Advanced Java Application Development for the BlackBerry Smartphone

BlackBerry Academic Program
Prior to subscribing for, installing or using any Third Party Products and Services it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers may not offer Internet browsing functionality with a subscription to BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use, Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided 'AS IS' with no express or implied conditions, endorsements, guarantees, representations or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, BlackBerry® Device Software and/or BlackBerry Handheld Software and may require additional development or Third Party Products and Services for access to corporate applications.

Certain products mentioned in this documentation include software developed by the Apache Software Foundation (http://www.apache.org/) and/or licensed pursuant to Apache License, Version 2.0 (http://www.apache.org/licenses/). For more information, see the NOTICE.txt file included with the software. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.
Chapter 2
Application control for mobile devices

Objectives

- Describe what application control does and how it affects applications
- List examples of application control handling for a mobile device
- Explain what is meant by requesting application control permissions

This chapter describes application control and discusses application control handling for a mobile device such as a BlackBerry® smartphone, application control policies, and how to request application control permissions.
Introducing application control

Application control determines how third-party applications operate on a BlackBerry smartphone.

BlackBerry smartphone users can configure permissions that control how third-party applications on their BlackBerry smartphone interact with the other applications on the smartphone. For example, BlackBerry smartphone users can control whether third-party applications can access the Internet, make calls, or use Bluetooth® connections. Administrators in a BlackBerry® Enterprise Server setting can use application control to establish what resources an application can access on a specific BlackBerry smartphone.

BlackBerry smartphones support the following three types of permissions for third-party applications:

- **Connection permissions** for third-party applications specify whether third-party applications can connect and share data with external resources. Connection resources include the following:
  - USB
  - Bluetooth
  - phone
  - location data
  - server network
  - Internet

- **Interaction permissions** for third-party applications specify whether third-party applications can communicate and share data with other applications. Interaction resources include the following:
  - BlackBerry Device Settings
  - media
  - application management
  - themes
  - input simulation
  - browser filtering
  - screen capturing
  - security timer reset

- **Data permissions** for third-party applications specify whether third-party applications can access files and other data on the BlackBerry smartphone. Data resources include the following:
  - email messages
  - Organizer data
  - files
  - security data
1. Which two of the following statements describe application control restrictions on resource access?

   A. A BlackBerry smartphone user can control whether your application can open a Bluetooth connection.
   B. An Internet service provider can control which Internet sites your application can access.
   C. An administrator in a BlackBerry Enterprise Server setting can prevent your application from running on a particular BlackBerry smartphone.
   D. Other third-party applications on a BlackBerry smartphone can control which color scheme your application can access.

2. Which two of the following resources require connection permissions?

   A. input simulation
   B. Bluetooth
   C. security data
   D. Internet
   E. security timer reset
   F. browser filtering

3. Which two of the following resources require interaction permissions?

   A. Phone
   B. Bluetooth
   C. BlackBerry Device Settings
   D. Email
   E. Organizer Data
   F. Security Timer Reset
Answers

1. A and C

2. B and D

3. C and F
Application control policies

The BlackBerry Enterprise Server application control policies are designed to permit or block the installation of specific third-party applications on the BlackBerry smartphone, and to limit the permissions of third-party applications that are installed on the BlackBerry smartphone. For example, administrators can use the application control policy to make sure that a game application on the BlackBerry smartphone cannot access the phone application on the BlackBerry smartphone.

If a default application control policy does not exist, the user can change some application control settings on the BlackBerry smartphone. If a default application control policy exists, the user cannot change the application control settings.

Note: The administrator can apply application control policies only when the BlackBerry smartphone is associated with a BlackBerry Enterprise Server.

Application control policy rules

The BlackBerry Device Keystore Medium Security application control policy rule specifies whether an application can access key store items stored at the medium security level. The application must prompt the BlackBerry smartphone user for the key store password when attempting to access the private key for the first time or when the private key password expires.

The Bluetooth Serial Profile application control policy rule specifies whether an application can access the Bluetooth SPP API.

The Browser Filter Domains application control policy rule specifies the list of domains to which an application can apply browser filters to web page content on the BlackBerry smartphone. For example, a user can identify www.google.com and www.yahoo.com as domains for which an application can use a browser filter for search engines.

The Browser Filters application control policy rule specifies whether an application can access browser filter APIs to register a browser filter on the BlackBerry smartphone. This rule can permit third-party applications to apply custom browser filters to web page content on the BlackBerry smartphone.

The Cross Application Communication application control policy rule specifies whether an application can perform cross application communication operations. This rule can permit two or more applications to share data or for one application to use the connection permissions of another application.

The Device GPS application control policy rule specifies whether an application can access the GPS APIs on the BlackBerry smartphone. BlackBerry smartphone users can configure this rule to prevent an application from accessing the GPS APIs on the BlackBerry smartphone or to prompt the user for permission before accessing the GPS APIs.
The Disposition application control policy rule specifies whether an application is optional, required, or not permitted on the BlackBerry smartphone. This rule can make a specific application mandatory on the BlackBerry smartphone or prevent users from installing unspecified or untrusted applications.

The Event Injection application control policy rule specifies whether an application can simulate input events, such as key presses or trackball actions, on the BlackBerry smartphone.

The External Domains application control policy rule specifies the external domain names to which an application can establish a connection.

The External Network Connections application control policy rule specifies whether an application can make external network connections. Users can configure this rule to prevent an application from sending or receiving any data on the BlackBerry smartphone using an external protocol (such as WAP or TCP) or to prompt the user for permission before making a connection.

The Internal Domains application control policy rule specifies the internal domain names to which an application can establish a connection.

The Internal Network Connections application control policy rule specifies whether an application can make internal network connections. BlackBerry smartphone users can configure this rule to prevent the application from sending or receiving any data on the BlackBerry smartphone using an internal protocol (for example, the BlackBerry MDS Connection Service), or to prompt the user for permission before making a connection.

The Local Connections application control policy rule specifies whether an application can make local network connections (for example, connections to the BlackBerry smartphone using a USB or serial port).

The Message Access application control policy rule specifies whether an application can send and receive email messages on the BlackBerry smartphone.

The Organizer Data Access application control policy rule specifies whether an application can access the BlackBerry smartphone PIM APIs, which control access to the user's personal information on the BlackBerry smartphone, such as the address book.

The Phone Access application control policy rule specifies whether an application can make calls and access call logs on the BlackBerry smartphone. Users can configure this rule to prevent the application from making calls on the BlackBerry smartphone or to prompt the user for permission before making a call.

The Security Data application control policy rule specifies whether an application can access the key store APIs on the BlackBerry smartphone.

The Themes application control policy rule specifies whether custom theme applications developed using the Plazmic® Content Developer's Kit are permitted as themes on the BlackBerry smartphone.

The User Authenticator application control policy rule specifies whether an application can access the user authenticator framework API. The user authenticator framework permits the registration of drivers that provide two-factor authentication to unlock the BlackBerry smartphone. Currently, only
smart card drivers are supported. This application control policy rule applies to the BlackBerry® Device Software and third-party applications.
1. Which three of the following are actual application control policy rules that can influence how your application runs on a BlackBerry smartphone?

A. Color Scheme application control policy rule
B. Themes application control policy rule
C. Speaker Volume application control policy rule
D. Device GPS application control policy rule
E. Organizer Data Access application control policy rule

2. Which three of the following application control policy rules can you configure so that your application prompts the user for permission before accessing the required resource?

A. Device GPS application control policy rule
B. Color Scheme application control policy rule
C. Browser Filter Domains application control policy rule
D. Themes application control policy rule
E. Phone Access application control policy rule
F. Internal Network Connections application control policy rule
G. External Domains application control policy rule
Answers

1. B, D, and E

2. A, E, and F
Requesting application control permissions

You can display a custom permission request message to a BlackBerry smartphone user when your application attempts an operation that the user must permit. If the current permissions are insufficient, the user is prompted to increase the level of permissions. You must create a separate permission request for each of the resources that your application requires.

Note:
Do not request unnecessary permissions. Request only the permissions required by your application.

Displaying a message requesting user permission

You can use the application control API to display information about the type of permission that the user must provide. For example, you can use PERMISSION_PHONE for an operation that requires access to the phone functionality of the BlackBerry smartphone.

You can use the following application permissions. Each of these permissions refers to a particular subset of the API that the application control policy can restrict.

- PERMISSION_APPLICATION_MANAGEMENT
- PERMISSION_BLUETOOTH
- PERMISSION_BROWSER_FILTER
- PERMISSION_CROSS_APPLICATION_COMMUNICATION
- PERMISSION_DEVICE_SETTINGS
- PERMISSION_EMAIL
- PERMISSION_FILE_API
- PERMISSION_IDLE_TIMER
- PERMISSION_INPUT_simulation
- PERMISSION_INTERNET
- PERMISSION_LOCATION_DATA
- PERMISSION_MEDIA
- PERMISSION_ORGANIZER_DATA
- PERMISSION_PHONE
- PERMISSION_RECORDING
• PERMISSION_SECURITY_DATA
• PERMISSION_SERVER_NETWORK
• PERMISSION_THEMES
• PERMISSION_WIFI

Displaying an application control message

1. Import `net.rim.device.api.applicationcontrol.ReasonProvider`.

2. In your implementation of the `ReasonProvider.getMessage` method, return a string value that contains the message to display to a BlackBerry smartphone user.

A BlackBerry smartphone application can include more than one registered `ReasonProvider`. The BlackBerry smartphone application displays messages from `ReasonProvider`s in the order that each `ReasonProvider` registers with the BlackBerry smartphone application. For example, if an application registers `ReasonProvider A` before `ReasonProvider B`, the BlackBerry smartphone application displays the message from `ReasonProvider A`, followed by the message from `ReasonProvider B`.

Permission request programming example

The following program illustrates how to request permission for event injection privileges, and how to determine the access control settings that the BlackBerry smartphone user permits.

1. Import the following classes:
   
   ```java
   net.rim.device.api.applicationcontrol.ApplicationPermissions
   net.rim.device.api.applicationcontrol.ApplicationPermissions
   net.rim.device.api.applicationcontrol.ApplicationPermissionsManager
   ```

2. Create an instance of the `ApplicationPermissions` class.

   ```java
   ApplicationPermissions permissions = new ApplicationPermissions();
   ```

3. Specify the build request to ask for event injection privileges.

   ```java
   permissions.addPermission(ApplicationPermissions.PERMISSION_EVENT_INJECTOR);
   ```
4. Determine the access control settings that the BlackBerry smartphone user specifies.

```java
if( ApplicationPermissionsManager.getInstance().invokePermissionsRequest(permissions)

{ System.out.println("The user saved equal, or more permissive settings");
} else {
 System.out.println("The user saved more restrictive settings");
}
```

If the application cannot access one of the protected resources, the associated method throws a ControlledAccessException. In the case of class level checks, it throws a ClassDefNotFoundError. The ClassDefNotFoundError occurs in Java® when an exception is thrown from a static constructor. Your application must handle both types of errors depending on what APIs you use.
1. Which three of the following are actual permissions that can be restricted by application control?

A. PERMISSION_THEMES
B. PERMISSION_COLOR_SCHEME
C. PERMISSION_BLUETOOTH
D. PERMISSION_SPEAKER_VOLUME
E. PERMISSION_CROSS_APPLICATION_COMMUNICATION
F. PERMISSION_SCREEN_SAVER
Answers

1. A, C, and E
Application control determines how third-party applications operate on a BlackBerry smartphone.

Both users and administrators can configure permissions that control how third-party applications on the BlackBerry smartphone interact with the other applications on the BlackBerry smartphone. For example, a BlackBerry smartphone user can prevent third-party applications from making calls, and an administrator can make sure that a game loaded onto a BlackBerry smartphone is not permitted to access the Phone API.

The BlackBerry Enterprise Server application control policy rules are designed to permit or block the installation of specific third-party applications on the BlackBerry smartphone, and to limit the permissions of third-party applications that are installed on the BlackBerry smartphone.

The administrator can apply application control policies only when the BlackBerry smartphone is associated with a BlackBerry Enterprise Server.

You can display a custom permission request message to a BlackBerry smartphone user when your application attempts an operation that the user must permit. If the current permissions are insufficient, the BlackBerry smartphone user is prompted to increase the level of permission. You must create a separate permission request for each of the resources that your application requires.
1. Which two of the following resources require interaction permissions?
   A. Phone
   B. Bluetooth
   C. BlackBerry Device Settings
   D. Email
   E. Organizer Data
   F. Security Timer Reset

2. Which three of the following application control policy rules can you configure so that your application prompts the user for permission before accessing the required resource?
   A. Device GPS application control policy rule
   B. Color Scheme application control policy rule
   C. Browser Filter Domains application control policy rule
   D. Themes application control policy rule
   E. Phone Access application control policy rule
   F. Internal Network Connections application control policy rule
   G. External Domains application control policy rule

3. Which three of the following are permissions that can you restrict using application control?
   A. PERMISSION_THEMES
   B. PERMISSION_COLOR_SCHEME
   C. PERMISSION_BLUETOOTH
   D. PERMISSION_SPEAKER VOLUME
   E. PERMISSION_CROSS_APPLICATION_COMMUNICATION
   F. PERMISSION_SCREEN_SAVER