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 8
Security considerations for developing applications for mobile devices

Objectives

- Explain why security is important when developing applications for mobile devices
- List methods of securing applications developed for mobile devices
- Describe how cryptography is used in the BlackBerry® Enterprise Solution
- Describe how developers can use data encryption to secure an application designed for mobile devices
- Explain why developers must consider file encryption on microSD media cards when designing an application for mobile devices
- Describe how developers can use authentication to secure an application designed for mobile devices
- Describe why developers must consider policies when designing applications for mobile devices
- Describe how RIM® restricts applications from accessing memory on mobile devices
- Describe development tools for securing mobile devices
- Explain how to obtain and install code signing keys
- Explain how to use the BlackBerry Signature Tool to sign your code
This chapter provides an overview of the importance of security when developing applications for mobile devices. This chapter describes the following considerations when securing applications for mobile devices: data encryption, file encryption on microSD media cards, authentication, policies, access to memory, and controlled APIs and code signing. This chapter also provides information about code signing keys and the BlackBerry Signature Tool, and describes how you can use these tools to secure your applications for mobile devices.
How to secure applications developed for mobile devices

Security is important when developing applications for mobile devices to help protect mobile device customers from data loss or alteration. Data protection is key for security-conscious organizations who store sensitive information. Different customers have different security needs, so your approach to application development must reflect the needs of the intended users. For example, for doctors and health care companies, the loss of patient data compromises patient confidentiality.

The BlackBerry Enterprise Solution is designed to provide corporate data security. It features an end-to-end security model designed to seamlessly protect corporate information from attack as BlackBerry smartphone users send and receive email messages and access data wirelessly.

Consider the following security features when developing applications for mobile devices:

- data encryption
- authentication
- policies
- access to memory
- controlled APIs and code signing

Data encryption

With the BlackBerry Enterprise Solution, you can secure data in several ways. The key data encryption considerations for BlackBerry® application programmers are data encryption in transport, data encryption on the BlackBerry smartphone, and file encryption on microSD media cards.

Cryptography in the BlackBerry Enterprise Solution

Encryption is a process you can use to protect data so that only certain people can access the data. The encryption process uses an encryption algorithm and a key to protect data. Only the recipient of an encrypted message who knows the key can use the key to decrypt, or descramble, the encrypted message into meaningful information.

The BlackBerry Enterprise Solution is designed to encrypt data in transit at all points between the BlackBerry smartphone and the BlackBerry® Enterprise Server to protect an organization from data loss or alteration. Only the BlackBerry Enterprise Server and the BlackBerry smartphone can decrypt this data.

The BlackBerry Enterprise Solution uses both asymmetric and symmetric key cryptography.

- Asymmetric key cryptography, also known as public key cryptography, is a form of cryptography that uses both a public key and a private key to encrypt and decrypt data. Using
asymmetric key cryptography, users keep the private key secret, while they can distribute the public key widely. The keys are related mathematically, but third parties cannot practically derive the private key from the public key. When sending data, the sender uses the intended recipient’s public key to encrypt the data. The encryption software then uses the recipient’s private key to decrypt the data. Because only the recipient has a copy of the private key, the recipient is the only entity who can decrypt the data.

- Symmetric key cryptography, also known as shared secret cryptography, is a form of cryptography that uses a single symmetric key to encrypt and decrypt data. The sender’s encryption software encrypts data using a symmetric key and an encryption algorithm. To decrypt the data, the recipient must use the same symmetric key and the same encryption algorithm in reverse. Although symmetric key cryptography is faster to perform than asymmetric key cryptography, it requires that both the sender and recipient have the same symmetric key prior to communication.

Data encryption in transport

Enterprise applications often require that a third-party application encrypts all of the data that it sends or receives during transport at all points outside of the organization’s firewall. The BlackBerry Enterprise Solution is designed to seamlessly implement data encryption in transport. If you use the BlackBerry Enterprise Server as the wireless gateway for your application, the BlackBerry Enterprise Server encrypts data automatically using AES or Triple DES at all points in the connection between the BlackBerry smartphone and the BlackBerry Enterprise Server behind the organization’s firewall. By default either AES or 3DES is enabled. This diagram shows a basic dataflow through the BlackBerry Enterprise Server using AES or Triple DES encryption.

[Diagram of data encryption in transport]

Figure 8.1 End-to-end encryption in the BlackBerry Enterprise Solution
If you require further data encryption between the BlackBerry Enterprise Server and the destination server, you can use the HTTPS protocol and use **SSL/TLS encryption**. This diagram shows a basic dataflow through the BlackBerry Enterprise Server using SSL/TLS encryption.

![Diagram of dataflow through BlackBerry Enterprise Server with SSL/TLS encryption](image)

**Figure 8.2 HTTPS secure data access in the BlackBerry Enterprise Solution**

If your application uses the BlackBerry® Internet Service or the Internet gateway of the wireless service provider, the system does not encrypt data traffic. If your BlackBerry smartphone users prefer, you can use HTTPS to encrypt the data, or you can use the Java® APIs for encryption to apply your own symmetric key or public key cryptography.

**Data encryption on the BlackBerry smartphone**

In an enterprise environment, system administrators can set an *IT policy* to dictate that BlackBerry smartphone encrypts all user data stored in BlackBerry core applications locally in flash memory. You can use additional APIs to register your application data with this encryption service so that the encryption service encrypts your data with the same security key before committing it to flash memory.

**File encryption on microSD media cards**

Some BlackBerry smartphone models accept a microSD media card, which extends the available memory on the BlackBerry smartphone for storing media files such as songs, ring tones, videos, or pictures.
Encryption of data on a microSD media card

When a BlackBerry Java Application accesses a file on the microSD memory card, if encryption is enabled, the microSD memory card decrypts the file and moves the file to main memory for the application to read. A BlackBerry Java Application can only access a password-protected file if the BlackBerry is unlocked. Encrypted files have an REM extension and non-BlackBerry platforms cannot decrypt these files.

If the user removes the **NVRAM** and locks the microSD media card with a BlackBerry smartphone key, the user can no longer access the data on the microSD media card. To remove inaccessible data, start the BlackBerry smartphone and remove all encrypted media files.

The BlackBerry smartphone uses a master key stored on the microSD media card to encrypt BlackBerry smartphone media files. The master key prevents the BlackBerry smartphone from having to decrypt or re-encrypt all media files after you disable encryption or change the password.

Using the microSD media card with more than one BlackBerry smartphone

The BlackBerry smartphone prompts users to enter the microSD media card password if they either move the microSD media card to a BlackBerry smartphone that does not use a BlackBerry smartphone password, or use a password that does not successfully decrypt the microSD media card master key. If the BlackBerry smartphone has a password, the BlackBerry smartphone user can use the prompt to change the microSD media card password to the BlackBerry smartphone password.

IT policies and the microSD media card

You can apply the *Encrypt data written to the microSD media card* IT policy to new or modified files that you store on the microSD media card. The system encrypts only the files that you store on the microSD media card after a system administrator sets the IT policy.

**Note:**

Application memory is not encrypted.

The microSD media card encrypts all content.
1. Asymmetric key cryptography uses which types of keys? *Choose two.*
   A. Public key
   B. Master key
   C. Session key
   D. Private key

2. If you use the BlackBerry Enterprise Server as the wireless gateway for your application, the BlackBerry Enterprise Server automatically uses one of the following two encryption algorithms to encrypt data? *Choose two.*
   A. SSL/TLS
   B. AES
   C. Symmetric key
   D. Triple DES
   E. Asymmetric key

3. What file extension is added to files encrypted on the microSD media card?
   A. REM
   B. JSE
   C. AES
   D. COD
Answers

1. A and D
2. B and D
3. A
Authentication

Authentication is the process of verifying that a user, BlackBerry smartphone, or application is truly what it claims to be.

BlackBerry smartphone authentication and IT policy

BlackBerry users can set up their BlackBerry smartphones with passwords for protection. If the password setting is active, BlackBerry smartphone users must provide the BlackBerry smartphone password periodically to access the data and applications.

In an enterprise environment, the system administrator can use BlackBerry Enterprise Server IT policies to enforce password protection for the BlackBerry smartphones in the organization. IT policies help keep an organization’s confidential information private. A system administrator can also issue wireless IT commands to remotely lock a BlackBerry smartphone, change the password, or remove all of the data.

Application authentication

For applications where security features are critical, you can provide a login screen that requires the BlackBerry smartphone user to log in to the application on the BlackBerry smartphone before using it. The UI classes provide simple password fields that hide the text entry with asterisk characters.

Note:
Login screens can negatively impact the BlackBerry smartphone user experience. If the BlackBerry smartphone user sets a password to protect the BlackBerry smartphone, you might not need a login screen in your application.

Server-side authentication

If your application connects to an application on a server or to the Internet or an intranet, you can include additional authentication features when the BlackBerry smartphone users log in to the server. Most applications that require user authentication rely on HTTP basic authentication, which uses a simple user name and password combination. You can use HTTP basic authentication by adding the correct HTTP headers while opening the HTTP connection. You can also add more advanced authentication using certificates; however, most applications do not require it.
Policies

The BlackBerry Enterprise Server is designed to allow system administrators to establish, enforce, and update BlackBerry smartphone settings using policies. The use of policies provides comprehensive control over all BlackBerry smartphones in an organization.

The following policies are the most common policies offered by the BlackBerry Enterprise Solution:

- IT policies
- application control policies

IT Policies

The BlackBerry IT policy API (net.rim.device.api.itpolicy) lets applications access the IT policy information on BlackBerry smartphones. An application can change its behavior or functionality by retrieving custom IT policy settings.

An IT policy is a collection of rules that system administrators use to set functionality for the BlackBerry smartphones and the BlackBerry® Desktop Software in an organization. IT policies only apply to the BlackBerry smartphone, but the policies govern what the BlackBerry smartphone can do when it is connected to DTM.

System administrators can configure over 400 rules to control BlackBerry smartphone functionality, including the following:

- forcing BlackBerry smartphone users to set a password, setting password complexity, and setting security timeouts
- restricting application availability (for example, browsers, SMS text messaging, MMS messaging, and PIN messaging) and the functions that a user can perform in each application
- disabling BlackBerry smartphone features and components, including Bluetooth® connections, Wi-Fi® connections, cameras, media cards, and peripheral devices
- enforcing encryption settings and certificate use
- configuring backup and synchronization settings
- controlling how the system handles email messages and organizer data

The BlackBerry Enterprise Solution synchronizes and updates BlackBerry smartphone IT policy settings over the wireless network. With earlier versions of BlackBerry smartphone software, the system updates the BlackBerry smartphone policy settings after the BlackBerry smartphone user synchronizes the BlackBerry smartphone with the computer.
Application control policies

The BlackBerry Enterprise Server application control policy rules are designed to permit or prevent the installation of specific applications on the BlackBerry smartphone and to control the permissions of applications on the BlackBerry smartphone. For example, system administrators can use the application control policy to make sure that a game application on the BlackBerry smartphone cannot access the phone application.

Note:
The BlackBerry Application Control policy works only if the BlackBerry smartphone connects to a BlackBerry Enterprise Server. This IT policy does not apply to BlackBerry smartphones that use the BlackBerry Internet Service only.

If the system administrator or a user denies the application access to one of the protected areas, the associated method throws a ControlledAccessException. For class level checks, the method throws a NoClassDefFoundError. Your application might need to handle both types of errors, depending on which APIs you use.

Access to memory

The BlackBerry Java Development Environment is designed to inhibit applications from causing problems accidentally or maliciously in other applications or on the BlackBerry smartphone. BlackBerry applications can write only to the BlackBerry smartphone memory that the BlackBerry Java Virtual Machine uses; they cannot access the virtual memory of other applications (unless RIM specifically grants access to do so). A BlackBerry Java Application can only access persistent storage or user data, or communicate with other applications, through specific BlackBerry APIs. RIM must digitally sign a BlackBerry Java Applications that use these BlackBerry APIs must be digitally signed using RIM issued code signing keys to provide an audit trail of applications that use sensitive APIs.

Controlled APIs and code signing

RIM tracks the use of sensitive APIs for security and export control reasons. In the BlackBerry API reference, RIM identifies a controlled class or method with a lock icon or a signed note. You must sign your application using a key, or signature, from RIM before you can either install the application COD on the BlackBerry smartphone, or use controlled classes or methods in your applications. You must also sign your applications to incorporate certain functionality, such as the ability to execute when the BlackBerry smartphone starts.

The RIM registration process covers the use of most controlled APIs, including cryptography classes that relate to public and private key cryptography containing technology from Certicom®. To use these
classes, follow the registration and installation process used for RIM APIs. The RIM registration process includes the use of Certicom classes.

To test and debug your code before you receive the code signatures, you can use the BlackBerry Smartphone Simulator. You must sign the application before you install it on BlackBerry smartphones. You do not send your actual code to RIM. You can use the BlackBerry Signature Tool to send a SHA-1 hash of your code file so that the signing authority system can generate the necessary signature.
1. When security features are critical, which method can you use to protect your applications?
   A. Wireless IT commands
   B. Login screens
   C. BlackBerry smartphone passwords
   D. IT policies

2. Which of the following actions can a system administrator perform using the BlackBerry Enterprise Server application control policy rules? *Choose two.*
   A. Enforce encryption settings and certificate use
   B. Force BlackBerry smartphone users to set a password
   C. Limit the permissions of applications on the BlackBerry smartphone
   D. Configure backup and synchronization settings
   E. Allow or prevent the installation of specific applications on the BlackBerry smartphone

3. If the system administrator or a user denies your application access to one of the protected areas, how many errors does your code need to handle? *Choose two.*
   A. One
   B. One or two, depending on whether your application is a game
   C. One or two, depending on which APIs you use in the code
   D. Two

4. Can a third-party BlackBerry application write to virtual memory on a BlackBerry smartphone?
   A. No
   B. Yes
   C. Yes, if the system administrator enables this feature with an IT policy
   D. Yes, if signed with RIM code signing keys
5. In the BlackBerry API reference, how does RIM identify a controlled class or method? *Choose two.*
   
   A. Key icon
   B. Lock icon
   C. Signed note
   D. Asterisk (*)

6. If you use sensitive APIs and you sign your application using a key from RIM, which of the following actions can you perform? *Choose three.*
   
   A. Test and debug your code in the BlackBerry Smartphone Simulator
   B. Install the application COD on the BlackBerry smartphone
   C. Use controlled classes or methods in your application
   D. Prevent all application permission prompts, which does not happen after signing.
Answers

1. B
2. C and E
3. C
4. D
5. B and C
6. A, B, and C
Development tools for securing applications designed for mobile devices

If you use APIs with controlled access, you must use the following development tools:

- code signing keys
- BlackBerry Signature Tool

Code signing keys

You must sign some applications using code signing keys, or signature, before you can deploy them on the BlackBerry smartphone. RIM uses code signing keys to track API use. Code signing adds protection by providing a greater degree of control and predictability to the loading and behavior of applications on BlackBerry smartphones.

You can sign code using three different signature methods.

- **BlackBerry signatures**: Applies to sensitive RIM APIs in the BlackBerry JDE.
- Certicom signatures: Applies to certain cryptography classes related to public/private key cryptography that contain technology from Certicom.
- Wireless service provider signatures: Applies to MIDP applications only. Wireless service providers sign **MIDlets** to indicate that they are trusted applications.

BlackBerry APIs with controlled access

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net.rim.blackberry.api.browser</td>
<td>set applications to invoke the BlackBerry® Browser</td>
</tr>
<tr>
<td>net.rim.blackberry.api.invoke</td>
<td>set applications to invoke BlackBerry applications, such as tasks, messages, MemoPad, and phone</td>
</tr>
<tr>
<td>net.rim.blackberry.api.mail</td>
<td>set applications to interact with the BlackBerry messages application to send, receive, and open email messages</td>
</tr>
<tr>
<td>net.rim.blackberry.api.mail.event</td>
<td>define messaging events and listener interfaces to manage mail events</td>
</tr>
<tr>
<td>net.rim.blackberry.api.menuitem</td>
<td>add custom menu items to BlackBerry applications, such as the address book, calendar, and messages</td>
</tr>
<tr>
<td>net.rim.blackberry.api.options</td>
<td>add items to the handheld options</td>
</tr>
</tbody>
</table>
Obtaining BlackBerry code signing keys

To obtain signing keys, complete the application form on the following BlackBerry web page: https://www.blackberry.com/SignedKeys.

To complete the registration process, you must pay an administration fee. You must also select a ten-digit PIN for installing your keys.

After you submit the form, RIM processes the request and sends three email messages that contain the signing keys.
Installing BlackBerry code signing keys

The three email messages from RIM contain the RBB, RRT, and RCR keys. Install each key on your computer according to the instructions in the email messages.

When registering with the signing authority, ensure that you enter your registration PIN correctly. If you enter an incorrect PIN five times, your keys are deactivated.

You must use the same password for all keys on the same computer. You must also install all three signing keys on the same computer, otherwise the signing keys do not work.

For more information, if you cannot install or register your signature keys, contact devsupport@rim.com.

Certicom keys with controlled access

The Certicom cryptographic classes within the RIM Cryptography API provide additional data security capabilities, including data encryption and decryption, digital signatures, data authentication, and certificate management. RIM Cryptography APIs are controlled by the RCR key. Certicom cryptography APIs are controlled by the RCC key.

Certicom classes within the RIM Cryptography API include the following:

- net.rim.device.api.crypto
- CryptoByteArrayArithmetic
- CryptoInteger
- DHCryptoSystem
- DHCryptoToken
- DHKey
- DHKeyAgreement
- DHKeyPair
- DHPrivateKey
- DHPublicKey
- DSACryptoSystem
- DSACryptoToken
- DSAKey
- DSAKeyPair
- DSAPrivateKey
- DSAPublicKey
- DSASignatureSigner
- DSASignatureVerifier
- ECCryptoSystem
- ECCryptoToken
- ECDHKeyAgreement
- ECDSASignatureSigner
- ECDSASignatureVerifier
- ECIESDecryptor
- ECIESEncryptor
- ECKey
- ECKeyPair

You must have a Certicom license to use these classes.
Obtaining and installing Certicom code signing keys

To obtain Certicom code signing keys, complete the application form on the following BlackBerry web page: https://www.blackberry.com/SignedKeys.

The registration and installation process for obtaining Certicom code signing keys is the same process as that for obtaining RIM code signing keys.

Wireless service provider keys with controlled access

Controlled wireless service provider keys only apply to MIDP applications. MIDP version 2.0 incorporates the concept of untrusted and trusted applications. If the wireless service provider signs an application, it is trusted; otherwise it is untrusted. Untrusted applications still work, but the BlackBerry smartphone prompts the user for permission to perform sensitive functions. For example, if users want to download an untrusted application, they see a notification that the application is untrusted and must choose whether to proceed.

To obtain a wireless service provider signature for your application, you must contact the specific wireless service provider. To run signed MIDlets on mobile devices, the users must install a signing certificate from that specific wireless service provider on their mobile devices. If users do not install the wireless service provider signing certificate, they receive the "909 Application Authentication Failure Error" message.

Wireless service provider code signing does not affect the application or the device IT policies.

Obtaining and installing wireless service provider code signing keys

Contact your wireless service provider to get more information about how to obtain, install, and use wireless service provider code signing keys.

BlackBerry Signature Tool

Use the BlackBerry Signature Tool to sign your application with the code signing keys you obtain from RIM. You can also use the BlackBerry Signature Tool to change your password or revoke a key.

Note:

If you revoke a code signing key, the code signing key becomes void and cannot be used for signing applications.

To sign your application, your computer must have an Internet connection to connect to the signing servers. You can open the BlackBerry Signature Tool by opening Eclipse®, and then selecting BlackBerry > Request Signatures.
To sign the code, select the COD file, and then click Request.

After you click Request, the application prompts you for your password, and then indicates the success or failure of the signing operation.

If the signing operation is successful, you can exit the BlackBerry Signature Tool and deploy your application to your BlackBerry smartphone.

**Note:**
You must sign the COD files each time you create a new version of those files.
1. Which of the following signature methods applies to MIDP applications only?
   A. BlackBerry signatures
   B. Certicom signatures
   C. Wireless service provider signatures

2. What additional security capabilities do the Certicom classes provide?
   A. Provide a standard mechanism for accessing PIM information on a device
   B. Provide data security, including data encryption and decryption, digital signatures, data authentication, and certificate management
   C. Enable applications to interact with the BlackBerry messages application to send, receive, and open email messages
   D. Provide access to advanced features of the phone application

3. Which type of signature can you use to mark an application as trusted?
   A. BlackBerry signature
   B. Certicom signature
   C. Wireless service provider signature

4. Which of the following functions can you perform with the BlackBerry Signature Tool? Choose three.
   A. Obtain code signing keys from RIM
   B. Install code signing keys on your computer
   C. Sign your application with the code signing keys
   D. Change your password
   E. Revoke all keys
Chapter 8

Answers

1. C
2. B
3. C
4. C, D, and E
Security considerations for developing applications for mobile devices

Security is important when developing applications for mobile devices to help protect users from data loss or alteration. The BlackBerry Enterprise Solution is designed to seamlessly protect corporate information transmitted between the BlackBerry Enterprise Server and the BlackBerry smartphone from attack as users send and receive email messages and access data wirelessly.

Encryption is a process you can use to protect data so that only certain people can access the data. The BlackBerry Enterprise Solution is designed to encrypt data transmitted between the BlackBerry smartphone and the BlackBerry Enterprise Server to protect an organization from data loss or alteration.

You can use AES or Triple DES to encrypt data that your application sends or receives to points outside of the organization's firewall. Additionally, you can use the HTTPS protocol and SSL/TLS encryption for further data encryption between the BlackBerry Enterprise Server and the BlackBerry smartphone.

A system administrator can apply an IT policy to encrypt content stored on a microSD media card. If your BlackBerry Java Applications access a file on the microSD memory card, the microSD card must decrypt the file (if encryption is enabled) and move it to main memory for your application to read.

BlackBerry users can set up their BlackBerry smartphones with passwords for protection. System administrators can also use IT policies to enforce password protection on all BlackBerry smartphones in the organization. If security is critical, you can add a login screen to prevent unauthorized use of your application on the BlackBerry smartphone. If security is critical, you can also add more advanced authentication using certificates.

The BlackBerry Enterprise Server is designed to allow system administrators to establish, enforce, and update BlackBerry smartphone settings using policies. Policies provide comprehensive control over all BlackBerry smartphones in an organization. The BlackBerry Enterprise Server application control policy rules are designed to permit or prevent the installation of specific applications on the BlackBerry smartphone and to control the permissions of applications on the BlackBerry smartphone.

Typically, BlackBerry applications can write only to the BlackBerry smartphone memory that the BlackBerry Java Virtual Machine uses. An application can only access user data, or communicate with other applications, if the BlackBerry Java Application that uses sensitive BlackBerry APIs is signed with RIM-issued code signing keys.

After you obtain a code signing key from RIM and install it, you can use the BlackBerry Signature Tool to sign your code. If the signing operation is successful, you can deploy your application to your BlackBerry smartphone.

Summary

Security is important when developing applications for mobile devices to help protect users from data loss or alteration. The BlackBerry Enterprise Solution is designed to seamlessly protect corporate information transmitted between the BlackBerry Enterprise Server and the BlackBerry smartphone from attack as users send and receive email messages and access data wirelessly.

Encryption is a process you can use to protect data so that only certain people can access the data. The BlackBerry Enterprise Solution is designed to encrypt data transmitted between the BlackBerry smartphone and the BlackBerry Enterprise Server to protect an organization from data loss or alteration.

You can use AES or Triple DES to encrypt data that your application sends or receives to points outside of the organization’s firewall. Additionally, you can use the HTTPS protocol and SSL/TLS encryption for further data encryption between the BlackBerry Enterprise Server and the BlackBerry smartphone.

A system administrator can apply an IT policy to encrypt content stored on a microSD media card. If your BlackBerry Java Applications access a file on the microSD memory card, the microSD card must decrypt the file (if encryption is enabled) and move it to main memory for your application to read.

BlackBerry users can set up their BlackBerry smartphones with passwords for protection. System administrators can also use IT policies to enforce password protection on all BlackBerry smartphones in the organization. If security is critical, you can add a login screen to prevent unauthorized use of your application on the BlackBerry smartphone. If security is critical, you can also add more advanced authentication using certificates.

The BlackBerry Enterprise Server is designed to allow system administrators to establish, enforce, and update BlackBerry smartphone settings using policies. Policies provide comprehensive control over all BlackBerry smartphones in an organization. The BlackBerry Enterprise Server application control policy rules are designed to permit or prevent the installation of specific applications on the BlackBerry smartphone and to control the permissions of applications on the BlackBerry smartphone.

Typically, BlackBerry applications can write only to the BlackBerry smartphone memory that the BlackBerry Java Virtual Machine uses. An application can only access user data, or communicate with other applications, if the BlackBerry Java Application that uses sensitive BlackBerry APIs is signed with RIM-issued code signing keys.

After you obtain a code signing key from RIM and install it, you can use the BlackBerry Signature Tool to sign your code. If the signing operation is successful, you can deploy your application to your BlackBerry smartphone.
1. Define each of the following security terms:
   A. Encryption
   B. Authentication
   C. IT policies
   D. Application control policies
   E. Code signing

2. Define symmetric key cryptography and explain how it is used in the BlackBerry Enterprise Solution.

3. Define asymmetric key cryptography and explain how it is used in the BlackBerry Enterprise Solution.

4. List five security considerations for developing applications for mobile devices.

5. List two development tools used for securing mobile devices.

6. List two types of signature methods and describe when to use each method.

7. Describe the purpose of the BlackBerry Signature Tool.