

TP n°0 – Applet faisant un écho de l'entrée

TP n°1 – Porte monnaie électronique simple sécurisé via un PIN

TP n°2 – Utilisation de la cryptographie

TP n°3 – Implémentation d'une confusion de type

Nous utiliserons dans cette série de TP l'environnement Eclipse avec le plugin JCOP déjà activé.

Je rappelle le fondement de Java, il n'y a pas d'arithmétique sur les types autres que numériques (et en Java Card sur les entiers). Pensez aux règles de base de génie logiciel, pas de constantes en dur dans le code, nommer correctement vos variables, etc.

Pour tous les TP, nous utiliserons des JCOP.

Pour charger dans la carte, on utilisera suivant les TP et les besoins soit Eclipse.

Procédure de création d'une application :

Donner un nom à votre projet, sélectionner les profils de votre carte (en général JC2.1.1 et OP2.0.1), à votre package et à votre applet. Donner également un AID à votre package et à l'applet (en le dérivant de celui du package).

Écrire le programme Java correspondant à la spécification. Pour ce faire, créer un projet Java Card (un projet par package). Le nom du projet et/ou des packages et applets n'ont pas de réelle importance c'est plus pour vous y retrouver.

Une fois l'application codée, vous la chargez sur la carte au travers du Run Configuration. Double cliquez sur Java Card Application et sélectionner le lecteur de carte comme destination et en avant « Run ».

À l'aide du shell de JCOP vous pouvez échanger avec la carte via des commandes prédéfinies ou directement vos APDU. Vérifiez le bon fonctionnement de votre application.

Si vous rencontrez des erreurs n'hésitez pas à me les signaler :

damien.sauveron@unilim.fr

Applet faisant un écho de l'entrée

Objectif : Connaissance des outils de gestion des applications (loader, debugger, script), de la chaîne de compilation et de conversion, écriture d'une applet Java Card, définition de l'AID, utilisation de l'API `javacard.framework` et compréhension de la communication carte/lecteur (réception de commande APDU et d'envoi de réponse APDU et de Status Word – SW).

Les spécifications de cette applet sont les suivantes :

- Si les deux premiers octets de la commande APDU sont égaux à 0x80 alors la carte renverra seulement 0x6B 0x00 (pour cela on utilisera la classe `ISOException`).
- Sinon on réalise un écho de l'APDU reçu.

Voici le code minimale d'une applet en Java Card.

```
package fr.cryptis.nullapp;
import javacard.framework.*;
public class NullApp extends Applet
{
    protected NullApp()
    {
        // Insérer ici les initiatisations
    }

    public static void install(byte[] bArray, short bOffset, byte bLength) throws ISOException
    {
        new NullApp().register();
    }

    public void process(APDU apdu) throws ISOException
    {
        // Insérer ici le code métier
    }
}
```

On compilera puis convertira l'applet d'écho obtenue pour ensuite la charger sur la carte. Son installation se fait en deux phases qui sont le chargement et l'instanciation (appel à la méthode statique `install`).

Porte monnaie électronique simple sécurisé via un PIN

Objectif : Connaissance des outils de gestion des applications (loader, debugger, script), de la chaîne de compilation et de conversion, écriture d'une applet Java Card, définition de l'AID, utilisation de l'API `javacard.framework`.

Ce porte-monnaie pourra être attaqué ultérieurement via un shell code afin d'en faire une « yescard ».

Les spécifications de cette applet sont les suivantes :

- Elle comportera une balance (le solde) exprimé sous forme d'un `short` qui devra toujours rester positive et qui ne dépassera pas la limite maximal du format de stockage.
- Elle comportera un PIN qui devra être vérifié pour les opérations de crédit et de débit. On utilisera pour ce PIN la classe `OwnerPin` qui fait tout le travail de gestion du PIN pour nous et de manière sécurisée. Nous le fixerons à 8 octets la longueur et à 3 le nombre maximal d'essai consécutifs faux. La valeur du PIN sera fixée lors de l'opération d'installation afin de pouvoir le personnaliser pour chaque carte.
- Elle acceptera 4 commandes `GET_BALANCE`, `CREDIT`, `DEBIT` et `VERIFY` :
 - `GET_BALANCE` renverra le solde ;

GET BALANCE APDU command						
Command APDU						
CLA	INS	P1	P2	Lc	Data field	Le
0x80	0x50	0x0	0x0	N/A	N/A	2
Response APDU						
Optional data		Status word	Meaning of status word			
Balance value		0x9000	Successful processing			

- `VERIFY` permettra de proposer un PIN à vérifier ;

VERIFY APDU command						
Command APDU						
CLA	INS	P1	P2	Lc	Data field	Le
0x80	0x20	0x0	0x0	Length of the PIN data	PIN data	N/A
• CLA byte denotes the structure of the command • INS byte (0x20) indicates a verify instruction • P1 and P2 are not used, and are both set to 0 • The data field contains the PIN value						
Optional data		Status word	Meaning of status word			
N/A		0x9000	Successful processing			
		0x6300	Verification failed			

- CREDIT permettra de créditer la balance et ne fonctionnera que si le PIN a été vérifié avec succès ;

CREDIT APDU command						
Command APDU						
CLA	INS	P1	P2	Lc	Data field	Le
0x80	0x30	0x0	0x0	1	Credit amount	N/A
The data field contains the credit amount						
Response APDU						
Optional data		Status word		Meaning of status word		
N/A		0x9000		Successful processing		
		0x6301		PIN verification required		
		0x6A83		Invalid credit amount		
		0x6A84		Exceed the maximum amount		

- DEBIT permettra de débiter la balance et ne fonctionnera que si le PIN a été vérifié avec succès.

DEBIT APDU command						
Command APDU						
CLA	INS	P1	P2	Lc	Data field	Le
0x80	0x40	0x0	0x0	1	Debit amount	N/A
The data field contains the debit amount						
Response APDU						
Optional data		Status word		Meaning of status word		
N/A		0x9000		Successful processing		
		0x6301		PIN verification required		
		0x6A83		Invalid debit amount		
		0x6A85		Negative balance		

Il suffit donc de programmer cette application simple. Vous trouverez dans la classe `Util` des méthodes intéressantes pour la manipulation de `short` et de tableau de `bytes`. L'interface `ISO7816` dans le paquetage `javacard.framework` contient déjà beaucoup des constantes dont vous aurez besoin pour retourner les erreurs.

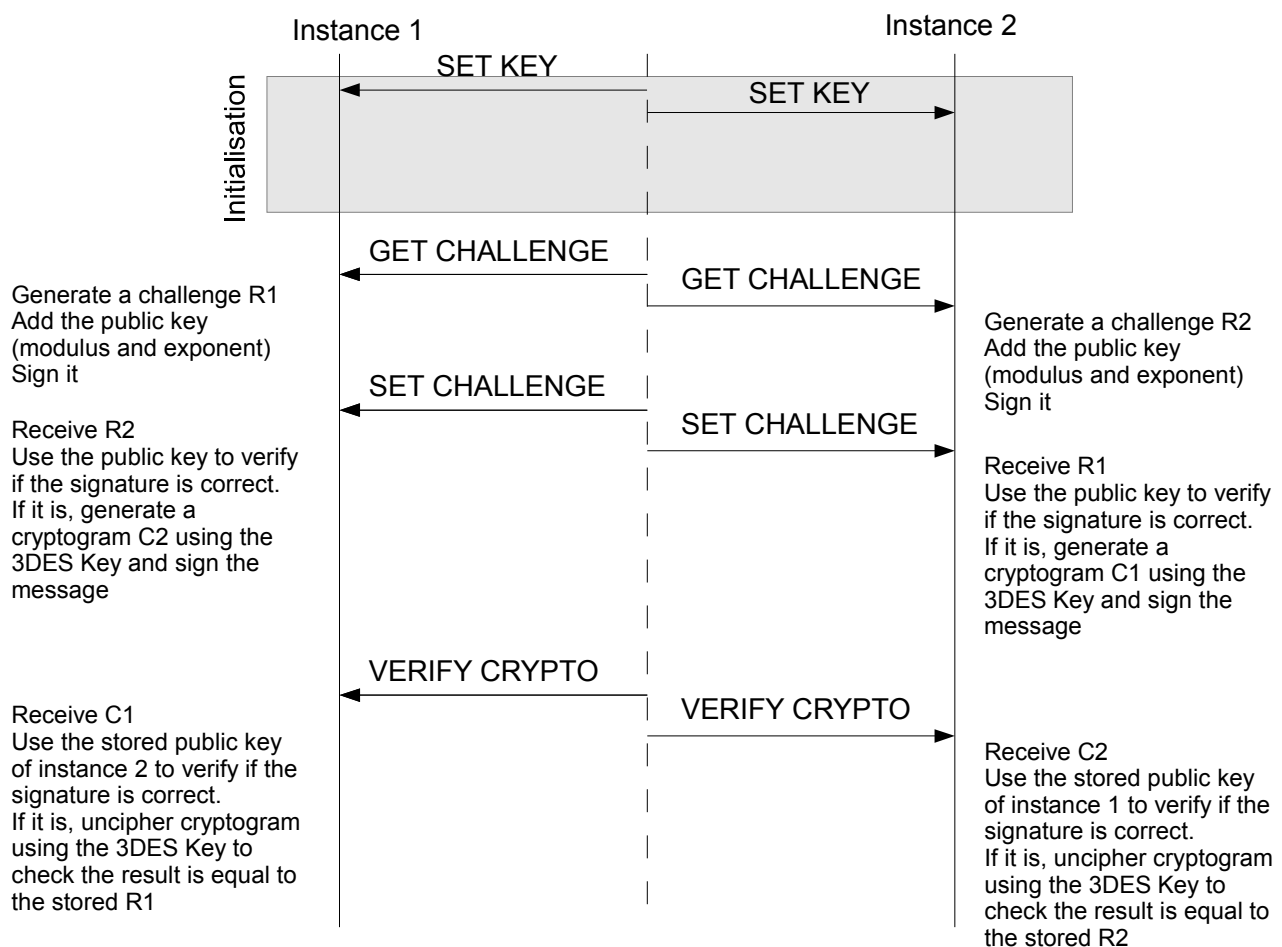
Utilisation de la cryptographie

Objectif : Manipulation des primitives de cryptographie.

Dans ce TP nous allons utiliser les primitives cryptographiques pour réaliser une authentification mutuelle. Pour cela nous implémenterons un protocole *challenge/response* dans lequel au départ les deux parties possèdent une clé symétrique 3 DES de 192 bits qui sera utilisé pour chiffrer les challenges (de 8 octets) en cryptogramme et inversement en utilisant l'algorithme ALG_DES_CBC_NOPAD.

Chaque partie disposera d'un générateur de nombres aléatoires et d'une paire de clés RSA de 512 bits (auto-généré au format CRT) qui sera utilisée pour signer et vérifier les messages avec l'algorithme ALG_RSA_SHA_PKCS1.

Les deux parties seront simulés par 2 instances de la même application. Idéalement si nos cartes supportent les canaux logiques, chaque instance utilisera un canal différent.



Utiliser des constantes pour les différentes instructions (respectivement dans l'ordre du schéma 0x10, 0x20, 0x30 et 0x40).

Allez y progressivement : création des différents objets, RNG, RNG+clé pub, RNG+clé pub+signature, ...

À l'issue de l'authentification mutuelle on pourrait poursuivre les échanges en chiffrant avec la clé 3DES et en signant.

Astuce : On peut ne travailler que sur une seule instance :-)

Implémentation d'une confusion de type

Objectif : Communication inter-applets via le firewall. Implémentation d'un modèle d'attaque. Teste sur des cartes afin de voir si elle fonctionne ou pas. Réflexion sur l'implémentation des objets sur la carte.

Programmer une application serveur exposant une interface partageable avec une méthode recevant un tableau de short.

```
void accArray(short[] array)
```

Programmer une application client souhaitant utiliser l'interface partageable du serveur avec une méthode recevant un tableau de byte.

```
void accArray(byte[] array)
```

1. Comment faire ?
2. Est-ce que si l'application cliente passe un tableau de byte au client, celui-ci pourra s'en servir et comment faire ?
3. Une fois tous les détails fixés, réalisez la confusion de type et essayez avec le serveur de lire toutes les données du tableau de short reçu alors qu'il s'agit d'un tableau de byte et renvoyez les dans une réponse APDU.
Que constatez vous ? Que faire ?
4. Essayez de passer outre cette limitation avec la solution proposée. Introduisez une classe A dans le premier package et changer l'interface.
Essayez d'exploiter cette nouvelle confusion.
Que constatez vous ? Que faire ?
5. Essayez les solutions proposées et que constatez vous ? Y a-t-il d'autres possibilités ?