la configuration initiale de la solution sur les environnements de l'INSA Lyon (mode on-premise) ou hébergés par le prestataire (mode SaaS),

La documentation technique et fonctionnelle éditeur de la solution,

Les sessions de formation adaptées aux différents profils (voir Article 6),

La maintenance corrective, préventive et curative de la solution pendant 4 ans, incluant les mises à jour des licences, les correctifs de sécurité et le support éditeur de niveau 3 (voir Article 7).

⚠ Note : Exigence critique – Intégration convergée : la solution DOIT proposer une intégration native entre provisionnement, gouvernance et PAM, sans bridges ni ETL complexes. Un modèle de données unifié est obligatoire. Les solutions assemblant plusieurs produits distincts sans modèle de données commun ne seront pas acceptées.

ARTICLE 3 – SPÉCIFICATIONS TECHNIQUES DE LA SOLUTION

3.1 – Architecture et mode de déploiement

Le soumissionnaire propose une architecture s'appuyant sur un déploiement en mode on-premise sur les serveurs de l'INSA Lyon ou en mode SaaS. Il précise dans son mémoire technique le mode de déploiement retenu et ses avantages.

3.1.1 Mode on-premise

Architecture haute disponibilité (HA) avec redondance des composants critiques,
Séparation des environnements : DEV, et PROD, sans facturation de licences supplémentaires,
Compatibilité avec la virtualisation et un déploiement en conteneurisation,
Compatibilité OS Linux (Ubuntu de préférence) et/ou Windows Server.

3.1.2 – Mode SaaS

Garanties de disponibilité contractualisées,
Conformité RGPD : données hébergées sur territoire de l'Union européenne, qualification SecNumCloud ou équivalent,
Auditabilité complète : journaux accessibles à l'INSA Lyon, export des données à tout moment,
PCA (Plan de Continuité d'Activité) /PRA (Plan de Reprise d'Activité) documentés, stratégie de sauvegarde définie contractuellement,
Accès sécurisé entre le SI de l'INSA Lyon et l'hébergement du prestataire (tunnel chiffré TLS, authentification mutuelle).

3.1.3 – Livrables attendus dans l'offre technique

Schéma d'architecture détaillé (Dossier d'Architecture Technique – DAT),
Prérequis infrastructure précis (CPU, RAM, stockage, réseau, ports) par environnement pour un mode onpremise,
Plan de sauvegarde et de restauration,
Prérequis de sécurité réseau (flux, VLANs, règles de pare-feu).

3.2 – Interopérabilité et protocoles

La solution doit supporter les standards suivants, décrits dans le mémoire technique :

LDAP / Active Directory pour la synchronisation des annuaires,
SAML 2.0 pour la fédération d'identités et le SSO,
OAuth 2.0 / OpenID Connect (OIDC) pour l'authentification déléguée,
SCIM pour le provisionnement standardisé,
API REST documentées (OpenAPI/Swagger), API SOAP,
Kerberos pour l'authentification Windows/AD,
CMIS pour la GED Alfresco/Gofast,

Compatibilité native avec Keycloak (broker IAM déjà déployé à l'INSA Lyon),

- La solution devra pouvoir provisionner Keycloak pour l'authentification mais aussi d'autres solutions. Il devra nécessairement exister une intégration forte avec Keycloak et une remontée d'éléments depuis Keycloak vers l'IGA.

Norme Supann pour les établissements d'enseignement supérieur,

Connectivité vers des bases de données (Oracle, PostgreSQL) et fichiers plats (CSV, XML).

3.3 – Sécurité de la plateforme

Chiffrement des communications : TLS 1.2 minimum, TLS 1.3 recommandé,

Chiffrement des données au repos : AES-256 pour les données sensibles (mots de passe, secrets, tokens),

Séparation des privilèges d'administration : comptes dédiés et traçés,

Journalisation exhaustive de toutes les actions (logs auditables, non modifiables) : la solution doit permettre une journalisation complète des accès, modifications d'habilitations, opérations d'administration, synchronisations, échecs d'authentification, exports et actions sensibles. Les journaux doivent être horodatés, intègres, exportables vers le SIEM de l'INSA Lyon, protégés contre l'altération, et conservés selon une durée paramétrable conforme à la politique de l'établissement,

Conformité aux recommandations ANSSI RGS niveau standard,

MFA obligatoire pour les accès administrateurs,

Durcissement selon les CIS Benchmarks applicables.

3.4 – Performances et disponibilité

Indicateur	Exigence
Taux de disponibilité (heures ouvrées)	≥ 99,5 % hors maintenance planifiée
Indisponibilité mensuelle cumulée max.	≤ 3h30 en heures ouvrées
Temps de réponse – transactions courantes	≤ 2 secondes en moyenne
Temps de réponse – requêtes complexes	≤ 5 secondes maximum
Perte de données max. admissible (PDMA)	8 heures ouvrées
RTO (durée de reprise max.)	4 heures ouvrées
Montée en charge	≥ 500 connexions simultanées sans dégradation

3.5 – Environnements et sauvegardes (mode on-premise)

En mode on-premise, l'INSA Lyon mettra à disposition les serveurs nécessaires aux trois environnements (DEV, REC, PROD). Le Titulaire est responsable de l'installation, de la configuration et de la documentation de ces environnements. Les sauvegardes seront réalisées par les équipes de la DSI selon le plan défini conjointement. Le Titulaire devra documenter précisément les données et paramètres à sauvegarder, définir les procédures de restauration (testées lors de la recette) et proposer une solution de rollback en cas d'incident sur une mise à jour.

ARTICLE 4 – SPÉCIFICATIONS FONCTIONNELLES DE LA SOLUTION

4.1 – Gestion du cycle de vie des identités (Joiner / Mover / Leaver)

La solution doit prendre en charge l'intégralité du cycle de vie des identités pour toutes les populations de l'INSA Lyon et les comptes de services. La gestion des identités à multiples profils est une contrainte forte : une même personne physique peut disposer de plusieurs identités logiques (ex : doctorant + vacataire) avec des droits cumulatifs ou distincts.

- Arrivée (Joiner) : déclenchement automatique depuis les référentiels sources (SIRH Mangué, Pégase) ou saisie manuelle pour les externes, création automatique des comptes selon les règles d'habilitation et les flux de validation, notifications aux acteurs,
- Mobilité (Mover) : déclenchement automatique en cas de changement de poste, d'affectation ou de statut, mise à jour des droits et gestion de la période de transition, gestion de délégations temporaires selon saisie manuelle, workflow de validation ou provisionnement automatisé,
- Départ (Leaver) : désactivation des comptes à la date de départ, révocation des accès, archivage des droits pendant la durée légale, suppression définitive selon les politiques définies.

Les données minimales à gérer : Nom, Prénom, Date de naissance, Mail institutionnel, Mail de contact, Catégorie/statut, Affectation(s), Date d'arrivée, Date de départ prévisionnelle, Identifiant unique.

La solution doit pouvoir permettre de gérer et de provisionner des groupes, sur plusieurs niveaux et en lien avec les différentes briques du SI (en tant que consommateur des données ou fournisseur de celles-ci).

4.2 – Authentification et gestion des accès

La solution devra intégrer nativement l'outil Keycloak, déjà déployé au sein de l'INSA Lyon, afin d'assurer la gestion centralisée de l'authentification des utilisateurs.

Elle devra également proposer un portail libre-service permettant aux utilisateurs de réinitialiser ou modifier leur mot de passe en lien avec Keycloak et l'Active Directory, de déverrouiller leur compte, ainsi que d'effectuer ces opérations depuis tout type de terminal grâce à une interface responsive.

La solution devra permettre de dissocier les temporalités d'activation et de désactivation des comptes et des droits d'accès selon des règles paramétrables définies par l'établissement.

L'authentification multifacteur (MFA) devra être prise en charge et être rendue obligatoire pour les comptes administrateurs disposant de privilèges élevés. Les méthodes d'authentification devront notamment inclure les mots de passe à usage unique basés sur le temps (TOTP) ainsi que les clés physiques conformes au standard FIDO2.

4.3 – Gestion des droits, rôles et habilitations

La solution devra s'appuyer sur un modèle de gestion des rôles (RBAC) intégrant à la fois des rôles métiers et des rôles techniques. L'affectation de ces rôles devra pouvoir être automatisée en fonction de critères tels que le statut de l'utilisateur, son affectation ou son département de rattachement.

La solution devra assurer le provisionnement automatique des comptes et des habilitations dans les systèmes cibles lors de chaque événement du cycle de vie des identités, notamment lors de leur création, modification ou révocation.

Le provisionnement applicatif devra être réalisé au moyen de connecteurs natifs ou de standards reconnus tels que SCIM, LDAP, Active Directory ou API REST.

Un portail libre-service devra permettre aux utilisateurs de formuler des demandes d'accès, lesquelles seront soumises à des workflows de validation entièrement configurables.

La solution devra permettre la mise en œuvre de circuits d'approbation multi-niveaux intégrant notamment le supérieur hiérarchique (N+1), le responsable applicatif et la DSI. Ces circuits devront prendre en charge les mécanismes de délégation, d'escalade et d'alerte.

La gestion de la séparation des tâches (Segregation of Duties – SoD) devra être assurée au moyen de matrices de conflits identifiant les rôles incompatibles. La solution devra être en mesure de générer des alertes ou de bloquer automatiquement les affectations contraires aux règles définies.

La solution devra permettre la gestion spécifique des comptes de service ainsi que la réalisation de campagnes de revue dédiées à ces derniers.

Elle devra également prendre en charge la gestion spécifique des comptes prestataires et permettre un interfaçage avec le bastion Teleport.

Enfin, la solution devra offrir la possibilité de mettre en œuvre des mécanismes de délégation et de dérogation de droits entre utilisateurs.

À titre souhaitable, la solution pourra intégrer des fonctionnalités de gestion des comptes à privilèges (PAM), incluant notamment un coffre-fort de mots de passe, l'enregistrement des sessions ainsi que des mécanismes d'accès temporaires de type « just-in-time access ».

4.4 – Gouvernance des accès

La solution devra permettre l'organisation de campagnes périodiques de recertification des droits d'accès, avec validation par les responsables métiers concernés.

Elle devra être en mesure d'identifier les comptes orphelins et de faciliter leur traitement conformément aux politiques de sécurité définies.

La solution devra offrir une visualisation exhaustive des droits attribués aux utilisateurs, en mettant particulièrement en évidence les droits sensibles, critiques ou potentiellement toxiques.

Elle devra permettre d'identifier et de traiter les écarts constatés entre la politique de sécurité théorique de l'établissement et la situation réelle observée au sein du système d'information.

L'ensemble des droits attribués ainsi que les actions réalisées devront faire l'objet d'un archivage complet, selon des durées de conservation configurables et conformes aux exigences réglementaires applicables.

La solution devra enfin permettre la génération de rapports de conformité exportables, notamment dans le cadre du respect du RGPD, des audits internes ou des exigences issues de la directive NIS2.

4.5 – Pilotage, reporting et tableaux de bord

La solution devra proposer des tableaux de bord paramétrables et adaptés aux différents profils d'utilisateurs, notamment la DSI, le RSSI, les services RH ou encore les responsables métiers.

Elle devra mettre à disposition un catalogue de rapports standards et permettre la création de rapports personnalisés répondant aux besoins spécifiques de l'établissement.

La traçabilité complète des actions réalisées dans la solution ainsi que des connexions devra être assurée au moyen de journaux d'audit non modifiables et exploitables à des fins de contrôle.

La solution devra également permettre de tracer les opérations d'authentification réalisées dans les applications connectées et d'en assurer la centralisation au sein de la plateforme.

Des mécanismes d'alerte paramétrables devront être disponibles afin de signaler les événements critiques, tels que les comptes expirés non désactivés, les conflits de séparation des tâches (SoD) ou les tentatives répétées d'authentification échouées.

Enfin, la solution devra proposer des fonctionnalités de recherche avancée permettant d'interroger l'ensemble du référentiel des identités, comptes, droits et habilitations.

4.6 – Administration de la solution

L'interface d'administration doit être intégralement graphique (GUI) et permettre, sans développement spécifique :

- Gérer les modèles de droits et les connecteurs,
- Administrer les utilisateurs, groupes et hiérarchies,
- Configurer les workflows d'approbation, les notifications et alertes,
- Définir et modifier les politiques de sécurité,
- Opérer des actions en masse sur des sélections d'utilisateurs ou de droits,
- Visualiser l'ensemble des interconnexions et leurs états.

4.7 – Portail utilisateurs finaux

La solution logicielle comprend un portail ergonomique et responsive permettant aux utilisateurs de :

- Consulter l'ensemble de leurs accès attribués,
- Consulter les données concernant leurs dernières authentifications en lien avec Keycloak (avec localisation),
- Consulter des données collectées d'applications connectées (utilisation des boîtes mails, liste de diffusion...),
- Effectuer des demandes d'accès complémentaires selon leur profil,
- Consulter et valider les accès des personnes dont ils sont désignés responsables,
- Consulter des rapports lorsque leur rôle l'exige (revue de droits...),
- Effectuer des demandes de délégation pour leurs droits qui peuvent en faire l'objet,
- Effectuer des demandes de modifications sur leurs données (Exemple Nom / Prenom) avec circuit de validation associé,
- Effectuer un changement de mot de passe (en lien avec keycloak) et accéder aux instructions d'usage du portail.

ARTICLE 5 – URBANISATION, RÉFÉRENTIELS ET INTERFACES SI

5.1 – Référentiels sources

5.1.1 – SIRH Mangue (Solution Cocktail)

Le SIRH Mangue constitue la source de vérité pour les personnels permanents et contractuels. L'interface sera de type synchronisation périodique incrémentielle. Les données transmises incluront notamment : matricule, nom, prénom, date de naissance, statut contractuel, affectation, date d'arrivée, date de fin de contrat.

5.1.2 – SI Sclarité (Pégase)

Pégase constitue la source de vérité pour les étudiants. L'interface gérera les inscriptions annuelles, réinscriptions, changements de formation et fins d'études. La solution absorbera les variations saisonnières importantes de volumétrie (rentrée universitaire, fin d'année scolaire).

5.1.3 – Identités externes (non référencées)

Pour les populations sans référentiel automatisé (vacataires, prestataires, hébergés de laboratoires, conférenciers, partenaires de recherche), la solution proposera une IHM de saisie manuelle avec processus de validation. Un identifiant unique sera généré automatiquement. La durée de validité du compte sera liée à la durée du contrat ou de l'intervention.

5.1.4 – Annuaire (LDAP et Active Directory)

Le LDAP de l'INSA Lyon constitue l'annuaire de référence prioritaire pour l'authentification, l'Active Directory est le deuxième système cible prioritaire. La solution alimentera le LDAP et l'AD (création, modification, désactivation de comptes, gestion des groupes). L'authentification au portail d'administration s'effectuera via SSO.

5.2 – Systèmes cibles à connecter

Les applications à connecter prioritairement :

- LDAP et Active Directory
- Messagerie (partages RENATER)
- VPN Cisco
- Keycloak (broker IAM)
- SIRH Cocktail (Mangue)
- GLPI
- Sympa (service de listes de diffusion)
- SI Sclarité (Pégase)
- GED Gofast
- SIGB Koha
- Brique WiFi invité
- Contrôle d'accès Unicampus
- Bastion Teleport
- Système de Softphonie

L'ensemble des applications métiers (130) doit être connectée à terme et la solution doit permettre la création de nouveaux connecteurs.

Une même identité est présente dans plusieurs applications cibles.

5.3 – Exigences techniques des échanges inter-applicatifs

La solution doit garantir la sécurisation de l'ensemble des échanges inter-applicatifs au moyen d'un chiffrement des flux reposant a minima sur le protocole TLS 1.2 ou toute version ultérieure assurant un niveau de sécurité équivalent ou supérieur.

Elle doit permettre la mise en œuvre d'une authentification mutuelle entre les systèmes communicants afin de garantir l'identité des parties prenantes aux échanges et de prévenir tout accès non autorisé.

L'ensemble des échanges réalisés entre les différents systèmes doit faire l'objet d'une journalisation exhaustive, incluant aussi bien les opérations réalisées avec succès que les erreurs ou anomalies rencontrées, afin de garantir la traçabilité des flux et de faciliter les opérations d'audit et de diagnostic.

La solution doit intégrer des mécanismes de reprise sur incident permettant la gestion des erreurs de transmission ainsi que le rejeu des flux lorsque cela est nécessaire, afin de garantir la continuité et la fiabilité des échanges.

Les interfaces mises en œuvre doivent être entièrement documentées. Cette documentation doit notamment préciser les modèles de données utilisés, les formats d'échange, les fréquences de synchronisation ainsi que les modalités techniques de communication entre les systèmes.

Enfin, la solution doit prendre en charge les principaux formats d'échange standards du marché, notamment JSON, XML et CSV.

ARTICLE 6 – PRESTATIONS D'INSTALLATION ET DE CONFIGURATION INITIALE

6.1 – Périmètre

Le Titulaire prend en charge l'installation et la configuration initiale de la solution sur les environnements de l'INSA Lyon (ou hébergés en mode SaaS).

6.2 – Contenu de la configuration initiale

La prestation de configuration initiale doit comprendre le déploiement de la solution sur les trois environnements de l'établissement, à savoir les environnements de développement (DEV), de recette (REC) et de production (PROD).

Elle doit inclure la configuration des principaux composants de la solution, notamment le moteur de gouvernance et d'administration des identités (IGA), le module de gestion des accès et d'authentification unique (SSO/Access Management), le module de gestion des comptes à privilèges (PAM) ainsi que l'interface d'administration. Les accès au PAM doivent pouvoir être gérés par une dizaine de personnes. Les accès à privilèges concernent plusieurs dizaines de personnes selon les périmètres concernés.

Le Titulaire doit assurer la configuration des connecteurs natifs LDAP et Active Directory nécessaires à l'intégration de la solution au système d'information de l'établissement.

La prestation comprend également l'activation des mécanismes d'authentification de base, incluant l'authentification via LDAP ou Active Directory, la mise en œuvre de l'authentification unique (SSO) ainsi que l'authentification multifacteur (MFA) pour les comptes administrateurs.

Le Titulaire doit procéder au paramétrage des politiques de sécurité initiales de la plateforme, notamment celles relatives à la complexité des mots de passe, à la gestion des sessions et aux règles de sécurité associées.

À l'issue des opérations de configuration, des tests de bon fonctionnement de la solution doivent être réalisés en présence des équipes de la Direction des Systèmes d'Information afin de vérifier la conformité des paramétrages effectués et le bon fonctionnement des différents composants.

Enfin, le Titulaire remet à l'établissement l'ensemble des fichiers de configuration nécessaires à l'exploitation de la solution ainsi que les accès administrateurs permettant son administration et sa maintenance.

6.3 – Calendrier prévisionnel

Le Titulaire doit proposer un calendrier adapté aux besoins de l'INSA Lyon, notamment en termes de prise en compte des spécificités métier et du personnel de la Direction des systèmes d'information (DSI) ou de la programmation des temps de livraison et de formation.

Le calendrier doit ainsi permettre une mise en place fluide de la solution et éviter des incohérences telles que des livraisons décalées ou séparées et formations tardives.

ARTICLE 7 – FORMATION

7.1 – Objectifs généraux

Le Titulaire prévoit un plan de formation complet adapté aux différents profils d'utilisateurs. Les formations sont dispensées de préférence sur site (campus INSA Lyon), en langue française.

7.1.2 – Formation des administrateurs techniques

Il prévoit d'abord une formation technique approfondie destinée aux équipes de la DSI / Direction du Numérique (5 à 8 personnes) sur :

- Architecture de la solution et composants techniques,
- Administration de la plateforme (installation, configuration, montée de version),
- Gestion des connecteurs et des interfaces,
- Exploitation et supervision (journaux, alertes, métriques),
- Procédures de sauvegarde, de restauration et de reprise d'incident.

Durée minimale : Trois (3) jours en présentiel. La formation sera accompagnée d'un guide d'exploitation détaillé.

7.1.3 – Formation des administrateurs fonctionnels RH

Il prévoit ensuite une formation fonctionnelle destinée aux équipes RH (6 à 12 personnes) sur :

- Gestion du cycle de vie des identités (Joiner / Mover / Leaver),
- Gestion des habilitations et des rôles,
- Utilisation des workflows d'approbation.

Durée minimale : Deux (2) jours.

7.1.4 – Formation des référents sécurité

Il prévoit également une formation fonctionnelle destinée aux équipes RSSI et correspondants sécurité (4 à 7 personnes) sur :

- Conduite des campagnes de recertification,
- Génération et exploitation des rapports de conformité,
- Gestion des comptes orphelins et des anomalies d'accès.

Durée minimale : Deux (2) jours.

7.1.5 – Formation des utilisateurs finaux

Enfin, il prévoit une formation courte destinée aux représentants de chaque population pour l'usage du portail self-service : connexion et authentification, demandes d'accès, consultation des droits. Durée : 0,5 jour. Des tutoriels vidéo et une aide en ligne contextuelle complèteront la formation.

7.1.6 – Modalités et livrables

Toutes les sessions sont accompagnées de supports pédagogiques adaptés aux publics cibles, remis en format éditable et PDF, incluant des exercices pratiques et un QCM de validation des connaissances. Un environnement de formation dédié (données fictives représentatives) sera préparé par le Titulaire. Les dates précises seront définies en concertation avec la DSI, postérieurement à la mise en service.

ARTICLE 8 – MAINTENANCE DE LA SOLUTION

8.1 – Périmètre et durée

Le Titulaire fournit un contrat de maintenance couvrant l'ensemble des licences logicielles et composants, pour une durée de 5 ans à compter de la date de mise en production validée par procès-verbal de recette.

8.2 – Types de maintenance

8.2.1 – Maintenance corrective

Correction des anomalies et bugs affectant le bon fonctionnement de la solution, déclenchée suite à détection d'un incident. Le Titulaire qualifie, traite et corrige les anomalies dans les délais définis à l'Article 8.4.

8.2.2 – Maintenance préventive

- Mises à jour de sécurité et correctifs éditeur (patches), avec préavis minimum de 5 jours ouvrés,
- Suivi des versions et gestion de l'obsolescence des composants,
- Revues périodiques de l'architecture et des performances,
- Mise à jour de la documentation en cohérence avec l'état réel du système,
- Adaptations liées aux évolutions réglementaires (RGPD, NIS2, ANSSI).

8.2.3 – Maintenance curative

La maintenance curative agit sur les causes profondes des dysfonctionnements. Elle peut impliquer le remplacement de composants logiciels ou des reconfigurations majeures. Un programme d'exécution sera établi d'un commun accord entre les parties.

8.2.4 – Maintenance évolutive

Les livraisons des nouvelles versions mineures et majeures du logiciel doivent faire l'objet d'un préavis et d'un ticket de suivi avec l'INSA Lyon selon les modalités du support. Ces livraisons doivent être livrées en base de test préalablement à leur livraison en base de production. Le dossier technique devra préciser le nombre de livraison prévues par an de version mineures et majeures.

Des modalités de prise en compte de demandes d'évolution et de priorisation de celles-ci doivent être mise en place.

8.3 – Support éditeur et accès

- Accès au support technique éditeur de niveau 3,
- Accès aux mises à jour des licences (versions majeures et mineures),
- Accès à la base de connaissances et à la documentation de la solution,
- Un interlocuteur technique dédié, désigné nominativement, servira de point de contact privilégié pour la DSI de l'INSA Lyon.

Le dossier technique précisera les modalités de support et les outils mis en place, ainsi que le nombre de personnes habilitées à créer un ticket pour l'INSA Lyon.

8.4 – Niveaux de sévérité et délais d'intervention

Sévérité	Description	Prise en charge	Résolution
S1 – Critique	Solution totalement indisponible ou perte de données. Impact sur tous les utilisateurs.	30 minutes	4 h ouvrées
S2 – Haute	Dysfonctionnement majeur. Fonction critique indisponible. Contournement difficile.	1 h ouvrée	8 h ouvrées
S3 – Moyenne	Dysfonctionnement partiel. Contournement possible. Impact limité.	4 h ouvrées	5 jours ouvrés
S4 – Faible	Anomalie mineure ou amélioration. Sans impact fonctionnel significatif.	2 jours ouvrés	30 jours ouvrés

Des pénalités sont prévues telles que précisées dans le CCAP en cas de dépassement des délais de prise en charge.

8.5 – Compte-rendu et pilotage

Chaque intervention donne lieu à un rapport transmis à la DSI dans les 5 jours ouvrés suivant la clôture, comprenant : la description de l'intervention, l'analyse des causes (pour les correctives), les actions préventives recommandées et l'état général de la plateforme. Un comité de pilotage mensuel passe en revue les incidents, niveaux de service et évolutions en cours.

8.6 – Réversibilité

Le Titulaire doit prévoir la réversibilité de la solution / son interopérabilité.

La réversibilité intervient lorsque la relation contractuelle cesse, quelle qu'en soit la cause. La réversibilité a pour objectif de permettre à INSA Lyon de récupérer l'ensemble des données et informations contenues dans la solution et ce, dans les meilleures conditions.

Le Titulaire s'engage à assurer une totale réversibilité sur le plan technique pour permettre à l'INSA Lyon, ou à un opérateur désigné par ce dernier, d'assurer la continuité de l'activité dans de bonnes conditions en apportant toute l'assistance technique nécessaire au bon déroulement de cette opération.

La réversibilité implique un transfert à l'INSA Lyon, et/ou au futur Titulaire de l'ensemble des données hébergées et archivées dans la solution durant la durée du contrat sous une forme directement utilisable par l'INSA Lyon ou le Titulaire suivant ;

Le Titulaire s'engage à ne garder aucune donnée à l'issue de la phase de réversibilité.

La méthodologie de réversibilité sera explicitée par le candidat dans son offre et fera l'objet d'un livrable spécifique (plan de réversibilité).

8.7 – Spécifications RGPD

Le Titulaire doit prévoir la suppression automatique de certaines données personnelles dans un temps qui sera défini en accord avec les règles RGPD. Des « mentions CNIL » doivent pouvoir figurer en bas des interfaces pour les utilisateurs finaux.

De façon générale, le Titulaire s'engage à veiller, au préalable et pendant toute la durée du contrat, au respect des obligations prévues par le règlement européen sur la protection des données.

ARTICLE - 9 PRESTATIONS SUPPLÉMENTAIRES ÉVENTUELLES FACULTATIVES (PSE)

L'INSA Lyon se réserve le droit de commander ou non, lors de la signature du contrat, les PSE facultatives suivantes :

- **PSE n°1 – Extension du périmètre PAM avancé** : Mise en place d'une solution avancée de gestion des accès à privilèges incluant l'enregistrement vidéo des sessions d'administration, le coffre-fort de mots de passe pour comptes techniques, et le contrôle just-in-time. Concerne les comptes d'administration des équipements réseau, des serveurs et des bases de données.
- **PSE n°2 – Gouvernance avancée et IA** : Intégration d'un moteur d'analyse comportementale et de recommandations automatisées par IA pour la détection des anomalies d'accès (comptes surpuissants, droits inutilisés, comportements inhabituels). Comprend des tableaux de bord avancés et des rapports de risque automatisés.
- **PSE n°3 – Connecteur SIEM** : Fourniture d'un connecteur certifié vers le SIEM de l'INSA Lyon pour l'envoi en temps réel des événements de sécurité IAM (authentifications échouées, modification de droits critiques, accès à des ressources sensibles). Inclut un catalogue de règles de corrélation IAM.
 - La solution devra être interfacée à un SIEM, quel que soit celui-ci, via des protocoles comme GELF, Syslog ou Beats, en utilisant des plugins pour les échanges de données via des protocoles sécurisés.

ARTICLE 10 – TRANCHE OPTIONNELLE

La tranche optionnelle, d'une durée de trois (3) ans à compter de l'expiration du marché initial, peut être affermie sur décision de l'Acheteur.

Cette tranche optionnelle a pour objet les prestations de maintenance telles que présentées à l'article 8 du présent Cahier des Clauses Techniques Particulières.

L'affermissement est une décision de l'Acheteur : le Titulaire ne peut, à ce titre, s'y opposer.

ARTICLE 11 – RÉCAPITULATIF DES FONCTIONNALITÉS ATTENDUES

Le tableau suivant récapitule les fonctionnalités attendues et leur périmètre de déploiement. Il constitue un document de référence pour évaluer la couverture fonctionnelle de la solution fournie.

Domaine	Fonctionnalité	Priorité
FONCTIONNALITÉS OBLIGATOIRES		
Cycle de vie des identités	Référentiel des identités (personnels, étudiants, externes)	Obligatoire
	Processus Joiner / Mover / Leaver	Obligatoire
	Gestion des identités multi-profil	Obligatoire
	Gestion des attributs et des statuts	Obligatoire
Authentification	Intégration native de Keycloak	Obligatoire
	Portail self-service (gestion du mot de passe)	Obligatoire
	MFA – comptes à privilèges	Obligatoire
Droits, rôles & habilitations	Modèle de rôles (RBAC)	Obligatoire
	Provisionnement automatique (AD, LDAP, messagerie)	Obligatoire
	Provisionnement applicatif (connecteurs systèmes cibles)	Obligatoire
	Workflow de demande d'accès en libre-service	Obligatoire
	Flux d'approbation multi-niveaux et délégation	Obligatoire
	Gestion des groupes	Obligatoire
	Interface centralisée avec visualisation et demandes	Obligatoire
Gouvernance & conformité	Détection et gestion des doublons	Obligatoire
	Archivage des droits et des actions	Obligatoire
Pilotage & administration	Catalogue de rapports standards et personnalisés	Obligatoire
	Interface d'administration graphique complète	Obligatoire
	Traçabilité et journalisation complète	Obligatoire
	Supervision des flux, gestion et remédiation des erreurs (avec rejeu)	Obligatoire
	Vision à 360° des données d'un individu	Obligatoire
FONCTIONNALITÉS SOUHAITABLES		
Authentification	MFA étendue – autres populations	Souhaitable
Droits, rôles & habilitations	Ségrégation des tâches (SoD)	Souhaitable
	Gestion des droits à haut privilège (PAM)	Souhaitable
	Dérogation et délégation	Souhaitable
Gouvernance & conformité	Campagnes de recertification des droits	Souhaitable
	Détection et suppression des comptes orphelins	Souhaitable
	Rapports de conformité (RGPD, NIS2, audit)	Souhaitable
Pilotage & administration	Tableaux de bord configurables	Souhaitable

ARTICLE 12 – GLOSSAIRE

Terme / Acronyme	Définition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DAD	Dossier d'Architecture Détaillé
DAT	Dossier d'Architecture Technique
DEV	Environnement de développement, pour les tests techniques et les montées de versions
DEX	Dossier d'Exploitation
DPGF	Décomposition du Prix Global et Forfaitaire
DSI	Direction des Systèmes d'Information (INSA Lyon)
FIDO2	Fast IDentity Online 2 – Standard d'authentification sans mot de passe (passkeys, clés physiques)
IAM	Identity and Access Management – Gestion des identités et des accès
IGA	Identity Governance and Administration – Gouvernance et administration des identités
JML	Joiner / Mover / Leaver – Cycle de vie : arrivée / mobilité / départ
MFA	Multi-Factor Authentication – Authentification multi-facteur
NIS2	Network and Information Security Directive 2
PAM	Privileged Access Management – Gestion des accès à privilèges
PAQ	Plan d'Assurance Qualité
Pégase	Système d'information de scolarité de l'INSA Lyon
PROD	Environnement de production
RBAC	Role-Based Access Control – Contrôle d'accès basé sur les rôles
REC	Environnement de recette, pour les tests métiers / les formations et démonstrations
RGAA	Référentiel Général d'Amélioration de l'Accessibilité
RGS	Référentiel Général de Sécurité
RGPD	Règlement Général sur la Protection des Données (UE 2016/679)
RPO/RTO	Recovery Point Objective / Recovery Time Objective
SCIM	System for Cross-domain Identity Management – Standard de provisionnement des identités
SIRH	Système d'Information des Ressources Humaines (Mangue / Solution Cocktail)
SoD	Segregation of Duties – Ségrégation des tâches
SSO	Single Sign-On – Authentification unique
Supann	Norme de description des identités pour les annuaires de l'Enseignement Supérieur et de la Recherche

TMA	Tierce Maintenance Applicative
VA	Vérification d'Aptitude
VSR	Vérification de Service Régulier