

INDUSTRIALISATION ET MAINTENANCE DU SYSTEME D'ARCHIVAGE ELECTRONIQUE (SAE) DU CEREMA

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (C.C.T.P.)

Version de juin 2025

1	PRESENTATION DU PROJET	3
1.1	Objet du contrat	3
1.2	Contexte	3
1.2.1	Présentation des acteurs	3
1.2.2	Démarche d'archivage électronique	4
1.3	Objectifs	4
1.4	Cadre réglementaire et normatif	5
1.4.1	Cadre réglementaire relatif aux archives publiques	5
1.4.2	Cadre de confiance de l'administration électronique	6
1.4.3	Cadre normatif	6
1.5	Environnement applicatif et sources de données à prendre à compte	6
1.5.1	Périmètre fonctionnel	6
1.5.2	Sources de données applicatives	7
2	Exigences fonctionnelles	7
2.1	Gestion des profils utilisateurs	7
2.2	Gestion des entrées / versements	7
2.2.1.1.1	Contrôle du versement	8
2.2.1.1.2	Profil d'archivage	9
2.3	Gestion des métadonnées	10
2.4	Pérennisation	11
2.4.1	Contrôle d'intégrité et d'exhaustivité	11
2.4.2	Migration de formats et d'environnement de stockage	11
2.4.3	Journal du cycle de vie des archives	11
2.4.4	Journal des évènements	12
2.5	Gestion des consultations / communications	12
2.5.1	Rechercher et consulter les archives	12
2.5.2	Communiquer des archives	13
2.6	Gestion des éliminations	13
2.7	Gel de l'élimination	14
2.8	Traçabilité	14
2.8.1	Traçabilité des entrées et contrôles	15

2.8.2	Traçabilité des communications.....	15
2.8.3	Traçabilité des éliminations et gels.....	15
2.9	Administration fonctionnelle.....	16
2.10	Formation fonctionnelle.....	16
3	EXIGENCES TECHNIQUES.....	17
3.1	Hébergement de la solution.....	17
3.2	Prérequis techniques minimaux.....	17
3.3	Accès à la solution.....	17
3.4	Gestion des droits.....	18
3.5	Volumétrie.....	18
3.6	Réversibilité, transférabilité des données.....	18
3.7	Principe d'écoresponsabilité.....	19
3.8	Supervision.....	19
3.9	Performance et évolutivité.....	19
3.10	Journalisation technique et interopérabilité.....	20
3.11	Montée de version Asalae 3.0.....	20
4	Exigences de sécurité.....	20
4.1	Gouvernance de la sécurité.....	20
4.2	Protection des accès.....	20
4.3	Sécurité applicative.....	21
4.4	Journalisation et détection.....	21
4.5	Maintien en condition de sécurité (MCS).....	21
4.6	Protection des données à caractère personnel (RGPD).....	21
5	CONDITIONS DE RÉALISATION DU CONTRAT.....	22
5.1	Gouvernance du projet.....	22
5.2	Organisation et phasage.....	22
5.3	Livrables attendus.....	22
5.4	Suivi de la qualité et des engagements.....	23
5.5	Réversibilité.....	23
5.6	Délais de maintenance et de correction.....	23

5.7	Traitement des incidents et support.....	23
6	Annexe 1 : Plan projet cible	24
6.1	Phase 0 : Préparation et prise en charge (mois M0 – M1)	24
6.2	Phase 1 : Montée de version Asalae 3.0 (M2 – M3)	24
6.3	Phase 2 : Industrialisation des versements (M4 – M6)*	25
6.4	Phase 3 : Formation & accompagnement des utilisateurs (M4 – M7)*	25
6.5	Phase 4 : Stabilisation & supervision du système (M7 – M9).....	25

1 PRESENTATION DU PROJET

1.1 Objet du marché

Le Cerema souhaite industrialiser son système d'archivage électronique (SAE) actuel basé sur les solutions Asalae et Versae de l'éditeur LIBRICIEL SCOP et assurer sa maintenance pour ses archives nativement numériques pour :

- Évaluer, trier et sélectionner ;
- Classer et décrire selon des métadonnées ;
- Exporter, transférer et gérer ;
- Préserver ;
- Communiquer et accéder ;
- Éliminer ;
- Valoriser.

Le SAE doit permettre la conservation des archives en garantissant leur confidentialité, leur intégrité, leur disponibilité, leur lisibilité et leur exploitabilité dans le temps.

Suite au pilote réalisé en 2024 avec la solution d'archivage électronique libre de droits Asalae et son module de versement Versae, le COPIL a décidé d'utiliser la solution gratuite et libre de droit Asalae et son module de versement Versae.

Dans le cadre du présent marché, le Cerema souhaite industrialiser le projet autour des solutions Asalae et Versae déjà installées sur les infrastructures techniques de l'établissement.

Le Cerema attend du titulaire de ce marché des prestations de maintenance applicative et de support helpdesk.

Il conviendra également que le titulaire propose une formation fonctionnelle à la prise en main pour les deux solutions à destination des archivistes du Cerema, ainsi qu'un plan de suivi de projet ponctuel (maximum deux fois par an).

Des prestations ponctuelles en lien avec le paramétrage, la formation ou encore l'assistance pourront être commandées au coup par coup par bon de commande conformément au bordereau des prix unitaires au regard des besoins exprimés par le Cerema.

La fourniture de l'infrastructure de stockage et de matériels est exclue du présent marché.

1.2 Contexte

1.2.1 Présentation des acteurs

Le Cerema est un établissement public relevant du Ministère de la Transition écologique.

Il accompagne l'État et les collectivités territoriales pour l'élaboration, le déploiement et l'évaluation de politiques publiques d'aménagement et de transport. Implanté au cœur des territoires, le Cerema bénéficie d'une connaissance historique des problématiques et contextes locaux. Cette proximité lui permet de proposer des solutions sur mesure aux acteurs des territoires et de mettre à leur disposition des interlocuteurs concernés, engagés et disponibles.

La mission Archives du Cerema est rattachée au pôle Gestion de la connaissance au sein du Département Diffusion des connaissances de la Direction de la Stratégie et de la Communication (DSC). Le pôle Gestion de la connaissance concentre des activités de veille documentaire, de gestion de la plateforme documentaire du Cerema, de documentation et de gestion des abonnements pour l'établissement. Le Département Diffusion des connaissances assure, en plus des missions liées à la gestion de la connaissance, les activités de web et de production éditoriale du Cerema.

Concernant la Direction des Systèmes d'Informations (DSI), la direction comporte environ 70 agents rassemblés dans 4 services distincts assurant les missions suivantes :

- La stratégie numérique et d'achats, les missions de sécurité du SI et d'homologation,
- La gestion des infrastructures (en projet et en fonctionnement)
- L'ingénierie informatique interne (activités de chefferie de projet et de développement)
- La plateforme d'accueil numérique (univers numérique et supports utilisateurs).

Le contrôle scientifique et technique (CST) est double pour le Cerema :

- Pour les archives produites par les directions territoriales, le contrôle est exercé par les Archives départementales territorialement compétentes - le Cerema possède 26 implantations, dans 26 départements différents. Le siège social se trouve à Lyon dans le Rhône.
- Pour les archives produites par les directions fonctionnelles, le contrôle est exercé par la mission archives du ministère.

Le Cerema est donc amené à verser ses archives définitives à ces deux types d'acteurs : les services d'archives départementaux et les Archives Nationales.

Ce double contrôle scientifique et technique s'applique également pour la validation des éliminations des archives nativement numériques. Aussi, un projet d'autorisation unique d'élimination en parallèle d'une synthèse des tableaux de gestion du Cerema par une fiche d'évaluation est en cours, en lien avec le Service interministériel des Archives de France (SIAF).

Le projet est co-porté par la DSC en position de maîtrise d'ouvrage et la DSI s'occupant de la mise en œuvre opérationnelle et technique.

1.2.2 Démarche d'archivage électronique

Le Cerema s'est engagé progressivement, depuis quelques années, dans la dématérialisation de ses processus : ainsi, de plus en plus de documents sont générés sous format numérique. La production croissante de documents et données numériques générés dans des formats très divers a amené le Cerema à lancer une démarche d'archivage électronique afin de répondre aux obligations réglementaires de conservation des documents administratifs et techniques. Ces obligations concernent aussi bien la collecte, le traitement, la pérennisation et la mise à disposition des documents collectés.

Depuis 2021, une mission archives s'est constituée et a construit progressivement un cadre de gouvernance de la gestion des archives (référentiels de conservation, procédure et base de la politique d'archivage).

Depuis février 2023, une démarche d'archivage bureautique est menée au sein du Cerema afin d'apporter une rationalisation de la production technique de l'établissement qui a vocation à permettre une centralisation des archives, une meilleure organisation et une meilleure structuration. Les travaux de records management entrepris ont permis de rassembler des typologies ainsi que des arriérés dans des répertoires afin d'obtenir des zones « tampon » qui préparent le versement dans un SAE. Ils ont également permis une meilleure identification des fonds et le façonnage d'objectifs d'archivage précis qui ont ouvert la voie au présent projet. En parallèle, la mission Archives réalise de multiples chantiers de reprise d'arriéré bureautique et planifie ses objectifs de collecte 2025-2026 en vue de l'industrialisation du SAE.

1.3 Objectifs

En se dotant d'un SAE, le Cerema souhaite répondre aux exigences suivantes :

- Exigences réglementaires :
 - Conformité avec la loi sur les archives de 2008 ;
 - Conformité avec la norme NF Z 42-013
- Exigences numériques :
 - Faire du SAE un système d'information central et de référence au sein de la cartographie SI du Cerema ;

- Répondre aux manquements de la solution de stockage actuelle BOX et des applications SI ne comportant pas de solution d'archivage conforme ;
- Faire du SAE une base de données remarquable et exploitable par l'intelligence artificielle, un nouvel axe de progrès au Cerema ;
- Exigences liées à la gestion de la connaissance :
 - Répondre à la vocation « centre de ressources » du Cerema ;
 - Constituer, gérer, conserver et valorisation un patrimoine technique remarquable (ouvrir le SAE vers les utilisateurs extérieurs) ;
 - Répondre aux limites de la plateforme documentaire CeremaDoc du Cerema
- Exigences liées aux ressources humaines :
 - Professionnaliser les agents utilisateurs du SAE et les correspondants archives du Cerema sur la fonction archive ;
 - Professionnaliser l'équipe d'archivistes de la mission Archives.

En ce sens, le SAE qui sera implanté au Cerema devra répondre à la démarche d'archivage électronique de l'établissement qui permet :

- D'accompagner les directions dans l'identification des documents et données à forte valeur juridique, administrative, technique ou patrimoniale ;
- De comprendre comment sont produits ces documents et données ;
- De mettre en place des procédures pour gérer leur cycle de vie : élaboration de référentiels de conservation, contrôle des éliminations dans le respect de la réglementation ;
- D'accompagner les direction dans l'organisation et la description des documents et données ;
- De planifier et sécuriser la conservation des documents/données à moyen et à long terme ;
- De planifier et sécuriser l'accès à l'information dans le temps pour que les utilisateurs, quels qu'ils soient, puissent réutiliser des documents et données fiables tout en évitant la banalisation de l'accès à l'information ;
- Faciliter la maîtrise des risques juridiques, opérationnels et financiers liés à la perte de documents et données nécessaires à la continuité des activités.

1.4 Cadre réglementaire et normatif

1.4.1 Cadre réglementaire relatif aux archives publiques

Les archives publiques sont régies par le Livre II respectif des parties législatives et réglementaires du Code du Patrimoine.

Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité (article L. 211-1 du Code du Patrimoine).

Les archives publiques sont plus particulièrement, à la lecture de l'article L.211-4 du Code du patrimoine :

- Les documents qui procèdent de l'activité de l'État, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ;
- Les documents qui procèdent de la gestion d'un service public ou de l'exercice d'une mission de service public par des personnes de droit privé ;
- Les minutes et répertoires des officiers public ou ministériels et les registres de conventions notariées de pacte civil de solidarité.

La conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche (article L. 211-2 du Code du patrimoine).

Le contrôle scientifique et technique (CST) porte sur les conditions de gestion, de collecte, de sélection et d'élimination ainsi que sur le traitement, le classement, la conservation et la communication des archives (article R. 212-3 du Code du patrimoine).

1.4.2 Cadre de confiance de l'administration électronique

- Règlement n°910/2014/UE du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS » ;
- Code civil, art. 1366, art. 1367 et art. 1368 ;
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée notamment par la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique ;
- Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du Code civil ;
- Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité ;
- Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

1.4.3 Cadre normatif

- Norme NF Z42-013, révisée en 2020, Archivage électronique – Recommandations et exigences ;
- Standard d'échange de données pour l'archivage (SEDA), version 2.
- ISO 3166 – codes internationaux pour les noms de pays
- ISO 639 – codes internationaux pour les langues
- ISO 15489 – principes directeurs de l'archivage
- ISO 14 641- Archivage électronique - Conception et exploitation d'un système informatique pour la conservation intégrée de documents électroniques – Spécifications.

1.5 Environnement applicatif et sources de données à prendre à compte

Ce chapitre permet d'identifier les flux de données à archiver en 2025 et en perspective des projets de collecte et d'archivage pour les années à venir.

1.5.1 Périmètre fonctionnel

Le périmètre fonctionnel se situe sur les archives intermédiaires, conservées pour leur valeur probatoire pendant un certain temps puis détruites ou versées chez l'organisme compétent.

L'archivage électronique est appréhendé de manière progressive. La mise en œuvre de ce projet sera itérative. Chaque itération correspondra à l'intégration d'un nouveau périmètre. Le socle fonctionnel du SAE devra être complet dès sa mise en œuvre.

Au regard de sa feuille de route 2025, dans un premier temps le Cerema a identifié deux périmètres :

- Périmètre administratif :
 - Archivage des pièces financières et comptables de l'ancien outil de gestion financière du Cerema (BFC de l'éditeur INETUM) ;
 - Archivage des serveurs messageries (archives des messageries des services) ;
- Périmètre technique :
 - Reprise d'arriéré :
 - Serveur Ulysse (archives des projets de la Direction Centre-Est du Cerema produites entre 2012 et 2018) ;
 - Arriéré bureautique BOX (multi chantiers) ;
 - « Données orphelines » des anciens serveurs ;
 - Portail documentaire CeremaDoc ;
 - Plateforme collaborative Expertises.Territoires.

Actuellement, le Cerema estime son besoin à environ 1,7 To pour 2025.

1.5.2 Sources de données applicatives

Le contexte logiciel au Cerema est composé d'un certain nombre d'applications métier, dont :

- Box, outil principal de gestion des documents, qui propose des règles de gestion, des métadonnées, des plans de classement, etc. Il s'agit d'un drive permettant le stockage de manière organisée, c'est sur celui-ci que sont organisés les ensembles d'archives ayant déjà été identifiés et traités au titre du pré-archivage,
- PEP d'Inetum, outil de gestion comptable, à noter qu'il n'est en place que depuis janvier 2024, il remplace BFC d'Inetum, qui n'est plus maintenu par l'éditeur (suppression à l'issue des DUA des derniers documents qu'il contient, soit 2033-2034)
- AC/D-sign, parapheur électronique développé maison, servant à signer les éléments grâce à la carte agent fournie par l'ANTS (uniquement sur certains profils), et permettant également la gestion d'étape de validation plus légère telles que des visas.
- CeremaDoc, un SIGB et un portail documentaire web tous deux basés sur le logiciel Syracuse (édité par Alfeo).

Comme le périmètre technique, la grande majorité des périmètres suivants sera versée depuis l'outil Box. Cet outil est central au Cerema. Il s'agit donc de penser une stratégie d'interopérabilité comprenant une connexion directe entre le SAE et Box.

Le système d'information du Cerema ne comprend pas d'outil de GED à proprement parler. OnlyOffice est utilisé en suite bureautique.

2 EXIGENCES FONCTIONNELLES

Les solutions Asalae et Versae déjà installées sur les environnements techniques du Cerema sont conformes aux exigences fonctionnelles décrites ci-après. Ces exigences sont en cohérence avec les exigences des normes NF Z 42-013, du SEDA et du modèle OAIS.

Le titulaire du présent marché devra être en mesure, dans le cadre de sa maintenance, d'assurer le bon respect des exigences fonctionnelles de base décrites ci-dessous.

2.1 Gestion des profils utilisateurs

Le SAE permet de définir un certain nombre d'habilitations selon le profil attaché à l'utilisateur du SAE. Un utilisateur ne peut avoir accès qu'aux actions autorisées par son profil.

Le SAE met en place les profils utilisateurs suivants :

- Administrateur technique
- Administrateur fonctionnel
- Archivistes
- Référent archives
- Service producteur
- Service versant
- Demandeur
- Autorité de contrôle (Archives départementales ou nationales).

2.2 Gestion des entrées / versements

Le processus de versement est conforme à l'étape « Transférer » du SEDA.

Le SIP prend la forme d'un message de transfert conforme au SEDA comprenant les fichiers et les métadonnées versées. Ce message comprend les informations suivantes :

- Des informations concernant le transfert lui-même (identification du service versant et du service d'archives, date d'émission du message...).
- Des informations de gestion (identification du service versant, du service d'archives, éventuellement du contrat de versement...).

- Des informations sur les archives à conserver (métadonnées techniques et métadonnées descriptives, gestion du cycle de vie...).
- Le cas échéant, les objets numériques versés.

Dans le cas d'un enrichissement de métadonnées, le SIP peut n'être constitué que d'un bordereau sans objet numérique rattaché.

Dans le cas d'un versement d'objets numériques, ces derniers sont, entre autres, des documents unitaires de formats divers, un ou des lots de documents sériels ou des documents classés dans une structure arborescente. La structure des SIP est déterminée avec les services versants.

Les versements de fichiers et métadonnées dans le SAE s'effectuent avec plusieurs modes d'entrée :

- Versement automatique avec ou sans intervention de l'archiviste.
- Versement manuel avec ou sans bordereau SEDA édité au préalable.

Le SAE est en mesure, en tout temps, d'accepter les versements de SIP provenant d'applications métier ou du service d'archives.

Le service d'archives peut verser manuellement un paquet d'archives constitué des objets numériques et du bordereau SEDA. La solution permet de simplifier la rédaction du bordereau en amont du versement en SAE.

Le SAE propose un nommage automatisé des fichiers numériques versés et attribue des identifiants uniques, non modifiables mais paramétrables par l'administrateur.

A réception du versement, le SAE émet un accusé de réception transféré au service versant par mail. Il effectue les contrôles décrits dans la partie *Contrôle du versement* (2.2.1.1.1).

Les transferts identifiés comme conformes doivent être validés. Ils peuvent l'être manuellement par les archivistes ou automatiquement par le SAE, notamment dans le cas d'un transfert via une application versante. Cette fonction est paramétrable.

2.2.1.1.1 Contrôle du versement

Les contrôles opérés par le SAE portent sur :

- La conformité des SIP (structure, informations contenues dans le SIP), à savoir :
 - Conformité de la structuration du SIP,
 - Complétude du SIP (présence des fichiers et des empreintes numériques correspondantes),
 - Présence des métadonnées obligatoires,
 - Conformité du format des métadonnées et de la valeur des métadonnées avec les règles définies,
 - Contrôle de l'unicité des métadonnées dans le SAE afin d'éviter des doublons involontaires. Le SAE possède un mécanisme de contrôle de doublons basé sur les métadonnées associées aux documents versés. Le contrôle de doublons ne bloque pas le versement, mais le notifie uniquement.
- La conformité des documents contenus dans le SIP (intégrité des documents et format des fichiers), à savoir :
 - Contrôle de l'intégrité des fichiers par comparaison de l'empreinte numérique contenue dans le SIP avec le résultat du calcul effectué par le SAE (dépôt contrôlé)
 - Contrôle de la conformité du format des fichiers avec la liste des formats d'archivage autorisés.
 - Le cas échéant, la validité de la signature électronique apposée sur le bordereau de versement.

Au regard de la politique de contrôle détaillée ci-dessus, les versements (automatiques ou manuels) non-conformes ne pouvant être traités ou n'étant pas validés par les archivistes sont rejetés par le système. En cas de non-conformité, les archivistes et le service versant seront alertés par mail. Les

archivistes autorisés peuvent modifier au coup par coup les paramètres selon leur appréciation (forcer les interdits).

Après validation automatique ou validation par l'archiviste, une attestation d'archivage certifiant que les données sont transformées en Paquet d'information archivé (AIP) est générée et transmise au service versant. Cette attestation d'archivage manifeste le transfert de responsabilité sur les archives et est conservée dans le SAE dans un format lisible, accessible et téléchargeable.

Lorsque le SIP est accepté dans l'espace de stockage du SAE, l'événement est enregistré dans le journal des événements et un identifiant unique est attribué à chaque fichier du SAE. Ce dernier assure que l'intégrité des documents est préservée lors du passage du SIP à l'AIP et que chaque objet contenu dans un SIP validé est contenu dans l'AIP. Le journal des événements est conservé dans un format lisible, accessible et téléchargeable. Les informations suivantes sont enregistrées dans le journal des événements :

- Entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal réussite ou échec de la tentative ;
- Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réunion ou échec de la tentative ; création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- Actions d'utilisateurs autorisés affectant la Sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

En cas d'anomalie, une alerte est adressée à l'administrateur fonctionnel du SAE.

Les contrôles et résultat de ces contrôles font l'objet d'un enregistrement historisé. Tout ou partie de ces contrôles, ainsi que la liste des anomalies sont exportables.

Le SAE devra fournir un tableau de bord avec les fonctionnalités d'un workflow simple pour faciliter la prise en charge des versements et la traçabilité des contrôles, ainsi que l'état des transactions en cours pour les utilisateurs.

2.2.1.1.2 Profil d'archivage

Les profils d'archivage permettent de contrôler les bordereaux de transfert SEDA en fonction d'attentes prédéfinies dans le profil.

Le service d'archives souhaite pouvoir créer des profils d'archivage et les gérer dans le SAE. La gestion des profils concerne aussi bien leur ajout, leur modification ou leur suppression. Les SIP ayant déclaré l'identifiant d'un profil d'archivage, dans leur bordereau de transfert, peuvent être contrôlés via le profil d'archivage correspondant dans le SAE.

Au minimum, les profils d'archivage devront comporter les informations suivantes :

- Identifiant du profil d'archivage.
- Objet du profil d'archivage.
- Nom du service versant.
- Niveaux de description (unités d'archives).
- Informations de description.
- Informations de gestion.
- Informations techniques.
- Informations de transfert.

Les archivistes peuvent créer, modifier, supprimer des fiches services versants sur le SAE.

2.3 Gestion des métadonnées

Les métadonnées sont de trois types :

- Métadonnées de description : les métadonnées de description sont des informations sur le contenu du document contribuant à son intelligibilité et permettant de le rechercher.
- Métadonnées de gestion : les métadonnées de gestion concernent les attributs nécessaires à la gestion du cycle de vie des archives
- Métadonnées techniques : les métadonnées techniques concernent l'identification du document, son format, sa taille, les éléments relatifs à son intégrité.

Les métadonnées respectent le standard SEDA.

Au regard des liens entre dossiers et documents, le SAE permet l'attribution automatique et manuelle des métadonnées du dossier communes à tous les documents au document entrant. Le SAE permet de déterminer le caractère obligatoire d'une métadonnée.

Au cours de leur conservation, les règles encadrant les archives peuvent être amenées à être modifiées. Le SAE doit donc permettre la modification des métadonnées de description et des métadonnées de gestion des archives.

Ces modifications ne peuvent être effectuées que par un utilisateur habilité, via un formulaire de saisie/modification des métadonnées paramétrables. Elles peuvent être faites sans notification au service producteur/versant.

Elles sont enregistrées dans le journal de cycle de vie des archives. Ce dernier permet notamment de consigner :

- La nature de la modification.
- La valeur d'origine.
- La date de la modification.
- L'auteur de la modification.
- L'empreinte des archives concernées.
- L'identifiant des archives concernées.

Plusieurs types de champ peuvent être prévus par le titulaire (champ simple, complexe, texte, numérique, liste déroulante, dates, cases à cocher, etc.) selon les besoins du Cerema. Cette liste n'est pas exhaustive.

Le SAE permet de déterminer si une métadonnée est obligatoire, et doit donner la possibilité d'effectuer un contrôle de validité des métadonnées.

Le SAE propose la gestion et la conservation des métadonnées descriptives :

- Possibilité d'intégrer des profils conformes aux schémas SEDA générés au format XML ou XSD :
 - Profil généré dans un autre outil que le SAE
 - Profil généré depuis la solution et possibilité d'accéder au fichier ainsi généré.
- Un même profil de données peut être utilisé pour plusieurs services producteurs ;
- Possibilité par les personnes habilitées de modifier les métadonnées de gestion et les métadonnées de description. Ces modifications sont enregistrées dans le journal de cycle de vie des archives.

Le format des métadonnées est indépendant du format d'échange des SIP (SEDA).

Le SAE permet de gérer des thésaurus et listes d'autorités pour l'indexation des archives.

2.4 Pérennisation

2.4.1 Contrôle d'intégrité et d'exhaustivité

La garantie d'intégrité des archives est notamment assurée par des mécanismes de contrôle basés sur le calcul d'empreinte et sur l'exhaustivité des fonds.

Les contrôles s'appliquent aux transferts, aux archives stockées, aux communications et aux restitutions. Le service d'archives du Cerema a souhaité qu'ils soient déclenchés de manière automatique selon un cycle prédéfini, ou manuellement via l'intervention d'un utilisateur agréé.

Les résultats des contrôles sont comparés avec les données enregistrées dans le journal du cycle de vie des archives au moment de l'entrée des SIP dans le SAE. En cas d'altération, un processus de restauration est mis en œuvre.

Le SAE s'assure de l'exhaustivité des fonds conservés et organise des contrôles quotidiens pour vérifier qu'aucun fichier n'est manquant.

Ces contrôles prennent en compte les transferts, les archives stockées, les communications et les restitutions.

Le SAE met en œuvre un mécanisme de contrôle permanent d'intégrité des documents, des fichiers et des journaux par échantillonnage.

Ce contrôle de l'intégrité des documents et dossiers s'effectue par comparaison du résultat du calcul de l'empreinte numérique actuelle du fichier par rapport à l'empreinte enregistrée dans le journal du cycle de vie des archives au moment de l'entrée du document dans le SAE.

Ce type de contrôle est opéré de manière régulière et cadencée (système d'alerte, responsable du traitement, tableau de bord etc.) pour les contrôles réalisés automatiquement. En cas d'anomalie, une alerte est adressée à l'administrateur fonctionnel du SAE par mail.

2.4.2 Migration de formats et d'environnement de stockage

Le Cerema dispose d'une importante variété de formats liés à son activité (production de scripts / SIG / bases de données sur plein de formats / fichiers sources / données sources de drones / vidéos / images / foncier / etc.). Le SAE a la capacité d'accueillir tous types de format et au besoin de répondre à une politique de conversion au sein du SAE.

Les changements de technologie peuvent être une menace pour la lisibilité des fichiers numériques. Le SAE assure cette lisibilité dans le temps en permettant au service des archives du Cerema de réaliser la migration en masse de fichiers depuis un format accepté en entrée mais non pérenne vers un format considéré comme pérenne. Cette migration doit être réalisée selon une politique de conversion, sans interruption de service.

Le SAE conserve la version convertie du fichier, comme indiqué dans la politique de formats.

Les succès ou échecs de conversion de format sont notifiés aux administrateurs fonctionnels. Les modalités de traitements des anomalies et de conversion sont explicités par l'éditeur dans sa proposition.

Les formats de conversion pris en charge par le SAE évoluent en fonction des mises à jour dans l'environnement professionnel, notamment pour les formats de conservation.

L'implémentation de nouveaux formats dans le SAE fait toujours l'objet d'une notification et d'une validation préalable par le service des archives du Cerema.

Les migrations sont tracées dans le journal des événements du SAE.

2.4.3 Journal du cycle de vie des archives

Pour chaque événement enregistré, les informations suivantes sont stockées :

- Action (type d'événement).
- Date de fin d'action.
- Auteur à l'origine de l'action.
- Identifiant de l'unité de gestion concernée par l'action.
- Résultat de l'action.

- Commentaire sur le résultat.
- Empreinte de l'unité de gestion en sortie de résultat.
- Contextualisation de l'action avec l'identifiant de la règle qui autorise la réalisation de l'action

Au minimum, les événements suivants sont enregistrés dans le journal du cycle de vie des archives :

- Modalités d'entrée.
- Migration de format.
- Élimination.
- Modification des métadonnées.
- Restitution.
- Restauration (traçage des opérations de correction à la suite de la détection d'une anomalie).

Ces informations sont aussi enregistrées automatiquement dans les métadonnées de gestion des documents.

Chaque enregistrement dans le journal du cycle de vie des archives est daté selon un mécanisme fiable. En cas d'usage d'une horloge interne au SAE, celle-ci doit être synchronisée par une autorité de temps agréée selon un protocole normé.

L'intégrité du journal du cycle de vie des archives est assurée par une empreinte numérique ainsi qu'une marque de temps fiable. Les journaux sont chaînés entre eux.

Les journaux sont conservés dans les mêmes conditions que les archives auxquelles ils se rapportent.

Le SAE inclut des fonctions qui permettent aux utilisateurs habilités de rechercher dans l'historique la trace d'événements particuliers, d'objets (séries, documents, etc.), d'utilisateurs, groupes ou profils, de dates ou de périodes.

2.4.4 Journal des évènements

Le SAE génère des journaux d'événements à des fins de contrôle interne. Il consigne les traces de connexion au système par un utilisateur ou un système automatique. Ils indiquent :

- Les dates et heures de l'opération conformément à la norme ISO 8601.
- La nature de l'opération effectuée.
- L'identification du système technique qui a été utilisé.
- Le nom du processus en cause et l'indication de sa version.
- L'identification de l'opérateur.
- Les tentatives d'intrusion dans le système.



2.5 Gestion des consultations / communications

2.5.1 Rechercher et consulter les archives

Le SAE permet la recherche dans les archives et dans tout ou partie des métadonnées qui leur sont associées, en fonction du profil du demandeur et de ses droits. Seuls les résultats autorisés par l'habilitation de l'utilisateur sont affichés dans les résultats de recherche.

A l'issue de la recherche, l'utilisateur pourra consulter l'archive trouvée.

Le Cerema a estimé que la présence d'un plan de classement n'est pas un critère essentiel pour le SAE. Au regard de la non-exigence du plan de classement, le module de recherche est poussé, pertinent et largement paramétrable.

L'interface de recherche et de consultation permet au demandeur de choisir différentes combinaisons de métadonnées comme critères de recherche, par exemple une recherche des documents par leur référence et/ou par les informations descriptives. Le SAE propose de gérer des thésaurus et listes d'autorités pour l'indexation contrôlée des archives.

Le SAE permet d'effectuer plusieurs types de recherche (plein texte, requêtes simples, combinées, opérateurs booléens, opérateurs de comparaison, troncature, équivalence majuscule/minuscule, ignorance des accents, exclusion des mots vides, etc.).

De manière générale, les archivistes souhaitent une interface paramétrable selon les résultats de recherche (liste courte puis liste détaillée, type d'affichage, nombre maximal de réponse, par exemple) et adaptée selon les profils de recherche.

La liste des résultats de recherche doit pouvoir être organisée et faire l'objet de tris par :

- La sélection de l'ordre de présentation des résultats ;
- Le paramétrage du nombre de réponses affichées sur chaque page de l'écran ;
- Le choix des métadonnées à afficher dans la liste des résultats.

Deux modes d'affichage des réponses ont été souhaités (simple et détaillé), l'idéal étant de pouvoir naviguer facilement entre les deux affichages.

Le SAE permet d'avoir accès à l'historique des recherches fréquentes (en tant qu'utilisateur) ainsi qu'un accès aux résultats de requêtes sauvegardées (via un panier par exemple), d'envoyer par mail un ensemble de résultats et/ou de pouvoir exporter une liste de résultat au format CSV.

2.5.2 Communiquer des archives

La communication concerne tant les archives elles-mêmes que leurs métadonnées. Le SAE permet également la communication des éléments de traçabilité pour les utilisateurs habilités.

La communication des archives et de leurs métadonnées se fait conformément aux étapes de la séquence « Communiquer » du SEDA.

A partir d'une sélection de résultats et en fonction de ses droits, l'utilisateur demande l'accès aux archives. Le service producteur a accès à ses propres archives.

La demande fait l'objet d'un contrôle et d'une validation par le service des archives, ou par le correspondant archives. La demande de consultation est envoyée au service d'archives ou au correspondant archives qui accuse réception de la demande et la traite. Dans le cas où des données ne sont pas librement communicables, des autorisations du service producteur et du service des archives peuvent être demandées. La gestion de ces autorisations est conforme aux transactions « Demande d'autorisation » du SEDA. Le processus de validation de la commande est paramétrable.

La gestion de la communicabilité des fichiers est une composante indispensable du SAE. La communicabilité des fichiers peut être modifiée par le service d'archives. Ce dernier peut aussi visualiser les demandes en cours et leur état d'avancement. La communicabilité est paramétrable dans les métadonnées de gestion.

Lors de la communication d'un fichier, le SAE constitue des Paquets d'information à diffuser (DIP) et les mets à disposition du demandeur. Les DIP produits par le SAE sont une copie de consultation des fichiers demandés. Les fichiers originaux ne sont pas communiqués aux demandeurs.

Un contrôle d'intégrité est effectué sur les documents restitués grâce à un processus de restitution.

2.6 Gestion des éliminations

Le SAE permet de gérer le cycle de vie des archives conformément à la durée de conservation et au sort final enregistrés dans les métadonnées attachées aux documents.

Le processus d'élimination doit être conforme aux étapes de la séquence « Éliminer » du SEDA.

Le SAE permet aux archivistes de visualiser la liste des documents qui ont atteint l'échéance de leur durée de conservation réglementaire (sous forme de filtrage et d'une fonctionnalité dédiée aux archives éliminables). L'opération de destruction ne s'applique qu'aux documents dont la durée est échue et dont

l'élimination n'a pas été gelée. Les éliminations peuvent porter sur les documents eux-mêmes et/ou leurs métadonnées.

Le SAE permet de sélectionner les archives électroniques à éliminer. Il propose des fonctionnalités de tri par service producteur et date d'élimination.

Si le service versant refuse l'élimination des données, le SAE permet la modification de la durée de conservation des données et de leur sort final, de geler l'ordre de destruction ou de restituer les données.

A l'issue de l'exercice du contrôle scientifique et technique de l'État sur les archives publiques, les objets numériques éliminés peuvent être effacés du système de manière à ce qu'aucune restitution des données ne soit possible.

Après élimination, le SAE fournit une attestation d'élimination téléchargeable et disponible.

2.7 Gel de l'élimination

Le SAE permet aux archivistes de geler l'élimination d'un document, qui est une fonction bloquant l'élimination du document à la fin de sa durée de conservation réglementaire. Le gel peut être suspendu manuellement par le service commun d'archives à tout moment. Une métadonnée enregistre le motif de ce gel, et ce afin d'assurer une meilleure traçabilité de l'action.

Le SAE permet d'inventorier les documents gelés et de désactiver le gel sur tout ou partie des documents inventoriés.

2.8 Traçabilité

Le SAE met en œuvre un ensemble de fonctions de traçabilité pour conserver l'historique des actions concernant son exploitation, son utilisation, des incidents survenus (sécurité, problème lors de l'import de versement, fichier corrompu), ainsi que l'ensemble des actions réalisées sur les archives.

Pour chaque événement enregistré, les informations suivantes seront stockées :

- Date,
- Nature de l'évènement,
- Auteur à l'origine de l'action,
- Identifiant de l'unité de gestion concernée par l'action,
- Résultat de l'action (restitution, effacement, gel, versement, etc.)
- Empreinte de l'unité de gestion en sortie de résultat,
- Commentaire sur le résultat,
- Contextualisation de l'action avec l'identifiant de la règle qui autorise la réalisation de l'action.

Les fonctions de traçabilité prennent plusieurs formes :

- Enregistrement et stockage des événements relatifs à l'exploitation du SAE et son utilisation dans une base de données et/ou dans des fichiers logs,
- Enregistrement et stockage des événements relatifs au cycle de vie des archives dans un journal du cycle de vie des archives.

Cette liste non exhaustive, peut être complétée au regard des choix du Cerema.

Les événements suivants considérés comme significatifs sont enregistrés dans le journal du cycle de vie des archives :

- Modalités d'entrée,
- Migration de format,
- Élimination,
- Modification des métadonnées,
- Restitution.

Ces informations sont aussi enregistrées dans les métadonnées des documents.

Chaque enregistrement dans le journal du cycle de vie des archives est daté selon un mécanisme fiable. En cas d'usage d'une horloge interne au SAE, celle-ci doit être synchronisée par une autorité de temps agréée selon un protocole normé.

L'intégrité du journal du cycle de vie des archives est assurée par une empreinte numérique ainsi qu'une marque de temps fiable qualifiés au sens eIDAS ou RGS. Les journaux sont chaînés entre eux.

Les journaux sont conservés dans les mêmes conditions que les archives auxquelles ils se rapportent.

Le SAE inclut des fonctions qui permettent aux utilisateurs habilités de rechercher dans l'historique la trace d'événements particuliers, d'objets (séries, documents, etc.), d'utilisateurs, groupes ou profils, de dates ou périodes et qui permettent d'établir des indicateurs de suivi statistiques (directement ou indirectement).

2.8.1 Traçabilité des entrées et contrôles

Le SAE est en mesure d'enregistrer les informations relatives aux entrées, aux contrôles et aux résultats des contrôles de SIP dans le journal de cycle de vie des archives. Ces informations sont liées aux transferts et conservées dans le SAE au même titre que les SIP qu'elles concernent. Au minimum, les informations suivantes devront être spécifiées :

- Référence du versement.
- Identité de l'utilisateur à l'origine du versement.
- Horodatage de la prise en charge du versement.
- Résultats des contrôles en entrée.
- Le cas échéant, détection d'anomalie à la suite d'un contrôle.
- Le cas échéant, nature de l'anomalie détectée.
- Empreintes numériques des fichiers contenus dans le SIP.
- Validation ou rejet du versement.
- Horodatage de la validation ou du rejet du versement.
- Identité de l'utilisateur qui a validé la prise en charge du versement.
- Horodatage de l'entrée du versement dans le système.

2.8.2 Traçabilité des communications

Le SAE enregistre et stocke les informations suivantes :

- Référence de l'unité documentaire communiquée.
- Date de la communication.
- En cas de dérogation, référence et date de l'autorisation.
- Identité du demandeur
- En cas de refus de la demande de communication.

2.8.3 Traçabilité des éliminations et gels

Le SAE enregistre et stocke les informations suivantes dans le journal du cycle de vie des archives :

- Référence de l'unité de gestion éliminée.
- Date de l'élimination.
- Référence de l'autorisation du Service producteur.
- Date de l'autorisation du Service producteur.
- Date de déclenchement ou de suspension du gel.
- Identité de l'utilisateur ayant gelé l'élimination.
- Motif du gel de l'élimination.
- Date du visa de la personne en charge du contrôle scientifique et technique.
- Référence du bordereau d'élimination des données.
- Référence de l'attestation de destruction des données.

2.9 Administration fonctionnelle

Le SAE en production propose une administration fonctionnelle permettant à l'archiviste de remplir de façon satisfaisante ses missions. Le SAE peut être supervisé au quotidien bien que les missions des archivistes du Cerema ne soient pas uniquement dédiées aux archives électroniques. Les archivistes du Cerema considèrent que le SAE doit être un outil de facilitation de leur mission.

Grâce au SAE, l'administrateur fonctionnel exerce son rôle et :

- Est le représentant du service des archives dans la gestion opérationnelle du SAE ;
- Assure le lien avec la DSI en instruisant les points qui nécessitent son intervention ;
- Assiste les utilisateurs dans leurs opérations de versement et de recherche ;
- Propose des évolutions fonctionnelles ;
- Suit et valide les évolutions ;
- Fait les recettes fonctionnelles ;
- Vérifie les flux documentaires ;
- Administre les données de référence (les mettre à jour, contrôler leur qualité) ;
- Contrôle la sécurité des données avec un plan d'assurance sécurité ;
- Coordonne et met en place les reprises de données ;
- Garanti le niveau de service et le faire évoluer ;
- Gère les statistiques et le reporting ;
- Organise et pilote les opérations de migration ;
- Participe aux projets de versement en apportant son expertise technique.

Pour cela, le SAE propose les fonctions paramétrables suivantes :

- Création et gestion des services producteurs ;
- Création et gestion des utilisateurs et rôles utilisateurs associés ;
- Création et gestion des circuits de validation ;
- Création et gestion des profils d'archives ;
- Création et gestion des accords de versement ;
- Création et gestion des mots-clés ;
- Création et gestion des niveaux de service ;
- Création et gestion de la durée de communicabilité des archives ;
- Création et gestion de la durée d'utilité administrative des archives ;
- Configuration du SAE.

2.10 Formation fonctionnelle

Pour garantir les exigences fonctionnelles ci-dessus, les archivistes du Cerema demanderont au titulaire de bénéficier d'une formation fonctionnelle à l'utilisation du système d'archivage électronique Asalae et de son module de versement Versae. Cette formation devra être réalisée lors de la première année du marché en présentiel sur le site de Lyon-Charial à destination de deux à quatre agents.

En cas de modification des équipes fonctionnelles ou techniques du Cerema, des prestations de formations complémentaires pourront être commandées pour assurer le niveau de fonctionnement du système d'archivage électronique du Cerema.

3 EXIGENCES TECHNIQUES

3.1 Hébergement de la solution

Le Cerema a fait le choix de se tourner vers une solution « On-Premise », c'est-à-dire installée dans son propre environnement.

L'installation comporte 2 environnements différents :

- Un environnement de qualification (QUAL) permettant de réaliser entre autres, les tests d'intégration, les connexions avec les outils tiers, les tests relatifs aux paramétrages de l'outil, les tests de performances, etc.
- Un environnement de production (PROD) ;

Sur chaque environnement, la configuration est la suivante :

- Une VM Asalae
- Une VM Versae

La solution et les données seront hébergées sur le cloud nutanix dans le respect de la norme NFZ 42-013 : une copie de la production est effectuée sur une autre machine virtuelle, et une sauvegarde physique stockée dans les locaux physiques du Cerema.

La copie en mode miroir d'Asalae sur une autre machine virtuelle est actuellement réalisée via une instance dite « PRA » (plan reprise d'activité). Dans le cadre du projet, ce PRA est branché sur l'instance Asalae QUAL, et devra faire l'objet dans le cadre du marché d'une reconfiguration vers Asalae PROD.

La solution est exploitée par la DSI du Cerema.

Le titulaire devra fournir un **schéma d'architecture technique et applicative** de la solution, incluant les composants Asalae et Versae, les environnements (QUAL, PROD, PRA), la topologie réseau, les modalités de connexion avec les outils tiers (ex : Box, SSO Orion, API RH), ainsi que les mécanismes de réplication et de sauvegarde.

Le schéma devra préciser la **zone de déploiement réseau** (DMZ, LAN interne, etc.) et les **protocoles utilisés** (https, sftp...). La description devra inclure les flux d'échange, les points de supervision, les modalités de journalisation technique et les mécanismes de sécurisation associés.

3.2 Prérequis techniques minimaux

La solution ainsi que le module de backoffice doivent être en mode full Web.

Pour le développement, le Cerema note une préférence pour le langage JAVA.

Au lancement du marché, une prise en charge sera réalisée par le titulaire du marché. Le Cerema transmettra l'ensemble des pièces techniques et fonctionnelles permettra la bonne compréhension du SAE dans le contexte de production du Cerema. Les livrables attendus associés à cette prise en charge sont : mise à jour des documents techniques (exemples : document d'architecture technique, document d'installation, document d'exploitation) ; réalisation d'un plan de réversibilité.

3.3 Accès à la solution

L'accès au SAE sera assuré via les infrastructures réseaux existantes (utilisation d'un pare-feu F5, avec connexion en interne et en externe) qui devront être prises en compte pour définir l'architecture technique puis déployer la solution dans l'environnement informatique.

Le SAE sera ouvert dans un premier temps uniquement en interne ainsi qu'aux CST, l'accès aux interfaces utilisateurs sera uniquement possible par les services du Cerema et par les CST.

Le SAE doit pouvoir s'interfacer avec le SSO Orion du Cerema, de type open IDConnect.

3.4 Gestion des droits

Actuellement, le Cerema ajoute manuellement les nouveaux utilisateurs du SAE. Dans le cadre de ce marché, le Cerema souhaiterait une importation « en masse » des agents du Cerema afin de faciliter le traitement, et donc récupérer les informations nécessaires pour le SAE (nom, prénom, adresse mail et place dans l'organigramme).

Cette importation doit être réalisée de manière récurrente (a minima deux fois par an). Les archivistes devront rester en mesure d'ajuster manuellement les droits et rajouter des utilisateurs au besoin.

La liste exhaustive des agents du Cerema à date est disponible par un webservice. Ces données sont récupérable via l'appel d'une API REST ou l'export d'un fichier type .csv . L'API REST pioche les information dans une base de donnée POSTGRESQL.

3.5 Volumétrie

Dans la perspective du déploiement du SAE, le Cerema a conscience de l'augmentation progressive des volumes de données auxquelles la solution sera confrontée dans les années à venir. Les projections de volumétrie doivent tenir compte de l'adhésion progressive de nouvelles directions à la dématérialisation de leurs périmètres.

À titre prévisionnel, le SAE devra être en mesure d'absorber une **volumétrie cumulée de 15 To et 10 millions d'objets numériques** à horizon 2028, en tenant compte de l'élargissement progressif des périmètres métiers et de la généralisation de la dématérialisation.

Le système devra garantir des **temps de réponse inférieurs à 3 secondes pour des recherches courantes** et permettre la montée en charge sans interruption de service.

Le titulaire devra fournir, dans les 6 mois suivant la mise en production, **un rapport de tests de performance et de charge** réalisés sur l'environnement de qualification.

3.6 Réversibilité, transférabilité des données

La réversibilité doit permettre de restituer l'intégralité de la base de données sans altération ainsi que tous les documents numériques conservés en garantissant pour chaque objet numérique : sa lisibilité, son intégrité, sa traçabilité et son authenticité.

Le titulaire s'engage à réaliser toutes les actions permettant au Cerema d'assurer la continuité de service. Cette continuité de service doit expressément être transparente pour les utilisateurs et n'occasionner aucune perte de données.

Dans le cas d'un changement de la solution d'archivage électronique, le titulaire décrira avec précision le scénario de réversibilité mis en œuvre au sein du produit : format de restitution des archives, modalités de mise à disposition, modalités de destruction des fichiers après transfert dans le SAE tiers, sous la forme d'un Plan de Réversibilité.

Le processus de réversibilité doit être conforme à la séquence « Restitution » du Standard d'Échange de Données pour l'Archivage (SEDA).

Le titulaire s'engage à fournir l'intégralité des données archivées et documents numériques dans le SAE, les paramétrages et autres informations ou fichiers dont le Cerema reste propriétaire, ainsi que toute documentation décrivant les éléments extraits :

- Documentation d'export et prérequis,
- Données électroniques archivées, éléments associés dans l'état où ils se trouvaient lors de la réception dans le SAE, journaux,
- Cahier de descriptif des tous les paramétrages techniques et fonctionnels réalisés dans la solution avec les durées et règles de rétention définies au cours du projet.

En outre, le titulaire s'engage également :

- Au transfert sécurisé auprès du Cerema ou de tout autre organisme mandaté par lui, des connaissances, données, documents et journaux nécessaires à la poursuite du service ;
- à assurer une période de recouvrement incluant une phase d'accompagnement et de tutorat du nouveau titulaire, et une phase de conservation des supports pendant une période permettant de garantir que le service commun d'archives n'ait pas de perte de qualité de service.
- À restituer toutes les informations (archives, journaux d'évènements, journaux d'archives, ...) sous forme de documents ou de données appartenant au Cerema dans des formats exploitables, lisibles et avec la description des données (Modèle Physique des Données).
- A l'issue de cette période de 6 mois, le titulaire s'engage à ne pas conserver d'exemplaires de jeu de données, informations ou de documents du Cerema qui auraient été présents dans le SAE.

La mise en place de la réversibilité se réalisera en mode projet avec un planning défini par le Cerema en lien avec les nouveaux intervenants. Elle devra au plus tard être réalisée 6 mois avant la fin du marché.

La prestation de réversibilité pourra être déclenchée par l'acheteur via l'émission d'un bon de commande et ce dans les délais mentionnés sur le bon de commande.

3.7 Principe d'écoresponsabilité

De préférence, le titulaire devra mettre en œuvre tous les moyens dont il dispose pour respecter ses objectifs de développement durable dans le cadre de l'exécution des prestations.

Le titulaire indiquera, en lien avec le principe d'écoresponsabilité, les **optimisations techniques mises en œuvre pour limiter la consommation des ressources (CPU, stockage, réseau)**, ainsi que toute mesure de rationalisation liée à la gestion du cycle de vie des données.

La mise en veille automatique des services inactifs, la limitation du nombre de traitements planifiés, ou encore la compression intelligente des données archivées pourront être proposées.

3.8 Supervision

La supervision de la solution et les méthodes de sauvegarde seront assurées, par les moyens existants au sein de la DSI du Cerema. Ils pourront le cas échéant être complétés par les outils proposés par le titulaire.

Pour information, le Cerema suit la charge CPU / RAM et l'espace disque disponible via l'outil de supervision **Zabbix**.

Actuellement, le profil d'administrateur technique du SAE permet de suivre les indicateurs suivants :

- Load average 1 min
- Load average 5 min
- Load average 15 min
- RAM
- SWAP
- L'état du système (serveurs, modules, volumes, tables, etc.)

Le titulaire proposera une **liste d'indicateurs techniques supplémentaires et suivis en temps réel**, incluant notamment :

- Taux d'échec des versements
- Nombre de requêtes par utilisateur
- Statuts des processus clés (accès, versement, consultation, suppression)

Cette liste d'indicateur devra être accessible à l'équipe technique via des **exports au format JSON, XML ou CSV** et via une interface de visualisation simple (ou API).

3.9 Performance et évolutivité

L'architecture technique mise en œuvre doit permettre de s'assurer d'un taux de disponibilité d'au moins 98 %. Cet indicateur sera suivi lors du bilan annuel de suivi de projet.

L'architecture mise en œuvre devra permettre l'**élasticité de la plateforme**, afin de s'adapter à l'évolution des volumes et des usages.

La solution devra supporter **au moins 100 connexions simultanées**, sans dégradation notable de performance.

Le titulaire détaillera dans son offre les **points de paramétrage ou de redimensionnement** possibles (RAM, CPU, indexation, cache, etc.) pour garantir la qualité de service.

3.10 Journalisation technique et interopérabilité

La solution doit générer des **journaux techniques complets** (logs applicatifs et systèmes) permettant de :

- retracer les événements système (accès, erreurs, processus),
- auditer les performances et les interactions inter-applicatives,
- détecter les anomalies ou intrusions (couplage avec outils SIEM si besoin).

Les journaux devront être conservés **au minimum 12 mois** et **être exportables dans un format ouvert** (CSV, JSON, syslog).

En complément, le SAE devra respecter les **standards d'interopérabilité** définis dans le **Référentiel Général d'Interopérabilité (RGI)**. Il devra s'appuyer sur des **protocoles et formats ouverts** (API REST, JSON, XML/SEDA) pour assurer une communication fluide avec les autres composants du SI du Cerema.

3.11 Montée de version Asalae 3.0

Le Cerema dispose actuellement d'une installation de la version 2.0 d'Asalae. Le titulaire devra assurer la **montée de version vers Asalae 3.0** sur tous les environnements (QUAL, PROD, PRA), avec :

- Reprise des paramétrages existants ;
- Préparation et validation des tests de non-régression ;
- Vérification post-migration de la conformité réglementaire.

4 EXIGENCES DE SÉCURITÉ

4.1 Gouvernance de la sécurité

Le titulaire s'engage à respecter l'ensemble des exigences en matière de sécurité de l'information, notamment :

- Le **Référentiel Général de Sécurité (RGS)**,
- La **Politique de Sécurité des Systèmes d'Information (PSSI)** de l'État,
- Le **RGPD** et la législation en vigueur sur la protection des données à caractère personnel,
- Les **recommandations de l'ANSSI** (guide d'hygiène informatique, bonnes pratiques de développement, etc.).

Un **Plan de Sécurité du Système (PSS)** devra être fourni en phase initiale du marché. Il décrira les principes de sécurité mis en œuvre (authentification, cloisonnement, journalisation, chiffrement des flux, gestion des incidents...).

4.2 Protection des accès

Le SAE devra s'interfacer avec le **SSO Orion** du Cerema via le protocole OpenID Connect. Le titulaire devra garantir :

- La gestion des comptes avec **séparation des privilèges** (administrateur technique, administrateur fonctionnel, utilisateurs métiers, etc.) ;
- L'interdiction des comptes non tracés ou en accès direct aux bases ;
- L'absence de mots de passe codés en dur dans les scripts ou fichiers de configuration ;
- Un mécanisme de **gestion centralisée des comptes** à partir d'un annuaire du Cerema ;
- Une journalisation de toutes les opérations d'authentification et de tentative d'accès.

4.3 Sécurité applicative

Le titulaire appliquera les bonnes pratiques suivantes :

- Intégration des recommandations de l'**OWASP Top 10** (2023) ;
- Revue de code de sécurité et vérification des dépendances ;
- Scan de vulnérabilités avant mise en production : les composants contenant des failles critiques (CVSS ≥ 7) doivent être corrigés avant livraison ;
- Utilisation d'un **framework de développement sécurisé** si des développements spécifiques sont réalisés ;
- Respect du **principe du moindre privilège** pour tous les composants logiciels.

Le titulaire devra fournir, pour chaque version livrée, une fiche de conformité sécurité précisant :

- Les versions applicatives utilisées,
- Les failles résiduelles connues,
- Les résultats des tests automatisés ou manuels réalisés.

4.4 Journalisation et détection

Les exigences de journalisation décrites au §3.10 sont complétées par les éléments suivants :

- Le SAE devra permettre l'**intégration de ses journaux** dans un système de supervision centralisée ou de type SIEM (ex : Graylog, Splunk, Elasticsearch) ;
- Le système devra **générer des alertes automatiques** en cas d'événements critiques (accès non autorisé, échec répété, dépassement de quota, altération d'intégrité) ;
- Tous les journaux doivent être **horodatés de manière fiable** (synchronisation avec une autorité de temps) ;
- Les journaux doivent être **conservés 12 mois minimum**, dans un format lisible et interopérable (CSV, JSON, syslog, etc.).

4.5 Maintien en condition de sécurité (MCS)

Le titulaire devra :

- Appliquer les **correctifs de sécurité** dans des délais compatibles avec le niveau de criticité :
 - Critique : < 3 jours ouvrés,
 - Majeure : < 5 jours ouvrés ;
- Proposer des **mesures compensatoires** si un correctif ne peut être appliqué immédiatement (ex : filtrage, désactivation temporaire, journalisation renforcée) ;
- Garantir la traçabilité de tous les correctifs applicables sur les composants serveurs et logiciels du SAE ;
- Mettre à jour un **plan de maintien en condition de sécurité**, validé par la DSI du Cerema ;
- Informer le Cerema en amont de toute opération sur l'environnement de production.

Une **revue annuelle de sécurité** sera organisée à l'initiative du Cerema ou du titulaire.

4.6 Protection des données à caractère personnel (RGPD)

Le titulaire s'engage à respecter le **Règlement général sur la protection des données (RGPD)** (UE 2016/679) ainsi que la **loi n°78-17 du 6 janvier 1978 modifiée**.

Responsabilités

- Le **Cerema**, en tant que responsable de traitement, définit les finalités et les moyens des traitements mis en œuvre dans le SAE.
- Le **titulaire**, agissant comme sous-traitant, ne peut agir que sur **instruction documentée** du Cerema.

Engagements du titulaire

Le titulaire s'engage à :

- Mettre en œuvre les **mesures de sécurité organisationnelles et techniques** appropriées (article 32 RGPD) ;
- Garantir la **confidentialité, l'intégrité, la traçabilité** et la **disponibilité** des données à caractère personnel ;
- Coopérer avec le Cerema en cas d'exercice des **droits des personnes** concernées (accès, rectification, opposition, etc.) ;
- Alerter **sans délai** en cas de **violation de données** ou de suspicion de faille de sécurité ;
- Ne pas sous-traiter tout ou partie du traitement **sans accord préalable écrit** du Cerema ;
- **Restituer ou détruire** les données à la fin du marché, conformément aux instructions du Cerema, avec **attestation écrite** à l'appui.

Documentation et audit

Le titulaire devra :

- Tenir un **registre des traitements sous-traités** dans le cadre du SAE ;
- Fournir un **plan de conformité RGPD** dans son offre, incluant notamment l'analyse d'impact si nécessaire, les mesures de minimisation, pseudonymisation, contrôle d'accès, etc. ;
- Accepter toute **demande d'audit RGPD** par le Cerema ou une autorité compétente.

5 CONDITIONS DE RÉALISATION DU MARCHÉ

5.1 Gouvernance du projet

Le titulaire désignera un chef de projet référent, interlocuteur unique du Cerema, accompagné d'un suppléant. Le Cerema mobilisera un chef de projet côté maîtrise d'ouvrage, et un interlocuteur technique désigné par la DSI.

Un **comité de suivi du marché** sera mis en place dès la phase de démarrage. Il se réunira en distanciel deux fois par an. Le comité assurera le suivi de l'avancement, la validation des livrables, et le traitement des écarts ou incidents. Le titulaire se chargera de livrer un compte rendu après chaque réunion dans un délai de 10 jours.

5.2 Organisation et phasage

Le déroulement du projet suit les jalons détaillés dans le **plan projet cible** (cf. annexe 1). Il est structuré en trois grandes phases :

- **Phase de lancement et reprise** : cadrage, vérification de l'environnement, préparation à la montée de version Asalae 3.0 le cas échéant ;
- **Phase d'industrialisation** : mise en production du dispositif cible, documentation, sécurisation, mise à jour des procédures et interface avec les autres SI ;

- **Phase de stabilisation et maintien en condition opérationnelle** : accompagnement au changement, mise en place de la supervision, traitements des ajustements.

5.3 Livrables attendus

Le titulaire produira les livrables suivants, selon le calendrier défini dans le plan projet :

- Plan de sécurité du système (PSS) ;
- Documentation d'architecture cible et plan de migration ;
- Dossier de tests et PV de recette ;
- Guide d'administration et manuel utilisateur ;
- Plan de conformité RGPD et fiches de conformité sécurité ;
- Rapport de fin de déploiement et plan de réversibilité.

Chaque livrable sera validé formellement par le Cerema dans un délai de 15 jours ouvrés après remise. En l'absence de réponse, le livrable est réputé refusé. En cas de refus motivé, le titulaire proposera une nouvelle version dans les 10 jours.

5.4 Suivi de la qualité et des engagements

Le titulaire s'engage à respecter les engagements en matière de qualité, de sécurité, de documentation et de continuité de service. En cas de manquement :

- Des plans d'actions correctifs seront définis en comité de suivi ;

Le titulaire tiendra un tableau de bord d'avancement et de suivi des incidents/mises à jour techniques, mis à disposition du Cerema.

5.5 Réversibilité

Le titulaire s'engage à permettre la reprise des données, de la documentation et de la configuration à l'issue du marché, selon un **plan de réversibilité** à définir en phase de cadrage.

Ce plan devra prévoir :

- L'export complet des données et des journaux ;
- La livraison de l'ensemble des livrables contractuels à jour ;
- La transmission des droits d'accès et comptes techniques documentés ;
- Un accompagnement technique à la réinstallation ou reprise si nécessaire.

Le titulaire s'engage à assurer une transition sans interruption de service ni perte de données.

5.6 Délais de maintenance et de correction

Le titulaire s'engage à respecter les niveaux de service suivants pour la prise en charge des demandes et des anomalies :

Niveau d'anomalie	Description	Délai de prise en charge	Délai de correction
Bloquante	Interruption totale du service ou de toute fonctionnalité critique	4 heures ouvrées	1 jour ouvré
Majeure	Fonctionnalité essentielle partiellement altérée, contournement possible	1 jour ouvré	5 jours ouvrés
Mineure	Dysfonctionnement n'affectant pas l'usage essentiel du service	2 jours ouvrés	10 jours ouvrés

Les délais s'entendent à compter de la **déclaration validée** de l'anomalie par le Cerema via le dispositif de ticketing mis en place.

5.7 Traitement des incidents et support

Le titulaire devra proposer un **dispositif de support** comprenant :

- Une interface de **déclaration des incidents** (outil de ticketing ou autre canal validé) accessible par le Cerema ;
- Un **journal de suivi des incidents** mis à jour et consultable ;
- Un **interlocuteur support dédié** pendant les jours et heures ouvrés (9h-17h, du lundi au vendredi hors jours fériés).

6 ANNEXE 1 : PLAN PROJET CIBLE

6.1 Phase 0 : Préparation et prise en charge (mois M0 – M1)

Objectifs

- S'assurer de la compréhension du contexte technique et fonctionnel.
- Réaliser la reprise de connaissances et documenter l'existant.

Actions principales

- Lancement du projet (réunion de cadrage).
- Audit de l'installation actuelle (Asalae 2.0 / Versae).
- Réception et analyse de la documentation technique et fonctionnelle.
- Revue de la configuration des environnements (QUAL, PROD, PRA).

Livrables

- Plan de projet détaillé.
- Dossier de prise en charge / diagnostic initial.
- Planning consolidé.
- Charte de gouvernance.

Jalons

- J0 : réunion de lancement.
- J30 : validation du plan de projet.

6.2 Phase 1 : Montée de version Asalae 3.0 (M2 – M3)

Objectifs

- Migrer en toute sécurité l'environnement vers la version 3.0.
- Conserver les paramètres existants.

Actions principales

- Atelier technique de cadrage (reprise de paramètres, PRA, configuration).
- Mise à jour de l'environnement de qualification (Asalae/Versae 3.0).
- Tests de non-régression fonctionnels.
- Mise à jour de la documentation d'exploitation.
- Déploiement en PROD après validation.

Livrables

- Compte-rendu d'atelier technique.

- PV de recette QUAL.
- Dossier de mise à jour technique.
- Procédures de PRA actualisées.

Jalons

- J60 : déploiement en QUAL.
- J75 : recette de la version 3.0.
- J90 : passage en PROD.

6.3 Phase 2 : Industrialisation des versements (M4 – M6)*

Objectifs

- Assurer l'intégration fluide des versements dans le SAE.

Actions principales

- Tests de versements (manuels, automatiques).

Livrables

- PV de validation daté

Jalons

- J120 : 1er flux qualifié.
- J150 : validation de l'automatisation de flux (test BOX > SAE).
- J180 : fin de l'itération 1 de déploiement fonctionnel.

6.4 Phase 3 : Formation & accompagnement des utilisateurs (M4 – M7)*

Objectifs

- Former les archivistes et référents archives à l'usage d'Asalae / Versae.
- Préparer l'autonomie de l'administration fonctionnelle.

Actions principales

- Formation initiale (présentiel Lyon-Charial).
- Documentation utilisateurs (fiches pratiques, FAQ).
- Réplication des cas d'usage (exercices sur des fonds tests).
- Réalisation de sessions de support post-formation.

Livrables

- Plan de formation.
- Supports de formation (ppt + manuels).
- Procédures fonctionnelles (consultation, élimination, traçabilité...).
- Rapport d'évaluation des formations.

Jalons

- J150 : fin des sessions de formation.
- J180 : évaluation des acquis.

6.5 Phase 4 : Stabilisation & supervision du système (M7 – M9)

Objectifs

- Superviser le fonctionnement du SAE.
- Finaliser les paramétrages métiers et l'exploitation des logs.

Actions principales

- Mise en place des tableaux de bord.
- Test de la traçabilité, du cycle de vie et des alertes.
- Monitoring technique (indicateurs volumétrie, sécurité, PRA).
- Consolidation des jeux de profils utilisateurs.

Livrables

- Interface de supervision opérationnelle.
- Revue de sécurité technique.
- Statistiques d'usage (archivage, consultation).
- Guide d'administration fonctionnelle.

Jalons

- J210 : supervision active.
- J240 : revue d'exploitation du système.

Tableau RACI

<i>Phase / Activité</i>	MOA (DSC, mission Archives)	MOE (DSI)	TIT (Titulaire du marché)	UTIL Utilisateurs finaux (archivistes, référents...)
Phase 0 – Préparation et prise en charge				
<i>Réunion de lancement</i>	A	C	R	I
<i>Audit technique et fonctionnel</i>	I	A	R	I
<i>Validation du plan projet</i>	R	C	A	I
Phase 1 – Montée de version Asalae 3.0				
<i>Atelier technique de cadrage</i>	R	C	A	I
<i>Mise à jour environnement QUAL</i>	I	A	R	I
<i>Tests de non-régression</i>	C	R	A	I

Passage en PROD	C	A	R	I
Phase 2 – Industrialisation des versements				
PV de validation flux pilotes	R	C	A	I
Phase 3 – Formation et accompagnement				
Planification de la formation	R	I	A	C
Réalisation des sessions	I	I	R	A
Évaluation des acquis	A	I	C	R
Documentation utilisateurs	R	C	A	I
Phase 4 – Stabilisation et supervision				
Mise en œuvre de la supervision	I	A	R	I
Suivi des indicateurs d'usage	R	C	A	I
Ajustements de configuration	C	A	R	I
Réversibilité et clôture				
Élaboration du plan de réversibilité	R	C	A	I
Exports tests / données	I	A	R	I
Atelier bilan projet	A	C	R	I
PV de clôture	R	C	A	I

Légende RACI

- **R** = Réalisateur (exécute la tâche)
- **A** = Autorité (valide et rend compte du résultat)
- **C** = Consulté (contribue à la réalisation)
- **I** = Informé (tient compte ou suit l'avancement)