Architecture Logicielle

Version	1.0
Date	28 novembre 2013
Rédigé par	Yves Nouafo
Relu par	
Approuvé par	Magali Bardet

MISES À JOUR

Version	Date	Modifications réalisées
1.0	28/11/2013	Création

Table des matières

1 Objet

Ce document met en évidence les éléments et les évènements qui interviendront dans la mise en place du transchiffrement. L'ensemble des composants formeront l'architecture du procédé que l'on va mettre en place. Chaque composant sera implanté de manière indépendante mais pourra communiquer avec les autres en respectant les critères suivants :

- Les connexions client / proxy et proxy / serveur seront chiffrées
- L'exécution du transchiffrement au niveau du proxy devra être rapide
- L'autorité intermédiaire doit signer les certificats auxquels le client veut se connecter
- Rechercher en parallèle des collisions MD5 et forger si possible un faux certificats

2 Documents applicables et de références

- STB (Spécification Techniques des besoins]
- MD5 considered harmful today (creating a rogue CA certificate) [Alexander Sotirov, Marc Stevens, ... 2008]

3 Terminologie et sigles utilisés

- IGC : Infrastructure de Gestion de Clés
- AC : Autorité de certification
- BDD : Base de données

4 Configuration requise

4.1 Performances du calculateur

- 2Go de RAM
- Intel Celeron
- Machine virutelle ? ? ?

4.2 Système d'exploitation

- Ubuntu serveur

4.3 Produits logiciels nécessaires

5 Architecture statique

5.1 Structure

Les principales parties à développer :

- L'application client-serveur : le proxy
- Le serveur : la fausse autorité intermédiaire
- Les données : base de données contenant les clés publiques des entités

5.2 Description des constituants

	Proxy
Rôle	Réalise le transchiffrement
Propriétés et attributs de caractérisation	Déchiffrement et rechiffrement des messages
Dépendances avec d'autres constituants	navigateur web client, fausse AC, base de données de la fausse A
Langages de programmation	Java, perl ? ? ?
Procédé de développement	établissement de fonctionnalités, schématisation des fonctionnalit
Taille complexité	35% du projet, complexité du à l'efficience du programme et à la