

Projet PGP

Étude et implantation d'un outil graphique de gestion de clé PGP



Compte rendu - Réunion Client

23 avril 2015

Contexte: Livraison 2

Auteur(s): Matthieu FIN

| Nom | Prénom | Présence |
|----------|---------------|----------|
| BALMELLE | Pierre | Présent |
| BARBAY | Lucas | Présent |
| BARRY | Ibrahima Sory | Présent |
| BOUILLIE | Bertille | Absente |
| FIN | Matthieu | Présent |
| LEROY | Guillaume | Absent |
| THIBAUT | Olivier | Présent |

1 Sujets

1. La spécification technique du besoin nécessite quelques modifications :
 - Dans l'objet l'équipe est composée de sept personnes.
 - Ajouter les nouvelles fonctionnalité dans la STB (chiffrement/déchiffrement et vérification de signature d'un fichier).
 - Le Cas d'utilisation 1 : Reformuler la description (l'application fait interface entre l'utilisateur et gpg).
 - Cas d'utilisation 2 : Il y a deux fois l'expression "dans son trousseau".
2. Retour sur l'application guipg Actions a terminer pour validation de l'application :
 - Il faut pouvoir signer une clé quand il y a plusieurs uid attaché a cette clé (on signe alors tous les uids de la clé).
 - Avant de signer une clé il faut afficher les informations de la clé que l'on va signer (fpr, uid, nom, commentaire, email).
 - Chiffrement de fichier : Il faut pouvoir sélectionner plusieurs destinataires (uid).
 - Mettre le fichier de configuration de l'application dans `/.guipgconf.xml` (déjà opérationnel)
3. Étude : Non validée en l'état.
4. Attaque : Non validée en l'état.

2 Actions

1. Préparation d'un rapport final pour le 22/05/2015 (Olivier, Matthieu, Pierre, Lucas, Ibrahima).
 - Ce rapport servira a préparer la soutenance.
 - Il doit donc rappeler le projet initial, les différentes étapes/problèmes/solutions traversé.
 - Présenter les différents aspects techniques.
 - L'état du projet final.
 - Retour d'expérience.
2. Les modifications de la STB doivent être faite pour le 24/04 (Olivier).
3. Les modifications de l'application doivent être faite avant le 30/04 (Olivier, Matthieu).
4. Modifier le CDR (Pierre, Lucas)
 - Indiquer que le test sur les signature ne fonctionne pas.
 - Réaliser de nouveaux tests pour s'assurer des dernières fonctionnalités.
 - Prévoir des tests concernant l'attaque.
5. Étude (Ibrahima)
 - La finaliser au plus vite pour l'envoyer sur la liste de diffusion (Ibrahima).
 - Tenir compte des retours.
6. Attaque (Lucas)
 - Fournir une clé et sa seconde pré-image forgée grâce au script.
 - La seconde pré-image doit être valide et utilisable par gpg.