

# Compte-rendu de réunion, 4

Florian GUILBERT

21 janvier 2013

## Participants :

- Magali BARDET (cliente);
- Zakaria ADDI;
- Baptiste DOLBEAU;
- Yicheng GAO;
- Florian GUILBERT;
- Giovanni HUET;
- Emmanuel MOCQUET;
- Maxence PÉCHOUX.
- Romain PIGNARD.

## Absents :

Pas d'absents.

## Ordre du jour : présentation de la STB, planning, analyse des risques

Pour tout : préciser si c'est les clefs privées de signature ou clef publique de chiffrement

### 1. Remarque sur la STB

- Génération nombre aléa : indistinguable en temps polynomial, distribution de probabilité uniforme.
- Tests : vérifier l'uniformité de l'aléa mettre la notion/définition d'aléa dans la terminologie
- Code PIN : description à changer par : "authentification de l'utilisateur auprès de la carte par code PIN"
- Rendre les cas d'utilisations plus génériques.
- Blocage de la carte : par paramètre (5 min exemple) + utilisation d'un code "PUK" pour déverrouiller la carte.
- Algo qui vérifie le code PIN doit être résistant aux attaques (par canaux cachés) et doit être lent  
→ à mettre dans les exigences fonctionnelles
- "Authentification sur SocialNetwork" : remplacer par "Transmission" précondition : smartcard s'authentifie auprès de FaceCrypt
- Réfléchir au choix clef publique/clef privée ou clef partagée
- C3 + C4 : à revoir, authentification qui ne concerne pas l'utilisateur va dans les exigences
- C6 : envoi de la clef publique et l'algo de chiffrement, pas besoin d'un certificat ?
- Vérification du certificat ! Le chiffrement de la clef de message fait par FaceCrypt, donc C6 à enlever.
- Exigence opérationnelle : changer F-FO-20 par "on doit être capable de vérifier que le nombre est bien aléatoire"
- Exigence de qualité : notion de rapidité de chiffrement/signature à fournir (Indispensable) (pareil pour facebook)

**2. Remarque sur le Plan de développement** Dernière répétition avec Mme Bardet possible le vendredi 22 février

**3. Analyse des risques** Inverser la description et le facteur pour le retard, pareil pour l'apprentissage.

## **Prochaine réunion**

Vendredi suivant.