

# Compte-rendu de réunion client du 13/02/14

## 1 Présents

- Ayoub Otmani (client)
- Pascal Edouard
- Claire Smets
- Julien Legras (Réd. CR)
- Mathieu Latimer
- William Boisseleau

## 2 Objet

Ce document reprend les points évoqués durant la réunion du 13 février 2014 avec le client. Il s'agissait de faire un point sur ce qui a été audité depuis le début du sprint pour savoir quels points devaient être approfondis.

## 3 Contenu abordé

Sujet	Actions à entreprendre	Assignment	Date limite
L'aléatoire	Ne pas implémenter des tests mais plutôt tester la génération de l'aléatoire dans openssl avec des outils comme diehard	Pascal, William	20/02/2014
OAEP	Analyser le procédé de la Manger's attack	Mathieu, William	20/02/2014
SSL	Tester s'il est possible de forcer l'utilisation d'un algorithme faible	Julien	20/02/2014
Rapport d'audit	<ul style="list-style-type: none"><li>— Décrire l'idée synthétique des attaques trouvées</li><li>— Conclure sur une politique de bonnes pratiques et donner des solutions et alternatives à openssl</li></ul>	Équipe	20/02/2014