1. What is smart card: types, structure, application

2. What is smartcard OS: purposed, structure, …

3. Compare between JavacardOS vs MULTOS…

|  |
| --- |
|  |
|  |

|  |
| --- |
|  |
|  |

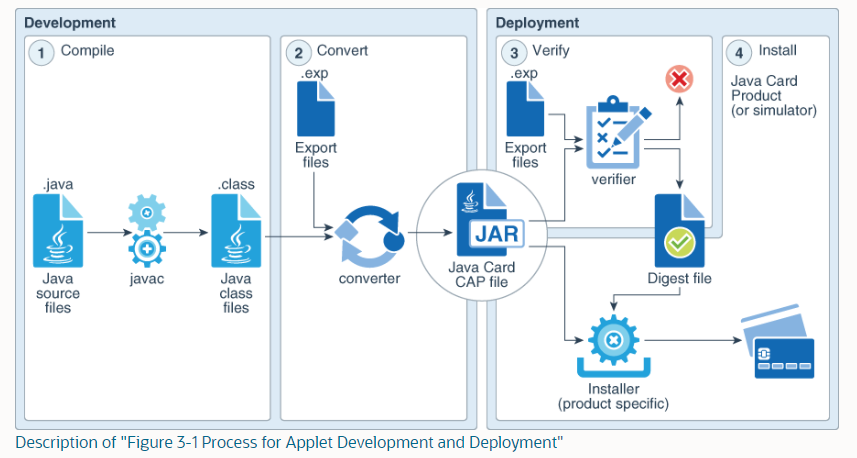
|  |
| --- |
|  |
|  |

<https://www.infoworld.com/article/2076617/understanding-java-card-2-0.html>

4. Development tools: software, HW, flow.., procedure..

+Javacard applet:



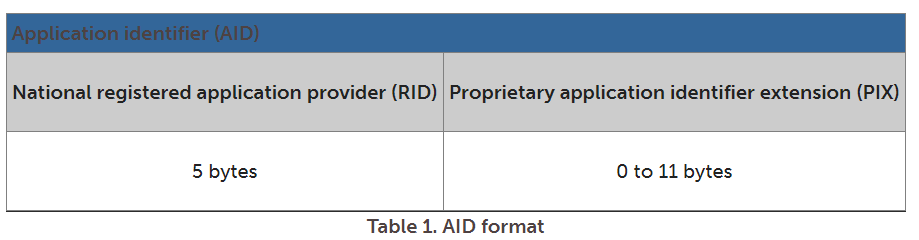


Four steps comprise the applet-design phase:

1. Specify the functions of the applet
2. Request and assign AIDs to both the applet and the package containing the applet class
3. Design the class structure of the applet programs
4. Define the interface between the applet and the terminal application

***B.*** In Java Card technology, however, each applet is identified and selected by an Application identifier (AID). Also, each Java package is assigned an AID. This is because a package, when loaded on a card, is linked with other packages, which have already been placed on the card via their AIDs. This naming convention is in conformance with the smart card specification as defined in ISO 7816.

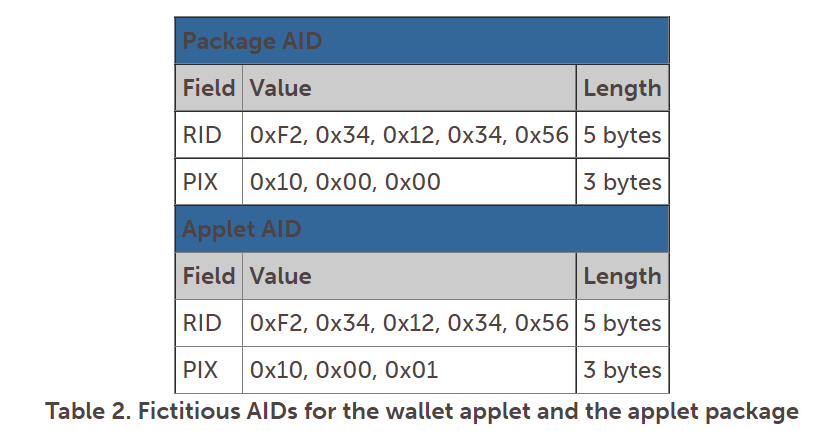
An AID is a sequence of bytes between 5 and 16 bytes in length.



ISO controls the assignment of RIDs to companies, with each company obtaining its own unique RID from the ISO. Companies manage assignment of PIXs for AIDs.

The Java classes of the wallet applet are defined in a Java package. The fictitious AIDs for the wallet applet and the applet package are defined as illustrated in Table 2.

The package AID and the applet AID have the same RID value; their PIX values differ at the last bit.



.

+MULTOS applet:

5. Suggestions..

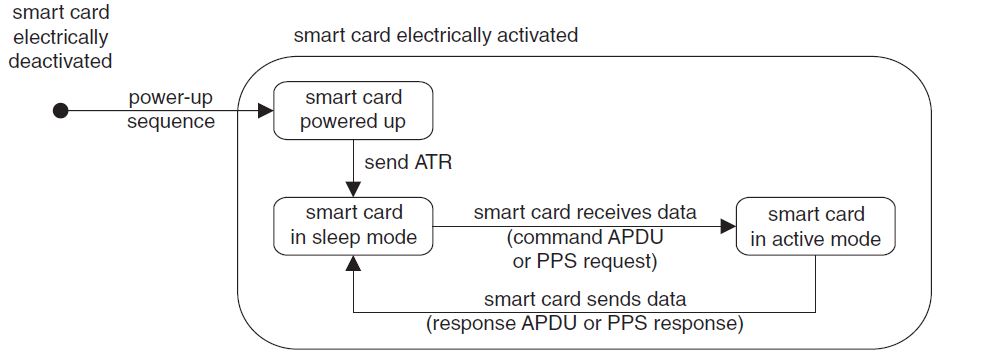
Application on card reader (IFD: Interface Device, CAD: Card Acceptance Device…)

- Actually, card reader’s side software (CDSW) should act as an APDU transceiver:

+ Create APDU command to send to card applet

+ Receive and parse APDU response from card applet

- Firstly, when the card is presented (physical IC or contactless), the CDSW should receive and parse ATRs data which include: “3.1 Answer-To-Reset The ATR is a series of signals, which form bytes, that are sent out by the smart card when it is powered up and reset for this first time, or subsequently reset. The term signal is used here to stress that the actual protocol to be used is undefined at this point. There are a number of low-level handshaking steps that take place, during the power-up and ATR cycle, which will establish the communication parameters to use. The document [7816-3] defines the Answer-To-Reset structure and the interpretation of the values found in it. However, the general structure of an ATR is easy to understand. It consists of two blocks of data: interface characters and the historical characters. The interface characters are used to define the operational parameters for the smart card. Information such as the transport protocols that are allowed, the voltage levels, the class of smart card and the speed at which the clock frequency may be run are all indicated. Historical characters consist of up to fifteen bytes of data that may be card or application specific and are often used to convey simple information. For example, some electronic purses could use the Historical Characters to convey the amount of value currently held on the card. This enables a simple IFD to reset the card and display the value on the purse by reading the Historical Characters.”…..



+..

+ List of applets on the card to show a menu of selectable apps on the IDF(CDA) screen and allow user to choose…

*“3.7.2 The Directory File*

*The Directory File, as called the DIR, is an Elementary File defined in [7816-4] and maintained by MULTOS. It is a variable length EF that can hold information on the applications that have been loaded onto the MULTOS Card. Each application loaded onto the MULTOS card may have an entry in the DIR file. The entry is created by the application provider and is usually stored in an [7816-4] defined TLV structure. These records*

*are ordered in the same sequence as the applications are loaded. The fact that DIR records have a defined structure permits IFD and other applications to read and to parse them. So, for example, an IFD can verify that a particular application is available by reading the DIR records assuming that the application does have a DIR record. If the required records are found, then the IFD could display application names for cardholder selection.*

*3.7.3 The Answer-To-Reset File*

*The Answer-To-Reset File, also called the ATR File, is maintained by MULTOS and each application may place an entry in the file. It is a variable length EF that can hold information related to the chip Answer-To-Reset. Contrary to the name, the ATR File is not used directly to generate the Answer-To-Reset. An Answer-To-Reset has historical bytes, but there are only 15 bytes available for use. If more than 15 were required, they would be placed in the ATR File.”*

+

-