

Dans ce cours mémoire, je parle de mon expérience professionnelle vécu au sein de la société de service XLM Aéro.

Mes principales missions étaient au nombre de 3 et sont succinctement évoquées dans le chapitre **2.1 Mes missions**. Puis j’entre plus en détails dans les chapitres qui suivent (**2.2, 2.3 et 2.4**).

Table des matières

[XLM Aero 4](#_Toc51341349)

[Mon expérience 4](#_Toc51341350)

[Mes missions 4](#_Toc51341351)

[KEOPS 4](#_Toc51341352)

[Contexte 4](#_Toc51341353)

[Démarche de travail 4](#_Toc51341354)

[Architecture 7](#_Toc51341355)

[Mise en œuvre 8](#_Toc51341356)

[Crew Web Access 9](#_Toc51341357)

[Contexte 9](#_Toc51341358)

[Mise en œuvre 9](#_Toc51341359)

[Crew Mobile Access 10](#_Toc51341360)

[Contexte 10](#_Toc51341361)

[Démarche de travail 10](#_Toc51341362)

[Conception 10](#_Toc51341363)

[Architecture 10](#_Toc51341364)

[Mise en œuvre 10](#_Toc51341365)

[Conclusion 11](#_Toc51341366)

# XLM Aero

XLM Aéro a été fondé en 2010 suite à l’acquisition du logiciel **KEOPS**.

# Mon expérience

## Mes missions

Au sein **d’XLM Aéro** je me suis vu confié 3 missions :

* Maintien et amélioration de **KEOPS**
* Mise à niveau et correction de failles de sécurité du portail web **Crew Web Access**
* Conception et développement d’un nouveau module : **Crew Mobile Access**

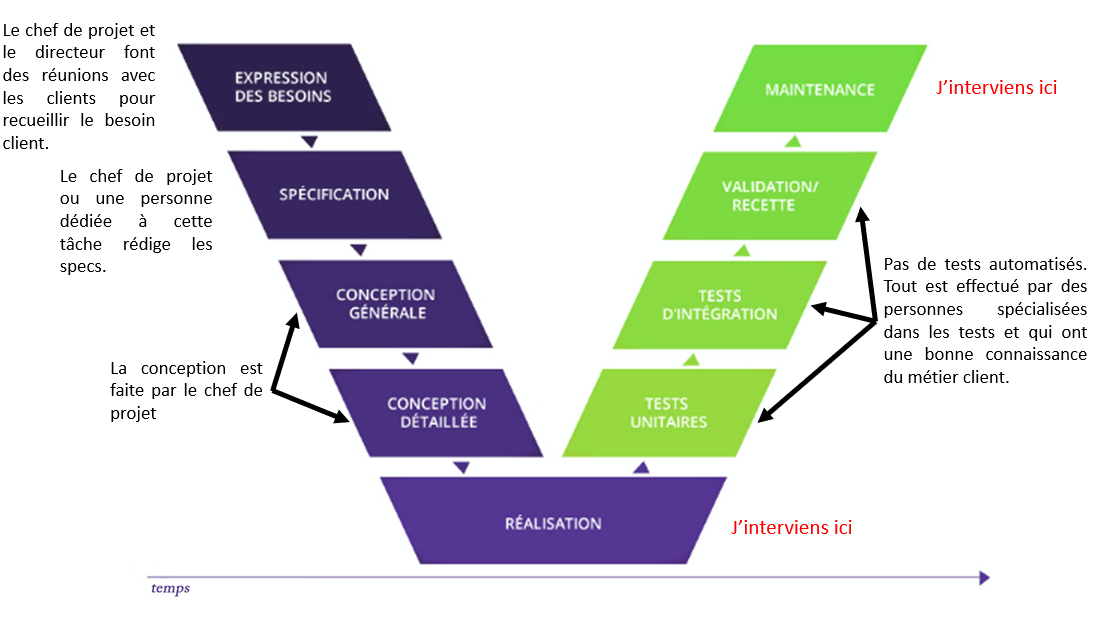
## KEOPS

### Contexte

KEOPS est une application de gestion des flottes et des coûts pour les compagnies aériennes. C’est tout un écosystème de modules qui offrent une multitude de service. Ces modules sont pilotés par le biais d’une application bureau développée en Java avec EMF (Eclipse Modeling Framework).

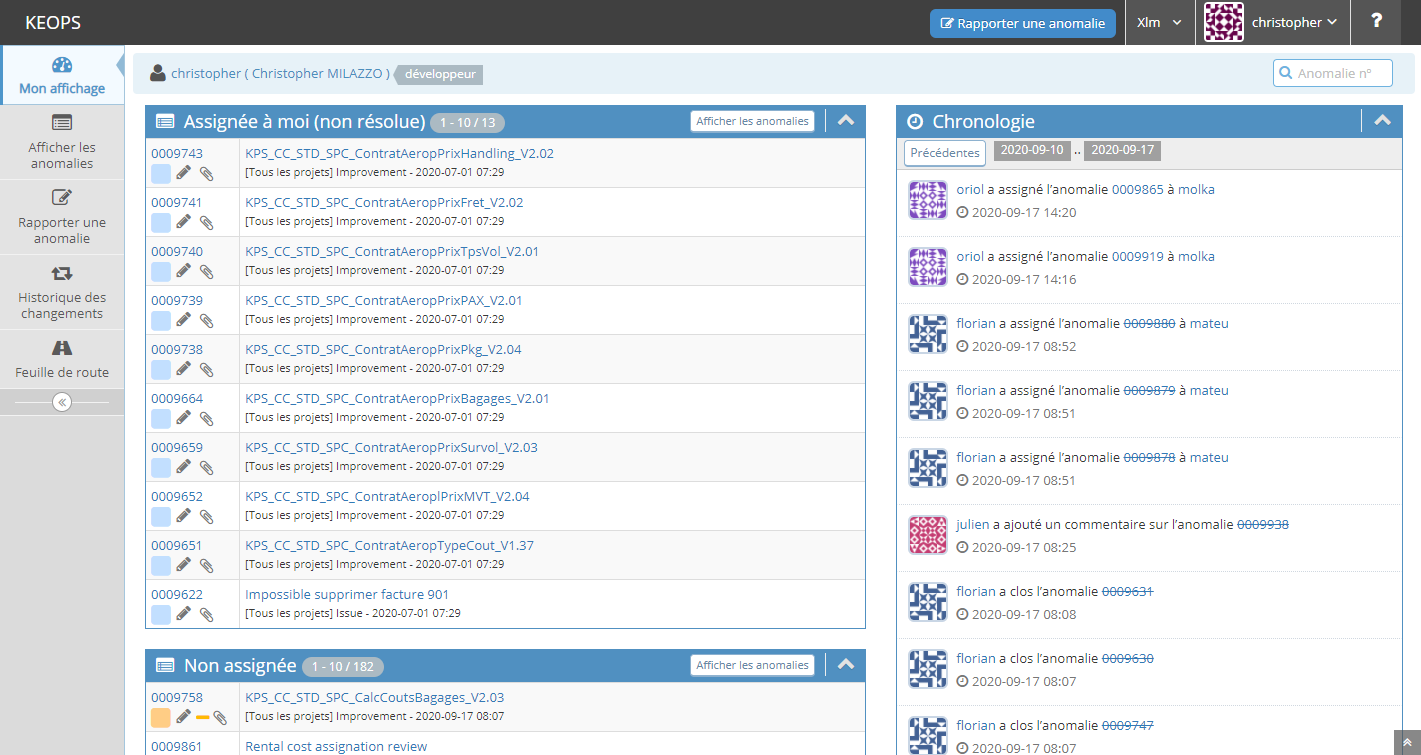
### Démarche de travail

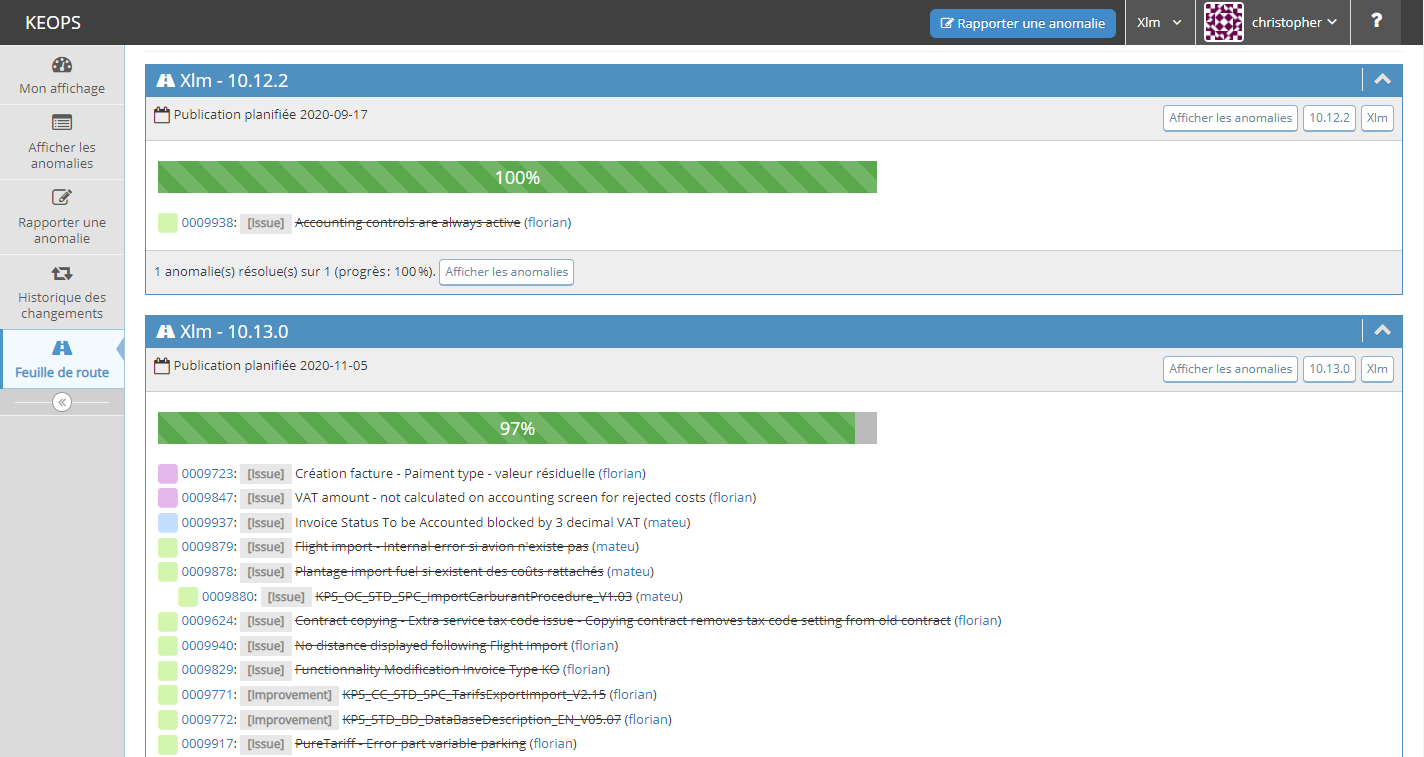
Le projet KEOPS suit la méthodologie classique (cycle en V) de la manière suivante :



*Figure 1*

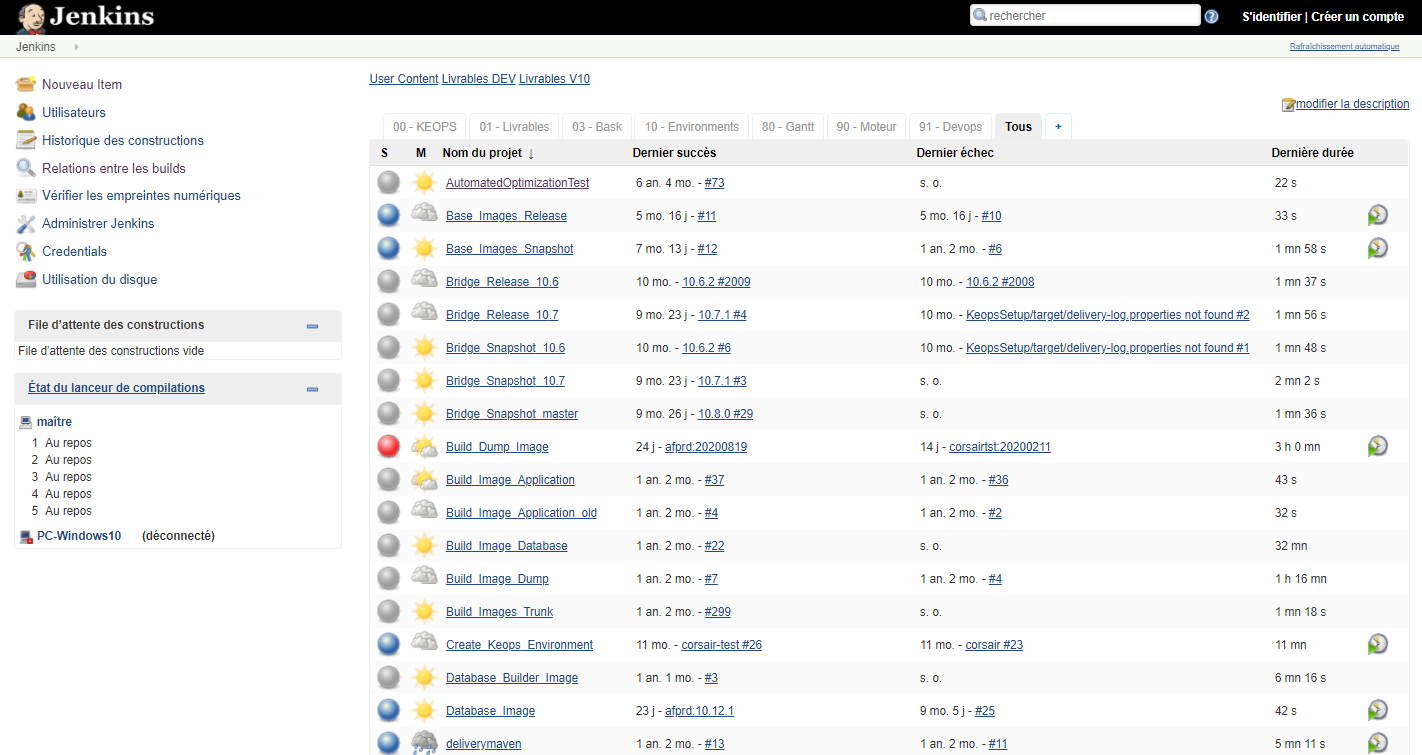
Pour la partie ‘issue tracking’ Mantis est utilisé. Cela permet au chef de projet d’avoir une vision global sur la roadmap et de pouvoir affecter les développements/corrections aux développeurs :

 *Figure 2*



*Figure 3*

Le projet ne compte pas de pipeline (au sens de ‘devOps’), il n’y a pas de contrôle qualité du code ou de tests unitaires lancés automatiquement. En revanche les builds sont tous automatisés par le biais de Jenkins :



*Figure 4*

### Architecture

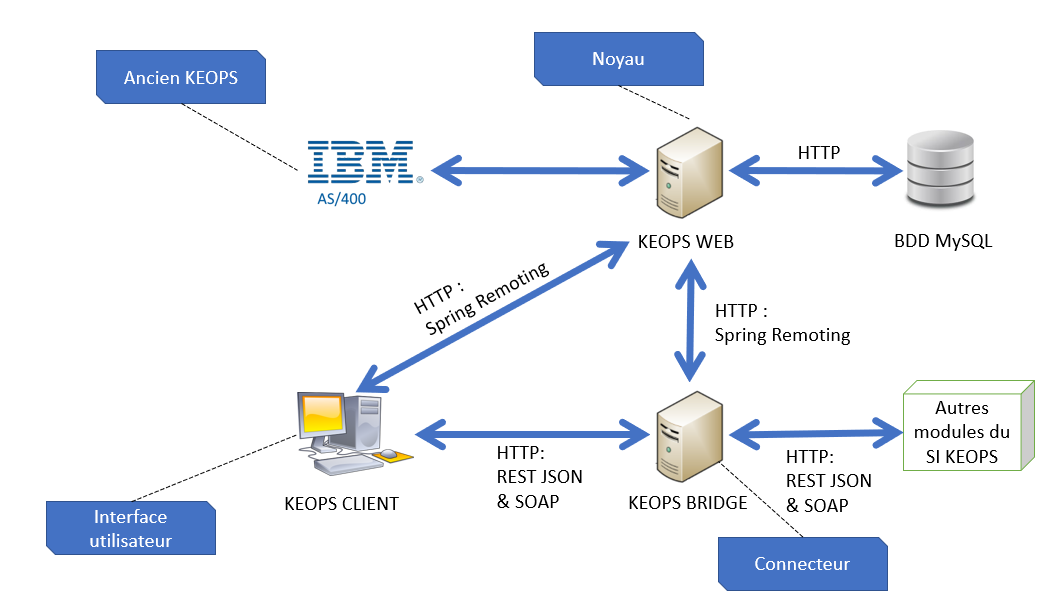
Le projet KEOPS date de 1987, à l’époque il fonctionnait sur AS400.

En 2006, la couche service (business layer) est modernisé et deviens un service backend en JAVA 1.6 et communique via HTTP en Spring Remoting.

En 2010, avec l’évolution de Java, il a été entrepris une refonte de l’interface utilisateur en technologie Java avec l’Eclipse Modeling Framework.

L’AS400 est maintenu pour certains clients, toutefois, afin de faire évoluer KEOPS et de proposer une interface plus récente (KEOPS CLIENT), il a fallu créer un connecteur (KEOPS BRIDGE) capable de faire du REST et du SOAP tout en maintenant la communication avec le noyau (KEOPS WEB).

L’architecture physique de KEOPS peut se résumer ainsi :



*Figure 5*

### Mise en œuvre

## Crew Web Access

### Contexte

Crew Web Access est un portail WEB qui vient se greffer au SI de KEOPS par le biais de l’AS400 (voir *Figure 5*).

C’est un portail permettant aux PN (Personnel Naviguant) de consulter leur planning, de recevoir des notifications (des messages) de la part de la compagnie et de communiquer des désidératas en matière de congés et d’activités sur le planning.

### Mise en œuvre

Lors d’une campagne de tests d’intrusion sur le portail « Crew Web Access » menée fin 2019, il a été découvert 4 failles majeures, listées ci-dessous, que j’ai eu à corriger :

• R13 – Mettre à jour la solution Crew. L’application doit contrôler la session et les droits de l’utilisateur avec la valeur du paramètre txtActId utilisé par plusieurs fonctions de l’application.

• R5 - Implémenter une politique de mot de passe robuste.

• R14 – Retourner un message d’erreur générique en cas d’échec d’authentification. Par exemple, le message suivant peut être retourné par l’application après un échec d’authentification : « L’identifiant ou le mot de passe sont incorrects. »

• R17 – HTTPS. Rediriger tous les flux HTTP vers le service Web correspondant en https en modifiant la configuration des serveurs applicatifs.

De plus, il a fallu migrer le code source en PHP4 vers PHP7 afin de le faire tourner sur des serveurs à jour pour limiter les failles de sécurité.

## Crew Mobile Access

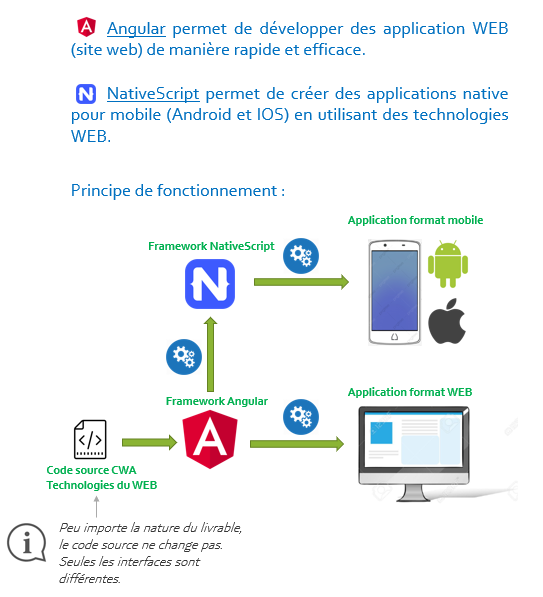
### Contexte

Crew Mobile Access est une refonte du **Crew Web Access**. Il permet de fournir les mêmes services que le portail Crew Web Access mais sout forme d’application mobile. Cela permettra aux PN (Personnel Naviguant) d’accéder au planning directement à partir du téléphone de manière plus ergonomique.

Le Crew Mobile Access est un service qui vient se gréffer au SI KEOPS par le biais du KEOPS BRIDGE (voir *Figure 5*).

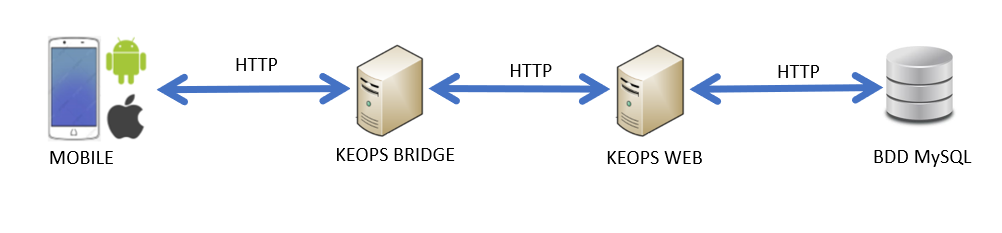
### Démarche de travail

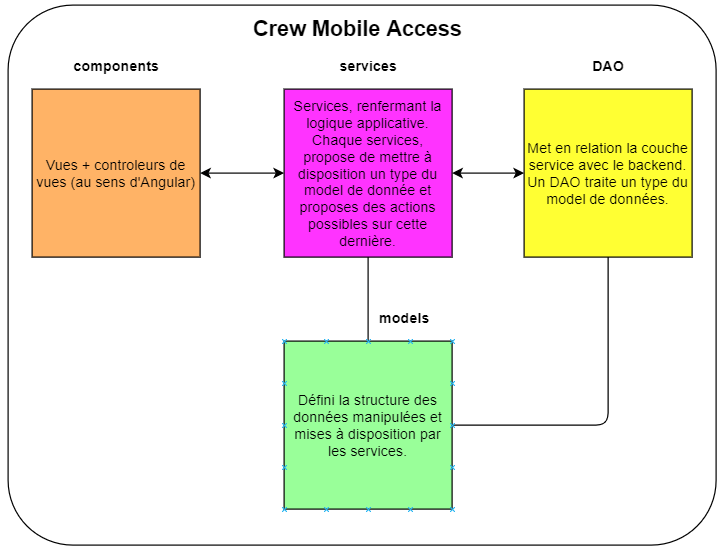
### Conception



### Architecture

Pour des raisons de compatibilité, le Crew Mobile Access ne communique pas directement au Web Service de KEOPS. En effet, le KEOPS BRIDGE est là pour jouer un rôle de connecteur entre les services nouvelle génération et le noyau de KEOPS : KEOPS WEB.





### Mise en œuvre

# Conclusion