Étude et mise en oeuvre de solutions d'authentification et de signature par cartes à puce

(Client: Mme Bardet)

Les solutions d'authentification fortes basées sur des supports type cartes à puce sont de plus en plus utilisées. Dans ce projet, on se propose d'étudier les solutions cryptographiques pouvant permettre l'authentification ou la signature, puis de mettre en oeuvre une ou plusieurs de ces solutions sur un support cartes à puce.

Les livrables demandés

- Un document technique de présentation des solutions cryptographiques étudiées.
- Une applet Java pour une carte et une application cliente communiquant avec la carte, mettant en oeuvre une ou plusieurs des solutions étudiées.
- Une documentation de votre outil et de votre code.

Outils et bibliographie Vous aurez à votre disposition pour la partie implantation des cartes Java Card J3A (marque NXP) avec 40K d'EEPROM et des lecteurs Omnikey 3121.

Les cartes sont conformes aux standards Java Card 2.2.2 et Global Platform 2.1.1.

Vous pourrez utiliser sous Eclipse le plugin jcde [1] qui permet de coder des API javacard (et qui propose un simulateur de test). L'outil GlobalPlatform [2] permet d'installer/supprimer/gérer des applets sur une javacard selon le standard globalplatform.

Les lecteurs sont compatibles PC/SC (Personal Computer/Smart Card). L'application cliente pourra être codée en utilisant par exemple l'API PCSC-lite[5] pour la communication avec la carte.

Références

[1] Plugin JCDE d'Eclipse. `http://sourceforge.net/projects/eclipse-jcde`.

[2] Standard GlobalPlatform. `http://sourceforge.net/projects/globalplatform/`.

[3] *Cartes à puce. Administration et utilisation*, LINUX Magazine Hors-Série n° 39. Diamond Editions, Nov./Déc. 2008.

[4] *Cartes à puce. Découvrez leurs fonctionnalités et leurs limites*, MISC Hors-Série n° 2. Diamond Editions, Nov./Déc. 2008.

[5] PC/SC. `http://pcsclite.alioth.debian.org/pcsclite.html`.