

Université de Rouen	Compte Rendu Réunion n° 3 10/11/2014	Projet_PGP
---------------------	---	------------

Contexte : Première présentation de la STB au client.

Auteurs : Olivier THIBAUT & Bertille BOUILLIE

Présence du groupe

Nom	Présent / Absent
BALMELLE Pierre	Absent
BARBAY Lucas	Absent
BARRY Ibrahima Sory	Présent
BOUILLIE Bertille	Présente
FIN Matthieu	Présent
LEROY Guillaume	Absent
THIBAUT Olivier	Présent

I. Actions

Chargé client – 16/11

- Reformuler « Résultat attendu » : document rapport d'attaque + implémentation de l'attaque.
- Séparer « modification paramètres : indispensable » et « Toile de confiance : important ».
- Livrable sous forme de paquet Linux.
- Ajouter signature/vérification via une zone de texte.
- Dans le cas d'utilisation « chiffrement », renseigner la clé du destinataire et plutôt que le destinataire (car il peut posséder plusieurs clés).
- Dans « affichage des commandes », le flux textuel sortant de GPG doit aussi être affichée.
- Modifier le cas d'utilisation « modif param : ordre de préférence » inclus dans « action GPG ».
- Ajouter en exigence opérationnelle la possibilité d'ouvrir deux instances de l'interface sur une même session avec deux fichiers de config différents.
- Ajouter en exigence « SSH : authentification par clé signée via GPG : optionnel ».
- Affichage du maximum d'info sur chaque clé (sous-clés, email, contenu textuel de la ou les clé(s)).

II. Autres sujets

- Attaque des KeyId : Déposer clé + clé « attaque » sur un serveur, puis regarder ce que le serveur propose lors de la recherche de la clé. Question : est-il possible d'imposer au serveur d'afficher une clé en priorité ?
- Modification du niveau de confiance, influence sur les clés signées ? Tout est géré par la commande update plus profondément que la clé modifiée dans l'arbre.