## Compte-rendu de la réunion du 08/03/2016

**Réunion n°3**

Lors de cette réunion nous avons déterminé deux points. D’une part, nous avons précisé le système d’authentification et d’autre part nous avons déterminé ce que le mail envoyé par le professeur devait contenir.

### Participants :

Rémi Morin, Clément Akriche, Mouna El Farissi, Fabio Zerilli.

### Ajout de fonctionnalités de l’application Professeur

L’application côté professeur pourra désormais :

* Calculer le résumé MD5 de l’application Etudiant.
* Créer le .jar de l’application Etudiant.
* Inclure dans le .jar le résumé MD5 et la clef publique du professeur.
* Joindre le .jar de l’application Etudiant dans le mail envoyé par le professeur.

### Contenu du mail envoyé

Il a été précisé lors de cette réunion le contenu du mail envoyé par le professeur à ses étudiants :

* Le fichier .jar de l’application Etudiant avec :
  + La clef publique du professeur.
* Un explicatif concernant l’exécution d’un .jar par l’étudiant(e).
* Un texte décrivant la démarche à suivre pour l’authentification concernant :
  + La note (fait par l’application Etudiant)
  + Le .jar (calcul d’un résumé MD5)
* La note cryptée + la signature du professeur.

### Authentification

Pour l’authentification du .jar, nous sommes restés sur la comparaison du MD5 donné par le professeur et le MD5 du .jar calculé par l’étudiant(e).

Pour l’authentification de la note, nous passons par une signature. Pour des questions de simplicité pour la communication de la clef secrète nous avons choisi le système d’AES pour la signature (nous passons d’une clef de 32 octets à une de 16).

Nous avons émis l’hypothèse d’une clef commune pour les deux authentifications précédentes, pour une communication plus simple étant donné que les deux clefs font plus ou moins la même taille. Il faudra décider de notre choix en fonction des enjeux puisqu’une seule clef augmente grandement les risques d’intrusion.

### Objectifs pour cette itération

Réalisation de :

* Cahier des charges
* Diagrammes de séquence
* Diagrammes de cas d’utilisation