Ref : 0011@2024-nov-27@08h40-CET@sc ; Author : Serge Chaumette

ASPIC / Drones, systèmes télé-opérés, essaims

Fiche de TD / Sécurité des systèmes de drones et des essaims de drones

Serge Chaumette

PKI

Dans ce TD on s'intéresse à la **conception et** à la **mise en œuvre d'une infrastructure d'horodatage**. Une telle infrastructure permet à un utilisateur Alice d'obtenir un horodatage d'un document *doc* à la date courante (*date_dépôt*) tout en le gardant confidentiel. Elle obtient une *preuve* qu'elle peut ensuite transmettre à une autre personne, Bob, qui pourra vérifier que Alice avait bien déposé (et donc avait créé) *doc*, à la date *date_dépôt*.

Votre travail sera à rendre sur le web dans le fichier ue-dste/securite-pki/

Exercice 1 : schéma d'architecture et diagramme de séquence

Concevez l'architecture de l'infrastructure proposée sous la forme d'un schéma global, puis décrire les interactions des différents intervenants sous la forme d'un diagramme de séquence simplifié à la UML, et ce pour les différentes opérations possibles (dépôt, vérification, etc.).

Informations potentiellement utiles :

- Diagramme de séquence : voir par exemple
  https://www.ibm.com/docs/fr/rsm/7.5.0?topic=uml-sequence-diagrams
-

Exercice 2 : mise en œuvre

Réalisez une mise en œuvre de votre architecture. Le langage recommandé est Java du fait des bibliothèques disponibles, mais libre à vous de faire un autre choix.

Informations potentiellement utiles :

- Chiffrement en Java
  https://java.developpez.com/sources/?page=cryptage

- Hashage MD5 en Java
  https://www.baeldung.com/java-md5

Exercice 3 : utilisation

Concevez et déroulez un scénario d'utilisation de votre architecture mettant en évidence une création d'horodatage et une opération de vérification de cet horodatage.