



ANNEXE 2 – ENVIRONNEMENT TECHNIQUE –CYBER

Cahier des Clauses Techniques Particulières

SOMMAIRE

1	Environnement technique.....	4
1.1	Respect des référentiels.....	4
1.1.1	Référentiel Général d'Amélioration de l'Accessibilité (RGAA).....	4
1.1.2	Référentiel Général Ecoconception de Services Numériques.....	4
1.1.3	Référentiel Général d'Interopérabilité (RGI).....	4
1.2	Normes et standards dans le cas d'une application web.....	4
1.2.1	Principes généraux.....	4
1.2.2	Navigateurs internet.....	5
1.2.3	Architecture logicielle dans le cas d'un développement spécifique.....	5
1.3	Législation et normes applicables à l'hébergement externe.....	6
1.4	Interopérabilité et ouverture des données.....	6
1.5	Environnement technique du système d'information de Rennes Métropole.....	7
1.5.1	Les solutions techniques d'authentification.....	7
1.5.2	Les postes de travail, tablettes et smartphone.....	7
1.5.3	Le réseau.....	7
1.5.4	Exigences sur les logiciels socles « intergiciels » (middleware).....	8
1.5.5	Pare-feux.....	8
1.5.6	API Manager.....	8
2	EXIGENCES EN MATIERE DE CYBER SECURITE.....	9
2.1	Introduction.....	9
2.2	Authentification.....	9
2.3	Sécurité physique et logique de l'hébergement (cas d'un hébergement externe).....	10
2.4	Sauvegardes et tests de restauration (cas d'un hébergement externe).....	10
2.5	Chiffrement et sécurité des flux.....	11
2.6	Sécurisation des envois de mails.....	11
2.7	Sécurité des développements.....	11
2.8	Sécurité des applications mobiles.....	12
2.9	Audits techniques et tests d'intrusion.....	12
2.10	Échanges de données avec la collectivité.....	13
2.11	Sécurisation des interfaces avec des applications tierces.....	13
2.12	Prise en main à distance.....	13
2.13	Lutte contre l'obsolescence.....	13
2.14	Référentiel Général de Sécurité (RGS).....	14
2.15	Maintenance relative à la sécurité.....	14

3	Architecture et documentation technique et sécurité	15
4	Clause de réversibilité	16
4.1	Objectifs de la réversibilité	16
4.2	Déclenchement de la réversibilité.....	16
4.3	Plan de réversibilité	16
4.3.1	Organisation et gouvernance de la réversibilité.....	16
4.3.2	Inventaire des éléments à restituer	17
4.3.3	Transfert des données	17
4.3.4	Transfert des matériels, des logiciels et des environnements techniques	17
4.3.5	Transfert de la documentation.....	18
4.3.6	Transfert des compétences.....	18
4.3.7	Itérations entre le Titulaire et le repreneur	18
4.3.8	Planning détaillé des opérations de réversibilité.....	18
4.3.9	Critères de validation par le repreneur.....	18
4.4	Obligations du titulaire	19
4.5	Coût de la réversibilité	19
4.6	Pénalités	19

1 Environnement technique

1.1 Respect des référentiels

La solution proposée doit respecter les normes établies par les référentiels généraux suivants. Le candidat indiquera dans son mémoire technique comment il propose de respecter ces référentiels.

1.1.1 Référentiel Général d'Amélioration de l'Accessibilité (RGAA)

Le Référentiel Général d'Accessibilité pour les Administrations (RGAA) est un recueil de règles et de bonnes pratiques qui visent à améliorer l'accessibilité des sites Web des administrations. Sa version applicable à ce jour est la version 4.1 (mise à jour le 18 février 2021), consultable à partir du lien suivant :

<https://www.numerique.gouv.fr/publications/rgaa-accessibilite/>

Le candidat fournira la déclaration d'accessibilité concernant sa solution. Voir à ce titre la page <https://www.numerique.gouv.fr/publications/rgaa-accessibilite/obligations/#cadre-g%C3%A9n%C3%A9ral>

1.1.2 Référentiel Général Ecoconception de Services Numériques

Le candidat doit s'attacher à répondre à l'ensemble des bonnes pratiques générales du RGEN et est invité à qualifier sa solution au regard des spécifications mentionnées dans son mémoire technique.

Voir à ce titre :

<https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>

1.1.3 Référentiel Général d'Interopérabilité (RGI)

Le candidat devra suivre les recommandations du référentiel général d'interopérabilité (RGI) en version 2.0, consultable à partir du lien suivant : [Référentiel Général d'Interopérabilité \(numerique.gouv.fr\)](https://www.numerique.gouv.fr/publications/referentiel-general-interopabilite/).

En particulier, les chapitres 3 (interopérabilité technique) et 4 (interopérabilité syntaxique) listent les technologies par statut (recommandé, en observation, en fin de vie, retiré).

L'utilisation de technologies ayant le statut « Retiré » est proscrite dans le cadre du projet. L'utilisation de technologies « en fin de vie » est à éviter, sauf justification.

Sauf précision contraire dans le présent CCTP, les technologies recommandées sont celles du profil d'interopérabilité P1.

1.2 Normes et standards dans le cas d'une application web

1.2.1 Principes généraux

L'application devra être une application de type web s'appuyant sur les protocoles et standards du W3C.

Toutes les technologies de client web doivent utiliser les standards fréquemment utilisés par les éditeurs logiciels :

- HTML 5
- CSS 3
- Javascript (version ES6 ou supérieure)

Ainsi, Adobe Flash, Silverlight, ActiveX, Applet java sont des technologies proscrites.

Afin de respecter les bonnes pratiques, une attention particulière sera apportée à la séparation du code métier et de la présentation. Dans ce domaine, une utilisation rigoureuse des CSS sera privilégiée.

1.2.2 Navigateurs internet

L'application sera accessible par des utilisateurs dont le parc informatique et l'environnement de travail sont variés et ne sont pas maîtrisés. Il en résulte qu'elle devra être compatible avec les navigateurs Internet standard les plus courants et dans les versions supportées par leurs éditeurs :

- Microsoft Edge Chromium,
- Firefox ESR,
- Google Chrome,
- Safari.

1.2.3 Architecture logicielle dans le cas d'un développement spécifique

L'architecture logicielle mise en œuvre devra être modulaire, évolutive, scalable et interopérable.

Les composants de la solution devront être logiquement regroupés en couches, afin de permettre une séparation entre :

- La présentation (partie de l'application exposée aux utilisateurs finaux),
- Les règles métier,
- L'accès aux données.

Des API / Web services devront être exposés par la solution afin de permettre son interfaçage avec d'autres solutions.

Les formats REST/JSON et GraphQL seront privilégiés.

Les bonnes pratiques minimales à respecter sont les suivantes :

- Chaque ressource est identifiée par une URL unique,
- Les ressources sont identifiées par des noms et les verbes sont interdits (ex: /users et non pas /getUsers),
- Les principaux verbes servant à la manipulation des ressources sont GET (lecture d'une ressource), POST (Création d'une ressource), PUT (modification d'une ressource), PATCH (modification d'une partie d'une ressource), DELETE (suppression d'une ressource),
- Respect la nomenclature des réponses des requête http (200, 400, 500, ...),
- Utilisation de l'encodage des caractères UTF-8 pour le contenu des requêtes au format JSON,
- Encodage au format ISO 8601 des champs de type date et heure
- La pagination sera systématiquement mise en œuvre côté serveur dès lors que les requêtes retournent un nombre de résultats important. La façon de réaliser la pagination sera unique pour l'ensemble des webservices réalisés.

Le choix d'un autre format (REST/XML, SOAP, etc.) devra être justifié par le contexte, par exemple au regard des logiciels tiers consommant les webservices exposés par le backend.

Les API seront documentées, le candidat indiquera l'outil utilisé pour produire cette documentation.

Les API seront également versionnées (pour chaque version Vn le format est : `https://<domaineName>/Vn/<ressourceName>`)

Au niveau sécurité, les clauses de [Sécurité des web services](#) seront respectées.

1.3 Législation et normes applicables à l'hébergement externe

Le prestataire devra s'engager à respecter la législation Française et Européenne (durée de conservation des logs, protection des données personnelles, etc.) et prendre en compte les recommandations de la CNIL en matière d'hébergement.

Rennes métropole et la Ville de Rennes souhaitent bénéficier des services d'un hébergeur capable de fournir des hébergements « dans la règle de l'art » (Nous nous appuyons en particulier sur les recommandations de la CNIL à destinations des entreprises et des collectivités qui souhaitent faire appel à des services d'hébergement : http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf. Recommandations qui peuvent s'appliquer aux divers types de solutions d'hébergement).

Ainsi, le candidat devra décrire dans son offre les mesures techniques et les procédures mises en œuvre pour garantir :

- Le respect de la loi Informatique et Libertés, tout particulièrement en matière de protection des données personnelles.
- La possibilité de limiter le transfert de données vers l'Espace Économique Européen ou de le limiter à la France pour les données sensibles et dans des conditions potentiellement encadrées par la loi. En particulier, indiquer comment le respect de la législation et la sécurité des données fournis sur une localisation nominale sont assurés sur la localisation de transfert.
- L'information immédiate de Rennes Métropole ou de la Ville de Rennes en cas de requête provenant d'une autorité administrative ou judiciaire française ou étrangère.

1.4 Interopérabilité et ouverture des données

Le pouvoir adjudicateur s'est engagé dans une politique pour l'innovation et le développement numérique faisant une place prioritaire au logiciel libre et à la réutilisation des données publiques conformément à la loi n°78753 du 17 juillet 1978, ainsi que dans la perspective de l'application de la directive 2013/37/UE du 26 juin 2013 modifiant la directive du 2003/98/CE concernant la réutilisation des informations du secteur public.

Pour cela, il permet aujourd'hui à des tiers de réutiliser librement les données publiques diffusées sur les plateformes accessibles aux adresses www.data.gouv.fr et data.rennesmetropole.fr. Sont expressément exclues de cette démarche les données à caractère personnel ainsi que celles sur lesquelles des tiers détiendraient des droits de propriété intellectuelle.

Le pouvoir adjudicateur se réserve la possibilité de publier sous une licence de réutilisation publique, qui précise les droits et les obligations rattachés aux données, les données issues de l'utilisation de l'outil approvisionné par le présent marché. À cette fin, le titulaire fournit au pouvoir adjudicateur, dans des standards ouverts (c'est-à-dire, selon l'article 4 de la LCEN du 21 juin 2004 « tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre »), en vue de la mise à disposition à titre gratuit des informations publiques à des fins de réutilisation à titre gratuit ou onéreux :

- Les outils permettant d'extraire et exploiter librement tout ou partie de ces données et bases de données,
- Ou le cas échéant, les données et bases de données collectées ou produites à l'occasion de l'exécution du présent marché.

1.5 Environnement technique du système d'information de Rennes Métropole

La DSN mutualisée de Rennes Métropole et de la Ville de Rennes mettra en place le matériel nécessaire au bon fonctionnement de la solution proposée en ce qui concerne le réseau, les postes de travail personnels et le ou les serveurs, en fonction des préconisations du candidat retenu.

Les paragraphes concernant l'infrastructure Rennes Métropole (sauvegarde, pare-feux, serveurs, supervision, ...) sont à ignorer pour les solutions SAAS. Pour les solutions SAAS, les exigences sur ces points sont spécifiées dans le chapitre [EXIGENCES EN MATIERE DE CYBER SECURITE](#).

1.5.1 Les solutions techniques d'authentification

Les détails relatifs aux exigences sécurité de l'authentification sont donnés dans le chapitre cyber.

1.5.1.1 Authentification Single Sign On (SSO)

LemonLDAP-NG est une solution d'authentification et d'autorisation mise en œuvre dans le système d'information de Rennes Métropole (<https://lemonldap-ng.org/welcome/>). Cette solution supporte, entre autres, OpenId Connect et SAML2.

1.5.1.2 Authentification à partir d'un annuaire

La DSN a également mis en place un annuaire OpenLDAP sécurisé pour l'authentification applicative (protocole ldaps).

1.5.2 Les postes de travail, tablettes et smartphone

Les terminaux sont équipés de :

- Windows 10,
- Navigateur par défaut,
- Enrôlement dans une solution EMM,
- Client de messagerie Outlook connecté à une solution de messagerie Zimbra. Le candidat précisera dans son mémoire technique les éventuelles contraintes ou prérequis complémentaires (matériels ou logiciels) nécessaires sur les postes de travail pour le fonctionnement et l'utilisation de sa solution. Par exemple : suite bureautique, navigateurs en backoffice et frontoffice, environnement windows (32/64 bits), plug-ins, messagerie.

Les utilisateurs n'ont pas les droits administrateurs sur leur poste. Par conséquent, la solution proposée par le candidat ne devra pas nécessiter de disposer des droits administrateurs pour fonctionner, ou en dernier recours uniquement sur une partie bien identifiée du poste (répertoires, clés de registre...). Le candidat précisera dans sa réponse les contraintes d'exécution de sa solution.

De même si l'installation nécessite des droits particuliers, le candidat le précisera.

1.5.3 Le réseau

Un réseau informatique mutualisé entre Rennes Métropole et la Ville de Rennes a été mis en œuvre en 2012, il est constitué d'environ 140 sites, soit raccordés en fibre optique via la fibre optique rennaise (FOR), soit via des liens opérés VPN MPLS majoritairement en ADSL.

Les postes de travail sont majoritairement raccordés en 1 Gb/s sur des switchs d'extrémités. Ceux-ci sont connectés au backbone (cœurs ou distribution) en double attachement 2*1 Gb/s à part exception. Le réseau mutualisé dispose de deux accès internet 900 Mb/s sécurisés via une offre opérateur. Tous les postes de travail accèdent à internet en mode proxyfié. Le proxy authentifie les utilisateurs, filtre les URL, les virus et fonctionne en mode explicite.

1.5.4 Exigences sur les logiciels socles « intergiciels » (middleware)

Si la mise en œuvre de la solution nécessite le déploiement d'un JDK, JRE et/ou JVM (Java Development Kit / Java Runtime Environment / Java Virtual Machine) l'utilisation d'une distribution Java gratuite est imposée : par exemple Eclipse Temurin/AdoptOpenJDK, Azul OpenJDK, ...

La distribution Java utilisée sera indiquée dans le mémoire technique.

1.5.5 Pare-feux

Le LAN est protégé par un cluster de pare-feux. Les flux web entrants seront protégés par un pare-feu applicatif.

1.5.6 API Manager

Rennes Métropole dispose d'une plate-forme de management d'API (WSO2 API Manager) permettant de sécuriser et de monitorer l'accès aux API.

Les formats supportés par WSO2 API Manager sont les suivants :

- Swagger 2.0 / OAS (OpenAPI Specification) 3.0 et supérieur,
- Soap (wsdl),
- GraphQL,
- AsyncAPI.

2 EXIGENCES EN MATIERE DE CYBER SECURITE

2.1 Introduction

Rennes Métropole a adopté une démarche systématique d'intégration de la sécurité dans ses projets. Les exigences et questions de ce chapitre s'intègrent dans ce cadre.

Tous les éléments de l'offre relatifs à la cybersécurité devront être regroupés dans un document séparé ou un chapitre spécifique du mémoire technique intitulé « Éléments relatifs à la cybersécurité ». Pour la notation des offres sur les aspects cybersécurité, seuls les éléments présents dans ce chapitre ou document spécifique seront pris en compte.

2.2 Authentification

Les profils ayant à se connecter à l'application sont décrits dans le CCTP.

Dans ce chapitre, on distinguera les utilisateurs internes, les utilisateurs externes et les administrateurs fonctionnels.

En vertu du principe de sécurité de séparation des rôles, la collectivité souhaite que les administrateurs fonctionnels qui sont aussi utilisateurs de la solution possèdent 2 comptes nominatifs distincts : l'un pour utiliser la solution comme tout agent de la collectivité et l'autre pour administrer la solution. La solution envisagée pour atteindre cet objectif est d'utiliser :

- Une authentification propre à l'application pour les administrateurs et une authentification SSO pour les autres si l'authentification SSO via le Lemon LDAP de la collectivité est possible
- 2 comptes distincts si des comptes locaux sont utilisés exclusivement pour l'accès à l'application

Les utilisateurs externes se connecteront via un compte local à l'application.

En ce qui concerne l'authentification par compte local, il est attendu que le candidat détaille les mesures techniques (dont les choix cryptographiques) et options de configuration de sa solution permettant la mise en œuvre des conseils publiés par l'ANSSI dans son document « Recommandations relatives à l'authentification multifacteur et aux mots de passe ».

En particulier :

- Le candidat indiquera s'il peut mettre en œuvre le MFA (multi factor authentication) a minima sur les comptes à hauts privilèges y compris ceux du titulaire qui est amené à effectuer des actions « sensibles » pour la collectivité,
- Le candidat fournira la complexité, la longueur, la durée de validité des mots de passe et les paramètres possibles accessibles à la collectivité,
- Une longueur de 12 caractères minimum est demandée,
- L'algorithme de hachage des mots de passe devra être robuste. SHA1 et MD5 seront prohibés. Les algorithmes préférés sont dans l'ordre Argon2, Scrypt et Bcrypt,
- L'emploi de sel et poivre serait apprécié : le candidat indiquera si c'est le cas dans sa proposition
- La gestion des mots de passe oubliés devra être disponible. Elle ne sera pas basée sur un système de questions secrètes mais sur un système d'activation de liens envoyés sur une adresse mail ou un numéro préenregistrés,
- Les comptes devront être bloqués automatiquement après n connexions infructueuses : le candidat indiquera quelles peuvent être les valeurs du nombre n dans son application,
- La session devra être automatiquement fermée après x mn : le candidat indiquera quelles peuvent être les valeurs du nombre x dans son application,

- Une vérification de la robustesse des mots de passe lors de leur choix par l'utilisateur serait appréciée : le candidat indiquera si c'est le cas dans sa proposition.

2.3 Sécurité physique et logique de l'hébergement (cas d'un hébergement externe)

Le candidat décrira de façon précise les conditions physiques de l'hébergement qu'il propose. Il est attendu un hébergement complètement sécurisé :

- Hébergement sur son propre datacenter ou hébergement chez un tiers,
- La raison sociale de l'hébergeur
- La localisation géographique des salles serveurs (datacentres). Il indiquera où seront hébergées les données de Rennes Métropole et de la Ville de Rennes, y compris dans le cas d'un transfert pour sauvegarde ou disponibilité (PRA)
- La description de la plateforme matérielle mise en œuvre (serveurs physiques, serveurs virtualisés, serveur dédiés ou partagés, le type de base de données utilisée, etc.).
- Le niveau de performance du service (bande passante, connexions simultanées, redondance des accès réseau, moyens de sauvegarde automatisée ...).
- Les redondances et sécurisations physiques permettant de sécuriser l'hébergement,
 - Sécurisation et redondance des accès internet,
 - Dispositifs de protection contre l'intrusion physique,
 - Dispositifs de protection relatifs au risque d'incendie,
 - Dispositifs de protection relatifs au risque d'inondation,
 - Dispositifs de protection et de redondance sur l'alimentation électrique,
 - Dispositifs de protection et de redondance sur le système de refroidissement,
- La liste des certifications de l'hébergement avec précision de leur périmètre d'application.

Le candidat devra également mettre en œuvre sur ses infrastructures ou celles de ses sous-traitants un ensemble de mesures visant à réduire les risques de cyberattaque ou d'en limiter la portée. Le candidat précisera les mesures de sécurité qu'il a effectivement mis en place sur l'infrastructure hébergeant la solution. Il ne se contentera pas de faire référence à la documentation générale de l'hébergeur :

- Journalisation,
- Supervision,
- Firewall applicatifs,
- Gestion des incidents,
- Cloisonnement des données entre clients (obligatoire),
- ...

Le candidat précisera dans son offre quelles mesures il met en œuvre sur ce point.

Il précisera également comment il gère techniquement le cloisonnement entre clients.

2.4 Sauvegardes et tests de restauration (cas d'un hébergement externe)

En ce qui concerne la partie hébergée par le titulaire et pour l'ensemble des données, il est attendu du candidat une ou plusieurs sauvegarde(s) quotidienne(s) des données et des fichiers hébergés dans la solution en respectant les exigences suivantes :

- Une sauvegarde devra impérativement être stockée dans un lieu différent du lieu de production,
- Une sauvegarde devra impérativement être une sauvegarde hors ligne, c'est-à-dire déconnectée du système d'information, ce qui lui permet d'être opérationnelle en cas de compromission du système d'information,

Le candidat précisera la fréquence, le lieu et le mode de sauvegarde retenu pour l'ensemble des données de la collectivité. Il précisera notamment son délai de restauration en cas de perte.

Il détaillera également le fonctionnement technique de la sauvegarde hors ligne.

Le candidat décrira la fréquence des tests de restauration effectués et le périmètre de ces tests de restauration (données infrastructures, données applicatives, données client, ...). A minima, ces tests devront être effectués une fois par an.

2.5 Chiffrement et sécurité des flux

Pour l'accès à la partie applicative aux web services, que ce soit en hébergement interne ou externe, il est attendu que les flux soient chiffrés avec des protocoles et algorithmes "up to date". Les recommandations de l'ANSSI devront être mises en œuvre et notamment les recommandations présentes dans le guide « Recommandations de sécurité relatives à TLS ». Sur le présent dossier ne seront acceptées que les versions 1.2 et 1.3 du protocole TLS pour l'ensemble des flux (application web, web services, ...) avec implémentation obligatoire de la version TLS 1.3. Il est également attendu un travail sur les suites cryptographiques autorisées et sur les extensions comme le stipule le document de l'ANSSI.

Le candidat précisera son offre sur ce point en détaillant les protocoles utilisés et les modalités de travail sur les suites cryptographiques qu'il a effectuées.

Le candidat précisera quels tests de sécurité du serveur il propose de mettre en œuvre (type Qualys ou autre) et quel niveau de sécurité il propose d'atteindre.

2.6 Sécurisation des envois de mails

Le candidat détaillera les éléments qui permettent d'assurer la sécurité des envois de mails et SMS à partir de sa solution.

En particulier pour la messagerie, il est recommandé que SPF, DKIM et DMARC soient utilisés et configurés.

2.7 Sécurité des développements

Le titulaire s'engage à sécuriser ses développements en mettant en œuvre de bonnes pratiques telles que :

- Formant les développeurs notamment aux questions de cyber sécurité,
- Appliquant des normes ou référentiels génériques de développement : OWASP, SDL (Security Development Lifecycle) ou autres,
- Appliquant des normes et référentiels de bonnes pratiques sur ses frameworks et technologies de développement,
- Sécurisant ses applications par rapport aux bonnes pratiques dispensées par l'owasp,
- Mettant en œuvre des processus de lutte contre l'obsolescence et la vulnérabilité des composants de l'application ou des composants de développement qu'il utilise,
- Protégeant les clés et les secrets,
- Isolant les environnements relatifs aux applications elles-mêmes par rapport aux outils d'administration des applications,
- Sécurisant le développement et l'utilisation des web services qu'il met en œuvre,
- Réduisant la surface d'attaque de l'application notamment par suppression des parties de code, des interfaces et des protocoles non utilisés,
- Gérant la journalisation des erreurs et des exceptions avec analyse a posteriori pour améliorer la sécurité de l'application,

- Utilisant des requêtes paramétrables pour les accès à la base de données et/ou autres techniques protégeant des injections sql,
- Analysant systématiquement de toutes les données entrées par les utilisateurs avant traitement,
- Supprimant les en-têtes de serveur standard pour éviter la prise d'empreinte des systèmes par les attaquants,
- Gérant de façon sécurisée des sessions de connexion avec notamment une protection des jetons de session contre le vol et le rejeu ainsi qu'une gestion automatique de leur durée de vie,
- Gérant la protection contre les attaques classiques type injection SQL, xss, ssrf, csrf, directory traversal, deny de service, ...
- Analysant des fichiers téléchargés via l'application.

Le candidat précisera quelles sont les bonnes pratiques implémentées dans la liste ci-dessus.

Le titulaire s'engage à tester son code avant chaque mise en production, ce par différents moyens : audit de code statique et/ou dynamique, utilisation d'outils d'audit de code, de scanners de vulnérabilités, ...

2.8 Sécurité des applications mobiles

L'OWASP fournit une série de documents de référence sur la sécurité des applications mobiles : OWASP_MASVS-v1.4.2-fr.pdf, OWASP_MSTG-v1.4.0.pdf, Mobile_App_Security_Checklist_fr.xlsx téléchargeables depuis internet (lien OWASP : <https://owasp.org/www-project-mobile-security/>). Le candidat indiquera si et comment il utilise ces référentiels. S'il utilise d'autres référentiels ou d'autres outils en complément ou en remplacement, il est invité à les détailler.

Le titulaire s'engage à ne pas publier sur internet d'informations susceptibles de faciliter l'attaque de l'application mobile.

Enfin, cette application mobile devra être compatible avec toute solution de MDM avec séparation de l'espace professionnel de l'espace personnel ou toute solution de MTD (MobileThreat Defense) que la collectivité mettrait en œuvre durant la durée de la maintenance de la solution.

2.9 Audits techniques et tests d'intrusion

Durant la période de maintenance couverte par le présent contrat, la collectivité compte effectuer ou faire effectuer par un de ses prestataires un ou plusieurs audits et/ou tests d'intrusion sur la solution. Le titulaire devra se comporter en facilitateur de ces opérations qu'elles se déroulent en boîte blanche, grise ou noire et procéder à la remédiation sur les vulnérabilités découvertes dans le cadre du contrat de maintenance sans supplément de prix.

Pour évaluer l'urgence d'un patch sur une vulnérabilité et donc les exigences de délai des remédiations, on se basera sur le score CVSS de cette vulnérabilité qui sera fourni par l'auditeur.

- Critical (score ≥ 9) : sans délai,
- High (score ≥ 7 et ≤ 8.9) : 7 jours ouvrés,
- Medium (score ≥ 4 et ≤ 6.9) : 1 mois,
- Low (score ≤ 3.9) : 3 mois.

Si le score EPSS existe sur les composants utilisés dans la solution, il pourra être proposé comme solutions alternative.

Le titulaire précisera s'il fait réaliser des tests d'intrusion sur sa solution ainsi que leur périmètre et leur fréquence.

2.10 Échanges de données avec la collectivité

Le titulaire, s'il a besoin de recueillir des données sur les bases de la collectivité, s'engage à les stocker de façon chiffrée par des algorithmes « up to date » et en sécurisant à l'état de l'art les « secrets » relatifs à ce chiffrement et à l'accès au conteneur de stockage.

Le titulaire s'engage à détruire les dites données dès que les opérations ayant justifié le recueil auront été réalisées.

De même, le titulaire s'engage à ce que les flux relatifs aux transferts de données susvisés soient chiffrés via une solution « up to date » conforme aux recommandations de la dernière version du RGS parue.

2.11 Sécurisation des interfaces avec des applications tierces

Le candidat détaillera la façon dont il gère la sécurité des interfaces d'échange de données avec des applications tierces :

- Authentification,
- Chiffrement des échanges,
- Chiffrement du stockage si utilisation d'exports,
- Préservation des secrets notamment les secrets d'authentification,
- ...

De plus en cas d'hébergement externe, si des interfaces doivent être réalisées avec des applications internes, le candidat devra décrire l'architecture envisagée via un schéma de flux et une matrice de flux auxquels il ajoutera un commentaire descriptif.

2.12 Prise en main à distance

Le titulaire devra s'adapter aux protocoles de la collectivité en matière de prise en main à distance. En effet, la collectivité va mener prochainement un projet d'homogénéisation et de sécurisation de ces procédures.

Le candidat s'engage sur une sécurisation à l'état de l'art des postes de travail de ses administrateurs qui interviennent directement sur le système d'information de la collectivité. Notamment, ces postes doivent être à jour, un pare-feu local doit y être activé et ils doivent disposer d'une solution antivirale et comportementale pour détecter les codes malveillants.

Au niveau de la collectivité, les comptes d'administration des fournisseurs et prestataires sont créés en respectant le principe du moindre privilège.

Ils ne seront pas activés en permanence mais seulement pour la période d'intervention qui ne pourra en aucun cas excéder une semaine.

Enfin, le fournisseur ou prestataire devra tenir la collectivité au courant de ses mouvements de personnel au plus près de la date de ces mouvements (délai inférieur à 7 jours) afin que la collectivité puisse supprimer le compte personnel d'administration lié à l'administrateur parti.

2.13 Lutte contre l'obsolescence

Il appartiendra au titulaire tout au long du marché d'être force de proposition auprès de la collectivité pour lutter contre l'obsolescence de la solution. À ce titre, il devra proposer régulièrement et a minima une fois par an des prestations de mise à niveau de la solution selon l'avancée de ses développements, l'intégration de nouveaux modules ou nouveaux protocoles.

2.14 Référentiel Général de Sécurité (RGS)

Le Référentiel Général de Sécurité (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information.

Dans tous les choix cryptographiques relatifs à sa solution et pendant toute la durée du marché, le titulaire devra se conformer aux recommandations du RGS **dans sa dernière version** et au guide de sélection d'algorithmes cryptographiques, tous deux publiés par l'ANSSI.

La version du RGS actuellement applicable est la version 2.0, consultable à partir du lien suivant : <https://www.numerique.gouv.fr/publications/referentiel-general-de-securite/>

2.15 Maintenance relative à la sécurité

Le titulaire s'engage à effectuer une veille a minima mensuelle sur les vulnérabilités présentes dans les composants qu'il utilise dans la solution qu'il fournit à la collectivité.

Pour toutes les parties de sa solution qui sont hébergées par lui ou par des sous-traitants, il s'engage à procéder à la remédiation dans un délai dépendant du score CVSS de la vulnérabilité (cf. [Audits techniques et tests d'intrusion](#)).

Pour toutes les parties de sa solution qui sont hébergées on premise, il s'engage à fournir à la collectivité les correctifs de sécurité et procédures de mise à jour dans le même délai.

Tous les 6 mois, le titulaire fournira un rapport de veille et de remédiation à la collectivité.

La maintenance sécurité est incluse dans la maintenance de base du logiciel. La maintenance sécurité et les remédiations inhérentes ne peuvent pas donner lieu à facturation supplémentaire.

3 Architecture et documentation technique et sécurité

Dans son mémoire technique, le candidat remettra une première version du document de spécifications technique de sa solution afin que la collectivité puisse analyser l'adéquation technique de la proposition.

Ce document de spécification technique devra couvrir l'entièreté du périmètre en lien avec la collectivité que ce soit sur les systèmes du prestataire ou ceux de la collectivité. Il contiendra a minima :

- Un ou plusieurs schéma(s) d'architecture physique et logique détaillés,
- Un ou plusieurs schéma(s) représentant les flux applicatifs,
- Un texte commentaire détaillé explicitant ce(s) schéma(s),
- Un récapitulatif des choix techniques sur les différents composants de la solution en précisant pour chaque composant :
 - L'identification de l'éditeur du composant,
 - L'identification du composant,
 - La ou les versions du composant qualifiées par le candidat pour sa solution,
 - Les prérequis et contraintes d'installation, si nécessaire par version du composant,
 - Les serveurs affectés au composant ainsi que leur configuration.
- Une matrice de flux détaillée et commentée indiquant les flux autorisés, les ports utilisés, la présence de chiffrement et la présence d'authentification.

Avant la mise en œuvre, un atelier spécifiquement dédié à la finalisation de l'architecture technique et à la sécurité devra être organisé par le titulaire (pour une solution OnPremise par exemple : spécifications serveurs, bases de données, protection antivirale, configurations réseaux, pare-feux, sauvegarde, réponse à l'ensemble des exigences en matière de cybersécurité présentées en annexe 3, etc.). Pour une solution SAAS, il s'agira d'échanger autour des moyens de sécurité proposés par le prestataire et le cas échéant de travailler sur leur configuration.

Le travail sur les interfaces sera réalisé dans un atelier spécifique.

L'atelier d'étude d'architecture et de sécurité se déroulera sous la forme de deux réunions a minima (une réunion d'étude et une réunion de validation). Le candidat pourra en proposer davantage s'il le juge utile tout en justifiant sa proposition dans son mémoire technique.

Cet atelier se déroulera à Rennes ou à distance, avec le service de la DSN en charge des infrastructures, la RSSI de la collectivité et éventuellement d'autres acteurs que la collectivité souhaitera faire participer.

Les livrables attendus par la collectivité suite à l'atelier sont la finalisation du document de spécifications techniques et le plan d'assurance sécurité (PAS) qui constituera une pièce contractuelle du marché.

Le PAS synthétisera l'ensemble des mesures de sécurité décidées lors des réunions d'architecture ou dans l'offre ou encore lors de réunions de mise en œuvre. Le PAS traduit non seulement l'engagement des 2 parties au niveau cybersécurité mais également les mesures de sécurité décidées qui doivent être maintenues durant tout le cycle de vie de la solution.

Le PAS sera élaboré et validé par la RSSI de Rennes Métropole mais le titulaire devra participer à son élaboration en particulier en répondant aux questions de la RSSI et si besoin en faisant les recherches nécessaires pour fournir les réponses si certains points nécessitent un approfondissement.

Le travail du titulaire sur le PAS devra être inclus dans l'offre initiale et ne pourra donner lieu à facturation supplémentaire.

Il appartiendra au titulaire de maintenir à jour la documentation technique (document de spécification technique et propositions d'évolution sur le PAS) tout au long du cycle de vie de la solution y compris en phase de maintenance. Les propositions d'évolution seront validées par la DSN et la RSSI. La mise à jour de la documentation devra être intégrée à l'offre de maintenance sans supplément de prix.

4 Clause de réversibilité

Dans le cadre de la fin du marché, qu'elle soit anticipée ou non, le titulaire s'engage à mettre en œuvre un plan de réversibilité visant à assurer la continuité et la reprise des services concernés dans les meilleures conditions pour le repreneur, minimisant les impacts pour la collectivité.

Il est précisé que :

- On entend par repreneur, le pouvoir adjudicateur et, éventuellement, le nouveau prestataire désigné par le pouvoir adjudicateur
- Le terme réversibilité couvre également la transférabilité quand il s'agit de la reprise des services par le nouveau prestataire désigné par le pouvoir adjudicateur
- Selon leur nature, et sans être exhaustif, les services peuvent inclure à la fois des matériels, des logiciels, des données et des documents à reverser au repreneur
- Les services désignent les fournitures et les prestations objets du marché attribué au titulaire.

4.1 Objectifs de la réversibilité

La réversibilité vise à, selon la nature des services :

- Garantir la continuité des services tout au long de la période de réversibilité.
- Faciliter le transfert le plus exhaustif possible des connaissances, des données, des outils et des compétences vers le repreneur.
- Minimiser les interruptions ou les dégradations du service.

4.2 Déclenchement de la réversibilité

Le pouvoir adjudicateur notifiera le titulaire par courrier de son intention de déclencher l'exécution des prestations de réversibilité en fin de marché ou, en cas de résiliation totale ou partielle, après la notification de la résiliation.

La réversibilité s'exercera pendant le délai nécessaire à sa bonne réalisation et selon le planning détaillé du plan de réversibilité, et s'achèvera à la mise en production effective des données dans le nouveau système. Par dérogation avec le CCAG TIC (Art. 38.3 et 38.4 du CCAG-TIC), elle pourra ainsi s'exercer dans les 6 à 9 mois précédant la fin du Marché, ou en cas de résiliation totale ou partielle, pendant les 6 à 9 mois suivant la notification de la résiliation.

En cas de retard d'exécution dû à un dysfonctionnement du titulaire, la charge sera aux frais du titulaire, y compris les coûts supplémentaires supportés par le pouvoir adjudicateur.

Le pouvoir adjudicateur notifiera le titulaire par courrier de la fin officielle de la réversibilité.

4.3 Plan de réversibilité

Le Titulaire doit fournir dans son mémoire un plan de réversibilité détaillé, qui inclut les éléments décrits dans les chapitres ci-dessous.

Le plan de réversibilité est mis à jour annuellement par le titulaire et validé par le pouvoir adjudicateur.

4.3.1 Organisation et gouvernance de la réversibilité

La gouvernance consiste en la mise en place d'un comité de réversibilité

- Identification des parties prenantes (pouvoir adjudicateur, titulaire, éventuel nouveau prestataire).

- Définition d'un interlocuteur dédié à la réversibilité côté titulaire.
- Description de l'équipe compétente en charge de la réversibilité côté titulaire
- Nature et fréquence des réunions du comité de réversibilité (réunion de lancement, suivi hebdomadaire ou bimensuel,...).

4.3.2 Inventaire des éléments à restituer

Le plan de réversibilité décrit l'ensemble des éléments à restituer au repreneur.

Selon la nature des services :

- Les données au jour de la bascule vers le repreneur.
- L'ensemble des matériels appartenant au pouvoir adjudicateur.
- L'ensemble des logiciels, outils de développement, de configuration, de test dont les licences appartiennent au pouvoir adjudicateur.
- Les codes sources éventuels (en particulier ceux des développements spécifiques réalisés pour le pouvoir adjudicateur).
- La documentation (technique, fonctionnelle, ...).

Cet inventaire permet de déterminer, selon la nature des services, le périmètre des éléments à transférer décrits dans les chapitres ci-dessous.

4.3.3 Transfert des données

- Inventaire complet des données à transférer. Toutes les données produites dans le cadre des services doivent pouvoir être restituées, ces données doivent être exhaustives, exactes, cohérentes et de qualité
- Format de restitution des données (conformité aux standards ouverts). Les données doivent être fournies dans un format standard, lisibles et exploitables sans transformation de manière à en automatiser la réutilisation par le repreneur. Pendant l'exécution de la réversibilité, le titulaire s'engage à informer le pouvoir adjudicateur de tout changement dans le format des données transmises.
- Modalités de transmission : les modalités de transmission doivent être sécurisées.
- Engagements de vérification de l'intégrité et de la complétude des données transmises.
- Engagement sur la suppression des données : le titulaire s'engage à supprimer les données sur ordre du pouvoir adjudicateur, après la dernière itération validée de transfert de données.

4.3.4 Transfert des matériels, des logiciels et des environnements techniques

- Le cas échéant, restitution des matériels
- Restitution des licences logicielles, documentations, codes sources et autres éléments nécessaires au fonctionnement.
- Remise des configurations des systèmes et fichiers de configuration
- Accès aux différents environnements (développement, test, formation, pré-production, production)

4.3.5 Transfert de la documentation

- Spécifications fonctionnelles et techniques,
- Installation et configuration,
- Exploitation
- Formation et transfert de compétence

4.3.6 Transfert des compétences

- Formation et accompagnement des équipes du repreneur sur les éléments repris.
- Organisation de sessions de transfert de compétences.
- Transfert des enregistrements des tickets anomalies déclarés et leurs solutions de résolution.

4.3.7 Itérations entre le Titulaire et le repreneur

Pour garantir le succès de la réversibilité, le processus comprendra un nombre défini d'itérations entre le titulaire et le repreneur. Ces itérations permettront de valider de manière itérative et incrémentale chaque étape de la réversibilité :

- Nombre d'itérations minimales prévues : un minimum de trois itérations est recommandé, à savoir :
 - Une première itération de transfert pour tester la transmission des données, outils et connaissances dans un environnement contrôlé.
 - Une seconde itération de validation pour ajuster les éventuelles erreurs ou omissions identifiées lors de la première transmission.
 - Une troisième itération de finalisation pour valider l'ensemble des éléments transférés, avec des tests en conditions réelles si nécessaire.
- La fréquence et le nombre exact d'itérations seront définis dans le cadre du plan de réversibilité en fonction de la complexité des services.
- Chaque itération sera suivie d'une réunion de bilan en comité de réversibilité pour formaliser les observations, les points d'amélioration et les jalons atteints.

4.3.8 Planning détaillé des opérations de réversibilité

Le planning proposé par le titulaire doit inclure les principaux jalons et leurs durées :

- Période de préparation (analyse des éléments à transférer).
- Période de mise en œuvre des transferts y compris transfert de compétences.
- Période de validation des livrables par le repreneur.
- Bascule de responsabilité.
- Éventuellement période de supervision post-transfert.

4.3.9 Critères de validation par le repreneur

- Planning de réversibilité.
- Validation des livrables (ex. complétude des données, tests des outils transférés...).
- Vérification de la bonne exécution de la réversibilité

4.4 Obligations du titulaire

- Le titulaire reste responsable de la continuité du service pendant la durée de la réversibilité.
- Il s'engage à coopérer pleinement avec le pouvoir adjudicateur et/ou le nouveau prestataire.
- Il exerce son obligation de conseil envers pouvoir adjudicateur sur les moyens techniques à mettre en œuvre et leur organisation pour la réversibilité, tel qu'il en a connaissance.
- Le titulaire doit garantir la confidentialité et la sécurité des données tout au long du processus conformément aux exigences de la PSSI.

4.5 Coût de la réversibilité

- Le coût des prestations de réversibilité doit être inclus dans la proposition financière du titulaire (BPU).
- En cas de demande de prestations spécifiques supplémentaires en phase de réversibilité, leur coût devra être validé au préalable par le pouvoir adjudicateur. Cela peut concerner par exemple tout élément à restituer dont le pouvoir adjudicateur ne serait pas propriétaire ou détenteur des droits d'utilisation (à indiquer dans le plan de réversibilité).

4.6 Pénalités

En cas de non-respect des obligations de réversibilité, des pénalités financières pourront être appliquées (CCAP – Pénalités pour retard d'exécution).