Smart Social Network - Projet de Master 2 SSI

Zakaria Addi Baptiste Dolbeau
Yicheng Gao Florian Guilbert
Giovanni Huet Emmanuel Mocquet
Maxence Péchoux Romain Pignard

Université de Rouen

1er mars 2013

Plan

Contexte

SmartCard

titi

Secure Social Network

toto

Gestion de projet

Introduction

Rappel sur la carte à puce

stockage et traitement d'infos de base assure authentification

Qu'est-ce que Java Card ?

- Désigne techno permettant dev applets "sécurisées" sur carte à puce
-
  - carte à puce programmable
  - carte à puce multi-appli

Fonctionnement

APDU

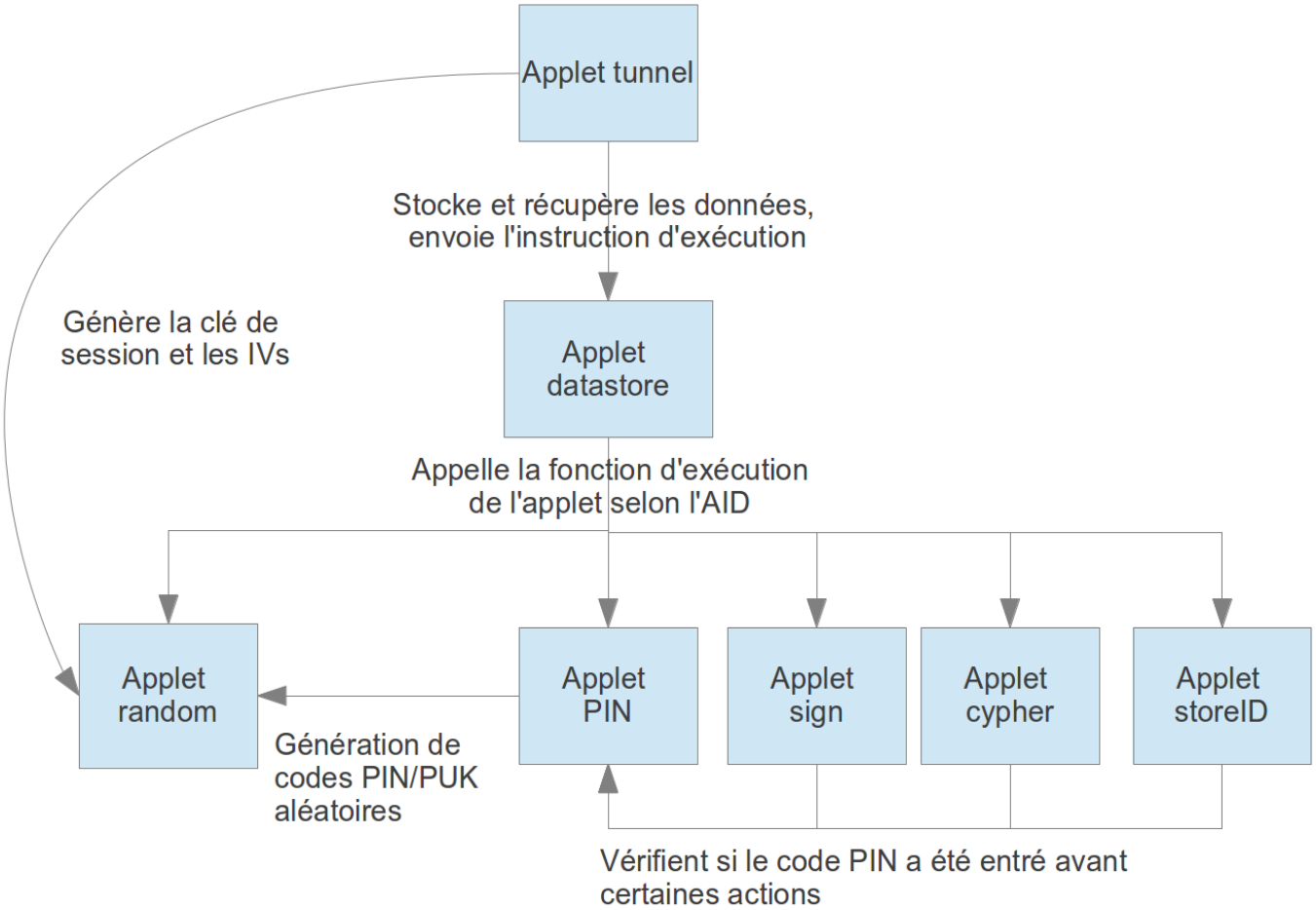
L'API JavaCard

Identifications des applets

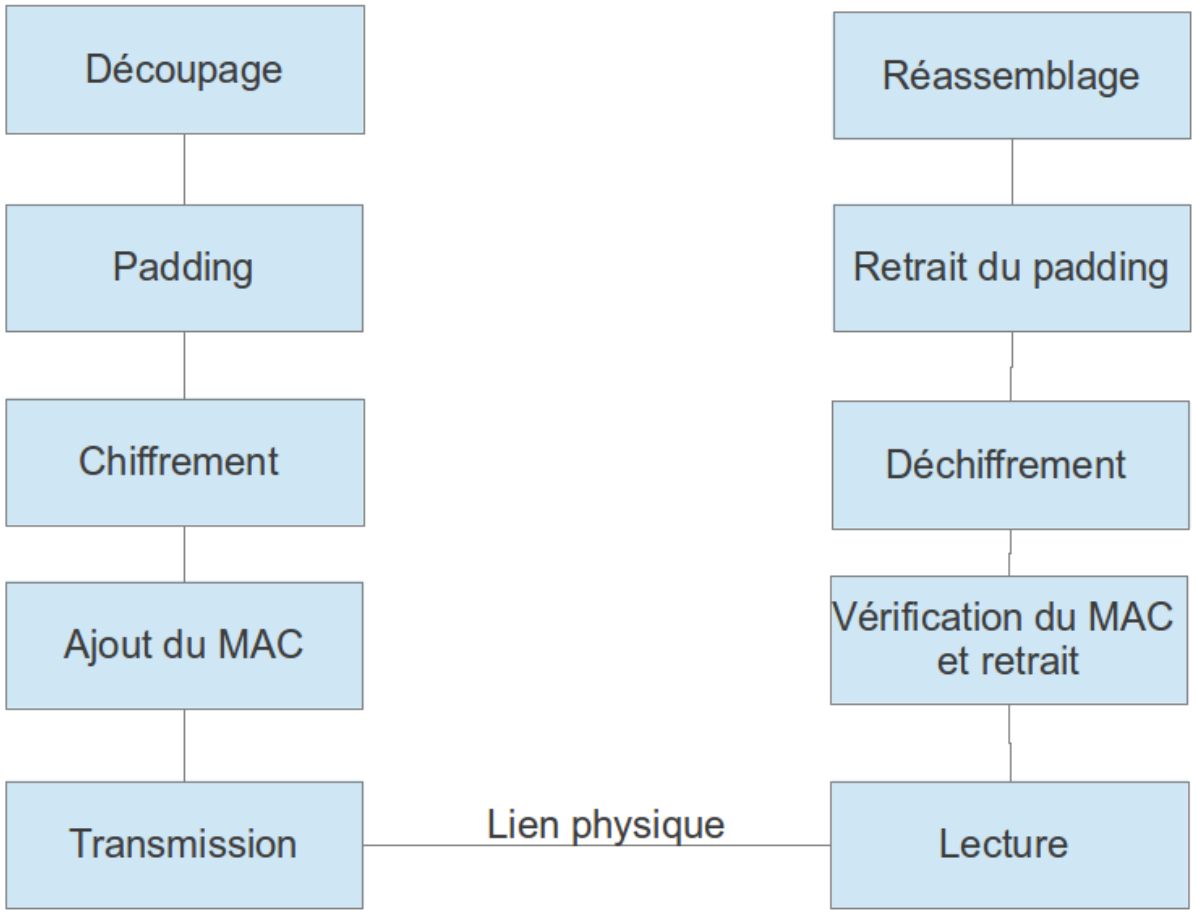
Principales limitations

types primitifs : boolean, byte, short pas de "garbage collector"

Les applications développées



L'aspect sécurité



Démonstration

L'interface avec SSN : SoftCard

Actuellement

- Applications de chiffrement, signature, stockage...
- Client testant ces applications

Mais par rapport à Facebook ?

L'interface avec SSN : SoftCard

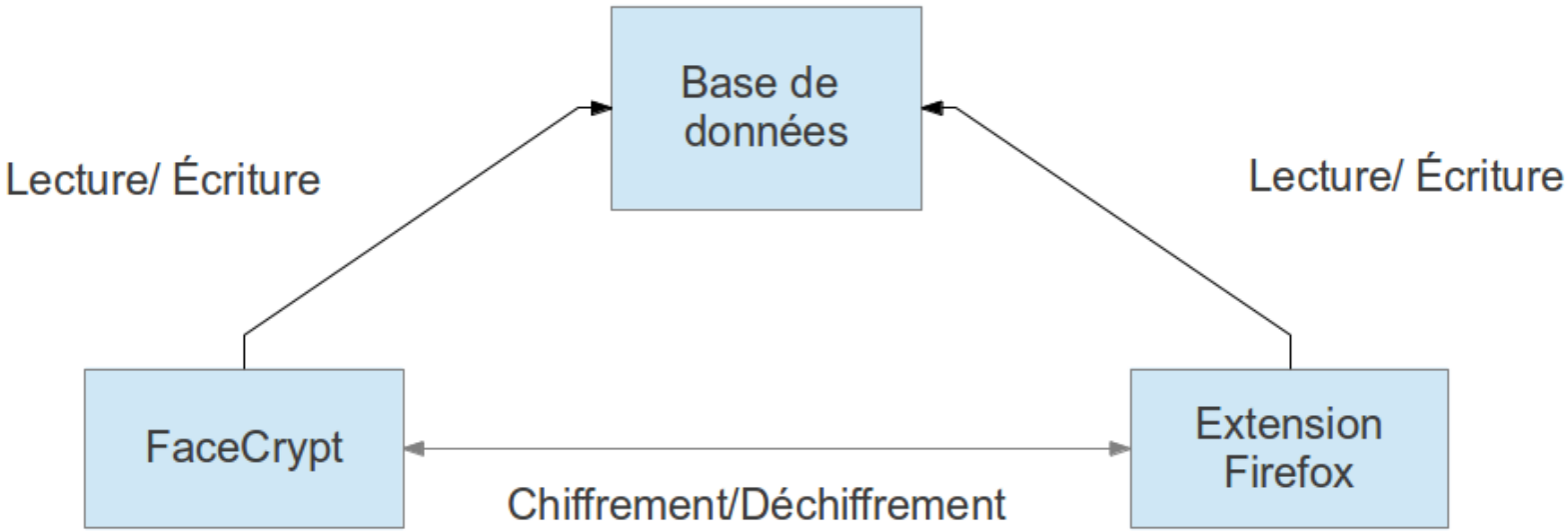
Un serveur

-

Les besoins et exigences

Protection des données utilisateur vis-à-vis de tiers
Authentification forte par carte à puce

Présentation des composants



Base de données

Moteur SQLite

Base de données locale

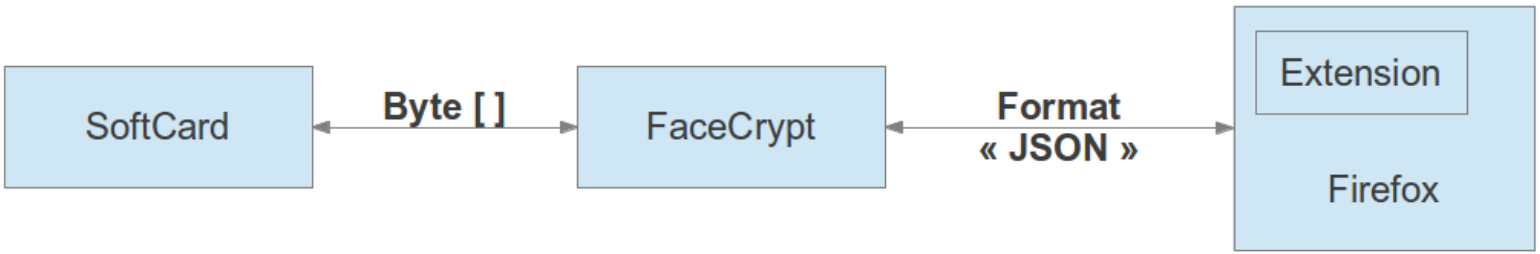
Accessible depuis Java et l'extension

Stockage des liens d'amitié dans la base

Listes d'amis

Clés publiques

La communication



Composition

Six classes java

- ASymCypher
- SymCypher
- ServerSSL
- Client
- Dataprocess
- CacheManager

Exemple de cycle

- Received from Facecrypt : {"action" :"getID"}
- Sent to Softcard : 47
- Received from Softcard : $\underbrace{666f6f2e6261722e333334343931 33}_{\text{login}}\ 20\ \underbrace{726f6f74726f6f74}_{\text{password}}$
- Sent to Facecrypt : {"action" :"getID" ,"login" :"foo.bar.3344913","firstConnection" :false, "pass" :"rootroot"}

Démonstration

schéma

Conclusion

Difficultés rencontrées

- SmartCard :
  - taille des données ;
  - communications sécurisées entre la carte à puce et l'application cliente ;
  - installations des lecteurs ;
  - stockage "caché" ;
  - algorithmes implantés sur la carte ;
- Secure Social Network :
  - manipulation de la page Facebook ;
  - communications sécurisées entre SSNExt et FaceCrypt ;
  - fonctionnement d'une extension.

Conclusion

Améliorations possibles

- SmartCard :
  - IHM pour entrer le code PIN ;
  - Gestion de l'arrachage de la carte ;
  - communications sécurisées entre la carte à puce et l'application cliente ;
  - One Time Password ;
  - prendre en compte les attaques (canaux cachés) ;
  - algorithmes implantés sur la carte ;
- Secure Social Network :
  - finalisation pour mise en production ;
  - étudier le tatouage d'images.

Conclusion

Les apports

- SmartCard :
  - manipulation d'une carte à puce ;
- Secure Social Network :
  - gestion d'une communication sécurisées entre plusieurs composants ;
- utilisation concrête de la cryptographie.