Univ. Grenoble Alpes **2016–2017**
M2 GI : Cours Cybersécurité

TP2 : Travaux pratiques sur GnuPG et applications signatures/chiffre

1. Familiarisez vous avec les versions 1.4 et 2.1 de GnuPG. Notamment «signatures» et «chiffrements».
2. Créer une clef GPG RSA de 4096 bits associée à votre adresse de messagerie avec GPG 1.4 (ou 2.1 si vous ne disposez que de cette version) dont la limite de validité sera le 8 juillet 2017. Exporter au format «armored» votre clef publique.
3. Signer avec votre clef le document PDF «bonnes pratiques» de l'ANSSI et m'envoyer la signature.
4. Déchiffrer le fichier en .gpg avec le mot de passe «What_is_it» et retrouver le fichier «caché».
5. Chiffrer et signer avec votre clef un document vide «toto.txt» (généré avec touch). Observer la taille du fichier chiffré signé. Vérifier la signature du fichier.
6. Créer un certificat de révocation pour votre clef.