



**MINISTÈRES
AMÉNAGEMENT
DU TERRITOIRE
TRANSITION
ÉCOLOGIQUE**

*Liberté
Égalité
Fraternité*



PLAT'AU

Dossier d'architecture technique

Date 01/2025

Etat Pour validation

Version 3.0.0

Table des matières

1 Introduction et objectifs

- 1.1 Vue d'ensemble
- 1.2 Objectifs principaux de qualité
- 1.3 Parties prenantes

2 Contraintes

- 2.1 Contraintes d'architecture
- 2.2 Contraintes de sécurité

3 Contexte et périmètre

- 3.1 Contexte métier
- 3.2 Contexte Technique

4 Stratégie de solution

- 4.1 Modèles de conception - Décisions d'architecture
- 4.2 Environnement technologique
- 4.3 Forge logicielle - CI/CD

5 Vue en Briques

6 Vue Exécution

- 6.1 Instruction d'un dossier DAU
- 6.2 Dépôt et récupération des binaires
- 6.3 Gestion des traces fonctionnelles et techniques

7 Vue Déploiement

- 7.1 Liste des environnements
- 7.2 Architecture physique
- 7.3 Dimensionnement
- 7.4 Accès aux environnements

8 Sujets transverses

- 8.1 Mesures de sécurité

9 Exigences de qualité

- 9.1 Fiabilité
- 9.2 Flexibilité
- 9.3 Sécurité
- 9.4 Interopérabilité

10 Risques et Dettes techniques

11 Crédits

12 Annexes

- 12.1 Glossaire
- 12.2 Points ouverts
- 12.3 Architecture technique détaillée

1 Introduction et objectifs

1.1 Vue d'ensemble

Le système d'information **XX'AU** vise à outiller les échanges dématérialisés entre les acteurs de la chaîne d'instruction et ne se substitue pas à leurs outils métiers.

Le système d'information est découpé en trois produits :

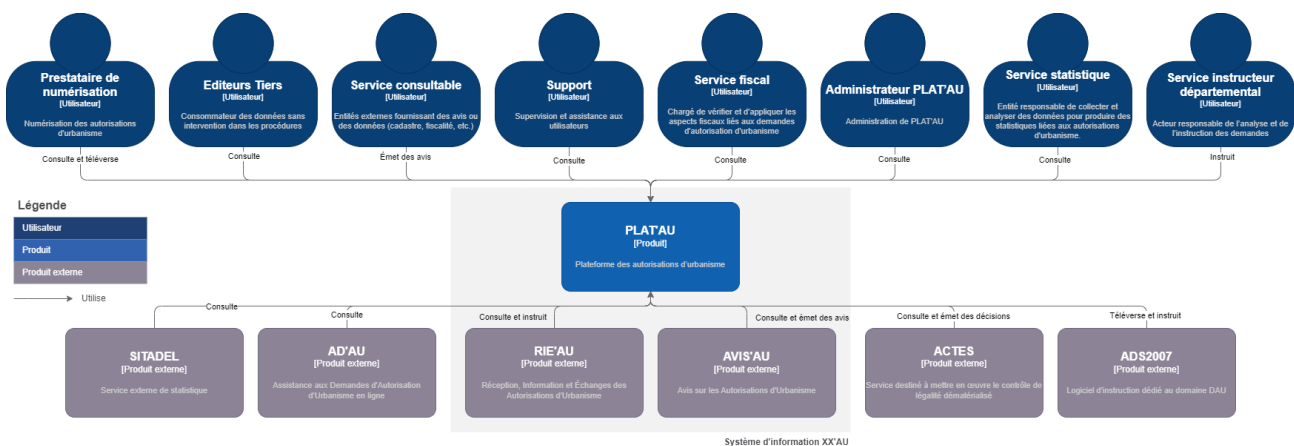
- **PLAT'AU**, pour Plateforme des Autorisations d'Urbanisme est l'outil central de la suite **XX'AU**. Il permet le partage de dossiers dématérialisés et l'horodatage des flux entre les acteurs de la chaîne d'instruction. Pour cela, chaque acteur a besoin de raccorder ses logiciels à **PLAT'AU**. En effet **PLAT'AU** fournit une interface technique (API) mais ne remplace pas les outils d'instruction ;
- **RIE'AU**, pour Réception, Information et Echanges des Autorisations d'Urbanisme pour outiller les communes non compétentes et les communes compétentes pour lesquelles la Direction Départementale des Territoires et de la Mer est mise à disposition ;
- **AVIS'AU**, plateforme de réception et de traitement des demandes d'AVIS relatifs aux Autorisations d'Urbanisme. Outil de gestion pour les services consultables sans SI de gestion et / ou rendant peu d'avis.

On notera l'existence de **AD'AU**, pour Assistance aux Demandes d'Autorisation d'Urbanisme en ligne, présent dans la suite logicielle **XX'AU**. Ce service n'est cependant pas inclus dans le système d'information **XX'AU**, ayant son propre cycle de vie.

Le système d'information **XX'AU** se veut évolutif avec l'ajout de nouveaux domaines métiers tel que la préemption (déclarations d'intention d'aliéner), la police de la publicité (autorisations préalables et déclarations préalables), les travaux en sites classés (demandes d'autorisations spéciales de travaux sur site classé), etc...

Ce dossier d'architecture porte uniquement sur la solution **PLAT'AU**.

Le schéma ci-dessous met en avant les principaux cas métiers du système d'information. Ce schéma se concentre sur le volet métier et omet certaines adhérences "techniques" (envoi de mail, base de données, etc...).



Vue d'ensemble

1.2 Objectifs principaux de qualité

1.2.1 Fiabilité

Le système doit fonctionner sans interruption en mode nominal pour garantir la continuité des services critiques. Cela inclut l'accessibilité constante des dossiers pour les utilisateurs (pétitionnaires, agents, etc.) et le traitement des processus métiers (instruction, taxation, consultations). Une panne prolongée pourrait entraîner des autorisations tacites, des retards dans les projets de construction et une perte de confiance des utilisateurs.

1.2.2 Flexibilité

L'architecture doit permettre l'intégration maîtrisée des nouveaux domaines métiers ou des évolutions réglementaires. Cela inclut la capacité de versionner les données et de gérer des contrats de services rétro-compatibles, afin de soutenir les mises à jour progressives tout en limitant

l'impact sur les utilisateurs.

1.2.3 Sécurité

Toutes les modifications, consultations ou échanges de données doivent être tracés pour répondre aux besoins de transparence, de conformité réglementaire et de sécurité. Les données doivent être accessibles uniquement par leurs ayants droit, et toute modification doit être journalisé. Cela protège l'intégrité des données et renforce la confiance des parties prenantes.

1.2.4 Interopérabilité

Le système doit pouvoir s'interfacer facilement avec des systèmes tiers (SDIS, gestionnaires de réseaux, etc.) via des API standardisées. Cela garantit un échange fluide de données entre les différentes parties prenantes et permet l'ajout futur de nouvelles fonctionnalités ou partenaires sans remise en question de l'architecture existante.

1.3 Parties prenantes

Cette section explicite l'ensemble des parties prenantes du système, c'est-à-dire toutes les personnes, rôles ou organisations qui soit :

- doivent connaître l'architecture ;
- doivent être convaincus de l'architecture ;
- doivent travailler avec l'architecture ou avec le code ;
- ont besoin de la documentation d'architecture pour leur travail ;
- doivent prendre des décisions concernant le système ou son développement.

Rôle/Nom	Contact	Attentes
Cheffe du groupe produits numériques / Sophie Quernec	sophie.quernec@developpement-durable.gouv.fr	Piloter les évolutions des produits numériques et garantir leur alignement avec la stratégie globale
Directeur Produit / Thierry Le Coroller	thierry.le-coroller@developpement-durable.gouv.fr	Assurer la vision stratégique et la priorisation des fonctionnalités liées au système XX'AU
Maitrise d'ouvrage		Garant de la cohérence fonctionnelle
Chef de projet XX'AU / Xavier Hardy	xavier.hardy@developpement-durable.gouv.fr	Coordonner les projets associés à XX'AU
Chef de projet XX'AU / Jonathan Pinvidic	jonathan.pinvidic@developpement-durable.gouv.fr	Coordonner les projets associés à XX'AU
Directeur technique / Josselin Maillard	josselin.maillard@developpement-durable.gouv.fr	Valider les choix techniques, leur faisabilité, et leur alignement avec les orientations stratégiques
Chef de projet Support / Mikael Cita	mikael.cita@developpement-durable.gouv.fr	Organiser et superviser le support utilisateur ainsi que la gestion des incidents
Directeur Projet TMA / Jeremy Maczuha	jeremy.maczuha@soprasteria.com	Planifier, prioriser et superviser les activités de maintenance applicative
Architecte TMA / Nicolas Coston	nicolas.coston@soprasteria.com	Garantir l'évolution cohérente de l'architecture technique tout en assurant sa maintenabilité
Architecte TMA / Sami Burillon	sami.burillon@soprasteria.com	Garantir l'évolution cohérente de l'architecture technique tout en assurant sa maintenabilité
Responsable technique TMA / Maxence Coutand	maxence.coutand@soprasteria.com	Coordonner les équipes techniques

Rôle/Nom	Contact	Attentes
Pilotage Infogérance	management.tdp@soprasteria.com	Gérer l'infrastructure technique

2 Contraintes

2.1 Contraintes d'architecture

2.1.1 Outillage

Les solutions techniques doivent s'appuyer sur des outils largement adoptés et disposant d'une communauté active ou d'un support éditeur fiable. La maturité est un indicateur de confiance notamment sur leur fiabilité et leur capacité à fonctionner de manière stable dans des environnements similaires. Par ailleurs, la documentation doit être complète et accessible, et les outils doivent être compatibles avec les standards et technologies déjà en place dans le système d'information pour limiter les coûts d'intégration et de maintenabilité.

2.1.2 Infrastructure

L'architecture cible doit être compatible avec un déploiement distribué sur OpenShift Container Platform. Cela implique la prise en charge des conteneurs applicatifs.

2.1.3 Optimisation des ressources

Compte tenu du volume important des données manipulées, il est demandé de :

- Limiter l'utilisation de l'espace de stockage au strict nécessaire ;
- Réduire la bande passante utilisée par les applications.

2.1.4 Gestionnaire d'interface applicative

L'architecture cible doit utiliser `PISTE` (solution ministérielle) comme gestionnaire d'interface applicative pour exposition de l'API du système d'information `XX'AU`. L'utilisation de cet outil engendre les contraintes suivantes :

- Limite de 1 000 appels par heure et par client d'API ;
- Limite de fréquence fixée à 20 appels par seconde par client d'API.

Tout dépassement entraîne le retour d'une erreur HTTP 429 (Too Many Requests).

En conséquence, il est crucial de prévoir une gestion efficace des erreurs incluant des mécanismes de résilience.

`PISTE` contraint l'application à un délai maximal de traitement des requêtes de 30 secondes, les actions en cours doivent être annulées.

2.1.5 Durée de vie d'une action

L'ensemble des actions métiers doivent être effectuées en 6h. De fait, concernant les fonctionnalités asynchrones (gestion des pièces jointes), toute action dépassant ce délai doit être notifiée en échec. En conséquence, il est nécessaire de mettre en place un mécanisme de repli (fallback) sur ces actions métiers.

2.1.6 Archivage

D'un point de vue métier, en particulier de la durée d'utilité administrative, tout dossier dont la date de dépôt est passée de plus de 10 ans doit être archivé.

2.1.7 Purge

Les traces fonctionnelles et techniques sont à purger au bout d'un an. Les notifications sont à purger au bout de 3 mois.

2.1.8 Fonctionnement parallèle

Le système d'information doit être en mesure d'instancier plusieurs versions des applicatifs en parallèle.

2.2 Contraintes de sécurité

2.2.1 Disponibilité

PLAT'AU doit garantir une disponibilité minimale de 99,98 %, ce qui correspond à une interruption maximale de 2 heures par mois, afin de maintenir une continuité de service en cas d'incident.

2.2.2 Intégrité

PLAT'AU doit garantir la préservation complète des données, afin d'éviter toute perte ou altération des informations traitées ou stockées.

2.2.3 Confidentialité

L'accès aux données de PLAT'AU doit être sécurisé par une authentification et une gestion des droits, garantissant un accès strictement réservé aux personnes habilitées sur un périmètre métier défini.

2.2.4 Preuve

Les opérations de modification des objets métiers doivent être tracées dans un objectif de preuve pour non-opposabilité légale des actions.

2.2.5 Performance

Cible performance des services backend

Traitement informatisé	Illustration	Temps maximal pour 90 % des requêtes côté serveur
Simple	Qualification d'un dossier	1 seconde
Moyen	Ajout d'un dossier	3 secondes (hors échanges réseau)
Complexe	Création d'un dossier volumineux	10 secondes (hors échanges réseau)
Asynchrone	Versement du contenu d'une pièce-jointe	Les traitements sont effectués en arrière-plan et sont contraints par des éléments comme le volume de données ou la charge des applicatifs tiers invoqués. Le temps d'intégration d'un contenu binaire est estimé en secondes. Cependant, le traitement restant asynchrone, un temps d'intégration plus important est possible dans le cas d'une pièce jointe particulièrement lourde ou lors d'un pic d'activité sur le sous-système d'intégration de pièces jointes par effet de lissage. Le délai maximum de traitement est de 6h.

Cible performance des services frontend

Traitement informatisé	Illustration	Temps maximal pour 90 % des requêtes côté serveur
Simple	Mentions légales	1 seconde
Moyen	Gestion des agents	3 secondes
Complexe	Gestion des consultations	10 secondes

3 Contexte et périmètre

3.1 Contexte métier

Le schéma ci-dessous décrit le contexte métier du système d'information **PLAT'AU** en spécifiant les produits et services en adhérences avec l'application **PLAT'AU**.

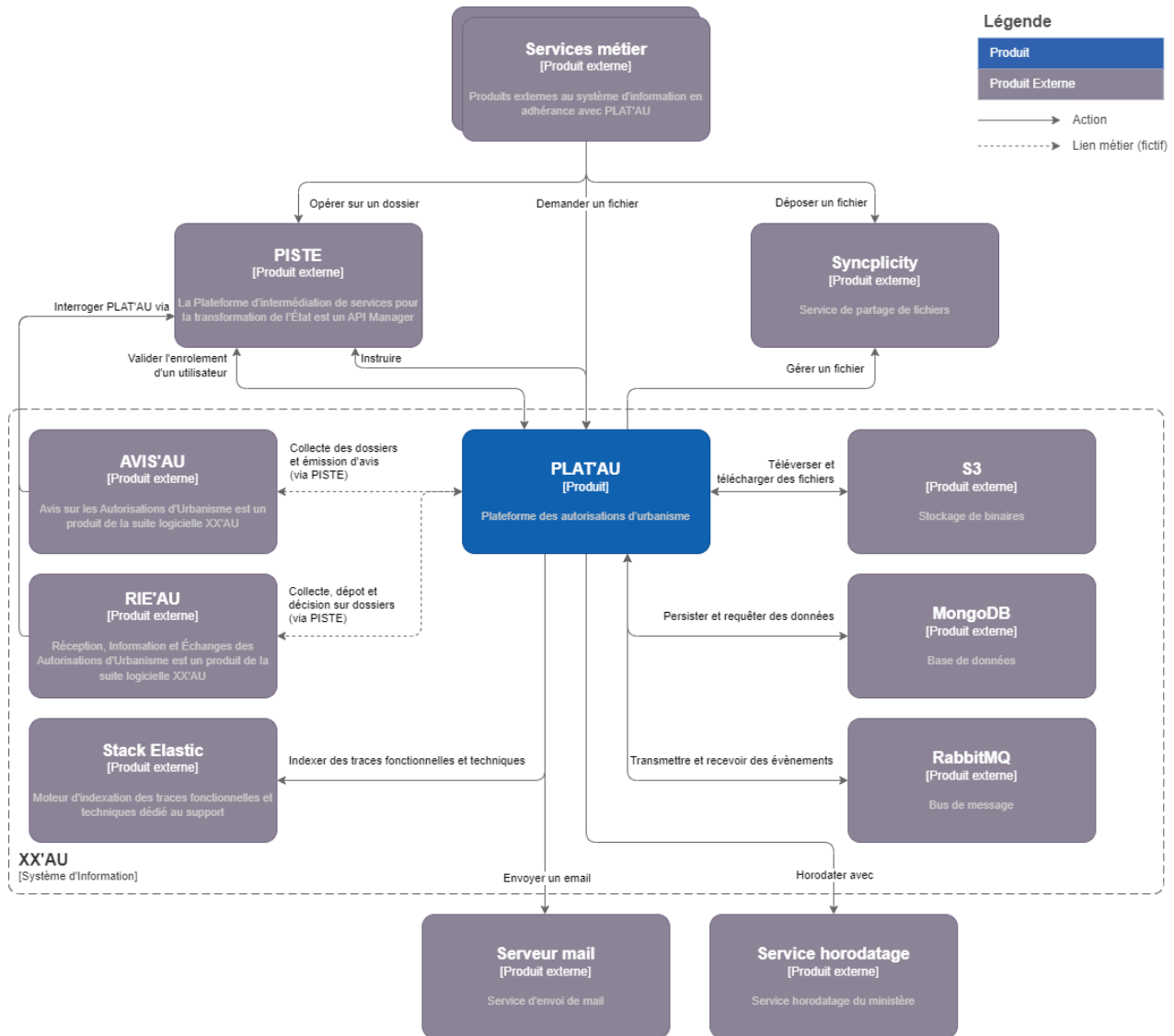


Schéma de description du contexte métier du système d'information

Le tableau ci-dessous détail l'ensemble des services métiers externes au système d'information en adhérence avec **PLAT'AU**.

Nom	Description	Utilisation
Actes	Service destiné à mettre en œuvre le contrôle de légalité dématérialisé	Collecte des dossiers et émission de décisions
Logiciels d'instruction	Service proposé par des éditeurs externes permettant l'instruction de dossiers via PLAT'AU	Collecte des dossiers et émission d'instructions
Logiciels de consultation	Services proposés par des éditeurs externes permettant la consultation de dossiers via PLAT'AU	Collecte des dossiers et émission de consultations

Nom	Description	Utilisation
ADS2007	Logiciel d'instruction dédié au domaine DAU	Collecte, dépôt de dossiers, avis, décisions et consultations
ADAU	Assistance aux Demandes d'Autorisation d'Urbanisme en ligne	Dépôt de dossiers
SITADEL	Service externe de statistique	Collecte de dossiers

3.2 Contexte Technique

Le schéma ci-dessous décrit le contexte technique du système d'information `PLAT'AU` en spécifiant les typologies de flux des produits et services en adhérences avec l'application `PLAT'AU`.

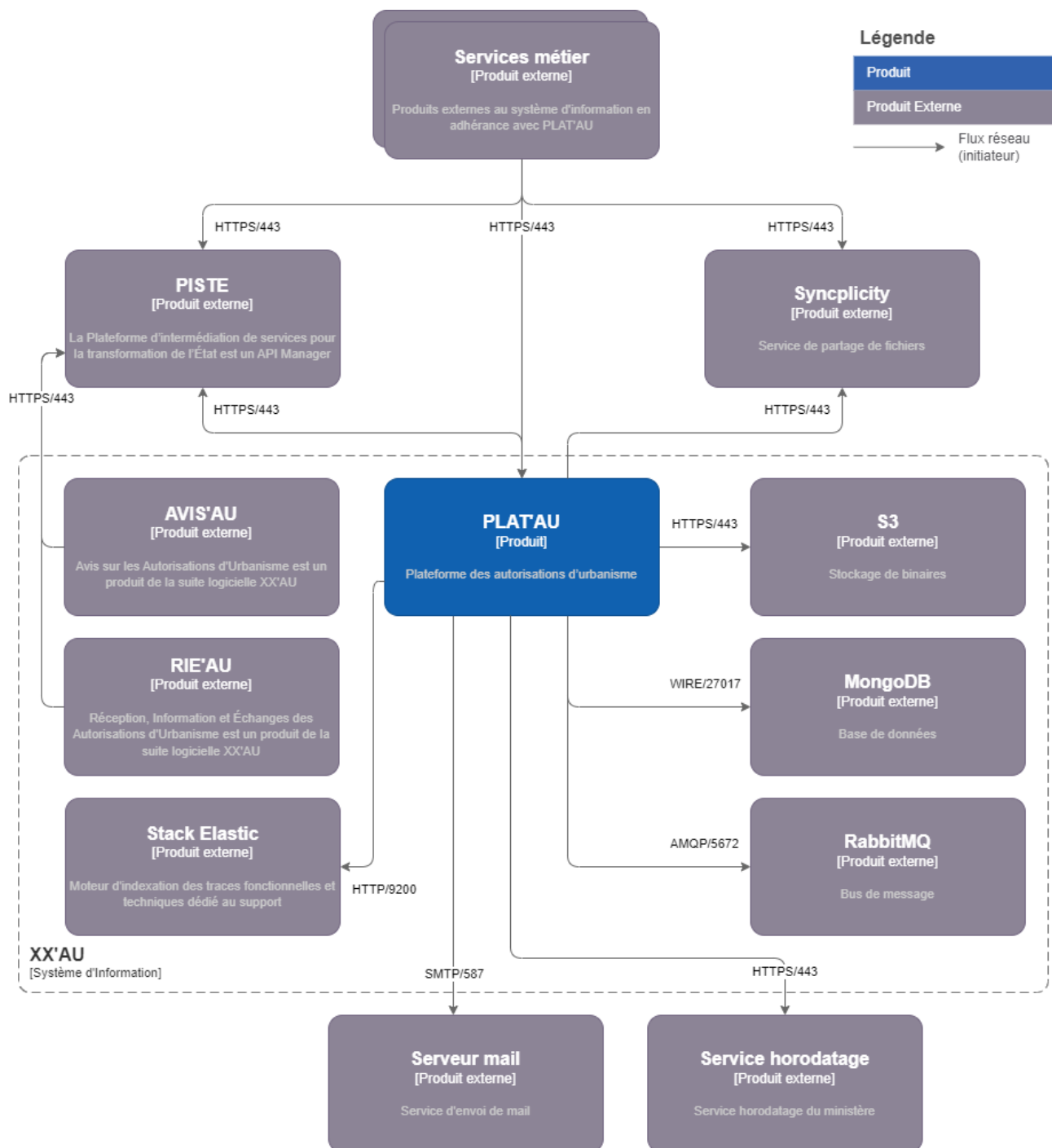


Schéma de description du contexte technique du système d'information

4 Stratégie de solution

4.1 Modèles de conception - Décisions d'architecture

La conception du système d'information `XX'AU` repose sur plusieurs décisions d'architecture :

- Conception du système d'information `XX'AU` en services par produit (`RIE'AU` , `AVIS'AU` et `PLAT'AU`) au vu de la distanciation des exigences et des cas d'utilisation ;
- Gestion événementielle des pièces jointes (fichiers) pour gestion asynchrone du téléchargement, analyse antivirus, etc..
- Utilisation d'une base de données NoSQL au vu du besoin de structures de données différentes en fonction du domaine métier, du besoin d'évolution du modèle de données et de capacité de haute disponibilité ;
- Utilisation d'un service S3 pour stockage massif de fichiers avec résilience et haute disponibilité ;
- Conteneurisation des services au vu du besoin de livrable standardisé partageable facilement avec un infogérant ;
- Services sans état de transaction (stateless) pour assurer une scalabilité horizontale de l'ensemble des services ;
- Conception de `PLAT'AU` en services techniques par cas d'usage : un composant API de gestion des dossiers, un composant API de récupération des notifications, un composant API de téléchargement des fichiers, un agent de traitement des fichiers et un agent d'agrégation des fichiers et traitement des pièces jointes d'un dossier et ses sous objets métiers (avis, consultation, décision) ;
- Horodatage des actions sur un objet métier avec cachet électronique pour non-opposabilité légale des actions.

4.2 Environnement technologique

4.2.1 Socle technique

Brique	Composant	Version
Environnement Java	OpenJDK	≥ 21
Framework de développement	Spring Boot	≥ 3.3.X
Framework de présentation	Angular	≥ 17
Description des interfaces	OpenAPI	3.0.0

4.2.2 Environnement de développement

Brique	Composant	Version
Serveur Web	Apache Tomcat	Embarqué par Spring Boot
Base de données	MongoDB	≥ 6.0.X
Bus de message	RabbitMQ	≥ 3.12.X
Export des journaux applicatifs	FluentBit	≥ 2.0.X
Stockage de binaires	AWSSDK	≥ 2.20.X

4.3 Forge logicielle - CI/CD

Description	Outil	Version
Construction / Tests	Apache Maven	3
Dépôt artefact Maven	Sonatype Nexus	3.69
Analyseur statique code	Sonarcube	8.9

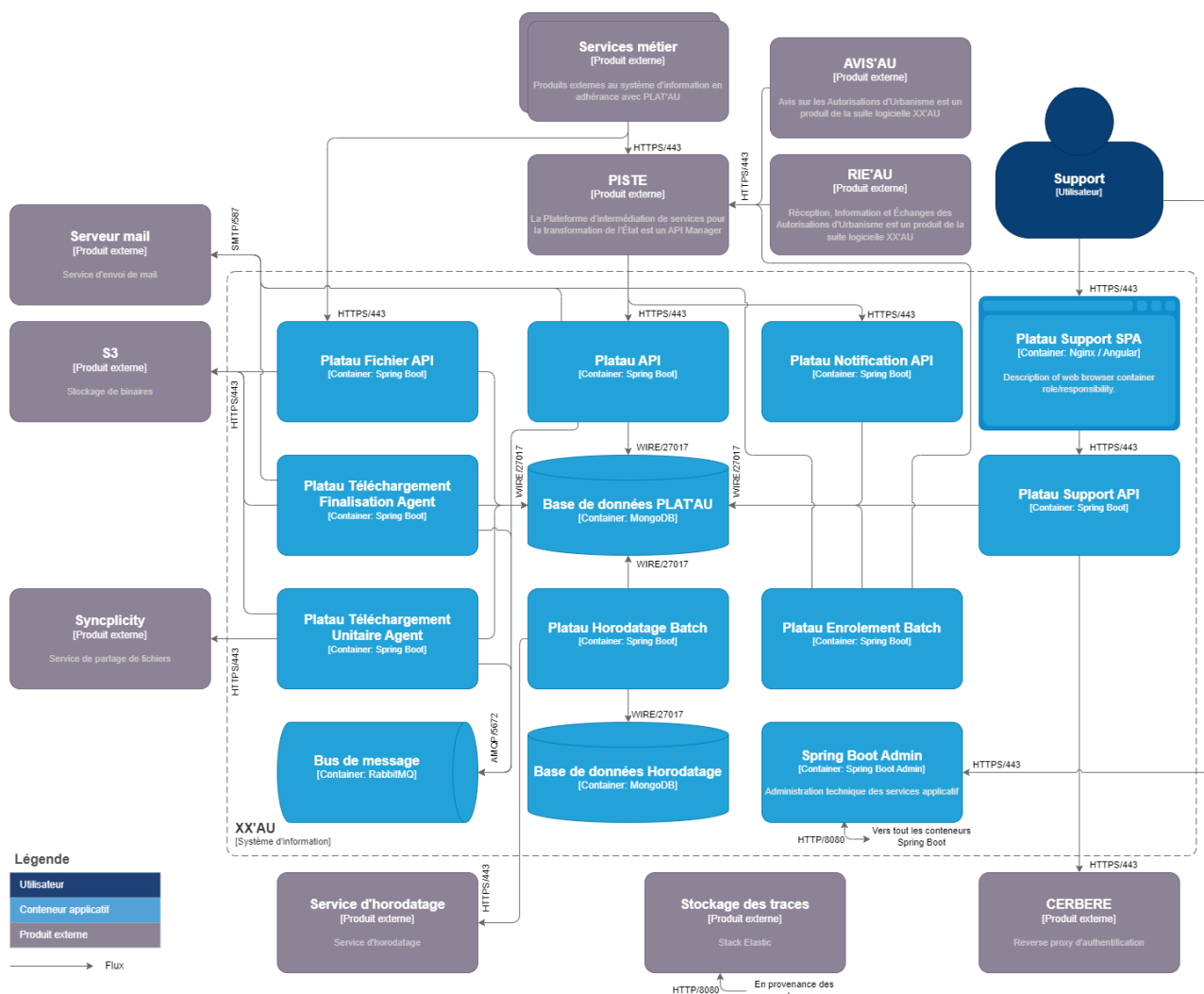
Description	Outil	Version
Analyseur statique code (sécurité)	Checkmarx	9
Analyseur statique dépendances	Dependency Check	11
Analyseur statique conteneurs applicatif	Trivy	0.4
Construction des conteneurs applicatif	Kaniko	1.2
Dépôt conteneurs applicatif	Harbor	2.9
Construction des livrables de déploiement	Helm	3.9
Orchestration	OpenShift Container Platform	Géré par l'infogérant

5 Vue en Briques

PLAT'AU est opéré par plusieurs services découpés par spécificité métier :

- PLAT'AU API est le service central de PLAT'AU mettant à disposition une API REST d'accès / édition des objets métiers ;
- PLAT'AU Fichier API est une API permettant de récupérer des fichiers binaires depuis l'espace de stockage. Cette API est accessible depuis internet sans passer par l'API Manager PISTE ;
- PLAT'AU Notification API est une API de consultation des notifications d'un utilisateur ;
- PLAT'AU Support SPA et PLAT'AU Support API représente un produit d'administration du système d'information XX'AU (PLAT'AU , RIE'AU et AVIS'AU) destiné à l'équipe Support ;
- PLAT'AU Téléchargement Unitaire et PLAT'AU Téléchargement Finalisation sont des agents de traitement des fichiers de manière événementielle au travers du bus de message ;
- PLAT'AU Horodatage Batch est un batch permettant de signer par cachet électronique les actions opérées sur un objet métier ;
- PLAT'AU Enrollement Batch est un batch de gestion de l'enrôlement des utilisateurs sur un domaine métier.

Le schéma suivant apporte une vue exhaustive des adhérences de l'ensemble des services du système d'information.



6 Vue Exécution

6.1 Instruction d'un dossier DAU

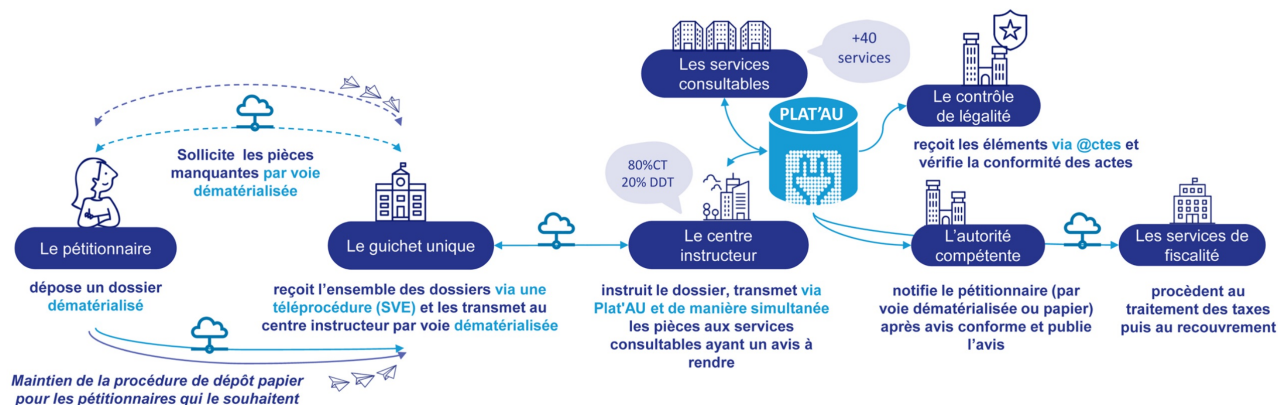


Schéma simplifié de l'instruction des demandes d'autorisation d'urbanisme

6.2 Dépôt et récupération des binaires

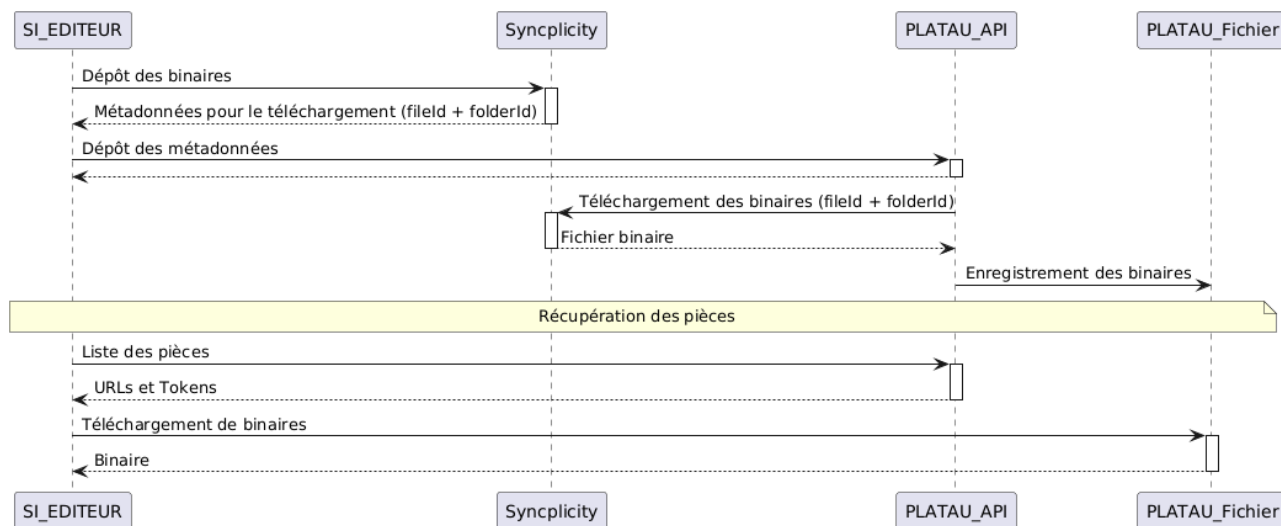


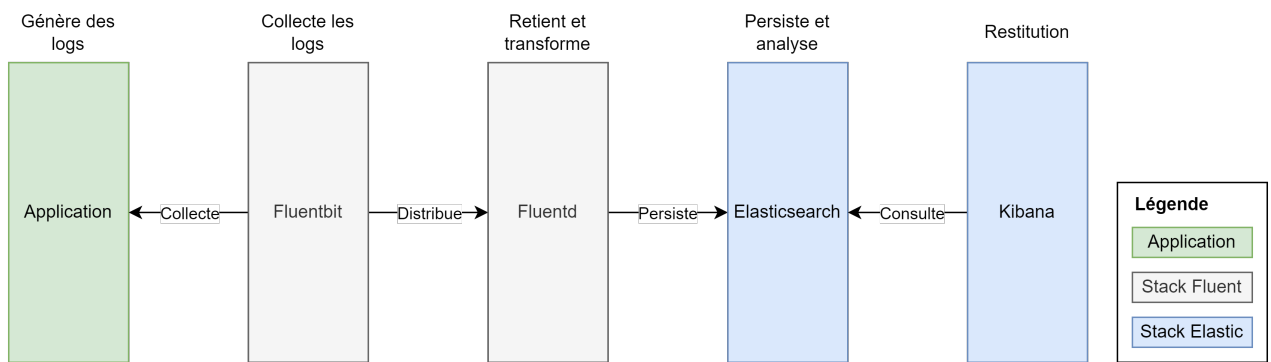
Diagramme de séquence du dépôt et récupération des binaires

Le service de téléchargement de binaire est exposé par l'applicatif **PLAT'AU** directement sur Internet, sans passer par l'API Management **PIS TE**. Ce service fait l'objet d'un examen particulier.

La sécurité du service **PLAT'AU** de téléchargement de fichier repose sur deux composants :

- L'URL retournée comporte l'identifiant de la pièce jointe. Un identifiant de pièce jointe est donc un prérequis obligatoire ;
- Le jeton de sécurité contient les informations suivantes :
 - UUID lié en base de données à la pièce jointe ;
 - Date de péremption du jeton ;
- L'identifiant de la pièce jointe doit correspondre en base à son UUID.

6.3 Gestion des traces fonctionnelles et techniques



Architecture fonctionnelle du système de gestion des traces fonctionnelles et techniques

7 Vue Déploiement

7.1 Liste des environnements

Environnement	Description	Dimensionnement	Présence
Recette	Il permet à l'équipe de tests d'effectuer une recette des nouvelles versions applicatives	Réduite	Obligatoire
XP Jalon	Il permet aux utilisateurs et éditeurs de tester les nouvelles versions applicatives avant la mise en service	Réduite	Obligatoire
Performance	Il permet aux équipes techniques d'effectuer des mesures de la performance du SI	Nominale	Facultatif
Préproduction	Il permet de tester et valider les procédures de mise en production	Nominale	Obligatoire
Production	Il permet aux utilisateurs et éditeurs d'exploiter l'application.	Nominale	Obligatoire

7.2 Architecture physique



Le dimensionnement et la gestion de l'infrastructure sont décrits dans le [dossier d'architecture de l'infogérant](#)

7.3 Dimensionnement

Le [dimensionnement des environnements](#) est disponible en annexe de ce document

7.4 Accès aux environnements

7.4.1 Production

Service	URL
PLAT'AU API	api.platau.cohesion-territoires.gouv.fr
PLAT'AU Fichier API	telechargement.platau.cohesion-territoires.gouv.fr
PLAT'AU Support	support.platau.cohesion-territoires.gouv.fr
Spring Boot Admin	sba.platau.cohesion-territoires.gouv.fr
Kibana	supervision.platau.cohesion-territoires.gouv.fr

7.4.2 Préproduction

Service	URL
PLAT'AU API	api.preprod1.platau.cohesion-territoires.gouv.fr
PLAT'AU Fichier API	telechargement.preprod1.platau.cohesion-territoires.gouv.fr
PLAT'AU Support	support.preprod1.platau.cohesion-territoires.gouv.fr
Spring Boot Admin	sba.preprod1.platau.cohesion-territoires.gouv.fr
Kibana	supervision.preprod1.platau.cohesion-territoires.gouv.fr

7.4.3 Performance

Service	URL
PLAT'AU API	api.perf.platau.dev
PLAT'AU Fichier API	telechargement.perf.platau.dev
PLAT'AU Support	support.perf.platau.dev
Spring Boot Admin	sba.perf.platau.dev
Kibana	supervision.preprod1.platau.cohesion-territoires.gouv.fr
TestTool	testtool.perf.platau.dev
TestTool API	api.testtool.perf.platau.dev

7.4.4 XP Jalon

7.4.4.1 Démonstrateur 1

Service	URL
PLAT'AU API	api.demo.platau.cohesion-territoires.gouv.fr
PLAT'AU Fichier API	telechargement.demo.platau.cohesion-territoires.gouv.fr
PLAT'AU Support	support.demo.platau.cohesion-territoires.gouv.fr

Service	URL
Spring Boot Admin	sba.demonstrateur.platau.dev
Kibana	supervision.demo.platau.dev

7.4.4.2 Démonstrateur 2

Service	URL
PLAT'AU API	api.demo2.platau.cohesion-territoires.gouv.fr
PLAT'AU Fichier API	telechargement.demo2.platau.cohesion-territoires.gouv.fr
PLAT'AU Support	support.demo2.platau.cohesion-territoires.gouv.fr
Kibana	supervision.demo.platau.dev
TestTool	testtool-traads.demonstrateur2.platau.dev
TestTool API	api.testtool-traads.demonstrateur2.platau.dev

7.4.5 Recette

Service	URL
PLAT'AU API	api.recette.platau.cohesion-territoires.gouv.fr
PLAT'AU Fichier API	telechargement.recette.platau.cohesion-territoires.gouv.fr
PLAT'AU Support	support.recette.platau.cohesion-territoires.gouv.fr
Spring Boot Admin	sba.recette.platau.cohesion-territoires.gouv.fr
Kibana	supervision.demo.platau.dev

8 Sujets transverses

8.1 Mesures de sécurité

8.1.1 Chiffrement des échanges

L'échange d'information en HTTP est soumis à un chiffrement de bout en bout (HTTPS), à savoir du client aux Ingress frontaux des clusters ou des serveurs applicatifs eux-mêmes.

L'envoi de messages électroniques est fait avec le protocole SMTP avec l'extension STARTTLS activée, assurant un chiffrement des données transmises. Les enregistrements DNS SPF et DMARC ont été également déclarés pour assurer l'authenticité des messages émis.

8.1.2 Accès au système de gestion des traces

Le système permettant la consultation des traces applicatives (techniques et fonctionnelles) repose dans un premier temps sur une instance Elasticsearch.

Le système d'authentification ciblé pour l'accès à la plateforme EFK est CERBERE.

8.1.3 Authentification, gestion des droits et des habilitations sur l'ensemble des API

L'authentification aux services métiers est scindée en deux parties :

- L'authentification des utilisateurs, donnant accès aux administrateurs à l'interface de paramétrage de PLAT'AU. L'accès utilisateur est géré par le portail d'authentification CERBERE du MTE par l'intermédiaire d'une librairie intégrée à l'applicatif PLAT'AU. Les applicatifs concernés sont uniquement des briques de supervision et d'exploitation ;
- L'authentification système, qui détermine les applications ayant accès à l'API PLAT'AU. Le système d'API Management est en charge de cette partie de l'authentification.

De nombreuses applications seront amenées à échanger des flux avec l'application PLAT'AU. Ces applications doivent donc s'identifier avant tout échange avec PLAT'AU.

L'identification et l'authentification de ces partenaires est réalisée par l'intermédiaire de deux mécanismes :

- le système d'API Management `PISTE` mis en place en amont de `PLAT'AU API` permettant de vérifier les SI appelants ;
- le système interne à `PLAT'AU` permettant de vérifier d'une part si les acteurs des opérations sont correctement associés aux SI appelants, d'autre part si les acteurs ont les droits suffisants pour effectuer les opérations demandées.

Il existe deux niveaux de gestion des habilitations sur `PLAT'AU API` :

- Habilitation basée sur le rôle (RBAC), appelé "droits de niveau 1" dans les spécifications de l'application ;
- Habilitation basée sur une correspondance entre les champs des objets métier et les caractéristiques de l'utilisateur (ABAC), appelé (droits de niveau 2) dans les spécifications de l'application.

L'association d'un rôle à un utilisateur est effectuée par l'équipe Support au travers de l'outil d'administration `PLAT'AU Support`. L'ensemble des API ont des critères de niveau 1 (rôle) et de niveau 2 (attributs).

8.1.4 Authentification via le gestionnaire d'interface applicative `PISTE`

L'ensemble des services REST offerts par `PLAT'AU API` et `PLAT'AU Notification API` le sont au travers d'un système d'API Management nommé `PISTE`.

D'un point de vue sécurité, `PISTE` prend en charge :

- L'identification et l'authentification des utilisateurs avec OAuth2 ;
- La communication de l'identité des utilisateurs à `PLAT'AU` en même temps que les appels que celui-ci souhaite soumettre sous la forme d'un jeton JWT ;
- La signature des jetons JWT ;
- La sécurité de la couche transport pour les échanges avec les applicatifs `XX'AU`.

Les identités `PISTE` et les acteurs `PLAT'AU` font l'objet d'une correspondance qui permet d'assurer une continuité de l'authentification `PIST`

E jusqu'au métier PLAT'AU .

Le jeton JWT distribué par PISTE contient un champ « not before » (voir <https://tools.ietf.org/html/rfc7519#section-4.1.5>) prévenant la décapsulation avant l'heure indiquée. Par défaut, le seuil de tolérance n'autorise pas de décalage dans le futur. Ainsi un jeton avec un champ « not before » dans le futur est refusé systématiquement.

Le SNUM a acté qu'une tolérance de maximum 10 secondes lors de la décapsulation est acceptable.

De par son positionnement en amont, PISTE participe également à la lutte contre les effets de déni de service.

Tout utilisateur doit être enrolé en pre-requis. L'enrolement correspond à un processus de validation par un tiers et est opéré par le batch d'enrolement.

8.1.5 Sécurisation par le portail Cerbère

Cerbère est un portail actuellement opérationnel au MTE. Il a vocation à permettre un accès sécurisé par les agents aux applicatifs disponibles dans le SI MTE. Il fonctionne sur la base d'un jeton d'authentification fourni par tout utilisateur accédant à PLAT'AU Support SPA (IHM) et dont la validité doit être vérifiée auprès de Cerbère.

8.1.6 Sécurisation par filtrage d'IP

Certains points d'entrée sont dédiés à un IP précis ou à une plage d'IP identifiée. Un filtrage par IP peut alors être positionné afin de limiter l'accès au service. C'est par exemple le cas pour les services n'acceptant de connexion qu'en provenance de l'API Management, qui doit donc être sur liste blanche.

9 Exigences de qualité

9.1 Fiabilité

Le système doit fonctionner sans interruption en mode nominal pour garantir la continuité des services critiques. Cela inclut l'accessibilité constante des dossiers pour les utilisateurs (pétitionnaires, agents, etc.) et le traitement des processus métiers (instruction, taxation, consultations). Une panne prolongée pourrait entraîner des autorisations tacites, des retards dans les projets de construction et une perte de confiance des utilisateurs.

La disponibilité du système repose sur plusieurs mécanismes de résilience :

- Redémarrage automatique des conteneurs applicatifs (Gestion par `ReplicaSet` depuis un `Deployment` sur environnement basé Kubernetes) ;
- Scalabilité horizontale automatisée en fonction de la sollicitation du système pour augmenter la capacité de traitement du système d'information ;
- Mécanisme de réessaie sur les opérations asynchrones ;
- Base de données et bus de message respectant une architecture haute disponibilité comportant plusieurs instances avec des capacités de redirection de charge en cas d'arrêt d'une instance.

A noter que l'infogérant propose également des mécanismes de continuité des services en cas de panne partielle ou complète de l'infrastructure.

Un indicateur de disponibilité est calculé par l'équipe support permettant de suivre, analyser et alerter.

9.2 Flexibilité

L'architecture doit permettre l'intégration maîtrisée des nouveaux domaines métiers ou des évolutions réglementaires. Cela inclut la capacité de versionner les données et de gérer des contrats de services rétro-compatibles, afin de soutenir les mises à jour progressives tout en limitant l'impact sur les utilisateurs.

La capacité d'ajout de nouveaux domaines est facilitée par :

- L'intégration d'une architecture logicielle modulaire basée sur un polymorphisme de l'ensemble des endpoints de `PLAT'AU API` ;
- La persistance des objets métiers est cloisonnée au périmètre métier ce qui limite l'impact des mises à niveau des objets métiers ;
- Une documentation de développement dédié à l'ajout de nouveaux domaines est partagée à l'équipe de développement. Ce document apporte : une liste exhaustive des actions de mutualisation et ajout de nouveaux domaines ; Propose un exemple complet d'intégration ; exprime les connaissances théoriques et conventions utilisées pour respecter cette exigence.

9.3 Sécurité

Toutes les modifications, consultations ou échanges de données doivent être tracés pour répondre aux besoins de transparence, de conformité réglementaire et de sécurité. Les données doivent être accessibles uniquement par leurs ayants droit, et toute modification doit être journalisée. Cela protège l'intégrité des données et renforce la confiance des parties prenantes.

Plusieurs mécanismes sont disponibles pour respecter ce critère de qualité :

- Cachet électronique des actions métiers par un service tiers (service horodatage) ;
- Remontée des journaux de l'ensemble des composants techniques du système d'information dans la stack de supervision (traces fonctionnelles et techniques) ;
- Les données des environnements hors production sont anonymisées ;
- Plusieurs niveaux d'authentification et d'habilitation pour accès aux données métiers.

9.4 Interopérabilité

Le système doit pouvoir s'interfacer facilement avec des systèmes tiers (SDIS, gestionnaires de réseaux, etc.) via des API standardisées. Cela garantit un échange fluide de données entre les différentes parties prenantes et permet l'ajout futur de nouvelles fonctionnalités ou partenaires sans remise en question de l'architecture existante.

Des moyens techniques et organisationnels sont mis en œuvre pour faciliter l'accès aux endpoints de **PLAT'AU** :

- Mise à disposition d'un contrat d'interface (Open API) aux éditeurs tiers ;
- Centralisation des accès via un API manager (**PISTE** , service externe au système d'information).

10 Risques et Dettes techniques

Voici une liste des risques et dettes techniques identifiés :

- Les applications reposent sur le framework Spring Boot, dont chaque version a un cycle de vie limité à 1 an, avec la publication d'une nouvelle version mineure tous les 6 mois. Il est recommandé d'effectuer une montée de version deux fois par an ;
- L'interface utilisateur du service Support s'appuie sur le framework Angular, également soumis à un cycle de vie de 1 an par version, avec une nouvelle version majeure tous les 6 mois. Il est recommandé d'effectuer une montée de version deux fois par an ;
- L'archivage des données métier n'est actuellement pas en place. La mise en service de **PLAT'AU** datant de 2019, l'implémentation d'un service de purge devra être mis en place avant ce jalon.

11 Crédits

Ce modèle est une adaptation des modèles de [Arc42](#) ([License](#)).

Principaux changements apportés :

- Regroupement des chapitres “Stratégie de solution” et “Décisions d’architectures” pour simplifier la rédaction du document et réduire les risques de redondances.

12 Annexes

12.1 Glossaire

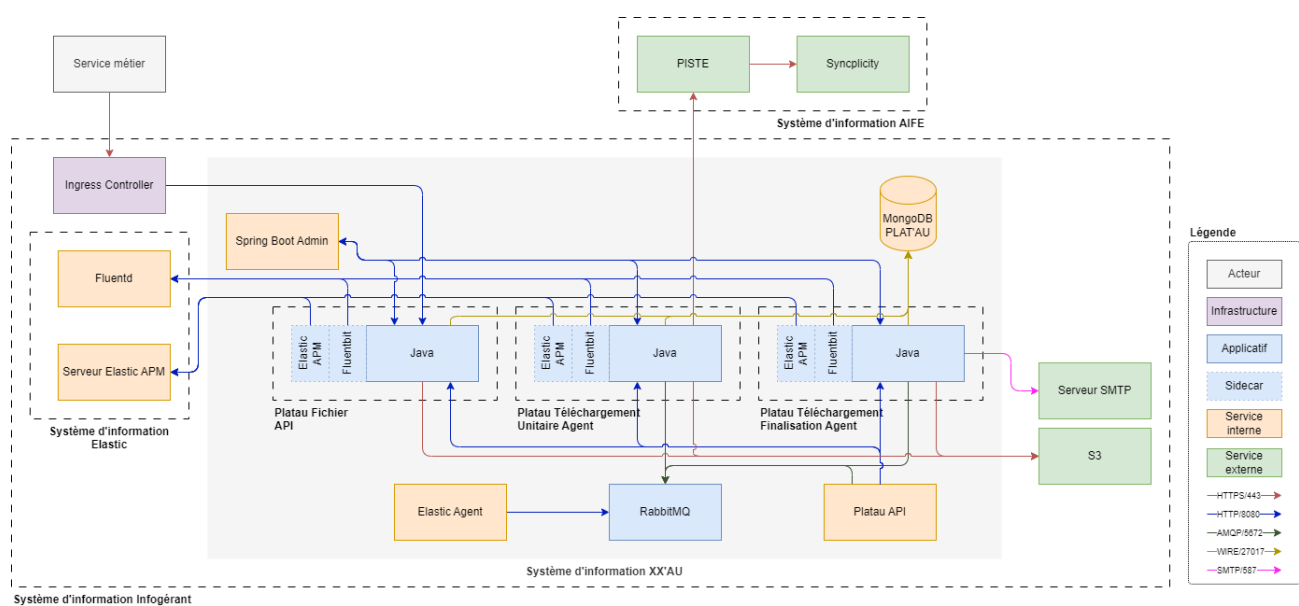
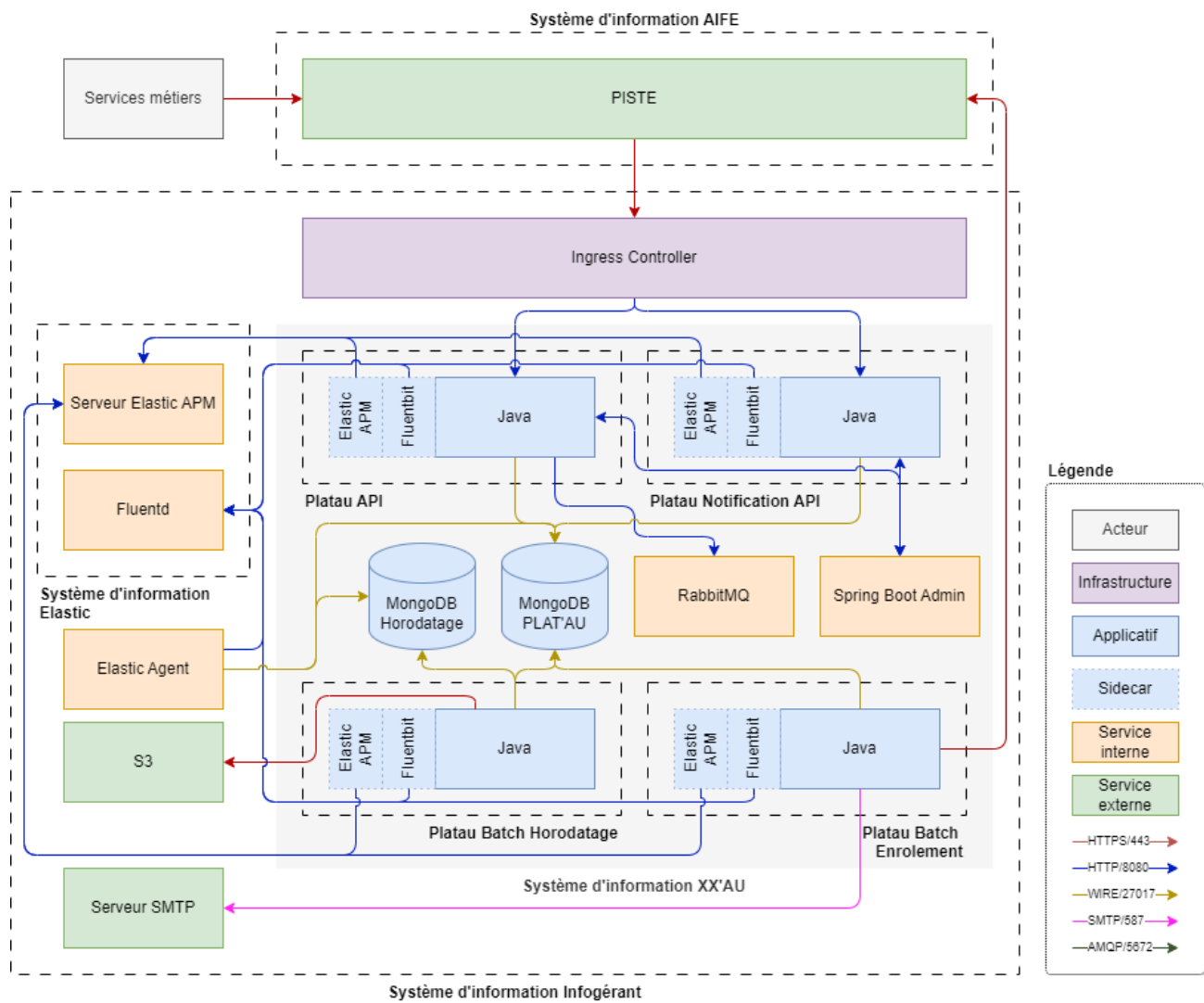
Terme	Définition
ABAC (Attribute-Based Access Control)	Gestion des droits basée sur des attributs spécifiques des utilisateurs et des objets métier, définie comme “droits de niveau 2” dans PLAT'AU .
AD'AU	Assistance aux Demandes d'Autorisation d'Urbanisme en ligne, service distinct de la suite XX'AU .
API	Interface de Programmation Applicative permettant l'échange standardisé de données entre systèmes.
AVIS'AU	Plateforme dédiée à la réception et au traitement des demandes d'avis relatifs aux Autorisations d'Urbanisme.
Batch	Processus automatisé permettant le traitement différé de données ou l'exécution d'actions spécifiques, comme l'horodatage ou l'enrôlement d'utilisateurs.
Cachet électronique	Mécanisme d'horodatage garantissant la non-opposabilité légale des actions réalisées sur les objets métiers.
Cerbère	Portail d'authentification sécurisé du MTE permettant aux agents d'accéder aux applicatifs avec un jeton validé.
DAU	Domaine des Autorisations d'Urbanisme, couvrant les processus comme l'instruction, la consultation, et les avis.
Elasticsearch	Système de recherche et d'analyse utilisé pour la gestion et la consultation des traces applicatives techniques et fonctionnelles.
FluentBit	Composant permettant l'export et la gestion des journaux applicatifs, garantissant une traçabilité centralisée.
Harbor	Dépôt sécurisé pour les conteneurs applicatifs, utilisé pour stocker et distribuer des images de conteneurs.
Horodatage	Processus d'enregistrement de la date et de l'heure d'une action, garantissant sa traçabilité.
IHM (Interface Homme-Machine)	Ensemble des moyens permettant l'interaction entre un utilisateur et un système informatique
Kaniko	Outil utilisé pour construire des conteneurs applicatifs de manière sécurisée sans nécessiter de démon Docker.
NoSQL	Type de base de données non relationnelle, adapté aux structures de données évolutives et diversifiées.
OpenShift	Plateforme de conteneurisation utilisée pour le déploiement distribué des applications de PLAT'AU .
PISTE	Plateforme d'Interopérabilité des Systèmes d'Échanges, utilisée pour exposer les API du système d'information.
PLAT'AU	Plateforme des Autorisations d'Urbanisme, outil central pour le partage et l'horodatage des flux dématérialisés.
RBAC (Role-Based Access Control)	Gestion des droits basée sur les rôles attribués aux utilisateurs, définie comme “droits de niveau 1” dans PLAT'AU .
RIE'AU	Réception, Information et Échanges des Autorisations d'Urbanisme, outil pour les communes compétentes ou non.
S3 (produit Swift)	Solution de stockage massif de fichiers offrant résilience et haute disponibilité, intégrée au système PLAT'AU .
S3	Service de stockage massif de fichiers, offrant une résilience et une haute disponibilité.
SDIS	Service Départemental d'Incendie et de Secours, acteur potentiel des consultations dans les dossiers.
SITADEL	Système de gestion des données statistiques sur les permis et autorisations d'urbanisme.
SPA (Single Page Application)	Application web qui charge une seule page HTML et met à jour dynamiquement son contenu via JavaScript

Terme	Définition
SPF/DMARC	Protocoles de validation des courriels pour prévenir les falsifications d'expéditeurs et garantir l'authenticité des messages électroniques émis.
STARTTLS	Protocole permettant d'assurer le chiffrement des échanges SMTP pour sécuriser les communications électroniques.
Stateless	Caractéristique des services sans état transactionnel, facilitant leur scalabilité horizontale.
XX'AU	Suite logicielle dédiée aux Autorisations d'Urbanisme, incluant les produits <code>PLAT'AU</code> , <code>RIE'AU</code> , <code>AVIS'AU</code> et <code>AD'AU</code> .

12.2 Points ouverts

Date	Sujet
Janvier 2025	Il est noté dans le précédent DAT le besoin d’archivage au bout de 10 ans des données métiers. Aujourd’hui cela n’est pas implémenté et ajouté comme risque dans ce DAT
Janvier 2025	Il est noté dans le précédent DAT un besoin de purge des traces fonctionnelles et techniques au bout d’un an. Aujourd’hui la purge des traces est effectuée au bout de 4 mois (géré par Elastic). La contrainte doit-elle être revue ?
Janvier 2025	Les schémas d’architecture technique détaillés semblent mieux représenter les adhérences entre les conteneurs applicatifs. La vue C4 étant difficilement lisible / complète. Sopra Steria préconise de passer sur un schéma hors C4 pour la vue “conteneur”

12.3 Architecture technique détaillée



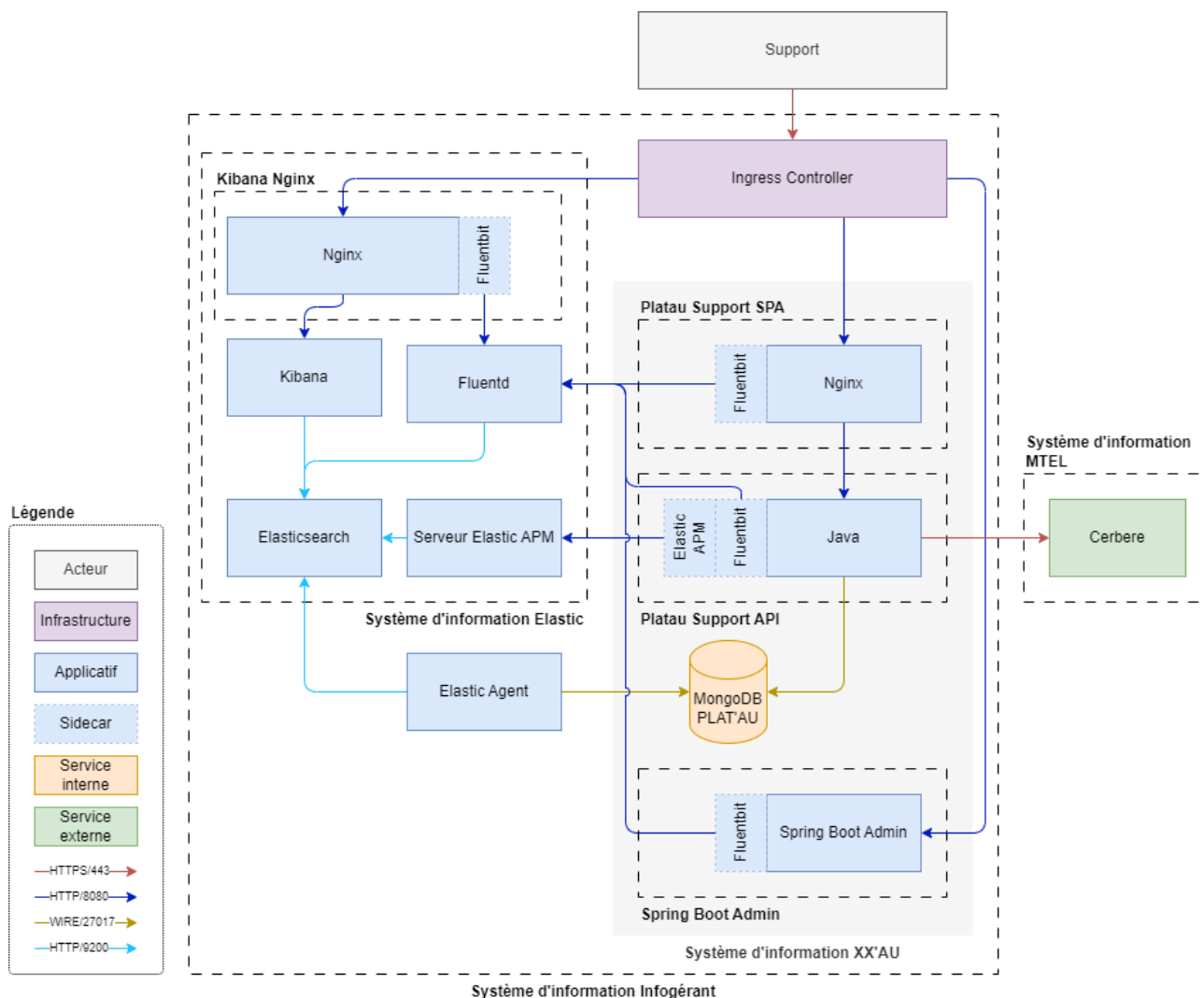


Schéma d'architecture technique de **PLAT'AU Support & Observabilité**