Cryptographic library for chip cards

Nicolas MINNIG

Travail de Bachelor 2020
Informatique - Développement Logiciel et Multimédia
Professeur: Ninoslav MARINA
Expert: Johan CHAVAILLAZ

Description

SIX Payment Services traite chaque jour des millions de transactions provenant de paiements par carte.

Toutes les cartes utilisées en Suisse sont dotées d'une puce qui sécurise leurs transactions. Ces puces sont basées sur une norme internationale pour la sécurité des cartes de paiement appelée EMV.

Le but du projet est de créer une simulation de ces cartes en mettant en œuvre le système cryptographique basé sur la documentation officielle.

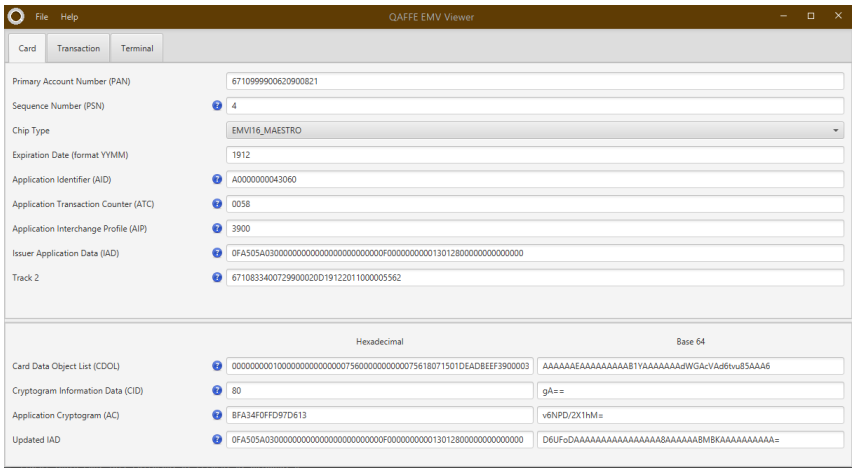
Cette simulation, sous forme de bibliothèque Java implémentant les spécifications EMV ainsi que celles de SIX Payment Services, sera utilisée dans les tests systèmes.

Résultats

La bibliothèque Java qui implémente la cryptographie de la spécification EMV a été créée et testée.

Elle a été conçue pour être aussi facile que possible à maintenir et mettre à jour.

L'interface graphique conçue pour simplifier la visualisation et la génération des données EMV a été mise à jour pour utiliser la nouvelle bibliothèque et a également été améliorée.



GUI pour la bibliothèque EMV

Déroulement

Les phases importantes du projet sont les suivantes :

- Compréhension de la spécification EMV.
- Compréhension de la cryptographie lors de la génération de l'Application Cryptogram.
- Analyse des besoins de l'entreprise.
- Analyse des cas d'utilisation business devant être testés.
- Obtention des données et création des tests.
- Conception de l'architecture de la librairie.
- Implémentation de la spécification EMV et des spécificités de l'entreprise en Java.
- Mise à jour de l'interface graphique existante.

Perspectives

Cette librairie permet à l'entreprise d'améliorer ses tests systèmes par la vérification de la cryptographie des cartes à puce.

La principale perspective future est la création d'une API REST permettant une utilisation encore plus facile dans les tests systèmes de l'entreprise.