Mobile Information Device Profile

The Java™ platform for mobile information devices.

The Mobile Information Device Profile (MIDP), combined with the Connected Limited Device Configuration (CLDC), is the Java™ runtime environment for today's mobile information devices such as phones and entry level PDAs.

The MIDP specification has been defined through the Java Community Process℠ program by an expert group of more than 50 companies — including leading mobile device manufacturers, wireless carriers and mobile software vendors. It defines a platform for dynamically and securely delivering highly graphical, networked applications to mobile information devices. MIDP provides the core application functionality required by mobile applications as a standardized Java runtime environment and set of Java APIs. Using MIDP, developers can write applications once that are optimized for today's mobile information devices.

MIDP has been widely adopted as the platform of choice for mobile applications. It is deployed globally on millions of mobile phones and PDAs, and supported by leading Java technology integrated development environments (IDEs). Companies around the world have already taken advantage of MIDP to write a broad range of consumer and enterprise mobile applications.

Designed for the Mobile User

MIDP enables truly networked applications with a great end user experience on mobile information devices. To download a MIDP application, a user browses a list of applications stored on a Web server. Once the application is selected, the device checks to make sure it can run the application. If it can, the device downloads the application, and then verifies and compiles its Java byte code to run on the device. Once installed, MIDP applications can be easily updated and removed by the end user.

MIDP applications provide the foundation for highly graphical and intuitive applications. The graphical user interface is optimized for the small display size, input methods and other native features of mobile devices. MIDP provides intuitive navigation and data entry by fully leveraging the phone keypads, extra buttons such as arrow keys, touch screens, and small QWERTY keyboards. MIDP applications are installed and run locally, can operate in both networked and disconnected mode, and have the ability to securely store and manage data locally.
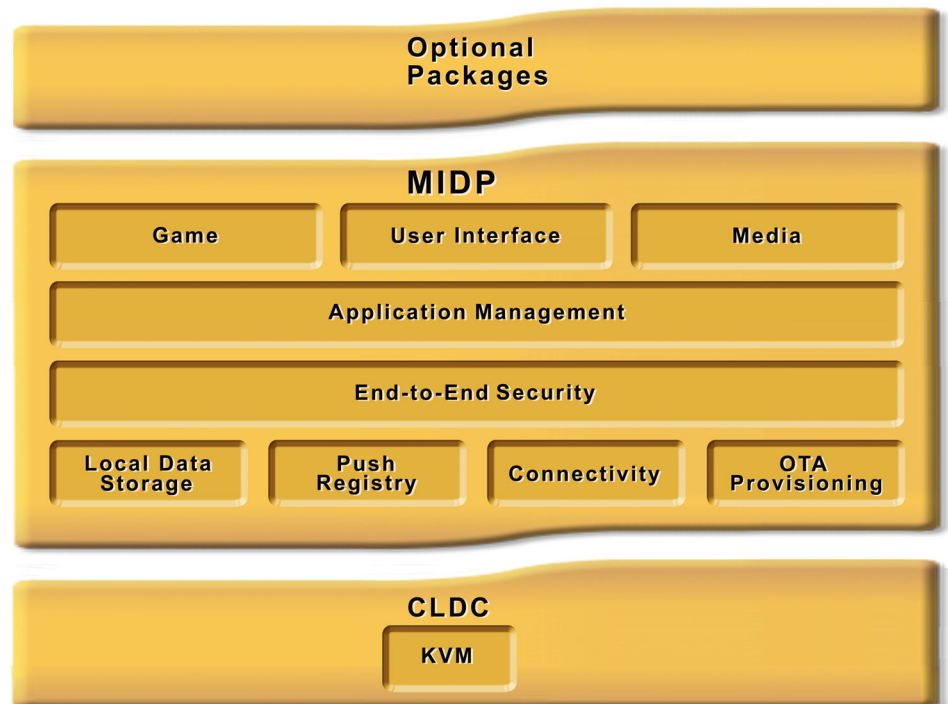
A mobile User Interface

MIDP features a high level user interface API that shields developers from the complexity of building portable applications. This high level API enables developers to build easy to use, highly graphical and portable applications optimized for mobile information devices, and reduces development effort.

MIDP user interface functionality includes predefined screens for displaying and selecting lists, editing text, popping up alert dialogs, and adding scrolling tickers. Forms are screens that can include any number of predefined items — images, read-only text fields, editable text fields, editable date and time fields, charts, and choice groups — as well as any custom items added by developers to provide unique functionality and graphics. All screens and items are device-aware, with built-in support for the native display size, input and navigation capabilities. This enables developers to define a highly portable, flexible user interface that changes its layout and navigation to fully leverage each device.

Multimedia and Game Functionality

MIDP is ideal for building portable games and multimedia applications. A low level user inter- face API complements the high level API, giving developers greater control of graphics and inputs when they need it. A game API adds game-specific functionality, such as sprites and tiled layers, that takes advantage of native device graphics capabilities. Built-in audio provides support for tones, tone sequences and WAV files. In addition, developers can use the

Mobile Media API (MMAPI), an optional package for MIDP, to add video and other rich multimedia content.

Extensive Connectivity

MIDP enables developers to fully leverage the native data network and messaging capabilities of mobile information devices. It supports leading connectivity standards, including HTTP, HTTPS, datagram, sockets, server sockets, and serial port communication. MIDP also supports the Short Message Service (SMS) and Cell Broadcast Service (CBS) capabilities of GSM and CDMA networks through the Wireless Messaging API (WMA) optional package.

MIDP connectivity and messaging support enables truly networked, event-driven applications. MIDP supports a server push model. A push registry keeps track of applications registered to receive inbound information from the network. When information arrives, the device decides whether to start the application based on user preferences. This push architecture enables developers to include alerts, messaging and broadcasts in MIDP applications, and leverage the event-driven capabilities of devices and carrier networks.

Over-the-Air Provisioning

A major benefit of MIDP is its ability to dynamically deploy and update applications over-the-air (OTA). The MIDP specification defines how MIDP applications are discovered, installed, updated and removed on mobile information devices. MIDP also enables a service provider

to identify which MIDP applications will work on a given device, and obtain status reports from the device following installation, updates or removal. The MIDP OTA Provisioning model has been defined and adopted by leading device manufacturers and service providers to deliver a reliable, secure provisioning solution.

End-to-End Security

MIDP provides a robust security model — built on open standards — that protects the network, applications and mobile information devices. The use of HTTPS leverages existing standards such as SSL and WTLS to enable the transmission of encrypted data. Security domains protect against unauthorized access of data, applications and other network and device resources by MIDP applications on the device. By default MIDP applications are not trusted, and are assigned to untrusted domains that prevent access to any privileged functionality. To gain privileged access, a MIDP application must be assigned to specific domains that are defined on the mobile device, and are properly signed using the X.509 PKI security standard. In order for a signed MIDP application to be downloaded, installed and granted associated permissions, it must be successfully authenticated.

Resources on the Web

To learn more about MIDP, please visit:
- MIDP: http://java.sun.com/products/midp
- Wireless Developer Portal:
  http://wireless.java.sun.com
- Java Community Process: http://jcp.org