



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

ASP

Agence de Services
et de Paiement

Direction du Numérique et des Systèmes d'Information
Tél. : 05 55 12 00 00

Cahier des charges

Infrastructure d'échange

traitement pris en charge par le prestataire éditique de l'ASP

Fiche de suivi et d'identité (FSI) du document

Caractéristiques du document		
Entité responsable	Direction du Numérique et des Systèmes d'Information (DNSI)	
Responsable du document	Responsable du Service Exploitation et DevOps (SEDO)	
Identité du projet	Infrastructure d'échange	
Titre du document	Cahier des charges	
Support de référence : papier ou électronique	<input type="checkbox"/> Papier	<input checked="" type="checkbox"/> Electronique
Mots-clefs (séparés par une barre oblique sans espaces)	infrastructure	

Validation du document			
	Date	Fonction	Nom
Rédaction	06/02/2025	Technicien d'exploitation	E. VILLESSOT
Vérification		Responsable du Service Exploitation et DevOps (SEDO)	P. DUVIEL
Validation			

Gestion du document validé	
Date d'applicabilité du document (par défaut, la date de diffusion)	06/02/2025
Date de révision prévue (obligatoire pour les documents SMSI)	
Document(s) lié(s) :	
Catégorie et série du document (Arcateg©)	

Diffusion du document	
Date	Destinataires (Entité ou liste de personnes)
06/02/2025	Suivi-editique (ASP siège Limoges DNSI/LPRO/SEDO)
06/02/2025	ASP MOA
06/02/2025	ASP MOE

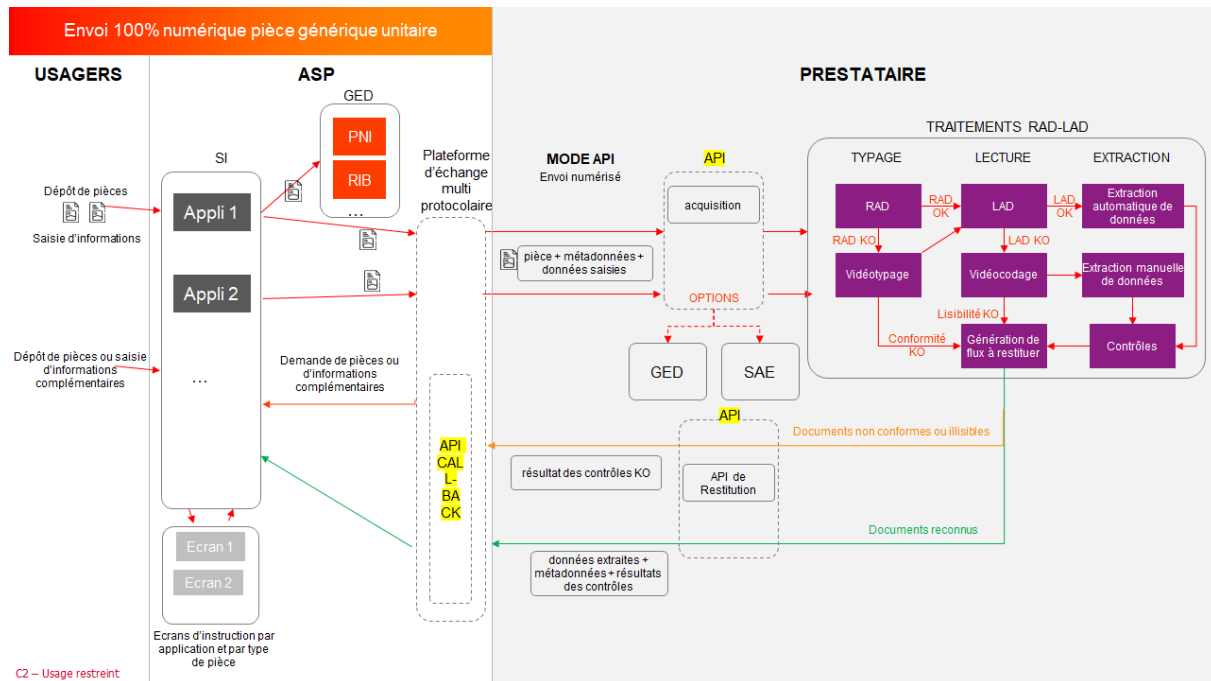
Historique des versions			
N° Version	Date	Auteur (nom/direction) (en toutes lettres)	Nature des modifications
1.0	06/02/2025	E. VILLESSOT DIT/SO/SEA	Création du document

Sommaire

I	Les modalités d'échanges	5
I.1	Echange par API	5
	Description des API produites par le titulaire et gestion des versions	6
	Pour les APIs produites par l'ASP et utilisées par le titulaire	6
I.2	Echanges d'archives	7
I.3	Traitement des flux papier	8
II	Métadonnées accompagnant les flux	9
III	La traçabilité et la sécurité des échanges	10
IV	Recette des flux d'échanges et des traitements de pièces	10

I Les modalités d'échanges

I.1 Echange par API



Pour les flux numériques de pièces unitaires, le mode d'échange privilégié pourra reposer sur l'utilisation d'une interface de programmation d'application (API) en mode REST qui fonctionnera en mode asynchrone. Pour certains projets, il pourrait être envisagé, en cours d'exécution du présent marché, de recourir à une API en temps réel pour certains types de pièces normées.

Aujourd'hui, la taille des transactions par API est limitée à 20 Mo par transaction complète (paramètre + données d'entrée et données de sortie). Au-delà, le mode d'échange privilégié sera celui des dossiers.

A la sollicitation de l'API, un code retour explicite devra être retourné afin notamment d'identifier si le prestataire a bien reçu l'envoi de l'ASP ou si l'envoi a fait l'objet d'un rejet (par exemple : code retour 200, 500, ...).

Par ailleurs, à réception, le titulaire devra générer un identifiant unique permettant de réconcilier l'envoi et la réception post traitement (sur l'API Call back).

Description des API produites par le titulaire et gestion des versions

Le titulaire doit présenter une API au format REST et fournir un contrat d'API qui suivent la norme OpenAPI : soit la version 2.0 qui s'appelle aussi Swagger, soit la version 3.0.* (pas la 3.1 et supérieure car ces dernières ne sont pas supportées en interne par l'ASP).

Les APIs disponibles doivent respecter les règles, normes et standard de l'industrie concernant le nommage des routes, les verbes utilisés, le passage des paramètres, la description des modèles des données manipulées, la gestion des cas passants mais aussi des erreurs (permettant une gestion programmatique des cas possibles) et la sécurisation des appels.

Le titulaire doit être en capacité de fournir un contrat de service qui décrive :

- ce qui peut être fait avec l'API,
- comment les données transmises sont gérées,
- la rétention qui en est faite,
- la qualité de service attendue (temps de réponse, niveau de disponibilité, taux d'erreur, etc...),
- ce qui peut être fait des données récupérées
- les conditions d'usage de ces données le cas échéant.

Le titulaire doit décrire la sécurité mise en place pour l'accès à son API : pour que l'ASP puisse savoir comment accéder à l'API et pour que l'ASP puisse s'assurer que les données transmises ne pourront pas être volées.

Le titulaire doit décrire la manière dont les données ASP vont être traitées, de quelle manière les données vont être sécurisées.

Il doit décrire sa gestion de version :

- Comment se fait une montée de version mineure, comment se fait une montée de version majeure, etc (contenu des nouvelles versions notamment) ;
- Les modalités d'information de l'ASP. Cette dernière doit être prévenue en amont suffisamment à l'avance (au moins 1 mois pour un changement de version mineure, 3 mois pour un changement de version majeure) pour gérer les changements non-rétro compatibles notamment (dans le cas de nouvelle version majeure) ;
- Dans le cadre d'une nouvelle version majeure, le titulaire doit s'engager à :
 - Maintenir les deux versions (la dépréciée et la nouvelle) pendant une période de six mois au moins afin de permettre à l'ASP de faire migrer ses applications consommatrices vers la nouvelle version majeure sans qu'il y ait de coupure de service qui serait préjudiciable,
 - Fournir l'ensemble de la documentation nécessaire décrivant la manière de passer de l'ancienne version à la nouvelle.
- Concernant la sécurisation des appels qui seraient faits à l'API du titulaire par l'ASP, il faut que le titulaire du marché, qui sera amené à recevoir des appels, ait sécurisé sa plate-forme: via un VPN ou avec du Two-way SSL (aussi appelé Mutual SSL) et via une sécurisation de type OIDC/OAuth 2.0 et que ces appels soient réalisables en HTTPS.

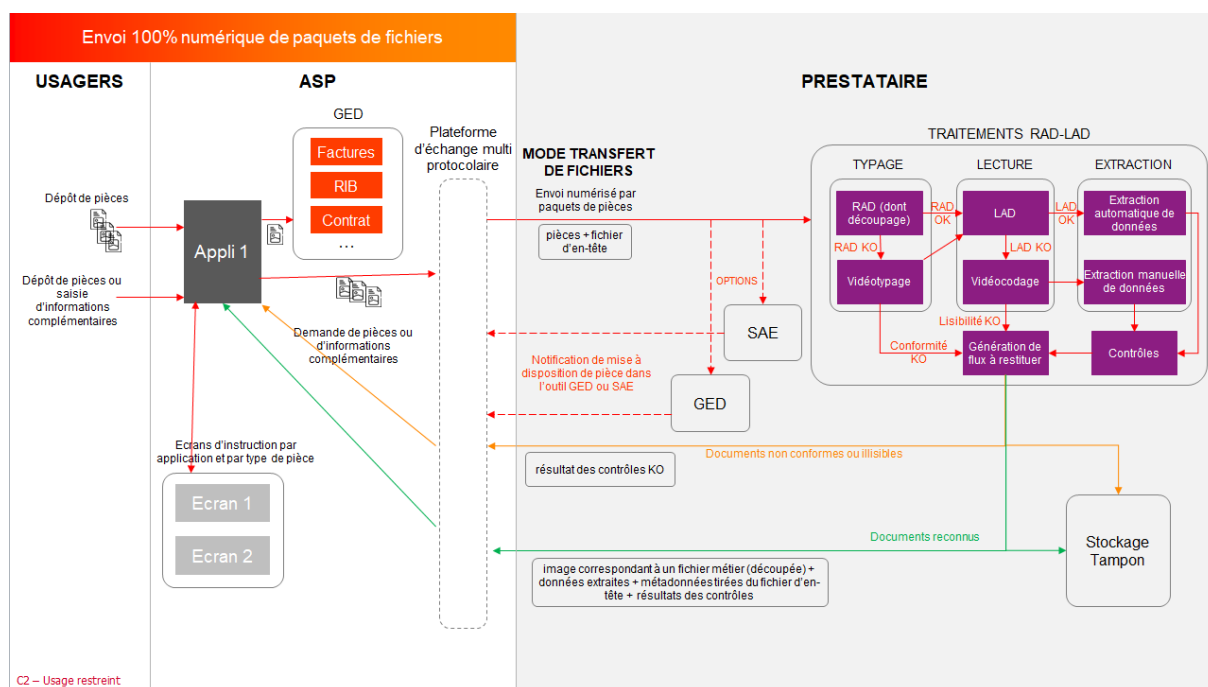
Pour les APIs produites par l'ASP et utilisées par le titulaire

Ces APIs seront des API REST et elles disposeront d'un contrat d'API qui suivra la norme OpenAPI soit la version 2.0 qui s'appelle aussi Swagger, soit la version 3.0.* (pas la 3.1 et supérieure).

Concernant la sécurisation des appels qui seraient faite à l'API de call-back présentée par l'ASP, il faut que le titulaire du marché, qui sera amené à utiliser l'API, puisse le faire de manière sécurisée : via un VPN ou avec du Two-way SSL (aussi appelé Mutual SSL) ou via une sécurisation de type OIDC/OAuth 2.0.

I.2 Echanges d'archives

Les échanges d'archives (ensemble de pièces regroupées dans un dossier compressé) : ce mode d'échanges sera utilisé lorsque le mode API ne sera pas adapté.



Les échanges d'archives entre l'ASP et le titulaire seront réalisés via la passerelle de télécommunication de l'ASP avec, de préférence, le moniteur d'échanges de données CFT IP (tunnel VPN) ou en mode FTPS ou SFTP via le serveur de dépôt de l'ASP (flux entrant et sortant).

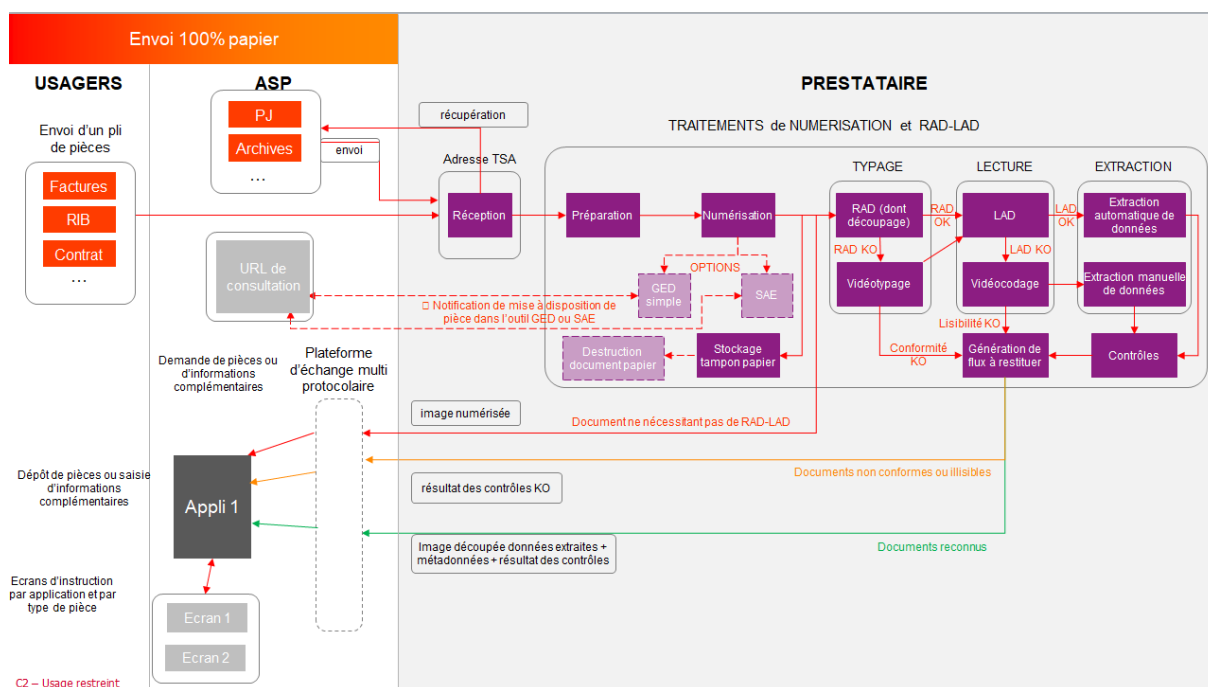
Les fichiers transmis par l'ASP seront regroupés dans une archive dont le format sera défini avec le titulaire (Zip, Tar, Gz,...).

Par ailleurs, **le titulaire devra produire une notification de réception d'archive.**

En fonction de la nature des fichiers échangés, des adaptations seront peut-être nécessaires en collaboration avec le titulaire, afin de répondre aux exigences de sécurité. Ces sujets seront, le cas échéant, abordés dans le cadre du build du projet concerné.

A noter que le titulaire devra conserver les résultats du traitement des flux (y compris contrôles et fichiers transmis par l'ASP) sur une durée de 3 mois par défaut (afin de pouvoir les retransmettre à l'ASP si un dysfonctionnement était constaté) ; cette durée pouvant varier d'un projet à l'autre. Elle sera précisée dans le cahier des charges du projet concerné ou elle sera validée lors de la phase de cadrage du BUILD du projet concerné.

I.3 Traitement des flux papier



Le retour vers l'ASP des traitements réalisés par le titulaire (dématérialisation simple ou dématérialisation et traitement RAD/LAD) pourront être réalisés soit par voie d'API (Call Back) soit par transmission de dossier compressé en fonction des caractéristiques de chaque projet.

A noter que le titulaire devra mettre en œuvre une GED afin d'assurer la conservation du résultat de ses traitements (dématérialisation et RAD-LAD potentiellement) sur une durée de 3 mois par défaut (afin de pouvoir les retransmettre à l'ASP si un dysfonctionnement était constaté) ; cette durée pouvant varier d'un projet à l'autre. Elle sera précisée dans le cahier des charges du projet concerné ou elle sera validée lors de la phase de cadrage du BUILD du projet concerné.

Les documents devront être stockés selon la période définie par chaque projet / marché subséquent.

II Métadonnées accompagnant les flux

S'agissant des flux numériques, chaque fichier (API) ou archive, transmis au titulaire, devra faire l'objet d'un seul et même retour à l'ASP, après le traitement de la ou des pièce(s), contenant l'ensemble des métadonnées et, le cas échéant, le résultat des traitements et contrôles réalisés. Ces métadonnées sont nécessaires pour alimenter les dossiers d'instruction des aides dans les applications de l'ASP.

Les métadonnées comprendront notamment, en mode API, les éléments suivants :

- L'application ASP source émettrice du document ;
- La référence au support contractuel liant l'ASP à son donneur d'ordre (facultatif)
- Un identifiant du dossier ;
- Des données métier rattachées à la pièce (exemple : nom et prénom dans le cadre d'une PNI) ;
- Le numéro d'itération (afin de matérialiser les dépôts initiaux et les dépôts complémentaires successifs) ;
- Un identifiant permettant de gérer la valeur probatoire et garantir son intégrité et son inaltérabilité tout au long du processus (identifiant de type « Hash ») **uniquement dans le cas de l'activation d'un « Système d'Archivage Electronique » (SAE) à valeur probatoire (cf. partie III.2.1.3 du CCTP).**

Les métadonnées comprendront notamment, en mode transfert de dossiers, les éléments suivants:

- L'application ASP source émettrice du document ;
- La référence au support contractuel liant l'ASP à son donneur d'ordre (facultatif) ;
- Un identifiant du dossier ;
- Des données métier rattachées au dossier (ex N° de SIRET) ;
- Un identifiant unique pour chacune des pièces (UID) déposées par l'utilisateur (une pièce pouvant comprendre plusieurs documents métiers : ex plusieurs factures) ;
- Le numéro d'itération (afin de matérialiser les dépôts initiaux et les dépôts complémentaires successifs) ;
- Un identifiant permettant de gérer la valeur probatoire et garantir son intégrité et son inaltérabilité tout au long du processus (identifiant de type « Hash ») uniquement dans le cas de l'activation de l'option « Système d'Archivage Electronique » (SAE) à valeur probatoire.

S'agissant des flux papier, chaque dossier numérisé par le titulaire et suite au traitement RAD/LAD devra être assorti notamment des métadonnées suivantes (produites par le titulaire) :

- Un identifiant unique du pli (dans cet identifiant pourra être matérialisée l'origine du courrier) ;
- La date de réception et de dématérialisation du pli ;
- Un identifiant unique de pièce (UID).

Ces éléments devront être arrêtés avec l'ASP lors de la phase de build de chaque projet.

III La traçabilité et la sécurité des échanges

Compte tenu de la dimension multi projets du présent marché et afin d'assurer la traçabilité des échanges et leur sécurité, il convient qu'un système d'acquittement soit mis en œuvre.

Ces acquittements doivent permettre de s'assurer, quelle que soit la modalité d'échange (API ou échanges de dossiers y compris suite à dématérialisation par le titulaire) que :

- Le fichier transmis par l'ASP a bien été réceptionné par le titulaire ;
- Celui transmis par le titulaire a bien été réceptionné par l'ASP.

Le titulaire doit alerter l'ASP par mail et/ou téléphone de toute anomalie constatée dans les échanges entrants ou sortants (flux retour vers l'ASP) par la création d'un ticket incident.

Le titulaire décrit, dans son mémoire, la solution qui garantit au mieux la sécurité et la traçabilité des échanges (par modalité d'échange). Il indique également comment il s'assure préalablement à l'envoi du fichier traité que son contenu est bien conforme à ce qui a été défini lors du cadrage de chaque projet (image de la pièce, typologie, données extraites et résultats des contrôles associés...).

IV Recette des flux d'échanges et des traitements de pièces

Le titulaire doit mettre à disposition une plateforme de qualification différente de l'environnement de production afin que l'ASP puisse vérifier pour ses applications :

- Le bon fonctionnement des API ;
- Le bon fonctionnement des échanges de dossiers.

Cet environnement de qualification est indispensable avant une mise en production d'un nouveau projet **ou d'une évolution importante d'une application de gestion d'un dispositif d'aide publique de l'ASP** (recette de bout en bout) ou à l'occasion d'une montée de version significative de la plateforme d'API ou des APIs du titulaire ou enfin à l'occasion d'une modification des modalités d'échanges des dossiers. Cette prestation de mise à disposition d'une plateforme de qualification doit être opérationnelle sur la durée de vie du marché ; elle n'est donc pas limitée à la phase de build d'un projet.

En effet, l'ASP peut être amenée, sur la durée de vie d'un dispositif d'aide publique, à réaliser des tests de bout en bout notamment dans le cas où elle apporterait des modifications fonctionnelles à son application de gestion du dispositif. Il faut donc que le titulaire maintienne en conditions opérationnelles l'environnement de recette du projet (l'ensemble de la chaîne).

Par ailleurs, le titulaire doit être réactif dans le traitement des flux qui lui parviendraient sur cet environnement.

Tout traitement de données réalisé sur l'environnement de recette, non rattaché à une demande d'évolution ou à une phase de build, fera l'objet d'une facture spécifique (libellée environnement de recette), conformément aux prix arrêtés au titre du RUN dans le devis définitif.