ED2 sur la Technologie Java Card

Samia Bouzefrane & Julien Cordry

Laboratoire CEDRIC

CNAM

Comment écrire une applet ?

1. Comment écrire une applet ?

Quatre étapes comprennent la phase de développement d'une applet:

1. Spécifier les fonctions de l'applet
2. Assigner des AIDs à l'applet et au paquetage contenant la classe de l'applet
3. Concevoir les programmes de l'applet
4. Définir l'interface entre l'applet et le terminal

Nous illustrons ces étapes à travers l'exemple d'une applet Echo.

2. Spécification des fonctions de l'applet :

Notre applet Echo est simple, elle se contente de stocker la donnée qu'elle reçoit pour la retourner au terminal.

3. Spécification des AIDs :

Dans la technologie Java Card, chaque applet est identifiée et sélectionnée par un identificateur (AID). De même, à chaque paquetage Java est assigné un AID. Cette convention de nommage est conforme à la spécification de la carte à puce définie dans l'ISO 7816.

Un AID est une séquence d'octets allant de 5 à 16 octets. Son format est donné au Tableau 1.

Application identifier (AID)	
National registered application provider (RID)	Proprietary application identifier extension (PIX)
5 octets	0 to 11 octets

Tableau 1. Format de l'AID

L'ISO gère l'affectation des RIDs aux compagnies, chaque compagnie obtient son propre et unique RID de l'ISO. Les compagnies gèrent l'affectation des PIXs pour leur AID.

Les classes Java de l'applet sont définies dans un paquetage Java. Leurs AIDs respectifs sont définis dans le Tableau 2.

Package AID		
Champ	Valeur	Longueur
RID	0xA0, 0x00, 0x00, 0x18, 0x50	5 octets

PIX	0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x52, 0x41, 0x44, 0x50	10 octets
Applet AID		
Champ	**Valeur**	**Longueur**
RID	0xF2, 0x34, 0x12, 0x34, 0x56	5 octets
PIX	0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x52, 0x41, 0x44, 0x41	10 octets

Tableau 2. AIDs fictifs pour l'applet et son paquetage

4. Définir les méthodes de l'applet :

Une applet Java Card doit étendre la classe `javacard.framework.Applet`. Cette classe est une superclasse des applets résident sur la carte. Elle définit les méthodes courantes que doit utiliser une applet pour interagir avec le JCRE, l'environnement d'exécution.

Tableau 3 liste les méthodes de type `public` et `protected` définies dans la classe `javacard.framework.Applet`:

Method summary	
`public void`	`deselect ()` Called by the JCRE to inform the currently selected applet that another (or the same) applet will be selected.
`public Shareable`	`getShareableInterfaceObject (AID client AID, byte parameter)` Called by the JCRE to obtain a sharable interface object from this server applet on behalf of a request from a client applet.
`public static void`	`install (byte[] bArray, short bOffset, byte bLength)` The JCRE calls this static method to create an instance of the `Applet` subclass.
`public abstract void`	`process (APDU apdu)` Called by the JCRE to process an incoming APDU command.
`protected final void`	`register ()` This method is used by the applet to register this applet instance with the JCRE and assign the default AID in the CAD file to the applet instance.
`protected final void`	`register (byte[] bArray, short bOffset, byte bLength)` This method is used by the applet to register this applet instance with the JCRE and to assign the specified AID in the array `bArray` to the applet instance.
`public`	`select ()`

`boolean`	Called by the JCRE to inform this applet that it has been selected.
`protected final boolean`	`selectingApplet ()` This method is used by the applet `process()` method to distinguish the `SELECT APDU` command that selected this applet from all other `SELECT APDU` APDU commands that may relate to file or internal applet state selection.

Tableau 3. Méthodes public et protected définies dans la classe `javacard.framework.Applet`

La classe `javacard.framework.Applet` fournit un framework pour l'exécution des applets. Les méthodes définies dans la classe sont appelées par le JCRE lorsque celui-ci reçoit des commandes APDU à partir du lecteur (CAD :Card Acceptance Device).

Une fois le code de l'applet proprement chargé sur la carte et lié aux autres paquetages se trouvant sur la carte, la vie de l'applet commence lorsqu'une instance de l'applet est créée et enregistrée au sein du JCRE. Une applet doit définir la méthode `install`() pour créer une instance d'applet et doit enregistrer l'instance au sein du JCRE en invoquant une des méthodes `register`(). La méthode `install`() prend un vecteur d'octets comme paramètre. Ce vecteur contient les paramètres d'installation pour l'initialisation et la personnalisation de l'instance d'applet.

Une applet Java Card reste inactive jusqu'à ce qu'elle soit explicitement sélectionnée. Lorsque le JCRE reçoit une commande `SELECT APDU`, il consulte sa table interne pour trouver l'applet dont l'AID correspond à celui spécifié dans la commande. S'il le trouve, le JCRE prépare la sélection de la nouvelle applet. Cette préparation se fait en deux étapes: d'abord, si une applet couramment sélectionnée est présente en mémoire, alors le JCRE la désélectionne en invoquant la méthode `deselect`(). L'applet exécute la méthode `deselect`() avant de devenir inactive. Le JCRE invoque alors la méthode `select`() pour informer la nouvelle applet de sa sélection. La nouvelle applet effectue éventuellement une opération d'initialisation avant d'être réellement sélectionnée. L'applet retourne vrai à la méthode `select`() si elle est prête à devenir active et à traiter n'importe quelle commande APDU. Sinon, l'applet retourne faux pour décliner sa participation. La classe `javacard.framework.Applet` fournit une implémentation par défaut pour les méthodes `select`() et `deselect`(). Une sous-classe de la classe `Applet` peut redéfinir ces méthodes pour associer un autre comportement à ces méthodes.

Une fois l'applet sélectionnée, le JCRE fait suivre toutes les commandes APDU (y compris la commande `SELECT`) à la méthode `process`() de l'applet. Dans la méthode `process`(), l'applet interprète chaque commande APDU et exécute la tâche spécifiée par la commande. Pour chaque commande APDU, l'applet répond au CAD en envoyant une réponse APDU qui informe le CAD du résultat du traitement de la commande APDU. La méthode `process`() de la classe `javacard.framework.Applet` est une méthode de type

`abstract`: une sous-classe de la classe `Applet` doit redéfinir cette méthode pour implémenter les fonctions de l'applet.

Ce dialogue commande-réponse continue jusqu'à ce que une nouvelle applet soit sélectionnée ou bien que la carte soit retirée du CAD. Lorsqu'elle est désélectionnée, l'applet devient inactive jusqu'à sa prochaine sélection.

La méthode `getShareableInterfaceObject` sert dans la communication inter-applet. Elle est appelée par une applet client qui demande, à une applet serveur, à partager l'interface d'un objet. L'implémentation par défaut de cette méthode est de retourner null. Dans ce document, on ne s'intéressera pas à la communication entre applets.

Étant donné que la commande APDU `SELECT` est aussi dirigée vers la méthode `process`(), la méthode `selectingApplet`() est utilisée par la méthode `process`() de l'applet pour distinguer entre la commande APDU `SELECT` qui sélectionne cette applet et les autres commandes APDU `SELECT` relatives à la sélection de fichiers ou de l'état interne de l'applet.

5. Définir une interface entre une applet et le terminal:

Une applet qui tourne sur une carte à puce communique avec l'application en utilisant le protocole APDU (Application Protocol Data Units défini par l'ISO 7816). Par essence, l'interface entre l'applet et l'application est un ensemble de commandes APDU qui sont supportées aussi bien par l'applet que l'application.

5.1 La notion d'APDU:

Les commandes APDU sont toujours des ensembles de paires. Chaque paire contient une commande (*command*) *APDU,* qui spécifie une commande, et une réponse (*response) APDU,* qui retourne le résultat d'exécution de la commande. Dans le monde de la carte, les cartes sont *réactives* – c-à-d qu'elles n'initient jamais des communications mais se contentent de répondre aux APDUs du monde extérieur. L'application envoie une commande APDU via le lecteur (CAD). Le JCRE en recevant une commande, sélectionne une nouvelle applet ou bien passe la commande à une applet courante (déjà sélectionnée). L'applet courante traite la commande et retourne une réponse APDU à l'application. Les commandes et réponses APDU sont échangées alternativement par la carte et le CAD.

Tableau 4 décrit le format des commandes et réponses APDU.

Command APDU						
Mandatory header				**Optional body**		
CLA	INS	P1	P2	Lc	Data field	Le
• CLA (1 byte): Class of instruction --- indicates the structure and format for a category of command and response APDUs						

- INS (1 byte): Instruction code: specifies the instruction of the command
- P1 (1 byte) and P2 (1 byte): Instruction parameters -- further provide qualifications to the instruction
- Lc (1 byte): Number of bytes present in the data field of the command
- Data field (bytes equal to the value of Lc): A sequence of bytes in the data field of the command
- Le (1 byte): Maximum of bytes expected in the data field of the response to the command

Response APDU		
Optional body	**Mandatory trailer**	
Data field	SW1	SW2

- Data field (variable length): A sequence of bytes received in the data field of the response
- SW1 (1 byte) and SW2 (1 byte): Status words -- denote the processing state in the card

Tableau 4. formats des commandes et réponses APDU

5.2 Définir des commandes APDU:

Une applet Java Card doit supporter un ensemble de commandes APDU, comprenant la commande `SELECT APDU` et une ou plusieurs commandes de traitement d'APDUs.

La commande `SELECT` invite le JCRE à sélectionner une applet sur la carte.

L'ensemble des commandes de traitement (process) définit les commandes que l'applet supporte. Elles sont définies en accord avec les fonctions de l'applet.

La technologie Java Card spécifie l'encodage de la commande `SELECT APDU`. Les développeurs sont libres de définir l'encodage des commandes de traitement. Cependant, les commandes de traitement doivent être cohérentes avec la structure définie au Tableau 4.

D'un point de vue structurel, la commande `SELECT` (`INS_SELECT = 0xA4`) et les commandes de traitement sont des paires de commandes et de réponses APDU.

Pour chaque commande APDU, l'applet doit d'abord décoder la valeur de chaque champ de la commande. Si les champs optionnels sont inclus, l'applet doit aussi déterminer leur format et leur structure. En utilisant ces définitions, l'applet sait comment interpréter chaque commande et lire chaque donnée. Elle peut alors exécuter la tâche spécifiée par la commande.

Pour chaque réponse APDU, l'applet doit définir un ensemble de mots d'état pour indiquer le résultat du traitement de la commande APDU. Dans un traitement normal, l'applet retourne un mot d'état contenant succès (0x9000, comme spécifié dans l'ISO 7816). Si une erreur survient, l'applet doit retourner un mot d'état différent de 0x9000 pour exprimer son état interne. Si par contre le champ de donnée optionnel est inclus dans la réponse APDU, l'applet doit définir ce qu'elle doit retourner.

Dans notre exemple, l'applet doit récupérer les données envoyées dans la commande APDU afin de les retourner dans une réponse APDU.

En plus des mots d'état déclarés dans chaque commande APDU, l'interface `javacard.framework.ISO7816` définit un ensemble de mots d'état qui signalent les erreurs courantes des applets, comme par exemple la commande APDU concernant l'erreur du formatage.

6. Le support APDU dans la technologie Java Card:

La classe `javacard.framework.APDU` encapsule les commandes APDU. Elle fournit une interface puissante et flexible qui permet aux applets de gérer les commandes APDU. La classe APDU est conçue pour cacher les complexités du protocole, afin que les développeurs d'applet se concentrent davantage sur les détails de l'application.

Lorsque le JCRE reçoit une commande APDU, il encapsule la commande dans un objet APDU qu'il passe à la méthode `process`() de l'applet courante. L'objet APDU comporte un vecteur d'octets qui contient le message APDU.

L'applet traite une commande APDU en invoquant des méthodes sur cet objet APDU. En général, l'applet effectue les étapes suivantes:

Étape 1. Extraire le buffer APDU:

L'applet invoque la méthode `getBuffer`() afin d'obtenir une référence au buffer APDU, qui contient le message. Lorsque l'applet reçoit l'objet APDU, seuls les 5 premiers octets sont disponibles dans le buffer. Il s'agit dans l'ordre des octets `CLA`, `INS`, `P1`, `P2`, et `P3`. L'octet `P3` désigne l'octet `Lc`, si la commande possède des données optionnelles. L'applet peut vérifier les octets entête pour déterminer la structure de la commande et l'instruction spécifiée par la commande.

Étape 2. Recevoir des données:

Si la commande APDU contient des données optionnelles, l'applet doit diriger l'objet APDU vers la réception de données entrantes en invoquant la méthode `setIncomingAndReceive`(). Les données sont lues dans le buffer APDU en suivant l'ordre des 5 octets d'entête. Le dernier octet de l'entête (`Lc`) indique la longueur des données entrantes. Si le buffer APDU ne peut contenir toutes les données, l'applet peut traiter les données en fragments, ou bien le copier vers un buffer interne. Dans les deux cas, elle doit faire appel de manière répétitive à la méthode `receiveBytes`() afin de lire les données additionnelles à partir du buffer APDU.

`arrayCopyNonAtomic(byte[] src, short srcOff, byte[] dest, short destOff, short length)` copie un vecteur à partir du vecteur source spécifié, en

commençant de la position spécifiée à la position spécifiée dans le vecteur destination de manière non atomique.

Étape 3. Renvoyer des données:

Après avoir traité une commande APDU, l'applet peut retourner des données à l'application sous forme de réponses APDU. L'applet doit d'abord faire appel à la méthode `setOutgoing`() pour obtenir la longueur de la réponse (`Le`). `Le` est spécifié dans la commande APDU associée à la réponse APDU.

Ensuite, l'applet appelle la méthode `setOutgoingLength`()pour informer le CAD de la longueur réelle des données de la réponse. L'applet peut transférer les données vers le buffer APDU et appeler la méthode `sendBytes`() pour envoyer les données. La méthode `sendBytes`() peut être appelée plusieurs fois si le buffer APDU ne peut pas contenir toutes les données retournées.

Si les données sont stockées dans un buffer interne, l'applet invoque la méthode `sendByteLong`() pour envoyer les données à partir du buffer.

Si les données de la réponse sont trop courtes pour tenir dans le buffer APDU, la classe APDU fournit une méthode appropriée: `setOutgoingAndSend`(). Cette méthode est une combinaison de `setOutgoing`, de `setOutgoingLength` et de `sendBytes`. Néanmoins cette méthode ne peut être invoquée qu'une seule fois, et aucune méthode d'envoi ne peut être appelée après.

Étape 4. Renvoyer le mot d'état (word status):

Après un succès de la méthode `process`(), le JCRE envoie automatiquement 0x9000 pour indiquer un traitement normal. A n'importe quel point, si l'applet détecte une erreur, l'applet peut lever l'exception `ISOException` en appelant la méthode statique `ISOException.throwIt(short reason)`. Le mot d'état est spécifié dans le paramètre `reason`. Si l'exception `ISOException` n'est pas gérée par l'applet, elle sera attrapée par le JCRE. Le JCRE extrait le code de `reason` code et l'envoie comme mot d'état.

7. Construire le code de l'applet:

Une fois la phase de conception de l'applet est finie, la seconde phase consiste à écrire le code de l'applet.

L'environnement de développement JBuilder/GemXplore utilisé ici nous permet de compiler l'applet en .class, de générer à partir de l'applet un fichier .cap qui sera le fichier à charger sur la carte, d'installer l'applet, de la sélectionner en vue de dialoguer avec elle en envoyant des commandes APDU. L'interface graphique étant très conviviale, il suffira de se laisser guider pour chaque étape. Notons par exemple que l'AID pour le package

ainsi que celui de l'applet seront fournis à la création du projet de l'applet. De plus, l'envoi de commandes APDU pourra se faire directement en utilisant cette interface.

Lorsque l'utilisateur choisit de créer une applet Java Card, GemXplore/JBuilder crée automatiquement une applet contenant des méthodes prédéfinies :

- la méthode `install()` : permet l'installation de l'applet sur la carte en faisant appel au constructeur de l'applet.

- le constructeur de l'applet : doit initialiser des variables internes et appeler la méthode `register`() en vue de s'enregistrer auprès du JCRE.

- la méthode `process()` : sert à traiter toute commande APDU en vue de retourner une réponse.

- les méthodes `select()` et `deselect()` servent respectivement à la sélection de l'applet ou à sa désélection.

Références

Zhiqun Chen, "**How to write a Java Card applet: A developer's guide**", http://www.javaworld.com/javaworld/jw-07-1999/jw-07-javacard.html.

Pierre Paradinas, Support de cours sur « **Java Card** », UV de Systèmes Enfouis et Embarqués, Valeur C, Laboratoire CEDRIC, CNAM. Accessible via : http://deptinfo.cnam.fr/~paradinas/cours/ValC-IntroJavaCard.pdf

Global Platform, Card Specification :
http://www.globalplatform.org/specificationform2.asp?id=archived

API Java Card : http://java.sun.com/products/javacard/htmldoc

Eric Vétillard : http://javacard.vetilles.com/2006/09/17/hello-world-smart-card/

Exercices

Exercice :

Utilisez l'environnement Eclipse pour écrire une applet echo qui retourne tout octet envoyé à la carte. Avant de dialoguer avec l'applet sur la carte, il faudra compiler l'applet, générer un fichier .CAP, l'installer sur la carte.