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

3 mars 2013

Plan

Contexte

SmartCard

titi

Secure Social Network

toto

Gestion de projet

Introduction

Besoins

- Authentification forte
- Contenir des informations confidentielles

Technologies étudiées

- Génération de nombres aléatoires
- Chiffrement/Déchiffrement
- Signature/Vérification
- Code PIN/PUK
- SoftCard

Présentation

Rappel sur la carte à puce

- Dispose d'un processeur pour du traitement d'informations.
- Permet de stocker des données cachées.
- Assure l'authentification de l'utilisateur.

Qu'est-ce que "Java Card" ?

- Désigne la technologie permettant de développer des applets ≪ sécurisées ≫ sur carte à puce.
- Mais c'est aussi une carte à puce :
  - programmable
  - multi-applications
  - interopérable

Fonctionnement

Les APDU

- Application Protocol Data Unit.
- Unité de communication entre le lecteur et la carte.

CLA	INS	P1	P2	Lc	Données	Le

Données	Status

TABLE : Structures d'une commande et d'une réponse

Exemple

- Commande : 0xB0 0x00 0x00 0x00 0x01 0x05
- Réponse : 0x02 0xf2 0x23 0x42 0xcf 0x90 0x00

Abstraction

L'API Java Card

- Permet de s'abstraire de l'assembleur $\rightarrow$ Java
- Fournit un certain nombres d'objets : PIN, clefs RSA...

Exemple

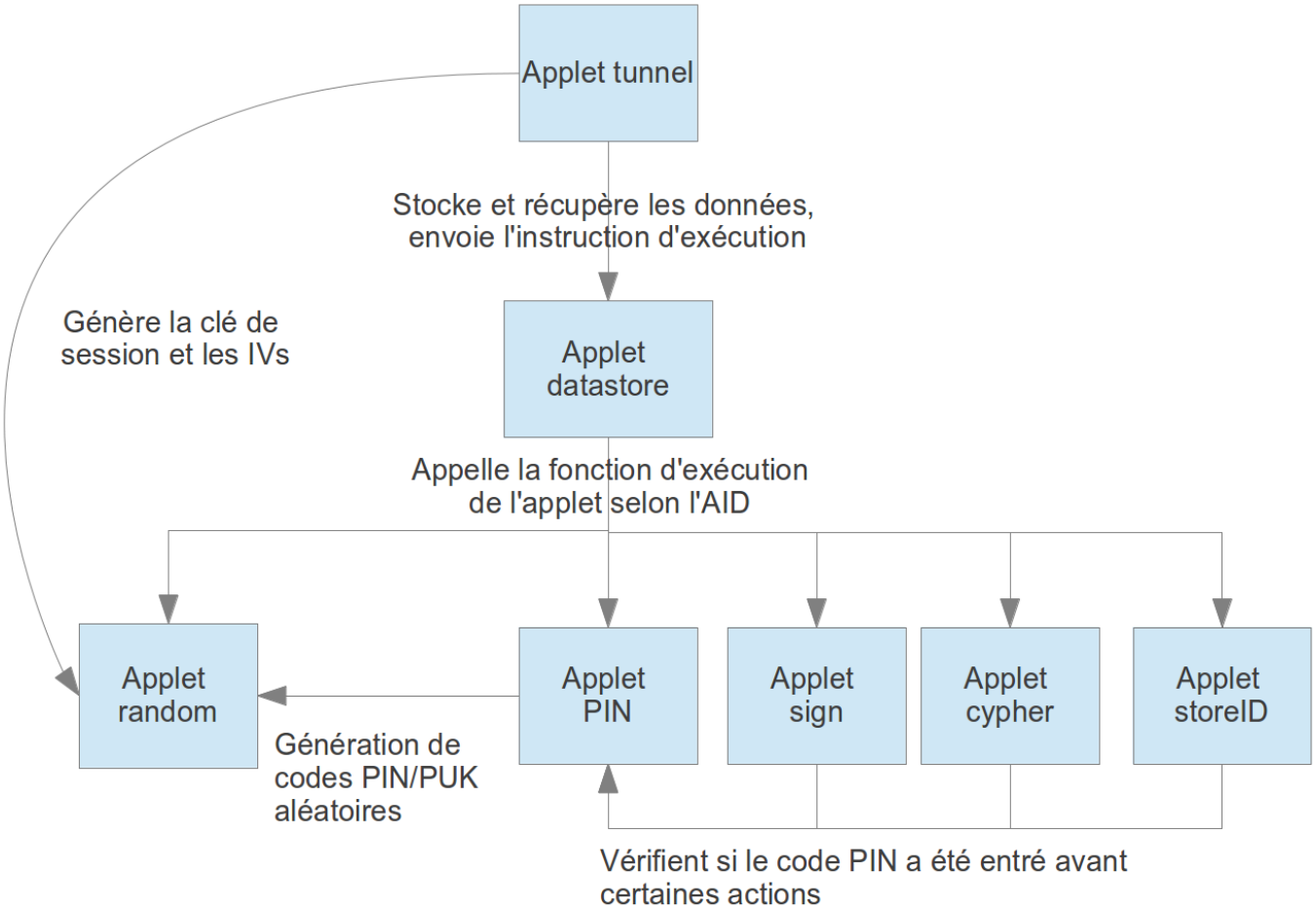
- Todo

Principales contraintes

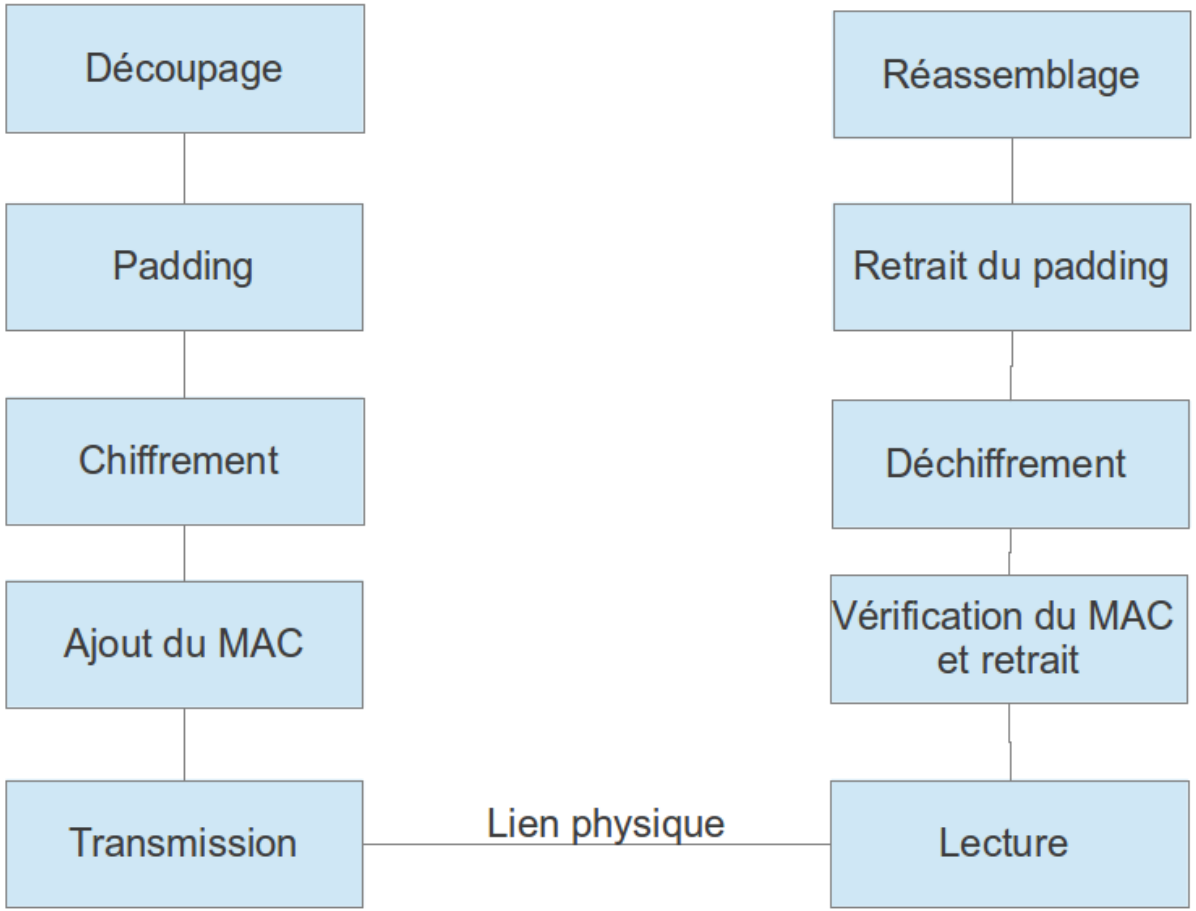
Les limitations de l'API Java Card

- types : boolean, byte, short, tableaux associés
- pas de ≪ garbage collector ≫

Les applications développées



L'aspect sécurité



Démonstration

L'interface entre SSN et la carte

Actuellement

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

Mais par rapport à Facebook ?

L'interface entre SSN et la carte

Un serveur vis-à-vis de SSN

- Une application (SoftCardServer) se met en attente de connexions.
- Pour chaque requête reçue, une action est transmise à une seconde application : SoftCard.
- SoftCardServer renvoie le résultat de SoftCard au client.

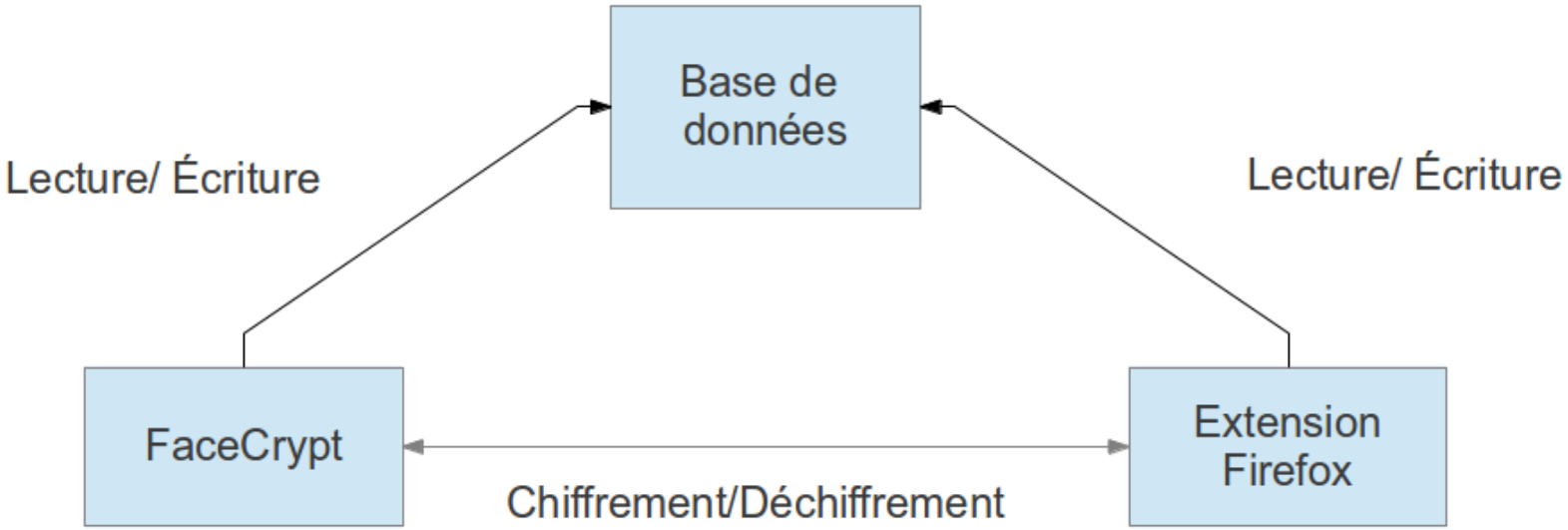
Un client vis-à-vis de la carte

- Une unique instance se connecte au lecteur puis à la carte.
- Différentes méthodes permettent de déchiffrer, signer...
- Pour certaines, sensibles, la carte devra être déverrouillée.

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

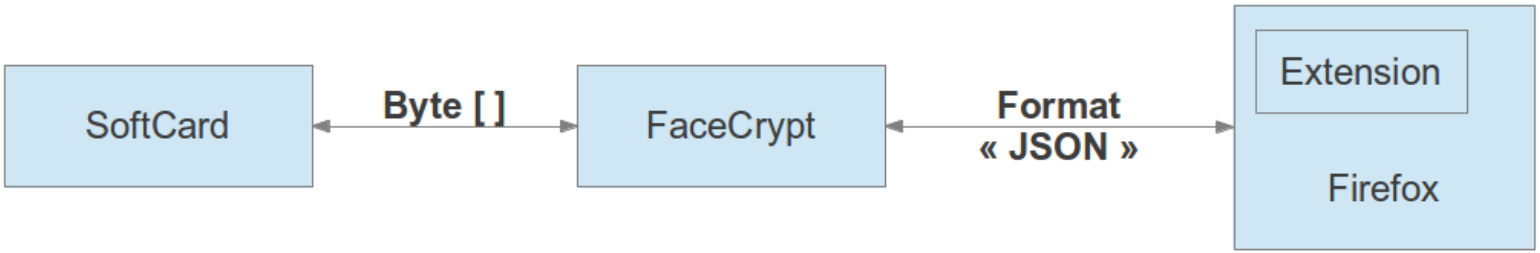
Accessible depuis Java et l'extension

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

Ce que cela nous a apporté

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

Merci pour votre attention.

Questions ?