Compte-rendu de réunion, 6

Florian Guilbert, Emmanuel Mocquet

06 février 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 : discussion à propos de la spécification technique des besoins

1. Remarque sur le STB

- Fusion de deux sous-projets → composé de deux sous-projets
- Il faut définir "sécurisé" dans la terminologie (chiffrement, intégrité) Le client exige que "sécurisé" comprenne l'intégrité.
- Donc : utilisation d'un code MAC pour le tunnel entre la carte et le PC. Possibilité de tronquer le code MAC si nécessaire (mais justifier)
- Définir "un générateur de nombre aléatoire"
- La priorité va à la vérification de l'intégrité qu'à la vérification de l'aléatoire.
- "La carte doit être capable de générer un nombre aléatoire" → "ON" doit être capable d'utiliser le générateur.
- PRN → à remplacer par RN ("fourni par la carte")
- nouveau use case : administration de la carte en permettant à l'utilisateur de fournir/changer ses identifiants
- Déchiffrement : flot d'exception : uniformiser les messages d'erreurs
- chiffrement : avec clef secrète à la place de "privée"
- vérification de données par softcard pas par smartcard
- Livraison le 1er mars.

Prochaine réunion

Vendredi 8 février à 11h.