



Parapheur électronique

Date :17/03/2025

Référence :

PEL-11476

Contexte

Objet:

Exigences SI Solution SaaS (Annexes au CCTP et Mémoire Technique)

Type de document:

Document SMI

Référence Socrate:

QUACSASDD240005

Indice:

B

Signataires

Date	Heure	Intervenant	Etape	Action
21/02/2025	09:48	MARCHESI Arnaud	Validation Rédacteur	Valider
21/02/2025	15:09	DELYSSE-HOFMAN Stéphane	Validation Vérificateur	Valider
26/02/2025	09:44	COUDERT Gaelle	Validation Valideur	Valider
26/02/2025	10:17	SAQUET Gaelle	Validation Approbateur	Valider

Émetteur	Date d'origine	Page
SG/DSIN	29/02/2024	1/8

Exigences SI Solution SaaS (Annexes au CCTP et Mémoire Technique)

Sommaire	Objet
1. Préambule 4 2. Domaine d'application 4 3. Sécurité informatique (partie CCTP) 4 4. Attendus du mémoire technique (partie règlement de consultation) de 8	Ce document fournit les exigences à insérer en annexe et en intégralité des Cahier des Clauses Techniques Particulières (CCTP) et le mémoire technique d'un besoin décrivant un besoin couvert par une application hébergé sur le Cloud en mode SaaS (cf INFNTAASI180012)
Documents applicables	Domaine d'application
INFNTAASI180012 - Préconisations pour la souscription à des services en nuage (cloud computing) et proposition de clauses contractuelles	Procédure achats TIC d'une solution SaaS

A 29/02/2024 Annule et remplace le document : INFNTASDD230014

Ind. Date Historique du dernier indice applicable

* CE DOCUMENT EST LA PROPRIÉTÉ DE L'ANDRA ET NE PEUT ÊTRE REPRODUIT OU COMMUNIQUÉ QUE SUIVANT LA MENTION INDIQUÉE CI-
 Communicable : document pouvant être diffusé à tout public
 Limitée : document pouvant être diffusé à tout le personnel Andra ainsi qu'au public averti
 Andra : document pouvant être diffusé au seul personnel Andra
 Confidentielle : document dont la diffusion est interdite à d'autres destinataires que ceux indiqués sur le document

Ind.	Date	Rédacteur	Nom(s)/visa(s)	Vérificateur	Validateur	Approbateur
		A. MARCHESI		S. DELYSSE-HOFMAN	J. RENGASSAMY	G. SAQUET
		<i>Signé</i>		<i>Signé</i>	<i>Signé</i>	<i>Signé</i>
B	26/11/2024	<i>électroniquement</i>		<i>électroniquement</i>	<i>électroniquement</i>	<i>électroniquement</i>

Identification

QUACSASDD240005

Page 2/8**Rév.** B

Révisions

Ind.	Date	Modifications
A	29/02/2024	Annule et remplace le document : INFNTASDD230014 Précision dans la trame objet
B	26/11/2024	Le §3.9 présent dans la version A a été supprimé, les informations étant déjà présentes par ailleurs dans le document

SOMMAIRE

1. Préambule	4
2. Domaine d'application	4
3. Sécurité informatique (partie CCTP)	4
3.1 <i>Exigences générales</i>	4
3.2 <i>Sécurité informatique</i>	5
3.3 <i>Gestion des évolutions</i>	5
3.4 <i>Plan Assurance Qualité (PAQ) et Sécurité (PAS)</i>	5
3.5 <i>Hébergement</i>	6
3.6 <i>Autorisation et authentification</i>	6
3.7 <i>Accès aux sites et locaux de l'Andra</i>	7
3.8 <i>Propriété et intégrité des données</i>	7
4. Attendus du mémoire technique (partie règlement de consultation)	8

1. Préambule

Ces clauses sont à insérer en intégralité dès qu'une solution est proposée sous la forme d'une application hébergée sur le Cloud en mode SaaS :

- Le § 3 : dans les Cahier des Clauses Techniques Particulières (CCTP) des marchés TIC.
- Le §4 : dans le règlement de consultation

2. Domaine d'application

Ces clauses correspondent au cas d'une application informatique hébergée par un éditeur en mode SaaS (Software as a Service)

3. Sécurité informatique (partie CCTP)

L'Andra a été désignée par l'Etat comme acteur sensible. Il est donc dans l'obligation de respecter un certain nombre d'exigences en la matière.

3.1 Exigences générales

Pour l'ensemble des prestations effectuées dans le cadre du présent cahier des charges, le Titulaire devra respecter et contribuer à la mise en œuvre de la sécurité des Systèmes d'Informations de l'Andra, afin de garantir la confidentialité des données saisies et d'empêcher leur divulgation à l'extérieur.

Le titulaire veillera bien à respecter les règles de sécurité des CCAG TIC (arrêté du 30 mars 2021) ainsi que celles mentionnées dans le CCAP.

En particulier :

- Le Titulaire imposera à ses salariés amenés à intervenir au titre de la prestation leur engagement individuel de confidentialité. Le Titulaire imposera cette même exigence à l'ensemble des sous-traitants sollicités dans le cadre des différentes phases de la prestation ;
- Les accès des personnels du Titulaire et de ses éventuels sous-traitants aux informations techniques sur le réseau Andra ou sur les procédures d'authentification Andra devront faire l'objet d'autorisations formelles préalables et reposer sur des mécanismes d'authentification nominatifs ;
- Les accès physiques des personnels du Titulaire et de ses éventuels sous-traitants à ses installations et locaux techniques devront faire l'objet d'autorisations formelles préalables et reposer sur des mécanismes de contrôle d'accès nominatifs ;
- Les échanges d'informations techniques, de données et de code entre le Titulaire et l'Andra se feront obligatoirement au moyen des dispositifs d'échange sécurisé de fichiers de l'Andra ou d'un dispositif d'échange du Titulaire approuvé par le RSSI (Responsable Sécurité des Systèmes d'Information) de l'Andra ;
- Pendant toute la durée du Marché (Préparation, Déploiement et Maintenance), le Titulaire s'engage à justifier de la mise en place des mesures de sécurité décrites dans le présent document, et de toutes les règles sur lesquelles il s'est engagé dans sa réponse à la consultation ;
- Le Titulaire est responsable de la rédaction initiale du Plan d'Assurance Sécurité (PAS) ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité pendant toute la durée d'exécution du marché ;

Le Titulaire devra indiquer dans son Plan d'Assurance Sécurité (PAS) les mesures mises en place pour sécuriser les fonctions d'administration de Solution.

3.2 Sécurité informatique

Si la solution est full-web, aucun composant pour faire fonctionner la future solution ne doit être à installer sur les postes informatiques de l'Andra : la solution doit fonctionner sur un simple navigateur à jour à date.

Le Titulaire doit assurer l'ensemble des tâches liées à la gestion de la sécurité : sécurité des données en transmission, filtrage des accès réseau au moyen de firewalls, détection des intrusions réseau, gestion complète des authentifications.

Le Titulaire assurera une surveillance 24 heures sur 24 et 7 jours sur 7 des accès aux services. En cas d'attaque virale ou cyber-informatique, le Titulaire pourra prendre toutes les mesures adéquates dont l'arrêt du service si nécessaire, jusqu'à éradication de la menace.

Par ailleurs, l'Andra attend que la solution ne contienne aucune faille exploitable parmi celles décrites dans le top 10 OWASP ; le Titulaire devra être à même de produire un rapport de test d'intrusion confirmant ce niveau de sécurité a minima pour chaque version majeure mise en production du logiciel.

L'application doit être protégée par un firewall applicatif (WAF).

3.3 Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences contractuelles et de sécurité, ou compromettre une éventuelle opération de réversibilité. En cas d'évolution, le Titulaire devra vérifier que sa mise en œuvre est conforme aux exigences de l'Andra.

3.4 Plan Assurance Qualité (PAQ) et Sécurité (PAS)

Les relations entre les parties, notamment au sein des différentes instances de gouvernance, la méthodologie de projet, le détail des rôles et responsabilités de chaque partie seront précisés dans le Plan d'Assurance Qualité (PAQ). De même, la démarche Sécurité sera précisée dans le Plan Assurance Sécurité (PAS).

Le titulaire du marché rédigera le PAQ et PAS qui sera validé par l'Andra en tout début de mission.

Le niveau de service fourni à l'Andra sera également défini dans le PAQ pendant la phase de lancement. Il contiendra la liste des valeurs mesurables permettant d'exprimer de manière factuelle le niveau de service rendu. L'obligation contractuelle du Titulaire quant à la qualité du service sera ainsi énoncée par ces grandeurs objectivement mesurables et représentatives. Le PAQ précisera également comment et avec quelle fréquence ces indices seront mesurés.

Le PAQ intégrera également un système de gestion de risques permettant de prioriser, identifier et suivre les actions de réductions de ces risques. La définition d'échéances et de personnes en charge de mener ces actions y sera intégrée.

Le Titulaire doit être proactif sur les solutions et bonnes pratiques à apporter et jouer un rôle de conseil pour l'accompagner afin de contribuer à l'amélioration de la performance des prestations qui lui sont confiées.

L'apport de conseil portera notamment sur :

- La dimension « SI », en matière de gestion du projet
- Les opportunités d'amélioration de la qualité des services
- Les opportunités de réduction de coûts
- Les technologies : tendances, opportunités, caractéristiques, valeur ajoutée, ...
- La sécurité
- La gestion des risques
- La gestion des changements
- Les modalités d'intégration ou d'interface avec des outils externes

Le Titulaire s'engage sur la mise en place d'un dispositif d'amélioration continue qui soit partagé avec les différentes parties prenantes du projet.

3.5 Hébergement

L'hébergement des données et des applications devra être opéré de manière professionnelle, c'est-à-dire dans un datacenter propre ou tiers, avec des restrictions d'accès physique et des protections techniques (pare-feu, IDS, anti-DDOS, etc).

Le Titulaire est tenu de communiquer à l'Andra l'adresse exacte du lieu (ou des lieux en cas de site de secours) d'hébergement, et de lui en notifier les modifications. En tout état de cause, cet hébergement devra être localisé de préférence en France et à minima en Union Européenne.

Tous les services annexes qui contribuent à la protection, à la disponibilité, aux accès comme par exemple les services WAF (Web Application Firewall), DDOS (Distributed Denial-of-Service), CDN (Content Delivery Network), API (Application Programming Interface), doivent également être localisés de préférence en France et à minima en Union Européenne.

Les données doivent être sauvegardées selon l'état de l'art qui doit être précisé dans le PAS avec une copie déconnectée des réseaux pour ne pas être atteinte en cas d'attaque cyber.

3.6 Autorisation et authentification

Le service devra inclure un module d'administration de comptes individuels nominatifs, permettant :

- de définir des profils d'accès tels que décrits précédemment,
- de créer, modifier et supprimer des comptes, affectés à un ou plusieurs profils,
- de consulter le journal des accès et des actions réalisées avec ces comptes.

Les accès au service se feront :

- obligatoirement après une authentification via SSO;
- exclusivement depuis le réseau Andra, par filtrage des adresses IP publiques,
- avec une journalisation des authentifications réussies et échouées.

Les objectifs de la fédération d'identités numériques (SSO) de l'Andra sont :

- Avoir pour les utilisateurs des applications de l'Andra une identité (identifiant/mot de passe) unique
- Ne pas avoir à se reconnecter si l'utilisateur est déjà connecté à une application de l'Andra
- Suivre l'évolution des standards de sécurité pour la gestion des authentifications des sites Web
- Uniformiser/Simplifier la gestion de l'authentification des sites Web de l'Andra.

L'Andra exige donc une authentification unique des utilisateurs, appuyée sur le référentiel Active Directory Azure de Microsoft (validée par l'ANSSI). Celle-ci devra être réalisée via le protocole d'échange SAML V2 si l'application est accessible via internet, sur une adresse IP qui sera déclarée accessible sur le firewall de l'Andra.

3.7 Accès aux sites et locaux de l'Andra

Pour les prestations effectuées dans les locaux de l'Andra, le Titulaire se conformera aux procédures et règles en vigueur au sein de l'Agence, et notamment lors d'accès sur les sites industriels pour lesquels des délais et formalités spécifiques sont en place :

- Renseignements administratifs à fournir préalablement à l'accès,
- Préavis minimum, différents pour les personnes de nationalité française ou étrangère,
- Droit de refus d'accès suite à des contrôles de sécurité

3.8 Propriété et intégrité des données

Le Titulaire mettra en place les mesures techniques et organisationnelles de nature à empêcher tout accès ou utilisations fraudueuses des données et à prévenir toutes pertes, altérations et destructions des données.

Tout incident affectant potentiellement la confidentialité ou l'intégrité des données de l'Andra doit être notifié à l'Andra dans les plus brefs délais et au maximum sous 72 heures, y compris en cas de fuite de données à caractère personnel. Le Titulaire coopère avec l'Andra, une entreprise missionnée par l'Andra, et/ou les autorités de police pour l'investigation sur la nature ou l'origine de l'incident.

4. Attendus du mémoire technique (partie règlement de consultation)

La Sécurité du système d'information de l'Andra est particulièrement sensible. C'est pourquoi il est demandé à chaque soumissionnaire de décrire les mécanismes et procédures proposés pour garantir une sécurité optimale de sa solution.

Le soumissionnaire devra fournir un chapitre Plan d'Assurance Sécurité (PAS), les outils et procédures qu'il s'engage à mettre en œuvre pour garantir une sécurité optimale de sa solution et le respect du niveau d'exigences sécurité définies ci-dessous, aussi bien au niveau de la solution fournie que de son système d'information utilisé pour l'administrer.

Le Plan d'Assurance Sécurité (PAS) sera analysé et pris en compte dans l'évaluation de la solution.

L'Andra attache une importance particulière au degré d'adaptation de la première version du Plan Assurance Qualité (PAQ) et du PAS au projet et au contexte de l'Agence, produits au moment de l'offre du soumissionnaire.

Le Plan d'Assurance Sécurité et les réponses du soumissionnaire constituent l'engagement contractuel du prestataire sur le niveau de sécurité de sa solution tout au long du marché, en complément des exigences indiquées dans le CCTP.

Hébergement : Le soumissionnaire transmet les attestations de qualification ou de certification du datacenter en matière de sécurité, ou à défaut précise les dispositifs de sécurité dans ces deux domaines. Il indique l'adresse exacte du lieu (ou des lieux en cas de site de secours) d'hébergement.

Gouvernance SSI : Le soumissionnaire décrit l'organisation interne pour la gestion de la sécurité du service délivré et joint tous documents utiles à l'appréciation de sa gouvernance SSI (PSSI, procédures, etc.) ainsi que, le cas échéant, les certifications ou rapports d'audits récents. Il communique à l'Andra les coordonnées de son RSSI, et indique dans quel cas il peut être sollicité dans le pilotage de la prestation.